Tillgång till passageraruppgifter i brottsbekämpningen

Betänkande av Utredningen om passageraruppgifter i brottsbekämpningen

Stockholm 2026

STATENS OFFENTLIGA UTREDNINGAR

SOU 2026:28

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2021:1.
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Multiply Solutions
Omslagsbild: Hovrättsassessorn Samuel Holmedal
Tryck och remisshantering: Multiply Solutions, Stockholm 2026

ISBN 978-91-525-1525-9 (tryck)
ISBN 978-91-525-1526-6 (pdf)
ISSN 0375-250X

Till statsrådet Gunnar Strömmer

Den 10 april 2025 bemyndigade regeringen statsrådet Strömmer att tillkalla en särskild utredare med uppdrag att analysera och ta ställning till vilka förändringar av den svenska regleringen i fråga om flygpassageraruppgifter som behöver göras med anledning av EU-domstolens praxis, om den svenska regleringen av flygpassageraruppgifter i brottsbekämpningen bör göras neutral vad gäller trafikslag, och se över nuvarande möjligheter att inhämta tillgängliga passageraruppgifter från andra transportföretag. Utredaren ska lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga. Regeringen beslutade samtidigt om direktiv för utredningen (dir. 2025:36).

Till särskild utredare förordnades från och med den 14 april 2025 lagmannen Peder Liljeqvist.

Till sakkunniga att biträda utredningen förordnades från och med den 2 maj 2025 rättssakkunniga Isabelle Waldenström, Justitiedepartementet. Till experter utsågs samma dag den kvalificerade utredaren Sara Berntsson, Trafikanalys, gruppchefen Mattias Fogelgren, Polismyndigheten, seniora åklagaren Lisa Hermanrud, Ekobrottsmyndigheten, verksjuristen Malin Lundberg, Tullverket, försvarsjuristen Anna Saarikoski, Försvarsmakten, seniora verksjuristen Fredrik Sjöberg, Säkerhetspolisen, vd:n Johan Wadman, Svensk kollektivtrafik, avdelningsjuristen Lisa Zettervall, Integritetsskyddsmyndigheten och juristen Eric Åmell, Polismyndigheten. Lisa Hermanrud entledigades genom beslut den 2 september 2025 med verkan fr.o.m. den 3 september 2025. Den 2 september 2025 förordnades i hennes ställe utvecklingschefen Cecilia Danielsson, Ekobrottsmyndigheten.

Som sekreterare anställdes den 14 april 2025 förvaltningsrättsfiskalen Tomas Lif.

Utredningen har antagit namnet Utredningen om passageraruppgifter i brottsbekämpningen (Ju 2025:09). Härmed överlämnas be-

tänkandet *Tillgång till passageraruppgifter i brottsbekämpningen* (SOU 2026:28).

Till betänkandet har fogats särskilda yttranden av experterna Cecilia Danielsson, Mattias Fogelgren, Malin Lundberg, Anna Saarikoski, Fredrik Sjöberg och Eric Åmell. Med undantag från vad som framgår där har de sakkunniga och experterna i huvudsak ställt sig bakom utredningens överväganden och förslag.

Uppdraget är härmed slutfört.

Stockholm i april 2026

Peder Liljeqvist

Tomas Lif

Innehåll

Förkortningar **15**

Sammanfattning **19**

1 Författningsförslag **31**

1.1 Förslag till lag om ändring i lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen 31

1.2 Förslag till lag om ändring i polislagen (1984:387) 54

1.3 Förslag till lag om ändring i lagen (2009:966) om Försvarsunderrättelsedomstol 57

1.4 Förslag till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område 59

1.5 Förslag till lag om ändring i lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område 61

1.6 Förslag till lag om ändring i tullbefogenhetslagen (2024:710) 62

1.7 Förslag till förordning om ändring i förordningen (2009:968) med instruktion för Försvarsunderrättelsedomstolen 64

1.8 Förslag till förordning om ändring i polisförordningen (2014:1104) 65

1.9 Förslag till ändring av förordningen (2018:1181) om flygpassageraruppgifter i brottsbekämpningen 66

1.10 Förslag till förordning om ändring i tullbefogenhetsförordningen (2024:759) 70

2 Inledning 71

2.1 Utredningens uppdrag 71

2.2 Utredningens arbete 72

3 Grundläggande fri- och rättigheter 73

3.1 Inledning 73

3.2 Regeringsformen 73

3.3 Europakonventionen 75

3.4 EU:s rättighetsstadga 76

3.5 Förenta nationernas allmänna förklaring om de mänskliga rättigheterna 77

3.6 Dataskyddskonventionen 78
3.6.1 Konventionens ställning och syfte 78
3.6.2 Konventionens innehåll 79
3.6.3 Modernisering av konventionen 80
3.6.4 Den moderniserade konventionens betydelse för underrättelsetjänsternas personuppgiftsbehandling 81

4 Dataskyddsregleringen 83

4.1 Inledning 83

4.2 EU:s dataskyddsförordning 84
4.2.1 Tillämpningsområde och definitioner 84
4.2.2 Grundläggande principer för personuppgiftsbehandling 85
4.2.3 Rättslig grund för behandling av personuppgifter 86

4.2.4 Grunden för behandling ska i vissa fall fastställas i rättsordningen ... 89
4.2.5 Behandling av särskilda kategorier av personuppgifter ... 91
4.2.6 Den personuppgiftsansvariges allmänna skyldigheter och säkerhet för personuppgifter ... 93
4.2.7 Konsekvensbedömning avseende dataskydd och förhandssamråd ... 94
4.2.8 Dataskyddsombud ... 97
4.2.9 Enskildas rättigheter ... 98
4.2.10 Tillsyn, sanktionsavgifter och skadestånd ... 99

4.3 Nationell kompletterande lagstiftning till EU:s dataskyddsförordning ... 100
4.3.1 Allmänna nationella dataskyddsbestämmelser ... 100
4.3.2 Särskilda registerförfattningar ... 101

4.4 Dataskyddsdirektivet ... 101

4.5 Brottsdatalagen ... 105
4.5.1 Grundläggande krav på personuppgiftsbehandling ... 106
4.5.2 Den personuppgiftsansvariges skyldigheter och säkerhet för personuppgifter ... 108
4.5.3 Enskildas rättigheter ... 110
4.5.4 Tillsyn och skadestånd ... 111
4.5.5 Särskilda registerförfattningar ... 112

4.6 Polisens brottsdatalag ... 113

4.7 Tullverkets behandling av personuppgifter inom brottsdatalagens område ... 117

4.8 Säpodatalagen ... 118
4.8.1 Nuvarande reglering ... 118
4.8.2 Ny säpodatalag ... 120

4.9 Behandling av personuppgifter vid Försvarsmakten ... 122

5 Reglering av passageraruppgifter i brottsbekämpningen 125

5.1 Inledning 125

5.2 PNR-direktivet 126
5.2.1 Allmänt om direktivet 126
5.2.2 Bakgrund 127
5.2.3 Innehåll 128
5.2.4 Överenskommelser i anledning av direktivet 132
5.2.5 Kommissionens översyn av PNR-direktivet 133

5.3 Lagen om flygpassageraruppgifter i brottsbekämpningen 136

5.4 Polismyndigheten och Säkerhetspolisen 140

5.5 Tullverket 141

6 API-uppgifter och transportörsansvaret 143

6.1 Inledning 143

6.2 Internationella åtaganden 144
6.2.1 Chicagokonventionen 144
6.2.2 FN:s resolution 2178 145

6.3 Vissa EU-rättsliga åtaganden 146
6.3.1 Schengenkonventionen och direktivet om transportörsansvar 146
6.3.2 Kodex om Schengengränserna 146

6.4 API-direktivet 147

6.5 API-direktivet i svensk rätt 149
6.5.1 Utlänningslagen 149
6.5.2 Befälhavares skyldigheter 150
6.5.3 Lagen om passagerarregister 151

6.6 Nya API-förordningar 152
6.6.1 API-förordning för brottsbekämpning 153
6.6.2 API-förordning för gränskontroll 156

7 PNR-domen 159

7.1 Inledning 159

7.2 Tillåtna ändamål för behandling av PNR uppgifter 160

7.3 Lagringstid för PNR-uppgifter 161

7.4 Flygningar inom EU 162

7.5 Prövning av domstol eller oberoende förvaltningsmyndighet 165
7.5.1 Förhandskontroll vid begäran om tillgång till PNR-uppgifter 165
7.5.2 Beslut om att tillämpa PNR-direktivet på samtliga flygningar inom EU 167

7.6 Jämförelser med relevanta databaser 167

7.7 Medlemsstaternas agerande efter PNR-domen 169

7.8 Diskussion efter PNR-domen 171
7.8.1 Europeiska dataskyddsstyrelsens uttalande 171
7.8.2 Kommissionens diskussionspromemoria 175
7.8.3 Medlemsstaternas synpunkter på kommissionens promemoria 177

8 Förändringar av svensk rätt i ljuset av PNR-domen 183

8.1 Utgångspunkter 183

8.2 Flygningar inom EU 184
8.2.1 Tillämpning av PNR-direktivet på flygningar inom EU 184
8.2.2 Beslut om att tillämpa PNR-direktivet på samtliga flygningar inom EU 186
8.2.3 Beslut om urval av flygningar 189
8.2.4 När ska ett urval av flygningar göras? 191

8.3 Prövning av beslut om utvidgad tillämpning av PNR-direktivet 197
8.3.1 Anhängiggörande av mål vid Försvarunderrättelsedomstolen 201
8.3.2 Förfarandet vid Försvarsunderrättelsedomstolen 202

8.4 Förhandskontroll vid begäran om tillgång till PNR-information ... 205

8.5 Prövning av begäran om tillgång till PNR-information ... 207
8.5.1 Förarbeten till den svenska beslutsordningen ... 208
8.5.2 EU-domstolens yttrande avseende PNR-avtalet mellan EU och Kanada ... 210
8.5.3 Är den svenska beslutsordningen förenlig med PNR-domen? ... 211
8.5.4 Våra överväganden och förslag ... 214
8.5.5 Ny beslutsordning under pågående förundersökning ... 218
8.5.6 Ny beslutsordning i andra fall ... 223
8.5.7 Begäran från behörig mottagare utanför Sverige eller från tredjeland ... 225
8.5.8 Rättslig prövning vid avsaknad av efterfrågad PNR-information ... 228
8.5.9 Särskilt om brådskande fall ... 229

8.6 Jämförelse med relevanta databaser ... 234

8.7 Lagringstid ... 239
8.7.1 Lagring av resultatet av behandling av PNR-uppgifter ... 242

8.8 Radering eller anonymisering? ... 244

8.9 Tillåtna ändamål med behandling av PNR-uppgifter ... 246

9 Trafikslagsneutral PNR-lagstiftning ... 249

10 Pågående arbete inom EU ... 251

10.1 Etias ... 251
10.1.1 Innehåll ... 251

10.2 Entry Exit System ... 258
10.2.1 Innehåll ... 258

10.3 Europeiska kommissionens studier om sjöfart och landtransport ... 259
10.3.1 Studien om land- och tågtransport ... 260
10.3.2 Studien om sjöfart ... 265

10.4 European Maritime Single Window environment ... 267

11 Reglering i utvalda EU-länder 269

12 Behöriga myndigheters behov av passageraruppgifter... 271

12.1 Inledning 271

12.2 Polismyndigheten 272

12.3 Tullverket 273

12.4 Ekobrottsmyndigheten..... 276

12.5 Försvarsmakten..... 277

12.6 Säkerhetspolisen..... 279

13 EU-domstolens praxis 281

13.1 Inledning 281

13.2 Digital Rights Ireland 282

13.3 Tele2 Sverige och Watson m.fl..... 284

13.4 La Quadrature du Net 287

13.5 Privacy International 289

14 Central databas för passageraruppgifter 293

14.1 Inledning 293

14.2 Befintlig databas vid enheten för passagerarinformation ... 293

14.3 Separat databas vid enheten för passagerarinformation..... 299

14.4 Databas vid annan myndighet 301

14.4.1 Databas hos Säkerhetspolisen..... 301

14.4.2 Databas hos Tullverket 302

14.5 Ändamålsbegränsning..... 303

15 Överväganden och förslag 307

15.1 PNR-lagstiftningen ska göras trafikslagsneutral 307

15.2 Lagen om flygpassageraruppgifter i brottsbekämpningen ska tillämpas 308
15.2.1 Lagens innehåll 309
15.2.2 Definitionen av en medlemsstat 309

15.3 Förordningen om flygpassageraruppgifter i brottsbekämpningen 310

15.4 Påverkan på befintlig lagstiftning 311
15.4.1 Lufttrafikföretagens skyldigheter enligt polislagen och tullbefogenhetslagen 316

16 Transportföretagens roll 319

16.1 Inledning 319

16.2 Varierande förutsättningar för transportföretag 319

16.3 Vilka trafikslag ska omfattas? 320
16.3.1 Särskilt om färjetrafiken 321

16.4 Vilka företag ska omfattas av uppgiftsskyldigheten? 325

16.5 Vilka uppgifter ska överföras? 328

16.6 Tidpunkt för överföring av PNR-uppgifter 331
16.6.1 Tåg- och busstrafik 331
16.6.2 Färjetrafik 332
16.6.3 Överföring vid andra tidpunkter 333

16.7 Administration och kostnader för transportföretagen 334

16.8 Inrikes trafik 337
16.8.1 Inrikesflyg 338

17 Speciallagstiftning för brottsbekämpande myndigheter .. 341

17.1 Inledning 341

17.2 Tullverket 342

17.3 Polismyndigheten och Säkerhetspolisen 343
17.3.1 Uppgiftsskyldigheten 344
17.3.2 Vem ska tillhandahålla uppgifterna? 346
17.3.3 Föreläggande 347
17.3.4 Överklagande 347
17.3.5 Terminalåtkomst ändras till direktåtkomst 348

17.4 Polismyndigheten 349
17.4.1 Tillåten tid för behandling 349
17.4.2 Tillåtna ändamål för behandling 351
17.4.3 Hur uppgifter ska lämnas 352

17.5 Försvarsmakten 353

17.6 Ekobrottsmyndigheten 355

18 Konsekvensutredning 359

18.1 Inledning 359

18.2 Förändringar till följd av PNR-domen 360
18.2.1 Konsekvenser för brottsbekämpningen 360
18.2.2 Konsekvenser för den nationella säkerheten 363
18.2.3 Konsekvenser för enskilda 364
18.2.4 Konsekvenser för lufttrafikföretagen 366
18.2.5 Konsekvenser för Åklagarmyndigheten, Ekobrottsmyndigheten och domstolarna 366
18.2.6 Övriga konsekvenser 370

18.3 Trafikslagsneutral PNR-lagstiftning och utökade befogenheter för brottsbekämpande myndigheter 370
18.3.1 Konsekvenser för brottsbekämpningen 370
18.3.2 Konsekvenser för enskilda 371
18.3.3 Konsekvenser för transportföretagen 372
18.3.4 Konsekvenser för Åklagarmyndigheten, Ekobrottsmyndigheten och domstolarna 374
18.3.5 Konsekvenser för Polismyndigheten 375
18.3.6 Övriga konsekvenser 377

19 Ikraftträdande 379

20 Författningskommentar 381

20.1 Förslaget till lag om ändring av lagen (2018:1181) om flygpassageraruppgifter i brottsbekämpningen 381

20.2 Förslaget till lag om ändring i polislagen (1984:387) 400

20.3 Förslaget till lag om ändring i lagen (2009:966) om Försvarsunderrättelsedomstol 402

20.4 Förslaget till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område 404

20.5 Förslaget till lag om ändring i lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område 406

20.6 Förslaget till lag om ändring i tullbefogenhetslagen (2024:710) 407

Särskilt yttrande 409

Bilaga

Bilaga 1 Kommittédirektiv 2025:36 419

Förkortningar

ANPR	Automatic Number Plate Recognition.
API	Advance Passenger Information.
API-direktivet	Europeiska rådets direktiv 2004/82/EG av den 29 april 2004 om skyldighet för transportörer att lämna uppgifter om passagerare.
Chicago-konventionen	Konventionen den 7 december 1944 om internationell civil luftfart.
Dataskyddsdirektivet	Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.
Dataskydds-förordningen	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Dataskydds-konventionen	Europeiska rådets konvention (ETS) av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av person-uppgifter.
Dataskyddslagen	Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.
dir.	Direktiv.
EAS	Europol Analysis System.
e-dataskydds-direktivet	Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).
EDPB	European Data Protection Board.
EES	Entry Exit System.
EIS	Europol Information System.
EMPACT	European Multidisciplinary Platform Against Criminal Threats.
EMSWe	European Maritime Single Window environment.
EMSWe-förordningen	Europaparlamentets och rådets förordning (EU) 2019/1239 av den 20 juni 2019 om inrättande av en europeisk kontaktpunkt för sjöfart och om upphävande av direktiv 2010/65/EU.
Etias	European Travel Information and Authorisation System.
EU	Europeiska unionen.
Eurodac	European Asylum Dactoscopy.

Europakonventionen	Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.
eu-Lisa	Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa.
EU:s rättighetsstadga	Europeiska unionens stadga om de grundläggande rättigheterna.
FN	Förenta Nationerna.
Frontex	EU:s gräns- och kustbevakningsbyrå.
IATA	International Air Transport Association.
ICAO	International Civil Aviation Organisation.
IMY	Integritetsskyddsmyndigheten.
Ju	Justitiedepartementet.
Kodex om Schengengränserna	Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016 om en unionskodex om gränspassage för personer (kodex om Schengengränserna).
Kommissionen	Europeiska kommissionen.
NSW	National Single Window.
OSL	Offentlighets- och sekretesslagen (2009:400).
PIU	Passenger Information Unit.
PNR	Passenger Name Record.
PNR-direktivet	Europaparlamentets och rådets direktiv (EU) 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet.

PNR-domen	EU-domstolens dom den 21 juni 2022, Ligue des droits humains mot Conseil des ministres, mål nr C-817/19.
Polisens brottsdatalag	Lag (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område.
Prop.	Regeringens proposition.
RF	Regeringsformen.
RB	Rättegångsbalken.
Rörlighetsdirektivet	Europaparlamentets och rådets direktiv 2004/38/EG av den 29 april 2004 om unionsmedborgares och deras familjemedlemmars rätt att fritt röra sig och uppehålla sig inom medlemsstaternas territorier och om ändring av förordning (EEG) nr 1612/68, och om upphävande av direktiven 64/221/EEG, 68/360/EEG, 72/194/EEG, 75/34/EEG, 75/35/EEG, 90/364/EEG, 90/365/EEG och 93/96/EEG.
Schengenkonventionen	Konventionen om tillämpning av Schengenavtalet av den 14 juni 1985.
SLTD	Stolen and Lost Travel Documents database.
SOU	Statens offentliga utredningar.
Säpodatalagen	Lag (2019:1182) om Säkerhetspolisens behandling av personuppgifter.
TDAWN	Travel Documents Associated with Notices database.
Tullverkets brottsdatalag	Lag (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område.
VIS	Visa Information System.

Sammanfattning

PNR-systemet

PNR-systemet bygger på Europaparlamentets och rådets direktiv (EU) 2016/681 av den 27 april 2016 om användning av passagerar-uppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet, hädanefter benämnt som PNR-direktivet. I svensk rätt är PNR-direktivet genomfört genom lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen.

PNR-uppgifter är enligt direktivet uppgifter som passagerare lämnar vid beställning och bokning av flygresor och vid incheckning. Det rör sig exempelvis om namn, kontaktuppgifter, resdatum och bagageinformation. Direktivet ställer upp en skyldighet för lufttrafikföretag att föra över PNR-uppgifter till en enhet för passagerarinformation, som i Sverige är en sektion placerad inom Polismyndigheten. Vilka uppgifter som ska överföras framgår i en bilaga till direktivet. Skyldigheten att överföra uppgifter gäller emellertid endast för de uppgifter som lufttrafikföretagen samlar in i sin normala verksamhet. PNR-systemet uppställer således ingen skyldighet att samla in några specifika uppgifter, utan endast att föra över vissa specifika uppgifter, under förutsättning att de faktiskt samlas in. PNR-uppgifterna ska normalt överföras vid två tillfällen inför varje flygning; 24–48 timmar innan flygningen avgång samt omedelbart efter att gatens dörrar har stängts.

När PNR-uppgifterna kommer in till enheten får en förhandsbedömning göras av passagerare före deras beräknade ankomst till eller avresa från Sverige i syfte att välja ut personer som behöver ytterligare utredas av behöriga myndigheter eller Europol.

Från enheten kan behöriga myndigheter i Sverige, andra medlemsstater och tredjeländer begära tillgång till PNR-information. En sådan

överföring får endast ske om det av begäran framgår att informationen ska användas i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet. De behöriga i svensk rätt är Tullverket, Polismyndigheten, Ekobrottsmyndigheten, Säkerhetspolisen och Försvarsmakten.

PNR-systemet innebär en skyldighet för lufttrafikföretag att överföra PNR-uppgifter för flygningar utanför EU, dvs. mellan en medlemsstat och ett tredjeland. Direktivet får även på frivillig basis tillämpas på flygningar inom EU. Flertalet medlemsstater, däribland Sverige, har valt att utvidga systemet till att omfatta samtliga flygningar inom EU.

Inom PNR-systemet samlas en mycket stor mängd uppgifter in. Behandlingen av uppgifter har därför på flera sätt begränsats, t.ex. genom ändamålsbegränsningen som nämnts ovan. Känsliga personuppgifter, dvs. uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller uppgifter som rör hälsa, sexualliv eller sexuell läggning får inte behandlas enligt lagen. Lagringen av uppgifterna får pågå under högst fem år. Efter sex månader ska uppgifterna behörighetsbegränsas. För att en behörig mottagare därefter ska få tillgång till PNR-uppgifterna krävs det beslut av en åklagare, om det pågår en förundersökning, eller i annat fall av Polismyndigheten.

En behörig myndighet som har mottagit PNR-information efter enheten för passagerarinformations förhandsbedömning ska omedelbart förstöra informationen om den saknar betydelse för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet.

PNR-domen och dess följder

Den 21 juni 2022 meddelade EU-domstolen den s.k. PNR-domen.[1] Avgörandet berörde flera delar av tillämpningen av PNR-direktivet. Även om domstolen konstaterade att det inte hade kommit fram någon omständighet som kunde påverka direktivets giltighet innebär flera av uttalandena i domen att tillämpningen av PNR-systemet kräver vissa förändringar. I detta avsnitt behandlas översiktligt domstolens

[1] EU-domstolens dom den 21 juni 2022, *Ligue des droits humains mot Conseil des ministres*, mål nr C-817/19.

uttalanden och de förändringar som vi anser att detta kräver i svensk rätt.

Flygningar inom EU

Flygningar inom EU har hittills inom ramen för PNR-systemet behandlats på samma sätt som flygningar utom EU. Enligt EU-domstolen innebär PNR-systemet ett allvarligt ingrepp i de grundläggande rättigheter som garanteras i artikel 7 och 8 i EU:s rättighetsstadga, dvs. rätten till respekt för privat- och familjelivet och rätten till skydd av personuppgifter. Lagstiftningen innebär vidare en inskränkning av den fria rörligheten inom unionen.

För att det ska vara tillåtet för en medlemsstat att överföra och behandla PNR-uppgifter för samtliga flygningar inom EU krävs det att det finns ett verkligt och aktuellt eller förutsebart terroristhot mot den aktuella medlemsstaten. I avsaknad av ett sådant terroristhot ska tillämpningen av systemet i stället begränsas till överföring och behandling av PNR-uppgifter för ett urval av flygningar för vilka det finns uppgifter som kan motivera en sådan tillämpning. Vid ett urval av rutter får således utöver terroristhotet även beaktas risken för annan allvarlig brottslighet.

Varje medlemsstat har alltså möjlighet att fatta ett beslut om att utvidga tillämpningen av PNR-systemet till att omfatta samtliga flygningar inom EU, under förutsättning att terroristhotet uppnår de krav som ställs i domen. Ett sådant beslut måste kunna bli föremål för effektiv kontroll antingen av en domstol eller av en oberoende förvaltningsmyndighet, vars avgörande har bindande verkan. Syftet med prövningen är att kontrollera om det föreligger skäl för utvidgad tillämpning av PNR-direktivet och att de villkor och garantier som måste ställas upp är uppfyllda.

Det framgår inte i domen vilken myndighet som ska fatta beslutet och vi bedömer därför att detta är upp till varje enskild medlemsstat att bestämma. Vårt förslag är att Säkerhetspolisen ges i uppgift att fatta sådana beslut. Säkerhetspolisen förfogar över beslutet om vilken terrorhotnivå på en femgradig skala och har den kompetens och erfarenhet som krävs för att bedöma terroristhotet mot Sverige.

Säkerhetspolisens beslut måste kunna bli föremål för en effektiv prövning. Vi anser att den prövningen bör genomföras av Försvarsunderrättelsedomstolen, efter underställning av Säkerhetspolisen.

I avsaknad av ett verkligt och aktuellt eller förutsebart terroristhot mot Sverige får PNR-systemet tillämpas på ett urval av flygningar. Urvalet bör bestämmas av enheten för passagerarinformation som inför beslutet ska inhämta synpunkter från de behöriga myndigheterna. Urvalsbeslutet ska regelbundet omprövas för att säkerställa att tillämpningen av systemet på flygningarna alltid är begränsat till vad som är absolut nödvändigt.

PNR-uppgifter för flygningar som inte ingår i urvalet ska fortfarande överföras från lufttrafikföretagen till enheten för passagerarinformation och där genomgå en förhandsbedömning. Därefter ska PNR-uppgifter från flygningar som ingår i urvalet samt PNR-uppgifter från flygningar där det förekommer personer som gett träff i förhandsbedömningen fortsatt bevaras hos enheten för passagerarinformation. Övriga PNR-uppgifter ska anonymiseras efter att förhandsbedömningen har genomförts. På så sätt begränsas tillämpningen av PNR-systemet på uppgifterna på ett sätt som vi anser vara förenligt med EU-domstolens uttalanden.

Förhandskontroll vid begäran om tillgång till PNR-information

I nu gällande lagstiftning anges att efter den inledande sexmånadersperioden som PNR-uppgifter har lagrats vid enheten för passagerarinformation ska uppgifterna behörighetsbegränsas. Därefter tillåts utlämnande av fullständiga PNR-uppgifter endast om det rimligen kan antas vara nödvändigt för direktivets ändamål. Det krävs vidare tillstånd från en rättslig myndighet eller en annan nationell myndighet som i enlighet med nationell rätt är behörig att kontrollera om villkoren för tillgång är uppfyllda. I svensk rätt ska en begäran från en behörig myndighet prövas av åklagare om det pågår en förundersökning, och av Polismyndigheten i andra fall.

I PNR-domen anges att en sådan rättslig prövning ska ske även om begäran om tillgång framställs innan den inledande sexmånadersperioden har löpt ut. Svensk rätt bör således ändras så att en förhandskontroll alltid ska ske vid utlämning av PNR-information.

Enligt domen ska en domstol eller oberoende förvaltningsmyndighet som ska besluta om tillgång till PNR-uppgifter. Myndigheten ska förfoga över alla befogenheter och lämna alla nödvändiga garantier för att säkerställa en avvägning mellan de olika intressena och rättigheterna i fråga. Myndigheten måste ha en ställning som innebär att den kan fullgöra sitt uppdrag på ett objektivt och opartiskt sätt, och den måste därför vara fri från all yttre påverkan. Detta krav på oberoende innebär att myndigheten måste vara fristående i förhållande till den som begär tillgång till uppgifterna, så att myndigheten kan utöva sin kontroll utan yttre påverkan. På det straffrättsliga området innebär kravet på oberoende att myndigheten dels inte får vara involverad i den aktuella brottsutredningen, dels att den ska ha en neutral ställning i förhållande till parterna i det straffrättsliga förfarandet.

För svensk rätt innebär detta att åklagare inte kan fatta beslut under pågående förundersökning och att Polismyndigheten inte kan fatta beslut i andra fall. Vi föreslår i stället att allmän domstol fattar beslut under pågående förundersökning och att åklagare fattar beslut i andra fall. Om en begäran framställs av en behörig mottagare i en annan medlemsstat eller ett tredjeland som har slutit avtal med EU om överföring och behandling av passageraruppgifter är det åklagare som fattar beslut, under förutsättning att sådant beslut inte redan har fattats i landet från vilket förfrågan har inkommit. För tredjeländer som saknar sådant avtal ska beslut alltid fattas av åklagare. Vid fara i dröjsmål kan tillgång till PNR-uppgifter medges behöriga mottagare och ett tredjeland som har slutit avtal med EU utan föregående rättslig prövning.

Lagringstid

Tillämpningen av PNR-systemet har hittills inneburit att samtliga PNR-uppgifter har lagrats i fem år vid enheten för passagerarinformation. I PNR-domen görs det avseende lagringstiden skillnad mellan den inledande sexmånadersperioden och den efterföljande tiden som uppgifter lagras. Under de första sex månaderna går det inte utöver vad som är strikt nödvändigt att lagra samtliga uppgifter. För den efterföljande perioden upp till fem år finns det dock enligt EU-domstolen inneboende risker för oproportionerlig användning och missbruk till följd av den stora mängd uppgifter som kan lagras konti-

nuerligt. För de passagerare för vilka varken förhandsbedömningen, eventuella kontroller som utförts under de första sex månaderna, eller någon annan omständighet har visat att det föreligger objektiva omständigheter som visar att det finns en risk för terrorbrott eller annan allvarlig brottslighet tycks det inte finnas något samband mellan PNR-uppgifterna och målen med direktivet som motiverar att uppgifterna lagras. Sådana uppgifter ska därmed enligt vårt förslag anonymiseras, vilket innebär att de upphör att vara personuppgifter och inte längre går att koppla till en viss person.

Tillåtna ändamål med behandling av PNR-uppgifter

PNR-direktivet anger att PNR-uppgifter som samlas in i enlighet med direktivet endast får behandlas i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. I PNR-domen förtydligas det att de uppräknade ändamålen är uttömmande och att detta innebär att PNR-uppgifter inte får lagras i en enda databas som kan användas för andra ändamål eftersom det skulle innebära en risk för att uppgifterna används för andra ändamål än vad som avses i direktivet.

I den svenska regleringen har de tillåtna ändamålen utvidgats genom att enheten för passagerarinformation får behandla PNR-information när det är nödvändigt för att tillhandahålla uppgifter som behövs i verksamhet som rör nationell säkerhet. Syftet med bestämmelsen är att t.ex. förebygga högmålsbrott och vissa brott mot Sveriges säkerhet som inte faller in under direktivets tillämpningsområde. Enligt vårt förslag är det endast tillåtet att behandla PNR-uppgifter som har samlats in i enlighet med direktivet i verksamhet som rör nationell säkerhet, om det sker för de ändamål som framgår av PNR-direktivet.

En trafikslagsneutral PNR-lagstiftning

PNR-systemet för flygtrafiken har varit framgångsrikt och utgör ett viktigt verktyg för brottsbekämpande myndigheter i arbetet mot den gränsöverskridande brottsligheten. Det faller sig därför naturligt att undersöka möjligheten att upprätta ett liknande system även för andra trafikslag. Det innebär i så fall att transportföretag som bedriver passagerartrafik med andra färdmedel än flyg åläggs en skyldighet att föra

över vissa uppräknade PNR-uppgifter till enheten för passagerarinformation. I likhet med flygtrafiken bör skyldigheten att överföra uppgifter endast omfatta sådana uppgifter som transportföretaget samlar in som en del av sin normala verksamhet. De trafikslag som bör omfattas av en trafikslagsneutral PNR-lagstiftning är gränsöverskridande tåg-, buss- och färjetrafik samt inrikes flygtrafik.

Det finns flera alternativ för hur ett sådant system kan se ut. De alternativ som har övervägts under utredningens gång är att använda den befintliga databasen eller en separat databas vid enheten för passagerarinformation, eller en separat databas vid en annan myndighet; Tullverket eller Säkerhetspolisen. Den största fördelen med en separat databas är att det är möjligt att bestämma en bredare ändamålsbegränsning än den som gäller inom PNR-systemet. Det skulle vara möjligt att behandla PNR-uppgifter för att bekämpa fler typer av brott och att behandla uppgifterna i verksamhet som rör nationell säkerhet utan begränsningen att det ska ske för de ändamål som PNR-direktivet anger.

Vi anser emellertid att fördelarna med att använda den befintliga databasen vid enheten för passagerarinformation väger tyngre och föreslår därför en sådan lösning. Det är den minst kostsamma och tidskrävande lösningen. Något som starkt talar för detta förslag är att det kommer att finnas möjlighet att utbyta passageraruppgifter med andra länder som har utökat PNR-systemet till att omfatta andra trafikslag än lufttrafik. Det gynnar brottsbekämpningen i Sverige och globalt.

Den befintliga lagen om flygpassageraruppgifter ska tillämpas även för övriga trafikslag, och namnet på den bör därför ändras till lagen om passageraruppgifter i brottsbekämpningen. Det kräver även ett flertal förändringar av begrepp i lagen, t.ex. bör lufttrafikföretag bytas ut mot transportföretag. Vidare måste hänvisningar till lagen i annan författning ändras.

Påverkan på befintlig lagstiftning

I 25 § polislagen och 7 kap. 12 § tullbefogenhetslagen ges Polismyndigheten och Säkerhetspolisen respektive Tullverket möjlighet att begära in vissa uppgifter från transportföretag, om de kan antas ha betydelse för den brottsbekämpande verksamheten. Vid genomförandet av

PNR-direktivet i svensk lagstiftning togs den möjligheten bort när det gäller lufttrafikföretag som omfattas av PNR-systemet. Bakgrunden till detta var att ett nationellt system för inhämtning av passageraruppgifter skulle kunna motverka PNR-direktivets bakomliggande syften, dvs. att förbättra den inre säkerheten samtidigt som man upprätthåller skyddet för de överförda uppgifterna.

I denna del gör vi en annan bedömning än den som gjordes vid genomförandet av PNR-direktivet. Möjligheten att, utöver den insamling som sker inom ramen för PNR-systemet, hämta in uppgifter innebär inte att syftet att förbättra den inre säkerheten inom unionen. Tvärtom bör ytterligare tillgång till uppgifter innebära bättre förutsättningar att bekämpa brott, vilket är ett led i att förbättra den inre säkerheten. När det gäller syftet att upprätthålla skyddet för de uppgifter som behandlas finns det ett omfattande dataskyddsregelverk som enligt vår mening utgör ett fullgott dataskydd.

Det förefaller inte heller rimligt att myndigheternas möjligheter att bekämpa brott som inte omfattas av PNR-systemets tillämpningsområde ska försämras om fler trafikslag inkluderas i systemet. Tillgång till uppgifter i syfte att bekämpa mindre allvarlig brottslighet är dessutom ett värdefullt verktyg för att bekämpa även den allvarliga brottsligheten. Det kan ifrågasättas om det är tänkt att den EU-rättsliga regleringen ska innebära att medlemsstaterna ställs inför ett val att antingen införa ett centralt system med insamling av en stor mängd uppgifter som endast får användas i syfte att bekämpa allvarlig brottslighet och terrorism, eller ett mer splittrat system där myndigheter begär tillgång till enstaka uppgifter för att bekämpa brott i allmänhet.

Vi anser att det är lämpligt och proportionerligt att inhämtning av uppgifter från transportföretag med stöd av polislagen och tullbefogenhetslagen omfattar även lufttrafikföretag samt att regleringen kvarstår även för övriga trafikslag efter implementeringen av dessa i den trafikslagsneutrala PNR-lagstiftningen.

Speciallagstiftning för brottsbekämpande myndigheter

Ett ytterligare tillvägagångssätt att förbättra förutsättningarna för brottsbekämpningen är att se över de brottsbekämpande myndigheternas tillgång till och behandling av passageraruppgifter vid sidan om PNR-systemet. I betänkandet läggs ett antal förbättringsförslag fram.

Tullverket

Tullverkets befogenhet att hämta in bokningsuppgifter i 7 kap. 12 § tullbefogenhetslagen utökas så att de uppgifter som är tillåtna att begära från transportföretagen även omfattar kön, utöver redan gällande uppgifter om t.ex. namn, födelsedatum, nationalitet och vissa kontaktuppgifter.

Polismyndigheten och Säkerhetspolisen

I 25 § polislagen ges Polismyndigheten och Säkerhetspolisen möjlighet att begära uppgifter från transportföretag. Regleringen liknar den som gäller för Tullverket, men har sedan den nya tullbefogenhetslagen trädde i kraft 2024 något mindre omfattande möjligheter att inhämta och behandla uppgifterna. En utgångspunkt är därför att undersöka om polislagen bör ändras för att efterlikna tullbefogenhetslagen.

Uppgiftsskyldigheten

De uppgifter om passagerare som är tillåtna att hämta in enligt 25 § polislagen är namn, resrutt, bagage, medpassagerare samt sättet för betalning och bokning. Vi anser att samma uppgifter bör få hämtas in som i tullbefogenhetslagen och att bestämmelsen därmed bör kompletteras med uppgifter om födelsedatum, kön, nationalitet, e-postadress och mobiltelefonnummer som transportföretaget har tillgång till.

Tillhandahållande av uppgifterna

Det förekommer att andra företag än själva transportföretaget sköter bokningen av transporter. Det kan t.ex. röra sig om en speditör eller något annat företag. I sådana fall bör skyldigheten att lämna uppgifter även gälla för det företaget.

Föreläggande

Transportföretag har en skyldighet att lämna de uppgifter om transporter som begärs, men Polismyndigheten och Säkerhetspolisen saknar i dagsläget ett effektivt påtryckningsmedel om företaget inte uppfyller sin skyldighet. Det bör därför införas en möjlighet för myndigheterna att förelägga ett transportföretag att fullgöra sina skyldigheter att lämna uppgifter om transporter. Ett beslut om föreläggande får överklagas till allmän förvaltningsdomstol och vid överklagande till kammarrätt krävs det prövningstillstånd.

Överklagande

En begäran om uppgifter från transportföretag är ofta tidskänslig och det är viktigt att myndigheternas arbete inte fördröjs. Det bör därför fastställas i polislagen att en sådan begäran inte går att överklaga.

Polismyndigheten

Vissa av förslagen avseende polislagen och anslutande lagstiftning påverkar endast Polismyndigheten och inte Säkerhetspolisen.

Tillåten tid för behandling

Enligt nuvarande reglering får Polismyndigheten behandla personuppgifter som begärs från transportföretag under den tid som är nödvändig med hänsyn till ändamålet med behandlingen. För att förbättra underrättelsearbetet, t.ex. genom att kunna upptäcka historiska samband och mönster och ta fram riskprofiler och kriterier för dessa bör uppgifterna få bevaras hos Polismyndigheten under sex månader. Det bör även vara möjligt att ta del av uppgifter genom direktåtkomst under sex månader efter att transportern har ankommit eller avgått.

Tillåtna ändamål för behandling

Polismyndigheten har behov av att kunna arbeta med riskprofiler för att selekteringen ska bli mer träffsäker. Det bör därför anges i polislagen att uppgifter som begärs in från transportföretag med stöd av lagen får, utöver det som gäller i dag, även behandlas för att planera

kontroller, välja ut kontrollobjekt och göra analyser som behövs för att uppdatera eller skapa nya kriterier som ska användas vid planering av kontroller eller urval av kontrollobjekt.

Hur uppgifter ska lämnas

Det finns ingen enhetlig standard för hur uppgifter ska lämnas från transportföretag till Polismyndigheten eller Säkerhetspolisen enligt 25 § polislagen. Det innebär att transportföretagen kan lämna uppgifter i flera olika filformat och struktur, vilket ökar den manuella hanteringen. Polismyndigheten bör därför ges möjlighet att meddela närmare föreskrifter om bestämmelserna om uppgifter från transportföretag.

Försvarsmakten och Ekobrottsmyndigheten

Försvarsmaktens har behov av uppgifter från transportföretag i försvarsunderrättelseverksamheten och i den militära säkerhetstjänsten. För Ekobrottsmyndigheten finns det motsvarande behov i den brottsbekämpande verksamheten. För att tillgodose dessa behov ska Polismyndigheten, på begäran från respektive myndighet, lämna sådana uppgifter.

Konsekvenser

I den del av betänkandet som rör ändringar i svensk rätt till följd av PNR-domen innebär förslagen att färre PNR-uppgifter vid varje enskild tidpunkt kommer att bevaras vid enheten för passagerarinformation och vara möjliga att använda i brottsbekämpningen. Detta har en påtaglig negativ påverkan på den brottsbekämpning som sker med hjälp av PNR-information. För den personliga integriteten innebär förslagen en skärpning av det skydd för personuppgifter som PNR-systemet innebär.

Förslagen avseende en trafikslagsneutral PNR-lagstiftning innebär å andra sidan att fler uppgifter tillgängliggörs, vilket stärker brottsbekämpande myndigheters möjlighet att följa misstänkta personers

resor in i och genom EU. Detta innebär ett ingrepp i grundläggande rättigheter som vi bedömer är lämpligt och proportionerligt.

För transportföretagen kommer detta innebära kostnader och administration. En del eller hela kostnadsökningen kommer enligt vår bedömning dock att kunna bäras av konsumenterna.

Förslagen innebär ökade kostnader för Sveriges domstolar och Åklagarmyndigheten, vilka inte bedöms kunna rymmas inom befintligt anslag utan bör finansieras genom det allmänna reformutrymmet. Förslagen innebär vidare ökade kostnader för enheten för passagerarinformation inom Polismyndigheten samt myndighetens it-avdelning.

Ikraftträdande

Samtliga författningsförslag föreslås träda i kraft den 1 januari 2028.

1 Författningsförslag

1.1 Förslag till lag om ändring i lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen

Härigenom föreskrivs i fråga om lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen

dels att lagens namn ska ha följande lydelse,

dels att 1 kap. 1 och 3–6 §§, 2 kap. 1–7 §§, 3 kap. 1, 4–5 och 9–11 §§, 4 kap. 11 §, 6 kap. 1–3 §§ och bilaga 1 ska ha följande lydelse,

dels att rubriken för 2 kap. och rubrikerna närmast före 4 kap. 11 § och 6 kap. 1 § ska ha följande lydelse,

dels att det ska införas ett nytt kapitel, 3 a, av följande lydelse,

dels att det ska införas sex nya paragrafer, 4 kap. 12–19 §§, närmast före 4 kap. 14, 16 och 17 §§ nya rubriker och nya bilagor 2–4 av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
Lag (2018:1180) om *flygpassageraruppgifter* i brottsbekämpningen	**Lag (2018:1180) om *passageraruppgifter* i brottsbekämpningen**
1 kap. Lagens innehåll	
1 §	
Denna lag *genomför Europaparlamentets och rådets direktiv (EU) 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter)*	Denna lag *innehåller bestämmelser om transportföretags överföring av PNR-uppgifter till enheten för passagerarinformation och om behandling av PNR-uppgifter*

för att förebygga, förhindra, upptäcka, utreda *och* lagföra *terroristbrott och grov brottslighet, här benämnt PNR-direktivet.* Med PNR-uppgifter avses i lagen uppgifter om varje enskild passagerare som har lämnats vid bokning av en *flygresa* och vid incheckning.

Lagen *innehåller bestämmelser om lufttrafikföretags överföring av PNR-uppgifter till enheten för passagerarinformation och om behandling av PNR-uppgifter i verksamhet* för att förebygga, förhindra, upptäcka, utreda *eller* lagföra *terroristbrottslighet eller annan allvarlig brottslighet.* Med PNR-uppgifter avses i lagen uppgifter om varje enskild passagerare som har lämnats vid bokning av en *transport, köp av biljett* och vid incheckning.

Lagen *genomför också Europaparlamentets och rådets direktiv (EU) 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter)* för att förebygga, förhindra, upptäcka, utreda *och* lagföra *terroristbrott och grov brottslighet, här benämnt PNR-direktivet.*

Med terroristbrottslighet avses i lagen brott enligt artiklarna 3–12 och 14 i Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF.

Med annan allvarlig brottslighet avses i lagen de brott som anges i bilaga II till PNR-direktivet och för vilka det i Sverige eller andra medlemsstater är föreskrivet fängelse i tre år eller mer.

Nuvarande lydelse

3 §

I lagen används följande uttryck med nedan angiven betydelse.

Uttryck	Betydelse
Behörighetsbegränsade PNR-uppgifter	Personuppgifter som har gjorts otillgängliga för en användare som saknar särskild behörighet för att få tillgång till uppgifterna.

Behörig mottagare	En behörig myndighet i Sverige, en enhet för passagerarinformation i en annan medlemsstat, en myndighet som har utsetts som behörig i en annan medlemsstat eller Europol.
Behörig myndighet	En myndighet utsedd av regeringen som har behörighet att behandla PNR-information i verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet.
Lufttrafikföretag	Ett företag som har giltig operativ licens eller motsvarande som ger rätt att mot ersättning utföra *lufttransporter* av passagerare och som i sin normala verksamhet samlar in och behandlar PNR-uppgifter i ett elektroniskt system för hantering av reservationer.
Medlemsstat	En stat som är medlem i Europeiska unionen och har antagit PNR-direktivet.
Passagerare	Alla personer, förutom besättningsmedlemmar, som transporteras eller ska transporteras med ett flygplan *och som finns upptagna i passagerarförteckningen*.
PNR-information	PNR-uppgifter och resultatet av en enhet för passagerarinformations behandling av sådana uppgifter.
Tredjeland	En stat som inte är en medlemsstat.

Föreslagen lydelse

3 §

I lagen används följande uttryck med nedan angiven betydelse.

Uttryck	Betydelse
Behörighetsbegränsade PNR-uppgifter	Personuppgifter som har gjorts otillgängliga för en användare som saknar särskild behörighet för att få tillgång till uppgifterna.
Behörig mottagare	En behörig myndighet i Sverige, en enhet för passagerarinformation i en annan medlemsstat, en myndighet som har utsetts som behörig i en annan medlemsstat eller Europol.
Behörig myndighet	En myndighet utsedd av regeringen som har behörighet att behandla PNR-information i verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet.
Transportföretag	Ett företag som har giltig operativ licens, *tillstånd*, *certifikat* eller motsvarande som ger rätt att mot ersättning utföra *transporter* av passagerare *med flygplan*, *tåg*, *buss eller färja*, och som i sin normala verksamhet samlar in och behandlar PNR-uppgifter i ett elektroniskt system för hantering av reservationer, *avgångskontrollsystem för att checka in passagerare*, *elektroniskt system för köp av biljetter eller likvärdiga system med motsvarande uppgifter*.

Medlemsstat	En stat som är medlem i Europeiska unionen och har antagit PNR-direktivet. När det gäller transporter med tåg, buss och färja avses samtliga stater som är medlemmar i Europeiska unionen.
Passagerare	Alla personer, förutom besättningsmedlemmar, som transporteras eller ska transporteras med ett flygplan, *tåg, buss eller färja*.
PNR-information	PNR-uppgifter och resultatet av en enhet för passagerarinformations behandling av sådana uppgifter.
Tredjeland	En stat som inte är en medlemsstat.
Transport utanför EU	*Transport som utförs av ett transportföretag, med avgång från ett tredjeland och planerad ankomst på en medlemsstats territorium eller transport från en medlemsstats territorium med planerad ankomst i ett tredjeland, i båda fallen inklusive eventuella mellanlandningar eller stopp på territorier i medlemsstater eller tredjeländer.*
Transport inom EU	*Transport som utförs av ett transportföretag, med avgång från en medlemsstats territorium och planerad ankomst på en eller flera andra medlemsstaters territorium, utan eventuella mellanlandningar eller stopp på tredjeländers territorier samt transport som utförs av ett transportföretag som bedriver lufttrafik mellan två inrikes flygplatser i Sverige.*

4 §

Det ska vid Polismyndigheten finnas en enhet för passagerarinformation. Enheten ska ansvara för att

1. samla in PNR-uppgifter från *lufttrafikföretag*, bevara och i övrigt behandla uppgifterna, och

1. samla in PNR-uppgifter från *transportföretag*, bevara och i övrigt behandla uppgifterna, och

2. överföra PNR-information till behöriga mottagare och tredjeländer.

5 §

PNR-information får endast behandlas i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet, om inte annat anges i *6 § eller* 5 kap. 3 §.

PNR-information får endast behandlas i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet, om inte annat anges i 5 kap. 3 §.

6 §

Lagens bestämmelser om behandling av personuppgifter gäller inte för behöriga myndigheter i verksamhet som rör nationell säkerhet.

Enheten för passagerarinformation får behandla PNR-information när det är nödvändigt för att tillhandahålla uppgifter som behövs för sådan verksamhet.

2 kap.

***Lufttrafikföretagens* skyldigheter**

***Transportföretagens* skyldigheter**

1 §

Lufttrafikföretag ska till enheten för passagerarinformation inför varje *flygning som ankommer till eller avgår från Sverige* överföra sådana PNR-uppgifter som anges i *bilagan* till lagen. PNR-uppgifterna ska endast överföras i de

Transportföretag ska till enheten för passagerarinformation inför varje *transport inom eller utanför EU* överföra sådana PNR-uppgifter som anges i *bilagorna* till lagen. PNR-uppgifterna ska endast överföras i de fall *transportföre-*

fall *lufttrafikföretagen* samlar in uppgifterna som en del av sin normala verksamhet.	*tagen* samlar in uppgifterna som en del av sin normala verksamhet.
	Skyldigheten för transportföretag som bedriver färjetrafik att överföra uppgifter enligt första stycket omfattar även de uppgifter om besättningen som anges i punkt 17 i bilaga 4.
Om *flygningens* linjebeteckning delas med ett eller flera andra *lufttrafik*företag, ska det *lufttrafikföretag* som utför *flygningen* överföra PNR-uppgifter om samtliga passagerare.	Om *transportens* linjebeteckning delas med ett eller flera andra *transportföretag*, ska det *transportföretag* som utför *transporten* överföra PNR-uppgifter om samtliga passagerare.
2 §	
PNR-uppgifterna ska överföras	PNR-uppgifterna *för en flygning* ska överföras
1. 24–48 timmar före flygningens avgång, och	
2. omedelbart efter det att gatens dörrar har stängts.	
Den andra överföringen får begränsas till uppdateringar och kompletteringar av de uppgifter som överfördes vid det första tillfället.	
	PNR-uppgifter för övriga transportföretag, med undantag för sådana som bedriver färjetrafik, ska överföras i samband med att en bokning eller avbokning av en transport sker.
3 §	
Lufttrafikföretag ska på begäran av enheten för passagerarinformation överföra PNR-uppgifter även vid andra tidpunkter än de som anges i 2 §, om enheten bedömer att det i ett enskilt fall är nödvändigt med tillgång till PNR-uppgifter för att avvärja en spe-	*Transportföretag* ska på begäran av enheten för passagerarinformation överföra PNR-uppgifter även vid andra tidpunkter än de som anges i 2 §, om enheten bedömer att det i ett enskilt fall är nödvändigt med tillgång till PNR-uppgifter för att avvärja en spe-

cifik och faktisk fara med anknytning till terroristbrottslighet eller annan allvarlig brottslighet.

cifik och faktisk fara med anknytning till terroristbrottslighet eller annan allvarlig brottslighet.

4 §

Lufttrafikföretag ska överföra PNR-uppgifterna elektroniskt. Enheten för passagerarinformation får inte medges direktåtkomst till PNR-uppgifter som behandlas vid *lufttrafikföretagen*.

Transportföretag ska överföra PNR-uppgifterna elektroniskt. Enheten för passagerarinformation får inte medges direktåtkomst till PNR-uppgifter som behandlas vid *transportföretagen*.

5 §

Lufttrafikföretag som är skyldiga att överföra PNR-uppgifter får anlita ett personuppgiftsbiträde för att utföra överföringen.

Transportföretag som är skyldiga att överföra PNR-uppgifter får anlita ett personuppgiftsbiträde för att utföra överföringen.

6 §

Lufttrafikföretag ska informera passagerare om överföringen av PNR-uppgifter till enheten för passagerarinformation och om skälen till överföringen.

Transportföretag ska informera passagerare om överföringen av PNR-uppgifter till enheten för passagerarinformation och om skälen till överföringen.

7 §

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om *lufttrafikföretagens* överföring av PNR-uppgifter till enheten för passagerarinformation.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om *transportföretagens* överföring av PNR-uppgifter till enheten för passagerarinformation.

3 kap.

1 §

PNR-uppgifter som har överförts från ett *lufttrafikföretag* ska bevaras i en databas vid enheten för passagerarinformation.

PNR-uppgifter som har överförts från ett *transportföretag* ska bevaras i en databas vid enheten för passagerarinformation.

4 §

Enheten för passagerarinformation får, *om inte 1 kap. 6 § är tillämplig,* endast behandla PNR-uppgifter som har överförts från ett *lufttrafikföretag* för att

Enheten för passagerarinformation får endast behandla PNR-uppgifter som har överförts från ett *transportföretag* för att

1. göra en förhandsbedömning av passagerare före deras beräknade ankomst till eller avresa från Sverige i syfte att välja ut personer som behöver utredas ytterligare av behöriga myndigheter eller Europol, på grund av att dessa personer kan vara inblandade i terroristbrottslighet eller annan allvarlig brottslighet,
2. fullgöra sina uppgifter att överföra PNR-information till behöriga mottagare eller tredjeländer, eller
3. göra analyser för att uppdatera eller skapa nya kriterier som ska användas vid förhandsbedömningar.

5 §

Vid en förhandsbedömning får PNR-uppgifter

1. jämföras med register eller andra uppgiftssamlingar som är relevanta för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet, och

Vid en förhandsbedömning får PNR-uppgifter

1. jämföras med register eller andra uppgiftssamlingar *över personer eller föremål som är eftersökta eller finns uppförda på en spärrlista samt med register eller andra uppgiftssamlingar* som är relevanta för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet, och

2. behandlas enligt på förhand utformade och fastställda kriterier som är riktade, proportionella och avgränsade och som inte grundas på sådana känsliga personuppgifter som avses i 1 kap. 7 §.

Med relevanta register och uppgiftssamlingar enligt första stycket 1 avses register och uppgiftssamlingar som förvaltas av de behöriga myndigheterna eller, när det gäller EU-databaser och internationella databaser, används av de behöriga myndigheterna för de syften som anges i första stycket 1.

Jämförelse enligt första stycket 1 får endast ske om registret eller uppgiftssamlingen används i samband med bekämpning av terroristbrottslighet eller annan allvarlig brottslighet som har ett åtminstone indirekt objektivt samband med transport av passagerare.

9 §

PNR-uppgifter som behandlas vid enheten för passagerarinformation ska bevaras i *fem år* från det att de kommit in från ett *luftrafikföretag*. Därefter ska de *förstöras*.

PNR-uppgifter som behandlas vid enheten för passagerarinformation ska bevaras i *sin fullständiga form i sex månader* från det att de kommit in från ett *transportföretag*. Därefter ska de *anonymiseras*. *Samtliga PNR-uppgifter som behandlas vid enheten för passagerarinformation ska förstöras senast fem år från det att de kommit in från ett transportföretag.*

PNR-uppgifter för transporter där det förekommer personer vars resor har ett direkt eller indirekt samband med en risk för terroristbrottslighet eller annan allvarlig brottslighet ska behörighetsbegränsas i enlighet med 3 kap. 11 § i stället för anonymiseras sex månader efter

	att de kommit in från ett transportföretag.
	10 §
PNR-uppgifter som inte anges i *bilagan* till lagen eller som utgör sådana känsliga personuppgifter som avses i 1 kap. 7 § ska omedelbart förstöras om de kommer in till enheten för passagerarinformation.	PNR-uppgifter som inte anges i *bilagorna* till lagen eller som utgör sådana känsliga personuppgifter som avses i 1 kap. 7 § ska omedelbart förstöras om de kommer in till enheten för passagerarinformation.
	11 §
Följande PNR-uppgifter ska behörighetsbegränsas sex månader efter att de har kommit in från ett *lufttrafikföretag* om de kan användas för att identifiera en person:	Följande PNR-uppgifter ska, *om de inte ska anonymiseras enligt 3 kap. 9 §*, behörighetsbegränsas sex månader efter att de har kommit in från ett *transportföretag* om de kan användas för att identifiera en person:
1. namn på passagerare,	
2. antal passagerare som reser tillsammans,	
3. adress och kontaktuppgifter,	
4. alla former av betalningsinformation, inklusive faktureringsadress,	
5. uppgifter om bonusprogram,	
6. allmänna anmärkningar, och	
7. uppgifter *enligt punkt 18* i *bilagan* till lagen.	7. uppgifter *om alla ändringar som har gjorts av de PNR-uppgifter som anges* i *bilagorna* till lagen.
	3 a kap. Behandling av PNR-uppgifter för transporter inom EU
	1 §
	Detta kapitel gäller för enheten för passagerarinformations behandling av PNR-uppgifter för transporter inom EU.

Om inte annat anges i detta kapitel, ska alla bestämmelser i lagen gälla för transporter inom EU som om de vore transporter utanför EU och för PNR-uppgifter för transporter inom EU som om det vore PNR-uppgifter för transporter utanför EU.

2 §

PNR-uppgifter för transporter inom EU ska anonymiseras efter att förhandsbedömningen enligt 3 kap. 4 § 1 har genomförts. PNR-uppgifter för transporter där det förekommer personer som efter förhandsbedömningen behöver utredas ytterligare av behöriga myndigheter eller Europol får fortsatt behandlas för de ändamål som anges i 3 kap. 4 § 2 och 3.

3 §

Om det föreligger ett verkligt och aktuellt eller förutsebart terroristhot mot Sverige får beslut fattas om att enheten för passagerarinformation får behandla PNR-uppgifter i sin fullständiga form för samtliga transporter inom EU även efter förhandsbedömningen enligt 3 kap. 4 § 1.

4 §

Om det inte föreligger något terroristhot mot Sverige i enlighet med 3 § får ett urval av transporter tillämpas för vilka PNR-uppgifter för samtliga passagerare får behand-

las i sin fullständiga form även efter förhandsbedömningen enligt 3 kap. 4 § 1.

Urvalet av transporter ska begränsas till vad som är absolut nödvändigt för att uppnå syftet med behandlingen av PNR-uppgifterna.

5 §

Beslut enligt 3 § ska fattas av Säkerhetspolisen. Inför beslutet kan Säkerhetspolisen vid behov inhämta synpunkter från Försvarsmakten och andra myndigheter. Beslutet upphör att gälla ett år efter den dag då det fattades.

Säkerhetspolisens beslut gäller omedelbart och ska expedieras till enheten för passagerarinformation.

6 §

Beslut om urval av transporter enligt 4 § ska fattas av enheten för passagerarinformation. Inför beslutet ska enheten inhämta synpunkter från de behöriga myndigheterna. Urvalet av transporter ska regelbundet ses över.

7 §

Beslut enligt 3 § ska underställas Försvarsunderrättelsedomstolen utan onödigt dröjsmål och senast inom en vecka från den dag då beslutet fattades.

8 §

När ett beslut har underställts Försvarsunderrättelsedomstolen ska domstolen hålla sammanträde. Till sammanträdet ska Säkerhetspolisen kallas.

9 §

Försvarsunderrättelsedomstolens beslut enligt denna lag får inte överklagas.

Nuvarande lydelse	*Föreslagen lydelse*
	4 kap.
Överföring av *behörighetsbegränsade PNR-uppgifter i sin fullständiga form*	**Överföring av *PNR-information på begäran***
	11 §
PNR-uppgifter som är behörighetsbegränsade enligt 3 kap. 11 § får endast överföras *i sin fullständiga form* till behöriga mottagare eller ett tredjeland om det rimligen kan antas vara nödvändigt för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet.	*PNR-information* får endast överföras till behöriga mottagare eller ett tredjeland om det rimligen kan antas vara nödvändigt för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet.
Om en förundersökning pågår ska en begäran från en behörig myndighet om att få tillgång till *fullständiga PNR-uppgifter* beslutas av *åklagare*.	Om en förundersökning *enligt rättegångsbalken* pågår ska en begäran från en behörig myndighet om att få tillgång till *PNR-information* beslutas av *allmän domstol*.

I de fall som inte omfattas av andra stycket *krävs att tillstånd till överföring har lämnats av Polismyndigheten.*

I de fall som inte omfattas av andra stycket *ska ett sådant beslut fattas av åklagare.*

12 §

Om en begäran om tillgång till PNR-information från en behörig mottagare i en annan medlemsstat har föregåtts av en prövning av om tillgång till informationen ska medges av en domstol eller oberoende förvaltningsmyndighet, ska beslut enligt 11 § tredje stycket inte fattas.

Det första stycket gäller även en begäran från ett tredjeland som har slutit avtal med EU om överföring och behandling av passageraruppgifter.

13 §

Om den efterfrågade PNR-informationen inte finns hos enheten för passagerarinformation ska det inte fattas något beslut enligt 11 § andra eller tredje stycket.

Prövningen i domstol

14 §

En begäran om tillgång till PNR-information under en pågående förundersökning enligt rättegångsbalken prövas av den domstol som anges i 19 kap. rättegångsbalken.

En begäran enligt första stycket från Försvarsmakten eller Säkerhetspolisen prövas av Stockholms tingsrätt.

15 §

Förfarandet i domstol är skriftligt. På förfarandet tillämpas reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande i sådana frågor. Det som föreskrivs om offentliga ombud i 27 kap. 28 § rättegångsbalken ska dock inte tillämpas.

Skyndsam handläggning

16 §

En begäran om tillgång till PNR-information ska handläggas skyndsamt.

Tillfällig tillgång till PNR-information utan tillstånd

17 §

Om det är fara i dröjsmål, får enheten för passagerarinformation medge tillgång till PNR-information efter en vederbörligen motiverad begäran från en behörig mottagare utan att tillstånd har meddelats av åklagare eller domstol.

Det första stycket gäller även för en begäran från ett tredjeland som har slutit avtal med EU om överföring och behandling av passageraruppgifter.

18 §

Om tillgång till PNR-information har medgetts utan tillstånd ska begäran om tillgång underställas rätt prövningsinstans utan onödigt dröjsmål och senast inom 24 timmar från det att tillgången medgavs.

Om tillgången har medgetts utan tillstånd och det inte längre finns skäl för behandling av informationen ska behandlingen hos den behöriga myndigheten omedelbart upphöra.

19 §

Om en begäran om tillgång till PNR-information avslås ska behandling som har påbörjats av en behörig myndighet utan att tillstånd har meddelats av åklagare eller domstol omedelbart upphöra.

6 kap.

Överträdelser av *lufttrafikföretag*	**Överträdelser av *transportföretag***
1 §	
En sanktionsavgift ska tas ut av ett *lufttrafikföretag* som inte har överfört PNR-uppgifter enligt bestämmelserna i denna lag eller föreskrifter som har meddelats i anslutning till lagen.	En sanktionsavgift ska tas ut av ett *transportföretag* som inte har överfört PNR-uppgifter enligt bestämmelserna i denna lag eller föreskrifter som har meddelats i anslutning till lagen.
2 §	
Sanktionsavgiften ska för varje *flygning* som har utförts utan att *lufttrafikföretaget* har fullgjort sin överföringsskyldighet bestämmas till lägst 20 000 kronor och högst	Sanktionsavgiften ska för varje *transport* som har utförts utan att *transportföretaget* har fullgjort sin överföringsskyldighet bestämmas till lägst 20 000 kronor och högst

100 000 kronor. När sanktionsavgiftens storlek fastställs ska särskild hänsyn tas till antal passagerare på *flygningen* och om *lufttrafikföretaget* tidigare har begått en överträdelse.	100 000 kronor. När sanktionsavgiftens storlek fastställs ska särskild hänsyn tas till antal passagerare på *transporten* och om *transportföretaget* tidigare har begått en överträdelse.

Sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

3 §

Polismyndigheten beslutar om sanktionsavgift för *lufttrafikföretag*.	Polismyndigheten beslutar om sanktionsavgift för *transportföretag*.

Sanktionsavgiften tillfaller staten.

Bilaga *Bilaga 1*

PNR-uppgifter som enligt 2 kap. 1 § ska överföras från *lufttrafikföretag* till enheten för passagerarinformation:

PNR-uppgifter som enligt 2 kap. 1 § ska överföras från *transportföretag som bedriver lufttrafik* till enheten för passagerarinformation:

1. PNR-uppgifternas lokaliseringskod,
2. datum för bokning och utfärdande av biljett,
3. planerat eller planerade resedatum,
4. namn,
5. adress och kontaktuppgifter (telefonnummer och e-postadress),
6. all betalningsinformation, inklusive faktureringsadress,
7. fullständig resplan,
8. uppgifter om bonusprogram,
9. resebyrå eller reseagent,
10. passagerarens resestatus, inklusive resebekräftelser, incheckningsstatus, upplysningar om passagerare som inte infinner sig och passagerare utan bokning,
11. delade PNR-uppgifter,
12. allmänna anmärkningar, inklusive alla tillgängliga uppgifter om ensamresande barn under 18 år, såsom namn, kön, ålder, språkkunskaper, namn och kontaktuppgifter för den person som följer barnet till incheckning för avresan och denna persons förhållande till barnet, namn och kontaktuppgifter för den person som hämtar barnet vid ankomsten och denna persons förhållande till barnet samt flygplatspersonal som ledsagar barnet vid avresan respektive ankomsten,
13. biljettinformation, inklusive biljettnummer, datum för utfärdande av biljetten, enkelbiljetter och automatisk biljettprisuppgift,
14. platsnummer och annan platsinformation,
15. information om gemensam linjebeteckning,
16. all bagageinformation,
17. antal medresenärer och deras namn,
18. all eventuell förhandsinformation (API-uppgifter) som har samlats in, inklusive typ av identitetshandling, identitetshandlingens nummer, utfärdandeland, sista giltighetsdag, nationalitet, efternamn, förnamn, kön, födelsedatum, lufttrafikföretag, flygnummer, utresedatum, ankomstdatum, avreseflygplats, ankomstflygplats, avresetid och ankomsttid, och

19. alla ändringar som har gjorts av de PNR-uppgifter som anges i punkt 1–18.

Bilaga 2

PNR-uppgifter som enligt 2 kap. 1 § ska föras över från transportföretag som bedriver tågtrafik till enheten för passagerarinformation:

1. datum och tid för bokning och betalning,
2. bokningsnummer,
3. biljettnummer,
4. kategori,
5. telefonnummer,
6. e-postadress,
7. tågnummer,
8. tåglinje,
9. vagnsnummer,
10. platsnummer,
11. all betalningsinformation, inklusive faktureringsadress,
12. försäljningskanal,
13. biljettpris,
14. resebyrå eller reseagent,
15. resetyp,
16. all eventuell förhandsinformation (API-uppgifter) som har samlats in, inklusive typ av identitetshandling, identitetshandlingens nummer, utfärdandeland, sista giltighetsdag, nationalitet, efternamn, förnamn, kön, födelsedatum, avgångstid, ankomsttid, avgångsstation, ankomststation, och
17. alla ändringar som har gjorts av de PNR-uppgifter som anges i punkt 1–16.

Bilaga 3

PNR-uppgifter som enligt 2 kap. 1 § ska föras över från transportföretag som bedriver busstrafik till enheten för passagerarinformation:

1. datum och tid för bokning och betalning,
2. bokningsnummer,
3. biljettnummer,
4. kategori,
5. telefonnummer,
6. e-postadress,
7. linjenummer,
8. linje,
9. vagnsnummer,
10. platsnummer,
11. all betalningsinformation, inklusive faktureringsadress,
12. försäljningskanal,
13. biljettpris,
14. resebyrå eller reseagent,
15. resetyp,
16. all bagageinformation,
17. all eventuell förhandsinformation (API-uppgifter) som har samlats in, inklusive typ av identitetshandling, identitetshandlingens nummer, utfärdandeland, sista giltighetsdag, nationalitet, efternamn, förnamn, kön, födelsedatum, avgångstid, ankomsttid, avgångsstation, ankomststation, och
18. alla ändringar som har gjorts av de PNR-uppgifter som anges i punkt 1–17.

Bilaga 4

PNR-uppgifter som enligt 2 kap. 1 § ska föras över från transportföretag som bedriver färjetrafik till enheten för passagerarinformation:

1. datum och tid för bokning och betalning,
2. bokningsnummer,
3. biljettnummer,
4. kategori,
5. telefonnummer,
6. e-postadress,
7. linjenummer,
8. linje,
9. platsnummer,
10. hyttnummer,
11. all betalningsinformation, inklusive faktureringsadress,
12. försäljningskanal,
13. biljettpris,
14. resebyrå eller reseagent,
15. all bagageinformation,
16. resetyp,
17. besättningens namn, telefonnummer, e-postadress, födelsedatum, identitetshandling och identitetshandlingens nummer,
18. fartygets namn,
19. fartygets flagga,
20. all eventuell förhandsinformation (API-uppgifter) som har samlats in, inklusive typ av identitetshandling, identitetshandlingens nummer, utfärdandeland, sista giltighetsdag, nationalitet, efternamn, förnamn, kön, födelsedatum, avgångstid, ankomsttid, avgångshamn, ankomsthamn, och
21. alla ändringar som har gjorts av de PNR-uppgifter som anges i punkt 1–20.

Denna lag träder i kraft den 1 januari 2028.

1.2 Förslag till lag om ändring i polislagen (1984:387)

Härigenom föreskrivs i fråga om polislagen (1984:387)

dels att 25 och 26 §§ ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 26 a–b §§, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	25 §
Ett transportföretag som befordrar varor, passagerare eller fordon till eller från Sverige ska på begäran av Polismyndigheten eller Säkerhetspolisen skyndsamt lämna de aktuella uppgifter om ankommande och avgående transporter, som företaget har tillgång till. Transportföretaget har endast skyldighet att lämna *de* uppgifter om passagerare *som avser* namn, resrutt, bagage *och* medpassagerare *samt* sättet för *betalning och* bokning.	Ett transportföretag som befordrar varor, passagerare eller fordon till eller från Sverige ska på begäran av Polismyndigheten eller Säkerhetspolisen skyndsamt lämna de aktuella uppgifter om ankommande och avgående transporter, som företaget har tillgång till. *Det som sägs om transportföretag gäller även andra företag som yrkesmässigt får tillgång till transportföretagets uppgifter om transporter.* Transportföretaget har endast skyldighet att lämna *följande* uppgifter om passagerare. – namn, – *födelsedatum,* – *kön,* – *nationalitet,* – resrutt, – bagage, – medpassagerare, – *betalningsinformation och* sättet för bokning, – *mobiltelefonnummer, och* – *e-postadress.*

Polismyndigheten får begära uppgifter enligt första stycket endast om uppgifterna kan antas ha betydelse för den brottsbekämpande verksamheten.

Lufttrafikföretag som omfattas av skyldigheten att överföra uppgifter enligt lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen är endast skyldiga att lämna uppgifter i enlighet med första och andra styckena om de behövs i verksamhet som rör nationell säkerhet.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om hur transportföretag ska lämna uppgifter.

En begäran om uppgifter om en transport får inte överklagas.

26 §

Transportföretag får lämna uppgifter enligt 25 § på så sätt att de görs läsbara för Polismyndigheten eller Säkerhetspolisen genom *terminalåtkomst*.

Polismyndigheten och Säkerhetspolisen får ta del av uppgifter genom *terminalåtkomst endast i den omfattning och under den tid som* behövs för att kontrollera aktuella transporter.

Transportföretag får lämna uppgifter enligt 25 § på så sätt att de görs läsbara för Polismyndigheten eller Säkerhetspolisen genom *direktåtkomst*.

Polismyndigheten och Säkerhetspolisen får ta del av uppgifter genom *direktåtkomst innan transporten har ankommit eller avgått och under högst sex månader därefter, om det* behövs för att kontrollera aktuella transporter.

26 a §

Polismyndigheten och Säkerhetspolisen får förelägga ett transportföretag att fullgöra sina skyldigheter enligt 25 och 26 §§.

Beslutet om föreläggande får förenas med vite. Beslutet gäller omedelbart.

26 b §

Ett beslut om föreläggande enligt 26 a § får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 1 januari 2028.

1.3 Förslag till lag om ändring i lagen (2009:966) om Försvarsunderrättelsedomstol

Härigenom föreskrivs i fråga om lagen (2009:966) om Försvarsunderrättelsedomstol

dels att 1, 5, och 16 §§ ska ha följande lydelse,

dels att det ska införas en ny paragraf, 14 a §, av följande lydelse.

Lydelse enligt SOU 2025:49

1 §

Försvarsunderrättelsedomstolen ska pröva frågor om tillstånd till signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Försvarsunderrättelsedomstolen ska även

1. pröva frågor om tillstånd till framtagning enligt lagen (2026:000) om säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar,

2. pröva beslut som ska överklagas dit enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter.

Föreslagen lydelse

1 §

Försvarsunderrättelsedomstolen ska pröva frågor om tillstånd till signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Försvarsunderrättelsedomstolen ska även

1. pröva frågor om tillstånd till framtagning enligt lagen (2026:000) om säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar,

2. pröva beslut som ska överklagas dit enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter, *och*

3. pröva underställda beslut enligt lagen (2018:1180) om passageraruppgifter i brottsbekämpningen.

Nuvarande lydelse

5 §

Ett integritetsskyddsombud ska bevaka enskildas integritetsintresse i mål vid domstolen. Ombudet har rätt att ta del av det som förekommer i målet och att yttra sig.

Föreslagen lydelse

5 §

Ett integritetsskyddsombud ska bevaka enskildas integritetsintresse i mål vid domstolen *om tillstånd till signalspaning*. Ombudet har rätt att ta del av det som förekommer i målet och att yttra sig.

	14 a §
	Domstolen får besluta att ett underställt beslut enligt lagen om passageraruppgifter i brottsbekämpningen (2018:1180) tills vidare inte ska gälla.
	16 §
Att Försvarsunderrättelsedomstolens beslut i frågor som rör signalspaning inte får överklagas framgår av 13 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. Inte heller domstolens beslut i övrigt enligt denna lag får överklagas.	Att Försvarsunderrättelsedomstolens beslut i frågor som rör signalspaning inte får överklagas framgår av 13 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. *Att domstolens beslut som rör underställda beslut i enlighet med lagen (2018:1180) om passageraruppgifter i brottsbekämpningen inte får överklagas framgår av 3 a kap. 9 § samma lag.* Inte heller domstolens beslut i övrigt enligt denna lag får överklagas.

Denna lag träder i kraft den 1 januari 2028.

1.4 Förslag till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område

Härigenom föreskrivs i fråga om lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område

dels att 1 kap. 3 § och 2 kap. 13–14 §§ ska ha följande lydelse,

dels att det ska införas en ny paragraf, 4 kap. 11 b §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
3 §	
Särskilda bestämmelser om behandling av personuppgifter finns	
1. i lagen (2017:496) om internationellt polisiärt samarbete och i föreskrifter som regeringen har meddelat i anslutning till den lagen,	
2. i lagen (2018:1180) om *flygpassageraruppgifter* i brottsbekämpningen och i föreskrifter som regeringen har meddelat i anslutning till den lagen,	2. i lagen (2018:1180) om *passageraruppgifter* i brottsbekämpningen och i föreskrifter som regeringen har meddelat i anslutning till den lagen,
3. i lagen (2022:613) om finansiell information i brottsbekämpningen och i föreskrifter som regeringen har meddelat i anslutning till den lagen, och	
4. i lagen (2023:474) om polisiära befogenheter i gränsnära områden.	
Om det i dessa författningar finns avvikande bestämmelser, ska de tillämpas i stället för bestämmelserna i denna lag.	
2 kap.	
13 §	
Personuppgifter som tillhandahålls av transportföretag enligt 25 § polislagen (1984:387) får behandlas för att utföra en uppgift som anges i 1 § 1 och 2.	
	Polismyndigheten ska på begäran lämna sådana personuppgifter som avses i första stycket till
	– Försvarsmakten, om de behövs i försvarsunderrättelseverk-

samheten eller den militära underrättelsetjänsten, och

– Ekobrottsmyndigheten, om de behövs i den brottsbekämpande verksamheten.

Personuppgifter som avses i första stycket får även behandlas för följande ändamål för att utföra en uppgift som anges i 1 § 1 eller 2:

– planera kontroller,

– välja ut kontrollobjekt, och

– göra analyser som behövs för att uppdatera eller skapa nya kriterier som ska användas vid planering av kontroller eller urval av kontrollobjekt.

Personuppgifter som avses i första stycket får endast i ett enskilt fall behandlas för nya ändamål enligt 2 kap. 4 eller 22 § brottsdatalagen (2018:1177).

14 §

Vid *terminalåtkomst* enligt 26 § polislagen (1984:387) får personuppgifterna inte ändras eller bearbetas på annat sätt.

Vid *direktåtkomst* enligt 26 § polislagen (1984:387) får personuppgifterna inte ändras eller bearbetas på annat sätt.

4 kap.

11 b §

Personuppgifter som med stöd av 25 § polislagen (1984:387) tillhandahålls på annat sätt än genom direktåtkomst, ska förstöras sex månader efter det att de behandlades första gången.

Denna lag träder i kraft den 1 januari 2028.

1.5 Förslag till lag om ändring i lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område

Härigenom föreskrivs i fråga om lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område att 1 kap. 2 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
2 §	
Särskilda bestämmelser om behandling av personuppgifter finns	
1. i lagen (2017:496) om internationellt polisiärt samarbete och i föreskrifter som regeringen har meddelat i anslutning till den lagen,	
2. i lagen (2018:1180) om *flygpassageraruppgifter* i brottsbekämpningen och i föreskrifter som regeringen har meddelat i anslutning till den lagen,	2. i lagen (2018:1180) om *passageraruppgifter* i brottsbekämpningen och i föreskrifter som regeringen har meddelat i anslutning till den lagen,
3. i lagen (2022:613) om finansiell information i brottsbekämpningen och i föreskrifter som regeringen har meddelat i anslutning till den lagen,	
4. i lagen (2023:474) om polisiära befogenheter i gränsnära områden, och	
5. i tullbefogenhetslagen (2024:710).	
Om det i dessa författningar finns avvikande bestämmelser, ska de tillämpas i stället för bestämmelserna i denna lag.	

Denna lag träder i kraft den 1 januari 2028.

1.6 Förslag till lag om ändring i tullbefogenhetslagen (2024:710)

Härigenom föreskrivs i fråga om tullbefogenhetslagen (2024:710) att 7 kap. 12 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
7 kap.	
12 §	
Om uppgifterna kan antas ha betydelse för Tullverkets brottsbekämpande verksamhet, får Tullverket begära att ett transportföretag, som befordrar varor, passagerare eller fordon till eller från Sverige, lämnar uppgifter om ankommande eller avgående transporter som företaget har tillgång till (bokningsuppgifter). Det som sägs om transportföretag gäller även andra företag som yrkesmässigt får tillgång till transportföretagets bokningsuppgifter. I fråga om passagerare omfattas endast uppgifter om	
– namn,	– namn,
– födelsedatum,	– födelsedatum,
– nationalitet,	– *kön*,
– resrutt,	– nationalitet,
– bagage,	– resrutt,
– medpassagerare,	– bagage,
– mobiltelefonnummer,	– medpassagerare,
– e-postadress,	– mobiltelefonnummer,
– *betalningssätt*, och	– e-postadress,
– bokningssätt.	– *betalningsinformation*, och
	– bokningssätt.
Det som sägs i första stycket gäller inte lufttrafikföretag som omfattas av skyldigheten att överföra uppgifter enligt lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen.	
Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om hur bokningsuppgifter ska lämnas.	

Tullverkets begäran om bokningsuppgifter får inte överklagas.

Denna lag träder i kraft den 1 januari 2028.

1.7 Förslag till förordning om ändring i förordningen (2009:968) med instruktion för Försvarsunderrättelsedomstolen

Härigenom föreskrivs i fråga om förordningen (2009:968) med instruktion för Försvarsunderrättelsedomstolen att 9 § ska ha följande lydelse.

Lydelse enligt SOU 2025:49	*Föreslagen lydelse*
	9 §
Domstolens beslut om signalspaning ska expedieras till ansökande myndighet och till Statens inspektion för försvarsunderrättelseverksamheten.	
Domstolens domar och beslut om framtagning från en särskild uppgiftssamling ska expedieras till Säkerhetspolisen och Säkerhets- och integritetsskyddsnämnden.	
	Domstolens domar och beslut avseende underställda beslut enligt lagen (2018:1180) om passageraruppgifter i brottsbekämpningen ska expedieras till Säkerhetspolisen och enheten för passagerarinformation inom Polismyndigheten.

Denna förordning träder i kraft den 1 januari 2028.

1.8 Förslag till förordning om ändring i polisförordningen (2014:1104)

Härigenom föreskrivs i fråga om polisförordningen (2014:1104) att 20 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
20 §	
Polismyndigheten får meddela närmare föreskrifter	
1. om rapporteftergift enligt 9 § polislagen (1984:387),	
2. om vilka hjälpmedel som får användas för att stoppa ett fordon eller annat transportmedel enligt 10 § 5 polislagen,	
3. om dokumentation enligt 27, 28 och 28 a §§ polislagen,	
4. enligt 2 kap. 33 § och 3 kap. 6 § tredje stycket ordningslagen (1993:1617) i fråga om	
a) utförande och besiktning av en anläggning för motorsport, olycksberedskap eller föreskrifter som i övrigt behövs från säkerhetssynpunkt vid en sådan anläggning, och	
b) utförande och besiktning av skjutbana,	
5. om polislegitimation, utöver vad som anges i förordningen (1958:272) om tjänstekort,	
6. om klädsel, utrustning och annat som krävs för enhetlighet i polisarbetet, *och*	6. om klädsel, utrustning och annat som krävs för enhetlighet i polisarbetet,
7. om verkställighet av denna förordning.	*7. om bestämmelserna om uppgifter från transportföretag i 25 § polislagen, och*
	8. om verkställighet av denna förordning.
Föreskrifter som avses i första stycket 1–3 och *5–7* och som berör Säkerhetspolisen ska meddelas i samråd med den.	Föreskrifter som avses i första stycket 1–3 och *5–8* och som berör Säkerhetspolisen ska meddelas i samråd med den.

Denna förordning träder i kraft den 1 januari 2028.

1.9 Förslag till ändring av förordningen (2018:1181) om flygpassageraruppgifter i brottsbekämpningen

Härigenom föreskrivs i fråga om förordningen (2018:1181) om flygpassageraruppgifter i brottsbekämpningen

dels att förordningens namn ska ha följande lydelse,

dels att 1–6, 9 och 20–21 §§ ska ha följande lydelse,

dels att rubrikerna närmast före 4 och 21 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
Förordning (2018:1181) om *flygpassageraruppgifter* i brottsbekämpningen	**Förordning (2018:1181) om *passageraruppgifter* i brottsbekämpningen**
1 §	
Denna förordning innehåller bestämmelser som kompletterar lagen (2018:1180) om *flygpassageraruppgifter* i brottsbekämpningen.	Denna förordning innehåller bestämmelser som kompletterar lagen (2018:1180) om *passageraruppgifter* i brottsbekämpningen.
2 §	
Uttryck som används i förordningen har samma innebörd som i lagen (2018:1180) om *flygpassageraruppgifter* i brottsbekämpningen.	Uttryck som används i förordningen har samma innebörd som i lagen (2018:1180) om *passageraruppgifter* i brottsbekämpningen.
3 §	
Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Tullverket och Försvarsmakten är behöriga myndigheter enligt lagen (2018:1180) om *flygpassageraruppgifter* i brottsbekämpningen.	Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Tullverket och Försvarsmakten är behöriga myndigheter enligt lagen (2018:1180) om *passageraruppgifter* i brottsbekämpningen.

Lufttrafikföretagens **skyldigheter**	*Transportföretagens* **skyldigheter**
4 §	
Lufttrafikföretag ska överföra PNR-uppgifter i enlighet med artikel 1 i kommissionens genomförandebeslut (EU) 2017/759 av den 28 april 2017 om gemensamma protokoll och dataformat som ska användas av lufttrafikföretag när PNR-uppgifter överförs till enheterna för passagerarinformation.	*Transportföretag som bedriver lufttrafik* ska överföra PNR-uppgifter i enlighet med artikel 1 i kommissionens genomförandebeslut (EU) 2017/759 av den 28 april 2017 om gemensamma protokoll och dataformat som ska användas av lufttrafikföretag när PNR-uppgifter överförs till enheterna för passagerarinformation.
Vid tekniska problem får uppgifterna överföras på annat lämpligt sätt som säkerställer ett tillfredsställande skydd för uppgifterna.	
	Polismyndigheten får meddela närmare föreskrifter om hur transportföretag som bedriver passagerartrafik med tåg, buss eller färja ska överföra PNR-uppgifter.
5 §	
Enheten för passagerarinformation ska fastställa och regelbundet se över de kriterier som avses i 3 kap. 5 § 2 lagen (2018:1180) om *flygpassageraruppgifter* i brottsbekämpningen i samarbete med de behöriga myndigheterna.	Enheten för passagerarinformation ska fastställa och regelbundet se över de kriterier som avses i 3 kap. 5 § 2 lagen (2018:1180) om *passageraruppgifter* i brottsbekämpningen i samarbete med de behöriga myndigheterna.
6 §	
Tillgång till PNR-uppgifter som är behörighetsbegränsade enligt 3 kap. 11 § lagen (2018:1180) om *flygpassageraruppgifter* i brottsbekämpningen får endast ges till dataskyddsombudet för enheten för passagerarinformation och den	Tillgång till PNR-uppgifter som är behörighetsbegränsade enligt 3 kap. 11 § lagen (2018:1180) om *passageraruppgifter* i brottsbekämpningen får endast ges till dataskyddsombudet för enheten för passagerarinformation och den

som har ett behov av fullständiga uppgifter för att kunna utföra sina arbetsuppgifter. Behörigheten får bara utnyttjas när det i ett enskilt fall är absolut nödvändigt med tillgång till fullständiga uppgifter.

9 §

Resultatet av en behandling av PNR-uppgifter får inte behandlas under längre tid än vad som behövs för att kunna informera behöriga mottagare om resultatet. Om ett sådant resultat inte behöver granskas vidare av en behörig mottagare, får resultatet ändå behandlas om syftet är att fortsättningsvis undvika motsvarande felaktiga träffar. Behandlingen av resultatet ska dock upphöra senast i samband med att PNR-uppgifterna ska *förstöras* enligt 3 kap. 9 § lagen (2018:1180) om *flygpassageraruppgifter* i brottsbekämpningen.

20 §

När det i ett enskilt fall är nödvändigt för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller annan allvarlig brottslighet, får enheten för passagerarinformation begära att en motsvarande enhet i en annan medlemsstat ska inhämta PNR-uppgifter från lufttrafikföretag vid andra tidpunkter än

som har ett behov av fullständiga uppgifter för att kunna utföra sina arbetsuppgifter. Behörigheten får bara utnyttjas när det i ett enskilt fall är absolut nödvändigt med tillgång till fullständiga uppgifter.

9 §

Resultatet av en behandling av PNR-uppgifter *enligt 3 kap. 4 § 1 lagen (2018:1180) om passageraruppgifter i brottsbekämpningen* får inte behandlas under längre tid än vad som behövs för att kunna informera behöriga mottagare om resultatet. Om ett sådant resultat inte behöver granskas vidare av en behörig mottagare, får resultatet ändå behandlas om syftet är att fortsättningsvis undvika motsvarande felaktiga träffar. Behandlingen av resultatet ska dock upphöra senast i samband med att PNR-uppgifterna ska *anonymiseras* enligt 3 kap. 9 § lagen (2018:1180) om *passageraruppgifter* i brottsbekämpningen.

20 §

När det i ett enskilt fall är nödvändigt för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller annan allvarlig brottslighet, får enheten för passagerarinformation begära att en motsvarande enhet i en annan medlemsstat ska inhämta PNR-uppgifter från lufttrafikföretag vid andra tidpunkter än

de som anges i 2 kap. 2 § lagen (2018:1180) om *flygpassageraruppgifter* i brottsbekämpningen, för vidareöverföring till enheten.	de som anges i 2 kap. 2 § lagen (2018:1180) om *passageraruppgifter* i brottsbekämpningen, för vidareöverföring till enheten.
Handläggning av sanktionsavgift för *lufttrafikföretag*	**Handläggning av sanktionsavgift för *transportföretag***
21 §	
Ett beslut om sanktionsavgift för *lufttrafikföretag* ska delges den som avgiften ska tas ut av.	Ett beslut om sanktionsavgift för *transportföretag* ska delges den som avgiften ska tas ut av.

Denna förordning träder i kraft den 1 januari 2028.

1.10 Förslag till förordning om ändring i tullbefogenhetsförordningen (2024:759)

Härigenom föreskrivs i fråga om tullbefogenhetsförordningen (2024:759) att det ska införas en ny paragraf, 6 kap. 4 §, av följande lydelse.

6 kap.

4 §

Tullverket ska på begäran lämna bokningsuppgifter som inhämtats med stöd av 7 kap. 12 § tullbefogenhetslagen (2024:710) till Ekobrottsmyndigheten, om de behövs i den brottsbekämpande verksamheten.

Denna förordning träder i kraft den 1 januari 2028.

2 Inledning

2.1 Utredningens uppdrag

Regeringen beslutade den 10 april 2025 att genom kommittédirektiv (2025:36) ge en särskild utredare i uppdrag att se över reglerna om passageraruppgifter i brottsbekämpningen i syfte att anpassa regleringen av flygpassageraruppgifter till EU-rätten samt analysera förutsättningarna och överväga förbättrade möjligheter att inhämta passageraruppgifter från andra trafikslag. Uppdraget ska redovisas senast den 24 april 2026. Direktiven för arbetet finns i bilaga 1.

I uppdraget ingår bl.a. att

- analysera och ta ställning till vilka förändringar av den svenska regleringen i fråga om flygpassageraruppgifter i brottsbekämpningen som behöver göras med anledning av EU-domstolens praxis,
- analysera och ta ställning till om den svenska regleringen i fråga om flygpassageraruppgifter i brottsbekämpningen ska göras neutral när det gäller trafikslag,
- se över nuvarande möjligheter att inhämta tillgängliga passageraruppgifter från andra transportföretag, och
- lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga, samtidigt som brottsbekämpande myndigheters tillgång till flygpassageraruppgifter upprätthålls i möjligaste mån och skyddet för enskildas personliga integritet säkerställs.

2.2 Utredningens arbete

Vårt arbete inleddes april 2025 och har skett i nära samarbete med de experter som förordnats att ingå i utredningen. Fram till lämnandet av detta betänkande har vi haft fem utredningssammanträden, tre under 2025 och två under 2026.

Utöver sammanträdena med experterna har sekretariatet haft omfattande kontakt med experterna som representerar Polismyndigheten och enheten för passagerarinformation inom Polismyndigheten. Det samråd som utredningen enligt direktiven ska ha med berörda myndigheter och andra aktörer har huvudsakligen skett genom experterna. Som ett led i arbetet har sekretariatet besökt och haft möten med representanter från enheten för passagerarinformation inom Polismyndigheten, Tullverket, Försvarsmakten, Säkerhetspolisen, Ekobrottsmyndigheten och Svensk kollektivtrafik. Vid mötet med Svensk kollektivtrafik deltog även representanter från Tågföretagen, SJ, Öresundståg och Sveriges bussföretag. Under oktober 2025 deltog utredningen tillsammans med representanter från Polismyndigheten vid ett studiebesök hos den belgiska enheten för passagerarinformation i Bryssel.

Arbetet bestod inledningsvis av att kartlägga följderna av den s.k. PNR-domen. Jämförelser med andra länders agerande har varit vanskliga att göra då mycket av informationen kring detta inte framgår i öppna källor. Utredningen har kontaktat ett flertal medlemsstaters enheter för passagerarinformation men endast fått svar från en. PNR-domen diskuterades vid sammanträden i september och november och experterna gavs möjligheter att inkomma med synpunkter. Under arbetet har möten hållits med representanter från Försvarsunderrättelsedomstolen, Åklagarmyndigheten och Domstolsverket.

Den del av utredningen som avser en trafikslagsneutral PNR-lagstiftning behandlades vid sammanträden i januari och februari 2026. I denna del har möten hållits med representanter från Transportstyrelsen och Sjöfartsverket. Även arbetet inom andra relevanta lagstiftningsprocesser och arbete inom EU har beaktats.

3 Grundläggande fri- och rättigheter

3.1 Inledning

Användningen av passageraruppgifter i brottsbekämpningen innebär ett intrång i den personliga integriteten. När förändringar i sådan användning övervägs ska därför den reglering som finns till skydd för enskildas fri- och rättigheter beaktas. Detta gäller särskilt om förändringarna som övervägs innebär en utökning av möjligheterna att behandla personuppgifter. Bestämmelser om grundläggande fri- och rättigheter finns i den svenska grundlagen och i vissa internationella rättsakter som Sverige är bundet av. I detta kapitel redogör vi för den regleringen. Användningen av passageraruppgifter i brottsbekämpningen måste dessutom vara förenlig med den generella dataskyddsregleringen som bl.a. syftar till att värna om enskildas personliga integritet. Den regleringen redogör vi för i kapitel 4. I kapitel 5 redovisas den internationella och svenska regleringen av passageraruppgifter i brottsbekämpningen.

3.2 Regeringsformen

I regeringsformen, RF, finns bestämmelser till skydd för enskildas grundläggande fri- och rättigheter. I 1 kap. 2 § första stycket slås det fast att den offentliga makten ska utövas med respekt för den enskilda människans frihet. I fjärde stycket anges att det allmänna ska värna den enskildes privat- och familjeliv. Bestämmelsen ger uttryck för vissa särskilt viktiga mål för den samhälleliga verksamheten, men den ger inte upphov till några rättigheter för medborgarna. De rättsligt bindande rättighetsreglerna har i stället samlats i regeringsformens andra kapitel.

I 2 kap. 6 § andra stycket stadgas att var och en är, gentemot det allmänna, skyddad mot betydande intrång i den personliga integriteten, om det utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Detta stycke infördes vid 2010 års grundlagsreform och innebär en förstärkning av skyddet mot integritetskränkningar. Av förarbetena framgår att avgörande för om en åtgärd ska anses innebära övervakning eller kartläggning är inte dess huvudsakliga syfte utan vilken effekt åtgärden har. Vad som avses med övervakning respektive kartläggning får bedömas med utgångspunkt i vad som enligt normalt språkbruk läggs i dessa begrepp.

Vid bedömningen av vilka åtgärder som kan anses utgöra *betydande intrång* ska både åtgärdens omfattning och arten av det intrång åtgärden innebär beaktas. Bestämmelsen omfattar endast sådana intrång som på grund av åtgärdens intensitet eller omfattning, eller av hänsyn till uppgifternas integritetskänsliga natur eller andra omständigheter, innebär ett betydande ingrepp i den enskildes privata sfär.[1]

Av 2 kap. 20 § följer att de rättigheter som uppställs i 2 kap. 6 § endast får begränsas genom lag. Enligt 2 kap. 21 § får en begränsning endast göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle och den får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. Begränsningen får inte heller göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

Genom det andra ledet i 2 kap. 20 § kommer en proportionalitetsprincip till uttryck. En begränsning av rättigheterna ska vara ändamålsenlig och nödvändig och den fördel som det allmänna vinner genom ingreppet ska stå i rimlig proportion till den skada som ingreppet förorsakar den enskilde. Denna proportionalitetsprincip har även kommit till uttryck i praxis från Högsta domstolen och Högsta förvaltningsdomstolen.[2]

[1] Prop. 2009/10:80, *En reformerad grundlag*, s. 182–185.
[2] Se t.ex. NJA 2012 s. 400, NJA 2015 s. 45, HFD 2015 ref. 80 och HFD 2016 ref. 44.

3.3 Europakonventionen

Europakonventionen[3] innehåller bestämmelser om grundläggande fri- och rättigheter och gäller sedan 1995 som svensk lag.[4] Enligt 2 kap. 19 § RF får lag eller annan föreskrift inte meddelas i strid med Europakonventionen.

Rätten till respekt för den personliga integriteten följer av rätten till respekt för privatlivet enligt konventionen. Av artikel 8 framgår att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Rättigheten är inte absolut och kan, under vissa förutsättningar, inskränkas. Inskränkningen ska vara föreskriven i lag och vara nödvändig i ett demokratiskt samhälle för att uppnå ett legitimt mål, t.ex. skydd för allmän säkerhet, allmän ordning eller för att värna folkhälsan. Det innebär i huvudsak att det måste finnas ett angeläget samhälleligt behov av inskränkningen och att denna måste stå i rimlig proportion till det syfte som ska tillgodoses genom ingreppet.[5] Europadomstolen har uttalat att en rättvis balans måste uppnås mellan det allmänna och enskilda intressen när det gäller åtgärder som inskränker rätten till privatliv.[6]

Europeiska domstolen för de mänskliga rättigheterna, Europadomstolen, har i flera fall konstaterat att artikel 8 ålägger staten en negativ förpliktelse att avstå från att göra intrång i rätten till respekt för privat- och familjelivet samt en positiv förpliktelse att skydda enskilda mot att andra enskilda handlar på ett sätt som innebär ett integritetsintrång.[7]

Registrering av personuppgifter kan omfattas av rätten till skydd för privatlivet. Enligt Europadomstolen gäller det särskilt om de uppgifter som har registrerats innehåller känsliga uppgifter, t.ex. informa-

[3] Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.
[4] Se lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.
[5] Danelius, *Mänskliga rättigheter i Europeisk praxis*, 6 upplagan, 2023, s. 460.
[6] Se t.ex. Europadomstolens domar *Peruzzo och Martens mot Tyskland*, nr 7481/08 och 57900/12, domar meddelade den 4 juni 2013, *Aycaguer mot Frankrike*, nr 8806/12, dom meddelad den 22 juni 2017 och *Gaughran mot Storbritannien*, nr 45245/15, dom meddelad den 13 februari 2020.
[7] Se t.ex. Europadomstolens domar *Airey mot Irland*, nr 6286/73, dom meddelad den 9 oktober 1979, *X och Y mot Nederländerna*, nr 8678/80, dom meddelad den 26 mars 1985 och *Söderman mot Sverige*, nr 5786/08, dom meddelad den 12 november 2013.

tion om politisk uppfattning, religionstillhörighet, missbruk eller liknande förhållanden.[8]

Vid inskränkningar i skyddet för privatlivet måste den enskilde tillförsäkras vissa grundläggande rättssäkerhetsgarantier, t.ex. en rättvis rättegång och ett effektivt rättsmedel. Enligt Europadomstolen är behovet av sådana garantier större när det gäller automatiserad behandling av personuppgifter. Nationell rätt måste säkerställa att uppgifterna är relevanta och inte för långtgående i förhållande till det ändamål för vilket de bevaras. Uppgifterna får inte heller sparas under en tid som överstiger vad som är nödvändigt med hänsyn till ändamålet. Det måste därutöver finnas garantier för att personuppgifterna skyddas från felaktig behandling, inte minst vid behandling av känsliga personuppgifter.[9]

3.4 EU:s rättighetsstadga

EU:s rättighetsstadga[10] trädde i kraft i och med Lissabonfördraget den 1 december 2009.[11] Enligt artikel 6.1 i fördraget om Europeiska unionen ska unionen erkänna de rättigheter, friheter och principer som fastställs i EU:s rättighetsstadga och stadgan ska ha samma rättsliga värde som fördragen. Rättighetsstadgan är därmed en del av EU:s primärrätt och den har företräde framför föreskrifter i medlemsstaternas nationella rättsordningar.

I EU:s rättighetsstadga finns ett flertal artiklar som berör personlig integritet och behandling av personuppgifter. I artikel 3.1 anges att var och en har rätt till fysisk och mental integritet. Artikel 7 innebär rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Artikel 8 ger var och en rätt till skydd av de personuppgifter som rör honom eller henne. Där slås även fast rätten att få tillgång till de insamlade uppgifter som rör en själv och att få rättelse av dem.

[8] Se Europadomstolens dom *Segerstedt-Wiberg m.fl. mot Sverige*, nr 62332/00, dom meddelad den 6 juni 2006.
[9] Se t.ex. Europadomstolens domar *B.B. mot Frankrike*, nr 5335/06, dom meddelad den 17 december 2009, *S. och Marper mot Storbritannien*, nr 30562/04 och 30566/04, dom meddelad den 4 december 2008 och *Aycaguer mot Frankrike*, nr 8806/12, dom meddelad den 22 juni 2017.
[10] Europeiska unionens stadga om de grundläggande rättigheterna (2016/C 202/02).
[11] Lissabonfördraget om ändring av fördraget om Europeiska unionen och fördraget om upprättandet av Europeiska gemenskapen (2007/C 306/01).

I artikel 51 och 52 behandlas stadgans tillämpningsområde och rättigheternas och principernas räckvidd och tolkning. Bestämmelserna i stadgan riktar sig till unionens institutioner, organ och byråer samt till medlemsstaterna endast när dessa tillämpar unionsrätten. Rättigheterna ska därför tillämpas under iakttagande av gränserna för unionens befogenheter enligt fördragen. Stadgan innebär inte någon utvidgning av tillämpningsområdet för unionsrätten utanför unionens befogenheter och medför inte heller i övrigt någon förändring i befogenheterna.

Varje begränsning av stadgans rättigheter och friheter ska vara föreskriven i lag och vara förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Begränsningar får endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

Ett flertal av de rättigheter som slås fast i stadgan överlappar med motsvarande rättigheter i Europakonventionen. Enligt artikel 52.3 i stadgan ska dessa rättigheter ha samma innebörd och räckvidd som i konventionen. Det finns dock inget hinder för unionsrätten att tillförsäkra ett mer långtgående skydd.

3.5 Förenta nationernas allmänna förklaring om de mänskliga rättigheterna

FN:s allmänna förklaring om de mänskliga rättigheterna antogs den 10 december 1948. Den består av 30 artiklar som uttrycker de grundläggande och universella fri- och rättigheterna. Förklaringen är en gemensam viljeyttring och ett moraliskt ställningstagande av världssamfundet och som sådant är det inte juridiskt bindande. Den har dock utgjort grunden för det internationella arbetet med att övervaka utvecklingen och efterlevnaden av mänskliga rättigheter.

I artikel 12 i den allmänna förklaringen anges att ingen får utsättas för godtyckligt ingripande i fråga om privatliv, familj, hem eller korrespondens. Var och en har rätt till lagens skydd mot sådana ingripanden och angrepp.

Av artikel 29.2 följer att inskränkningar av rättigheter och friheter endast får göras genom lag och enbart i syfte att trygga tillbörlig hänsyn till och respekt för andras rättigheter och friheter samt för att

tillgodose ett demokratiskt samhälles berättigade krav på moral, allmän ordning och allmän välfärd.

3.6 Dataskyddskonventionen

3.6.1 Konventionens ställning och syfte

Europarådets ministerkommitté antog 1981 Dataskyddskonventionen[12], som trädde i kraft den 1 oktober 1985. Sverige ratificerade konventionen den 24 juni 1982. Konventionen var det första bindande internationella instrumentet på dataskyddsområdet och har status som ett rättsligt bindande multilateralt avtal om personuppgiftsskydd. Konventionen gäller inte som lag i Sverige, men ställer krav på konventionsparterna att införa bestämmelser i nationell rätt som upprätthåller de principer om skydd för personuppgifter som uppställs i konventionen.

Medan EU:s dataskyddsförordning har övertagit konventionens roll som grundläggande dokument för automatiserad behandling av personuppgifter inom stora delar av EU:s kompetensområde, är konventionen fortsatt av särskild betydelse för områden som ligger utanför unionsrätten, såsom nationell säkerhet, försvar och statens säkerhet. I Sverige är den del av Säkerhetspolisens verksamhet som rör nationell säkerhet ett av de få områden där konventionen gäller i stället för EU:s dataskyddsregelverk.

Dataskyddskonventionen anses vara en precisering av det skydd som följer av artikel 8 i Europakonventionen. Ändamålet med konventionen, vilket anges i artikel 1, är att säkerställa respekten för grundläggande fri- och rättigheter, särskilt rätten till personlig integritet i samband med automatisk databehandling av personuppgifter. Konventionen ställer upp ett flertal principer för automatisk databehandling av personuppgifter och omfattar sådan behandling inom både allmän och enskild verksamhet.

[12] Europeiska rådets konvention (ETS) av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter.

3.6.2 Konventionens innehåll

Enligt artikel 5 i konventionen ska personuppgifter erhållas och behandlas på ett korrekt och lagligt sätt, de ska lagras för särskilt angivna och lagliga ändamål och inte användas på ett sätt som är oförenligt med dessa ändamål. Personuppgifterna ska vara ändamålsenliga, relevanta och inte nödvändiga. Vidare ska uppgifterna vara korrekta och hållas aktuella samt bevaras på ett sådant sätt att de registrerade personerna inte kan identifieras under längre tid än vad som är nödvändigt.

I artikel 6 anges att personuppgifter som avslöjar rasursprung, politiska åsikter liksom uppgifter som rör hälsa eller sexualliv inte får undergå automatisk databehandling, såvida inte nationell lag ger ett ändamålsenligt skydd. Detsamma gäller uppgifter som hänför sig till att någon dömts för brott.

Artikel 8 slår fast vissa skyddsåtgärder för registrerade personer. Var och en har rätt att få veta om ett automatiserat personregister finns, dess huvudsakliga ändamål samt vem som är registeransvarig. Det finns även en rätt att med rimliga mellanrum få bekräftat om personuppgifter finns lagrade i register och att få ta del av sådana uppgifter i begriplig form. Om uppgifterna har behandlats i strid med gällande bestämmelser ska uppgifterna rättas eller raderas. Ett beslut som innebär att någon inte efterkommer en begäran om bekräftelse eller meddelande, rättelse eller utradering ska gå att överklaga.

Enligt artikel 9 får avvikelse från vissa bestämmelser i konventionen göras endast om sådan avvikelse medges i partens nationella lagstiftning och den är nödvändig i ett demokratiskt samhälle för att skydda statens säkerhet, den allmänna säkerheten, statens penningintressen eller brottsbekämpning eller för att skydda enskildas frioch rättigheter.

Europarådets ministerkommitté antog 2001 ett tilläggsprotokoll till dataskyddskonventionen som trädde i kraft den 1 juli 2004.[13] Protokollet, som Sverige har ratificerat, innehåller två huvudsakliga kompletteringar. Det infördes bestämmelser som innebär ett krav på tillsynsmyndigheter. Varje medlemsstat ska inrätta en eller flera oberoende tillsynsmyndigheter för att kontrollera efterlevnaden av dataskyddsprinciperna. Myndigheterna ska ha utrednings- och ingripandebefo-

[13] Europeiska rådet, Tilläggsprotokoll till konventionen om skydd för individer vid automatisk behandling av personuppgifter, rörande tillsynsmyndigheter och gränsöverskridande dataflöden, ETS 181, den 8 november 2001.

genheter samt kunna delta i rättsliga förfaranden. Det infördes även bestämmelser om gränsöverskridande dataflöden. Överföring av personuppgifter till länder som inte är parter till konventionen får bara ske om mottagarlandet säkerställer en adekvat skyddsnivå för de aktuella uppgifterna.

Dataskyddskonventionen kompletteras vidare av ett antal rekommendationer antagna av ministerkommittén om hur personuppgifter bör behandlas inom olika områden, t.ex. digital spårning och bevakning samt inom polissektorn.

3.6.3 Modernisering av konventionen

Efter en omfattande översyn antog Europarådets medlemsstater Ministerkommittén den 18 maj 2018 ett ändringsprotokoll till Dataskyddskonventionen.[14] Protokollet, som informellt kallas *dataskyddskonventionen 108+*, har som syfte att modernisera konventionen för att kunna hantera den tekniska utvecklingen och globaliseringen av information när det gäller skyddet av privat information. I protokollet understryks vikten av att individer får kännedom om, förstår och har möjlighet att kontrollera behandlingen av deras personuppgifter.

I artikel 3 tydliggörs det att konventionen kommer ha ett enhetligt tillämpningsområde för alla konventionsparter. Det kommer alltså inte vara möjligt att helt undandra sektorer eller verksamheter från dess tillämpning, t.ex. med hänvisning till nationell säkerhet. Även för sådan verksamhet gäller således de förutsättningar för undantag och inskränkningar i rättigheterna som framgår av artikel 9. Konventionen kommer därmed att omfatta all typ av databehandling under parternas jurisdiktion inom såväl offentlig som privat sektor.

Bland de viktigaste förändringarna i den moderniserade konventionen kan nämnas stärkta krav på proportionalitet och rättslig grund för behandling, krav på inbyggt dataskydd och konsekvensbedömningar samt förstärkta rättigheter för registrerade, bl.a. avseende automatiskt beslutsfattande.

[14] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS no. 223), den 10 oktober 2018.

Protokollet träder i kraft när det har ratificerats av samtliga Europarådets medlemsstater, men tillåter även ett partiellt ikraftträdande. Sverige har undertecknat men ännu inte ratificerat protokollet.

3.6.4 Den moderniserade konventionens betydelse för underrättelsetjänsternas personuppgiftsbehandling

Dataskyddskonventionen gäller även för personuppgiftsbehandling som rör nationell säkerhet, men medger undantag från alla centrala principer. Detta gäller inte för den moderniserade konventionen 108+. För kraven på proportionalitet, rättslig grund och författningsenlig behandling är det inte möjligt att göra undantag. Detsamma gäller för bestämmelserna om särskilt skydd för känsliga personuppgifter; en kategori som dessutom utökats genom tilläggsprotokollet. Det finns därutöver endast begränsade möjligheter att undanta behandling som rör nationell säkerhet från kravet på oberoende tillsyn.

Detta gör den moderniserade dataskyddskonventionen till ett viktigt rättsligt instrument för underrättelsetjänsters verksamhet. Konventionens principer för dataskydd kommer att utgöra en bindande minimistandard som medlemsstaterna måste iaktta i sin nationella lagstiftning. Avvägningen mellan dataskydd och nationell säkerhet är dock fortsatt en fråga som hanteras på nationell nivå inom de ramar som konventionen sätter upp.

4 Dataskyddsregleringen

4.1 Inledning

Under 2018 genomfördes en genomgripande dataskyddsreform inom EU. Anledningen till reformen var teknisk utveckling och ökande hantering av personuppgifter. Reformen omfattar dels EU:s dataskyddsförordning[1], dels EU:s dataskyddsdirektiv.[2] I samband med reformen anpassades den svenska lagstiftningen till den nya EU-rättsliga regleringen.

EU:s dataskyddsförordning innefattar en generell reglering för behandling av personuppgifter inom EU. Syftet med förordningen är att säkerställa en enhetlig skyddsnivå för behandlingen av personuppgifter inom hela unionen och att undvika avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden. Förordningen är direkt tillämplig i alla EU:s medlemsstater[3], men både förutsätter och medger samtidigt kompletterande och specificerande nationella bestämmelser av olika slag.

Kompletterande bestämmelser av generell karaktär finns i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, dataskyddslagen. Dataskyddslagen i sin tur kompletteras av förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning. Det finns även ett flertal kompletterande registerförfattningar som reglerar vilka uppgifter som får behandlas och hur uppgifterna får behandlas på särskilda områden eller i vissa verksamheter.

---

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[2] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.
[3] Jfr artikel 288 i fördraget om Europeiska unionens funktionssätt.

EU:s dataskyddsförordning ska inte tillämpas på personuppgiftsbehandling som behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot och förebygga och förhindra hot mot den allmänna säkerheten. Sådan personuppgiftsbehandling omfattas i stället av EU:s dataskyddsdirektiv.[4]

Syftet med direktivet är att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, samt att säkerställa att det utbyte av personuppgifter som krävs inom unionen mellan behöriga myndigheter varken begränsas eller förbjuds av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter. På många områden överensstämmer regleringen i dataskyddsdirektivet med motsvarande reglering i dataskyddsförordningen. Det finns dock vissa skillnader, t.ex. vad gäller informationsplikten, enskildas rättigheter och kraven på konsekvensbedömningar och förhandssamråd.

Eftersom det rör sig om ett direktiv är det inte direkt tillämpligt i medlemsstaterna.[5] I Sverige är direktivet huvudsakligen genomfört i nationell rätt genom brottsdatalagen (2018:1177), som kompletteras av brottsdataförordningen (2018:1202).

4.2 EU:s dataskyddsförordning

4.2.1 Tillämpningsområde och definitioner

EU:s dataskyddsförordning är enligt artikel 2.1 tillämplig på behandling av personuppgifter som helt eller delvis företas på automatiserad väg samt på annan behandling än automatiserad av personuppgifter som ingår i eller kommer att ingå i ett register.

Med begreppet behandling avses en åtgärd eller en kombination av åtgärder beträffande personuppgifter, oberoende om de utförs automatiserat eller manuellt. Exempel på åtgärder som utgör behandling enligt artikel 4.2 är insamling, registrering, lagring, bearbetning, användning, spridning eller radering av personuppgifter. I syfte att förhindra risk för kringgående av förordningens bestämmelser har behandlingsbegreppet getts en teknikneutral utformning.[6]

[4] Se artikel 2.2 i EU:s dataskyddsförordning och artikel 2.2 i EU:s dataskyddsdirektiv.
[5] Jfr artikel 288 i fördraget om Europeiska unionens funktionssätt.
[6] Se skäl 15 till EU:s dataskyddsförordning.

Enligt artikel 4.1 är varje upplysning som avser en identifierad eller identifierbar fysisk person en personuppgift. Uppgifter gällande juridiska personer omfattas alltså inte av begreppet personuppgift. För att avgöra om en uppgift avser en identifierbar fysisk person bör man beakta alla hjälpmedel som rimligen kan komma att användas för att direkt eller indirekt identifiera personen. EU:s dataskyddsförordning är alltså inte tillämplig på uppgifter som inte kan hänföras till en viss person.[7] Detta gäller även för avlidna personer.[8]

Personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk peson, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning utgör enligt artikel 9.1 särskilda kategorier av personuppgifter (känsliga personuppgifter). Behandling av sådana uppgifter är förbjuden, med vissa i artikeln angivna undantag.

Personuppgiftsansvarig är normalt en juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. En fysisk person kan också vara personuppgiftsansvarig. Avgörande för placeringen av personuppgiftsansvaret är vem som har rätt att bestämma ändamål och medel för behandlingen. Om ändamålen och medlen bestäms av unionsrätten eller medlemsstaternas nationella rätt är det dock enligt artikel 4.7 möjligt att reglera vem som är personuppgiftsansvarig i lagstiftningen. I svensk rätt finns sådan särskild reglering gällande personuppgiftsansvar i många sektorsspecifika specialförfattningar.

4.2.2 Grundläggande principer för personuppgiftsbehandling

EU:s dataskyddsförordning ställer krav på att all behandling av personuppgifter ska ha en laglig grund (rättslig grund) och genomföras i enlighet med vissa grundläggande principer. Något förenklat kan man förklara det genom att förordningens krav på rättslig grund utgör en förutsättning för att en personuppgift alls ska få behandlas, medan övriga principer reglerar hur behandlingen får genomföras.

[7] Se skäl 26 till EU:s dataskyddsförordning.
[8] Se skäl 27 till EU:s dataskyddsförordning.

I artikel 5.1 anges de grundläggande principerna för behandling av personuppgifter. Personuppgifter ska

a) behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (laglighet, korrekthet och öppenhet),

b) samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte behandlas på ett sätt som står i strid med dessa ändamål (ändamålsbegränsning),

c) vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering),

d) vara riktiga och, om nödvändigt, uppdaterade (riktighet),

e) inte möjliggöra identifiering av den registrerade under längre tid än nödvändigt (lagringsminimering), och

f) behandlas på ett sätt som säkerställer säkerheten för uppgifterna (integritet och konfidentialitet).

Den personuppgiftsansvarige måste även följa principen om ansvarsskyldighet. Denna princip kommer till uttryck i artikel 5.2 och innebär att den personuppgiftsansvarige ska ansvara för och kunna visa att bestämmelserna i artikel 5.1 efterlevs.

4.2.3 Rättslig grund för behandling av personuppgifter

Allmänt om kravet på rättslig grund

Behandling av personuppgifter är endast laglig om och i den mån den utförs med stöd av en rättslig grund. De rättsliga grunderna för personuppgiftsbehandling anges i artikel 6. Uppräkningen av de rättsliga grunderna är uttömmande. Enligt artikel 6 får personuppgifter behandlas

a) med stöd av den registrerades samtycke,

b) för att fullgöra ett avtal eller en rättslig förpliktelse,

c) för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige,

d) till skydd för intressen som är av grundläggande betydelse för en fysisk person,

e) för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning, eller

f) utifrån en intresseavvägning mellan den personuppgiftsansvariges eller tredje parts berättigade intressen och den registrerades intressen och grundläggande fri- och rättigheter.

De rättsliga grunderna är i viss mån överlappande och viss behandling kan i och med det omfattas av mer än en rättslig grund. Om ingen av de rättsliga grunderna är tillämplig är behandlingen inte laglig och får inte utföras.

Behandlingen av personuppgifter är, med undantag för personuppgifter som behandlas med stöd av den registrerades samtycke, endast laglig om behandlingen är nödvändig i förhållande till den rättsliga grunden. Nödvändighetskravet har en nära koppling till principerna om ändamålsbegränsning och uppgiftsminimering och medför ett krav på ett direkt samband mellan behandlingen och den rättsliga grunden. Att behandlingen ska vara nödvändig ska dock inte tolkas som ett krav på att det ska vara omöjligt att utföra en viss uppgift utan att utföra en viss behandlingsåtgärd. En viss behandling av personuppgifter kan exempelvis anses vara nödvändig om den leder till effektivitetsvinster, även om behandlingen inte är en förutsättning för att uppnå syftet med den. Som exempel kan nämnas att det mer eller mindre regelmässigt anses vara nödvändigt att använda tekniska hjälpmedel och på så sätt behandla personuppgifter på automatiserad väg, eftersom en manuell informationshantering i dag inte är ett realistiskt alternativ för vare sig myndigheter eller företag. Den metod som den personuppgiftsansvarige väljer måste dock var ändamålsenlig, effektiv och proportionerlig och får alltså inte medföra ett onödigt intrång i enskildas privatliv. Även administrativa behandlingsåtgärder som i praktiken krävs för att en personuppgiftsansvarig ska kunna fullgöra en viss uppgift utgör nödvändig behandling enligt dataskyddsförordningen.[9]

[9] Jfr prop. 2017/18:105, *Ny dataskyddslag*, s. 47–48 och 60–61.

Begränsningar av möjligheten att behandla personuppgifter med grund i samtycke eller ett berättigat intresse

Möjligheten att behandla personuppgifter med hänsyn till den personuppgiftsansvariges berättigade intresse (led f i artikel 6) är en form av generalklausul som möjliggör behandling utifrån en avvägning mellan den personuppgiftsansvariges och den registrerades intressen. Tillämpning av bestämmelsen kräver dock under alla omständigheter en noggrann intresseavvägning. Vid bedömningen ska bl.a. beaktas om den registrerade vid tidpunkten för inhämtandet av personuppgifter rimligen kunde förvänta sig att den aktuella personuppgiftsbehandlingen kunde komma att ske.

Det är den nationella lagstiftarens uppgift att genom lagstiftning tillhandahålla rättslig grund för myndigheters behandling av personuppgifter. En myndighet kan med anledning av detta inte behandla personuppgifter utifrån den rättsliga grunden i artikel 6.1 f när myndigheten fullgör sina uppgifter. I dessa fall måste myndighetens rättsliga grund vara fastställd av lagstiftaren på nationell eller EU-rättslig nivå.[10]

En myndighet har också begränsade möjligheter att behandla personuppgifter med stöd av den registrerades samtycke, eftersom det kan antas råda betydande ojämlikhet mellan den registrerade och myndigheten.[11]

Uppgift av allmänt intresse och myndighetsutövning

Den rättsliga grund som aktualiseras vid myndigheters behandling av personuppgifter är främst att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning, vilken framgår av artikel 6.1 e i EU:s dataskyddsförordning.

Med *uppgift av allmänt intresse* avses i första hand uppgifter som utförs av myndigheter och andra offentliga organ såsom förvaltning av hälso- och sjukvårdstjänster och sjukförsäkring.[12] Begreppet har dock en vid betydelse och omfattar uppgifter av vitt skilda slag. Uppgifter som riksdag eller regering har gett i uppdrag åt statliga myndig-

[10] Jfr skäl 47 samt artikel 6.1 andra stycket och artikel 6.3 i EU:s dataskyddsförordning.
[11] Jfr skäl 43 i EU:s dataskyddsförordning.
[12] Jfr skäl 45 och 52 till EU:s dataskyddsförordning.

heter att utföra är som utgångspunkt av allmänt intresse. På motsvarande sätt är det obligatoriska uppgifter som ålagts kommuner och regioner att utföra av allmänt intresse.[13] Uppgifter av allmänt intresse kan även utföras av privata aktörer på uppdrag av en myndighet eller på eget initiativ. I Sverige har avskaffandet av statliga monopol och konkurrensutsättning av offentlig verksamhet inneburit att privaträttsliga organ numera utför en inte obetydlig del av de uppgifter som är av allmänt intresse. En privat aktör som, på uppdrag av en myndighet eller på eget initiativ, utför en uppgift av allmänt intresse som är fastställd i lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning kan alltså vidta nödvändig behandling av personuppgifter på samma grund som om en myndighet hade utfört arbetsuppgiften.[14]

Begreppet *myndighetsutövning* karaktäriseras av beslut eller andra ensidiga åtgärder som ytterst är ett uttryck för samhällets maktbefogenheter. Myndighetsutövning kan både medföra förpliktelser för enskilda och mynna ut i gynnande beslut. Inom begreppet myndighetsutövning faller t.ex. en stor del av den behandling av personuppgifter som en myndighet utför inom ramen för dess behandling av ärenden. Råd, upplysningar och andra inte bindande uttalanden omfattas dock inte av begreppet.[15] Myndighetsutövning genomförs av naturliga skäl i första hand av statliga, regionala och kommunala myndigheter. Även juridiska och fysiska personer kan dock med stöd av lag enligt 12 kap. 4 § RF anförtros förvaltningsuppgifter som innefattar myndighetsutövning.

4.2.4 Grunden för behandling ska i vissa fall fastställas i rättsordningen

Den rättsliga grunden ska i vissa fall fastställas i unionsrätten eller i en medlemsstats nationella rätt

För behandling av personuppgifter som är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning ska enligt artikel 6.3 första stycket grunden för behandling fastställas i enlighet med unionsrätten eller

[13] Jfr prop. 2017/18:105, *Ny dataskyddslag*, s. 56–57.
[14] Prop. 2017/18:105, *Ny dataskyddslag*, s. 58–59.
[15] Prop. 2017/18:105, *Ny dataskyddslag*, s. 62.

en medlemsstats nationella rätt. Tillämpningen av denna rättsliga grund förutsätter alltså särskilt stöd i rättsordningen. Detta gäller även för den rättsliga grunden i artikel 6.1 c, dvs. att behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Övriga rättsliga grunder kan tillämpas direkt med stöd av bestämmelserna i EU:s dataskyddsförordning.

Unionsrätten och medlemsstaternas nationella rätt ska vid fastställelse av en rättslig grund uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas. Den rättsliga grunden kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i dataskyddsförordningen, t.ex. de allmänna villkor som ska gälla för den personuppgiftsansvariges behandling och vilken typ av personuppgifter som ska behandlas. Detta framgår av artikel 6.3 andra stycket.

Det är grunden för behandlingen, dvs. uppgiften av allmänt intresse eller rätten att utföra myndighetsutövning, som ska fastställas i rättsordningen. Det finns dock inte något krav på att själva behandlingen av personuppgifter ska fastställas.[16] Kravet på fastställelse medför inte heller något krav på en särskild lag till grund för varje behandling, utan det kan räcka med en lag som grund för flera behandlingar. De rättsliga grunderna bör dock fastställas på ett sådant sätt att grunderna är tydliga och precisa och att tillämpningen av dessa är förutsägbar för dem som omfattas av regleringen.[17] Vilken grad av tydlighet och precision som krävs vid fastställelse av den rättsliga grunden får bedömas från fall till fall, utifrån behandlingens och verksamhetens karaktär. Ett mer kännbart intrång i den personliga integriteten, t.ex. omfattande behandling av känsliga personuppgifter eller annan integritetskänslig behandling, kräver en högre grad av precision av den rättsliga grunden och alltså en hög grad av förutsebarhet.[18]

Fastställelse av rättslig grund i svensk rätt

I Sverige följer det av grundlag att den offentliga makten utövas under lagarna. De grundläggande bestämmelserna om hur normgivningen går till finns i 8 kap. RF. Föreskrifter ska meddelas av riksdagen genom lag bl.a. om föreskrifterna avser förhållanden mellan enskilda och

[16] Jfr prop. 2017/18:105, *Ny dataskyddslag*, s. 49.
[17] Jfr skäl 41 och 45 i EU:s dataskyddsförordning.
[18] Jfr prop. 2017/18:105, *Ny dataskyddslag*, s. 51.

det allmänna under förutsättning att föreskrifter gäller skyldigheter för enskilda eller i övrigt avser ingrepp i enskildas personliga och ekonomiska förhållanden. Regeringen får dock, efter bemyndigande från riksdagen, meddela sådana föreskrifter i en förordning. Normgivningskompetensen kan även vidaredelegeras till en myndighet eller en kommun, som därmed bemyndigas att meddela föreskrifter på ett visst område.[19]

Enligt lagen (1994:1500) med anledning av Sveriges anslutning till Europeiska unionen gäller EU:s rättsakter i landet med den verkan som följer av EU-fördragen. Detta innebär att även unionsrätten har stöd i svensk lag, t.ex. i fråga om förpliktelser, myndighetsutövning och uppgifter av allmänt intresse som följer av direkt tillämpliga EU-förordningar eller som meddelas med stöd av sådana förordningar.[20]

Sammanfattningsvis är rättslig grund fastställd i enlighet med svensk rätt om den följer av författning eller beslut som meddelas i enlighet med regeringsformens bestämmelser. Som följd av den svenska arbetsmarknadsmodellen kan en rättslig grund även följa av kollektivavtal.[21] En uppgift av allmänt intresse kan alltså vara fastställd i enlighet med detta.[22] Befogenhet att bedriva myndighetsutövning i Sverige är dock alltid fastställd i lag eller annan författning.[23]

4.2.5 Behandling av särskilda kategorier av personuppgifter

Allmänt om särskilda kategorier av personuppgifter

Utöver de grundläggande principerna för personuppgiftsbehandling och kravet på rättslig grund för behandling gäller särskilda krav för behandling av uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och för behandling av genetiska uppgifter, biometriska uppgifter och för att entydigt identifiera en fysisk persons sexualliv eller sexuella läggning, dvs. särskilda kategorier av personuppgifter, s.k. känsliga personuppgifter. Dessa kategorier av personuppgifter är till sin natur särskilt känsliga och därmed särskilt skyddsvärda. Behandling av sådana uppgifter kan innebära betydande risker för de grund-

[19] Jfr prop. 2017/18:105, *Ny dataskyddslag*, s. 51.
[20] Jfr prop. 2017/18:105, *Ny dataskyddslag*, s. 51–52.
[21] Jfr prop. 2017/18:105, *Ny dataskyddslag*, s. 52.
[22] Jfr prop. 2017/18:105, *Ny dataskyddslag*, s. 61.
[23] Jfr prop. 2017/18:105, *Ny dataskyddslag*, s. 63.

läggande fri- och rättigheterna och EU:s dataskyddsförordning ställer med anledning av detta upp särskilda bestämmelser om skydd för sådana personuppgifter.[24]

Behandling av känsliga personuppgifter är som utgångspunkt förbjuden enligt artikel 9.1. Detta förbud kompletteras dock med en rad undantag som anges uttömmande i artikel 9.2. Likt de rättsliga grunderna för behandling av personuppgifter är vissa av dessa undantag direkt tillämpliga, medan andra grunder förutsätter fastställelse i EU-rätt eller nationella rätt.

Enligt de undantag som kan tillämpas direkt med stöd av EU:s dataskyddsförordning får nödvändig behandling av känsliga personuppgifter utföras bl.a. om den registrerade har lämnat sitt samtycke eller på ett tydligt sätt offentliggjort uppgifterna samt för att skydda en fysisk persons grundläggande intressen.[25]

Behandling av hänsyn till ett viktigt allmänt intresse

Undantag från förbudet mot att behandla känsliga personuppgifter gäller vid behandling som är nödvändig av hänsyn till ett viktigt allmänt intresse.[26] Detta undantag tillämpas huvudsakligen inom myndigheters verksamhet, men kan även aktualiseras vid viss behandling som utförs av privata aktörer.[27] Viktiga allmänna intressen är enligt EU:s dataskyddsförordning exempelvis EU:s eller en medlemsstats viktiga ekonomiska och finansiella intressen, folkhälsan och social trygghet.[28] Det är svårt att på ett generellt plan definiera vad som skiljer ett allmänt intresse från ett viktigt allmänt intresse.[29] Att en svensk myndighet kan bedriva den verksamhet som tydligt faller inom ramen för myndigheters befogenheter på ett korrekt, rättssäkert och effektivt sätt anses dock utgöra ett viktigt allmänt intresse. Detta gäller inte minst i sådan verksamhet som innefattar myndighetsutövning.[30]

Vid behandling av känsliga personuppgifter av hänsyn till ett viktigt allmänt intresse krävs att uppgifterna behandlas på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska

[24] Skäl 51 i EU:s dataskyddsförordning.
[25] Artikel 9.2 a, c och e i EU:s dataskyddsförordning.
[26] Artikel 9.2 g i EU:s dataskyddsförordning.
[27] Skäl 19 i EU:s dataskyddsförordning.
[28] Artikel 23.1 e i EU:s dataskyddsförordning.
[29] Jfr artikel 6.1 e och 9.2 g i EU:s dataskyddsförordning.
[30] Prop. 2017/18:105, *Ny dataskyddslag*, s. 83.

stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.[31] För att känsliga personuppgifter ska får behandlas på denna grund ställs alltså särskilda krav på ett rättsligt stöd som uppfyller villkor gällande proportionalitet och skyddsåtgärder.

4.2.6 Den personuppgiftsansvariges allmänna skyldigheter och säkerhet för personuppgifter

I avsnitt IV i EU:s dataskyddsförordning finns bestämmelser om allmänna skyldigheter för den personuppgiftsansvarige. Enligt artikel 24.1 ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med förordningen. Av bestämmelsen framgår att behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter ska beaktas samt att åtgärderna ska ses över och uppdateras vid behov. I artikel 25 finns krav på att den personuppgiftsansvarige, både vid fastställande av vilka medel behandlingen utförs med och vid själva behandlingen, ska genomföra lämpliga tekniska och organisatoriska åtgärder, såsom pseudonymisering[32], så att kraven i förordningen uppfylls och de registrerades rättigheter skyddas. Lämpliga tekniska och organisatoriska åtgärder ska också vidtas för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer enligt artikel 25.2. Det finns alltså ett uttryckligt krav på behörighetsbegränsningar. Ju högre risk med behandlingen, desto högre krav ställs på säkerheten.

Enligt artikel 30 ska den personuppgiftsansvarige föra ett register över den behandling som utförs under dess ansvar. Registret ska inne-

[31] Artikel 9.2 g i EU:s dataskyddsförordning.
[32] Med begreppet pseudonymisering avses behandling av personuppgifter på så sätt att personuppgifterna inte längre kan kopplas till en viss person utan kompletterande uppgifter.

hålla en mängd uppgifter, bl.a. namn och kontaktuppgifter för den personuppgiftsansvarige, rättslig grund för och ändamålen med behandlingen, en beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter, om möjligt tidsfristerna för radering och en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1.

I artikel 32 finns bestämmelser om säkerhet i samband med behandlingen. Den personuppgiftsansvarige ska, enligt artikel 32.1, med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. När det är lämpligt inbegriper detta bl.a. pseudonymisering och kryptering av personuppgifter, förmågan att fortlöpande säkerställa konfidentialitet, tillgänglighet och motståndskraft hos behandlingsystemen och tjänsterna samt ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Om en personuppgiftsincident inträffar är den personuppgiftsansvarige enligt huvudregeln i artikel 33 skyldig att utan dröjsmål anmäla detta till tillsynsmyndigheten. Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige enligt artikel 34 utan onödigt dröjsmål även informera de registrerade om personuppgiftsincidenten. Enligt artikel 33.5 finns det även ett krav på att den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, dess omständigheter, effekter och vidtagna korrigerande åtgärder. Detta oberoende av om det finns en skyldighet att anmäla eller informera.

4.2.7 Konsekvensbedömning avseende dataskydd och förhandssamråd

I fråga om särskilt riskfyllda behandlingar ställer EU:s dataskyddsförordning upp krav på konsekvensbedömningar och ibland förhandssamråd med tillsynsmyndigheten. Bestämmelser om konsekvensbedömningar finns i artikel 35. Av punkten 1 framgår att vid en typ av behandling, särskilt med användning av ny teknik och med beak-

tande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker. Enligt punkten 3 ska en konsekvensbedömning särskilt krävas bl.a. vid systematisk övervakning av en allmän plats i stor omfattning (led c). I skäl 91 till EU:s dataskyddsförordning nämns i detta sammanhang särskilt optiskelektroniska anordningar. En konsekvensbedömning ska enligt punkten 7 innehålla åtminstone

a) en systematisk beskrivning av den planerade behandlingen och behandlingens syften,

b) en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena,

c) en bedömning av de risker för de registrerades rättigheter och friheter som avses i punkt 1, och

d) de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att förordningen efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

Av punkten 11 framgår att den personuppgiftsansvarige vid behov ska genomföra en översyn för att bedöma om behandlingen genomförs i enlighet med konsekvensbedömningen avseende dataskydd åtminstone när den risk som behandlingen medför förändras.

Europeiska dataskyddsstyrelsen, EDPB, (tidigare benämnd arbetsgruppen för skydd av enskilda med avseende på behandling av personuppgifter, artikel 29-gruppen) har utarbetat riktlinjer för konsekvensbedömningar.[33] I dessa riktlinjer anges bl.a. att en enda konsekvensbedömning kan användas för att bedöma flera behandlingar som liknar varandra vad gäller art, omfattning, innehåll, ändamål och risker. Man uttalar vidare att syftet med en konsekvensbedömning är att systematiskt studera nya situationer som kan

[33] Artikel 29-gruppen, *Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679*, antagna den 4 april 2017.

medföra hög risk för fysiska personers fri- och rättigheter och att det inte föreligger något behov av att utföra en konsekvensbedömning i situationer, dvs. behandlingar som utförs i ett särskilt sammanhang och av en särskild anledning, som redan har studerats. Detta kan vara fallet när liknande teknik används för att samla in samma slags uppgifter för samma ändamål. Som exempel anges att en järnvägsoperatör kan täcka videoövervakning i samtliga tågstationer med en enda konsekvensbedömning.[34]

Den personuppgiftsansvarige ska, enligt artikel 36.1, begära förhandssamråd med tillsynsmyndigheten före en behandling om en konsekvensbedömning avseende dataskydd visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken. I skäl 94 i förordningen anges att förhandssamråd ska hållas om det av en konsekvensbedömning framgår att behandlingen utan skyddsåtgärder, säkerhetsåtgärder och mekanismer för att minska risken kommer att innebära en hög risk för fysiska personers rättigheter och friheter, och den personuppgiftsansvarige anser att risken inte kan begränsas genom åtgärder som är rimliga med avseende på tillgänglig teknik och genomförandekostnader. Om behandlingen inte medför sådana risker behöver man alltså inte begära förhandssamråd med tillsynsmyndigheten. I EDPB:s nämnda riktlinjer förtydligar man att förhandssamråd krävs när den personuppgiftsansvarige inte kan vidta tillräckliga åtgärder för att minska risken till en godtagbar nivå, alltså att den kvarstående risken fortfarande är hög.[35]

Av artikel 36.2 framgår att om tillsynsmyndigheten inom ramen för ett förhandssamråd anser att den planerade behandlingen skulle strida mot förordningen, ska tillsynsmyndigheten inom en viss period ge den personuppgiftsansvarige skriftliga råd. Tillsynsmyndigheten får även nyttja alla de befogenheter som den har enligt artikel 58.

Av artikel 36.5 framgår också att det i medlemsstaternas nationella rätt får krävas att personuppgiftsansvariga ska begära förhandssamråd med, och erhålla förhandstillstånd av, tillsynsmyndigheten när det

[34] Artikel 29-gruppen, *Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679*, antagna den 4 april 2017, s. 8.
[35] Artikel 29-gruppen, *Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679*, antagna den 4 april 2017, s. 21.

gäller en personuppgiftsansvarigs behandling för utförandet av en uppgift av allmänt intresse.

4.2.8 Dataskyddsombud

I artikel 37 ställs det upp krav på att den personuppgiftsansvarige under alla omständigheter ska utnämna ett dataskyddsombud om behandlingen genomförs av en myndighet eller ett offentligt organ. Detsamma gäller om den personuppgiftsansvariges kärnverksamhet består av behandling, som på grund av sin karaktär, sin omfattning eller sina ändamål, kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning. En offentlig myndighet eller ett offentligt organ definieras inte i EU:s dataskyddsförordning. Av EDPB:s riktlinjer om dataskyddsombud framgår följande.

> […] Det är inte bara offentliga myndigheter eller offentliga organ som kan bedriva offentlig verksamhet och myndighetsutövning, utan även andra offentligrättsliga eller privaträttsliga fysiska eller juridiska personer inom olika sektorer enligt varje medlemsstats nationella lagstiftning, såsom kollektivtrafik, vatten- och energiförsörjning, väginfrastruktur, radio och tv i allmänhetens tjänst, allmännyttiga bostäder eller disciplinorgan för reglerade yrken.
>
> I sådana fall kan de registrerade befinna sig i en mycket liknande situation när deras personuppgifter behandlas av en offentlig myndighet eller ett offentligt organ. Personuppgifter kan behandlas för liknande ändamål och enskilda personer har ofta mycket små eller inga möjligheter att välja om och i så fall hur deras personuppgifter ska behandlas, och behandlingen kan därför kräva det ytterligare skydd som utnämnandet av ett dataskyddsombud kan ge.
>
> Även om det inte föreligger någon skyldighet i sådana fall rekommenderar artikel 29-arbetsgruppen, som god praxis, att privata organisationer som bedriver offentlig verksamhet och myndighetsutövning utser ett dataskyddsombud […].[36]

Dataskyddsombudet ska enligt artikel 37.5 utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att utföra de uppgifter som åligger ett dataskyddsombud enligt artikel 39. Enligt artikel 38.1 ska dataskyddsombudet medverka i alla frågor som rör skyddet av personuppgifter. I dataskyddsombudets uppgifter ingår enligt artikel 39.1 a att informera och ge råd till den personuppgiftsansvarige

[36] Artikel 29-gruppen, *Riktlinjer om dataskyddsombud*, antagna den 13 december 2016, s. 8.

och de anställda som behandlar uppgifter om deras skyldigheter enligt förordningen. Av artikel 39.1 b framgår att dataskyddsombudet även har i uppgift att övervaka efterlevnaden av förordningen och av den personuppgiftsansvariges strategi för skydd av personuppgifter, vilket inbegriper ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning. Dataskyddsombudet ska även enligt artikel 39.1 d och e samarbeta med tillsynsmyndigheten och fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling och vid behov samråda i alla andra frågor.

4.2.9 Enskildas rättigheter

I avsnitt III i EU:s dataskyddsförordning finns bestämmelser om den registrerades rättigheter. Något förenklat kan bestämmelserna om enskildas rättigheter sägas innebära en rätt att veta vem som behandlar vilka uppgifter, och varför. Informationen ska vara klar och tydlig liksom villkoren för utövandet av den registrerades rättigheter.

I artikel 13 respektive 14 finns bestämmelser om information som ska tillhandahållas om personuppgifter samlas in från den registrerade respektive om personuppgifterna inte har erhållits från den registrerade. Utöver kontaktuppgifter till den personuppgiftsansvarige och dataskyddsombudet rör det sig bl.a. om information om rättslig grund för och ändamålen med behandlingen, den period under vilken uppgifterna kommer att lagras (om möjligt), rätten att begära information, rättelse eller radering samt möjligheten att lämna in klagomål till tillsynsmyndigheten. Den registrerade har enligt artikel 15 rätt att av den personuppgiftsansvarige få bekräftelse på om personuppgifter som rör henne eller honom behandlas. I artiklarna 16 och 17 finns bestämmelser som innebär att den registrerade, under vissa närmare angivna förutsättningar, har rätt att begära rättelse eller radering av uppgifter.

4.2.10 Tillsyn, sanktionsavgifter och skadestånd

Integritetsskyddsmyndigheten, IMY, är tillsynsmyndighet enligt den generella dataskyddsregleringen.[37] Tillsynsmyndigheten ska, enligt artikel 57.1 i EU:s dataskyddsförordning, bl.a. övervaka och verkställa tillämpningen av förordningen samt behandla klagomål från registrerade.

Myndigheten har en rad undersökande, förebyggande och korrigerande befogenheter. Dessa framgår av artikel 58. Tillsynsmyndighetens utredningsbefogenheter innebär bl.a. en rätt att från den personuppgiftsansvarige få tillgång till alla personuppgifter och all information som tillsynsmyndigheten behöver för att kunna fullgöra sina uppgifter. Tillsynsmyndigheten har också rätt att få tillträde till alla lokaler som tillhör den personuppgiftsansvarige, inbegripet tillgång till all utrustning och alla andra medel för behandling av personuppgifter i överensstämmelse med unionens processrätt eller medlemsstaternas nationella processrätt.

Gällande korrigerande befogenheter kan tillsynsmyndigheten bl.a. utfärda varningar, reprimander och förelägga en personuppgiftsansvarig eller ett personuppgiftsbiträde att se till att behandlingen sker i enlighet med bestämmelserna i förordningen. Tillsynsmyndigheten kan även införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, behandling.

Tillsynsmyndigheten kan även påföra administrativa sanktionsavgifter i enlighet med artikel 83. Av punkten 4 framgår att en sanktionsavgift får påföras den personuppgiftsansvarige vid överträdelse av bl.a. skyldigheterna att tillämpa inbyggt dataskydd eller dataskydd som standard, föra förteckning över behandling, vidta lämpliga tekniska och organisatoriska åtgärder samt genomföra konsekvensbedömningar och förhandssamråd. Sanktionsavgifter får, enligt punkten 5, även tas ut av en personuppgiftsansvarig vid överträdelser av förordningens grundläggande principer för behandling. Detsamma gäller för bestämmelserna om rättslig grund och de registrerades rättigheter.

För överträdelser enligt punkten 4 får en sanktionsavgift påföras på upp till 10 miljoner euro eller, om det gäller ett företag, på upp till två procent av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst. Vid överträdelser av de bestämmelser som anges i punkten 5 får det påföras administra-

[37] 2 a § förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten.

tiva sanktionsavgifter på upp till 20 miljoner euro eller, om det gäller ett företag, på upp till fyra procent av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst. Av 6 kap. § dataskyddslagen framgår att bestämmelser i EU:s dataskyddsförordning om sanktionsavgifter gäller även för myndigheter. Sanktionsavgiften för myndigheter ska enligt samma bestämmelse bestämmas till högst 5 miljoner kronor vid överträdelser som avses i artikel 83.4 och till högst 10 miljoner kronor vid överträdelser som avses i artikel 83.5.

Det finns slutligen en bestämmelse om skadestånd i förordningen. Enligt artikel 82 ska varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av förordningen ha rätt till ersättning från den personuppgiftsansvarige för den uppkomna skadan.

4.3 Nationell kompletterande lagstiftning till EU:s dataskyddsförordning

4.3.1 Allmänna nationella dataskyddsbestämmelser

EU:s dataskyddsförordning är direkt tillämplig och ska inte genomföras i medlemsstaternas nationella rätt. Dataskyddsförordningen är dock utformad på ett sådant sätt att förordningen till viss del både förutsätter och medger nationell dataskyddsreglering som kompletterar förordningens bestämmelser. Särskilt stort är utrymmet i fråga om den offentliga sektorn. Detta gäller inte minst för behandling enligt de rättsliga grunder som, enligt förordningen, ska fastställas i nationell rätt eller unionsrätt.[38] Möjligheten att anta kompletterande dataskyddsbestämmelser på nationell nivå medför även en möjlighet för medlemsstaterna att i viss mån anpassa förordningens bestämmelser till det nationella sammanhanget.[39] Dataskyddsförordningen tillåter även att delar av förordningen införlivas i nationell rätt, om det är nödvändigt för samstämmigheten och för att göra de nationella bestämmelserna begripliga för de personer som bestämmelserna ska tillämpas på.[40]

I svensk rätt har kompletterande bestämmelser till dataskyddsförordningen på generell nivå antagits genom dataskyddslagen och för-

[38] Se artikel 6.3 i EU:s dataskyddsförordning.
[39] Se t.ex. artikel 6.2 och 23 i EU:s dataskyddsförordning.
[40] Jfr skäl 8 till EU:s dataskyddsförordning.

ordningen med kompletterande bestämmelser till EU:s dataskyddsförordning. Dessa författningar innehåller bl.a. bestämmelser som tydliggör innebörden av vissa bestämmelser i dataskyddsförordningen och ger vägledning om hur dessa ska tillämpas i den svenska rättsordningen.

4.3.2 Särskilda registerförfattningar

Utöver bestämmelserna i dataskyddslagen finns i svensk rätt kompletterande bestämmelser om behandling av personuppgifter i ett stort antal sektorsspecifika registerförfattningar och särskilda informationshanteringsförfattningar. Sådana särskilda lagar har antagits på områden där det är nödvändigt för myndigheter att behandla uppgifter om ett stort antal registrerade och med ett särskilt känsligt innehåll.[41] Som exempel på sådan sektorsspecifik dataskyddsreglering kan nämnas patientdatalagen (2008:355), domstolsdatalagen (2015:728) och utlänningsdatalagen (2016:27). I dessa sektorsspecifika författningar finns bl.a. särskilda bestämmelser om skyddsåtgärder vid behandling av personuppgifter såsom föreskrifter om vilka personuppgifter som får behandlas, hur uppgifterna får behandlas, sökförbud och åtkomst till personuppgifter samt särskilda begränsningar gällande behandling av känsliga personuppgifter.

4.4 Dataskyddsdirektivet

Dataskyddsdirektivet[42] är tillsammans med Dataskyddsförordningen en del av EU:s dataskyddsreform. Direktivet ersatte ett rambeslut[43] om skydd för personuppgifter som behandlas i bl.a. straffrättsligt samarbete. Eftersom direktivet är ett s.k. minimidirektiv står det medlemsstaterna fritt att föreskriva ett mer långtgående skydd för registrerades rättigheter och friheter.

[41] Jfr bet. 1997/98:KU18, *Personuppgiftslag* och prop. 1997/98:44, *Personuppgiftslag*, s. 41.
[42] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.
[43] Rådets rambeslut 2008/977 RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete.

Syftet med direktivet är att bidra till ökat förtroende och underlätta samarbetet i brottsbekämpningen i Europa genom att harmonisera skyddet av personuppgifter inom brottsbekämpande myndigheter i medlemsstaterna och Schengenländerna. I direktivet fastställs en omfattande ram för att säkerställa en hög nivå av dataskydd inom polis- och straffrättsområdet. Skyddet för personuppgifter gäller för fysiska personer som är involverade i straffrättsliga förfaranden och omfattar såväl vittnen som brottsoffer och brottsmisstänkta.

Direktivet innehåller bestämmelser om personuppgiftsansvar, överföring av personuppgifter, tillsyn, samarbete, rättsmedel och sanktionsavgifter. Bestämmelserna i direktivet överensstämmer i stora delar med EU:s dataskyddsförordning, men innehåller också skillnader, t.ex. när det gäller informationsplikten, enskildas rättigheter och kraven på konsekvensbedömningar och förhandssamråd.

Direktivet är tillämpligt på både inhemsk och gränsöverskridande brottsbekämpning och det är det första instrumentet som tar ett samlat grepp om brottsbekämpningsområdet. Tidigare har varje brottsbekämpningsinstrument styrts av sina egna dataskyddsregler. Genom direktivet ger unionslagstiftaren verkan åt den grundläggande rätt till skydd av personuppgifter som fastställs i artikel 8 i EU:s rättighetsstadga i samband med behandling av personuppgifter som utförs av brottsbekämpande myndigheter.

I artikel 4.1 i direktivet ställs det upp grundläggande principer för behandling av personuppgifter. Medlemsstaterna ska föreskriva att personuppgifter ska

a) behandlas på ett lagligt och korrekt sätt,

b) samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte behandlas på ett sätt som står i strid med dessa ändamål,

c) vara adekvata, relevanta och inte för omfattande i förhållande till de syften för vilka de behandlas,

d) vara korrekta och, om nödvändigt, uppdaterade,

e) inte möjliggöra identifiering av den registrerade under längre tid än nödvändigt, och

f) behandlas på ett sätt som säkerställer säkerheten för personuppgifterna.

Enligt artikel 4.2 är behandling som utförs för något annat ändamål som anges i artikel 1.1 än det för vilket uppgifterna samlades in tillåten om den personuppgiftsansvarige är bemyndigad att behandla personuppgifterna för ett sådant ändamål och behandlingen är nödvändig och proportionerlig. Behandlingen kan enligt artikel 4.3 inbegripa arkivändamål av allmänt intresse och vetenskaplig, statistisk eller historisk användning för de ändamål som anges i artikel 1, under förutsättning att det finns lämpliga skyddsåtgärder för de registrerades rättigheter och friheter.

I artikel 5 anges att medlemsstaterna ska förskriva att lämpliga tidsgränser fastställs för radering av personuppgifter eller för periodisk översyn av behovet av att lagra personuppgifter. Procedurrelaterade åtgärder ska säkerställa att tidsgränserna fastställs.

Artikel 6 innebär att det ska göras åtskillnad mellan olika kategorier av registrerade. Den personuppgiftsansvarige ska i tillämpliga fall och så långt det är möjligt göra en klar åtskillnad mellan personer avseende vilka det finns tungt vägande skäl att anta att de har begått brott eller är på väg att begå brott, personer som dömts för brott, brottsoffer samt andra som berörs av brott. Den sistnämnda kategorin kan t.ex. omfatta personer som kan komma att kallas att vittna i samband med brottsutredningar eller personer som kan ge information om brott.

I artikel 7 anges att det ska göras åtskillnad mellan personuppgifter och kontroll av kvaliteten på personuppgifterna. Personuppgifter som grundar sig på fakta ska så långt det är möjligt skiljas från personuppgifter som grundar sig på personliga bedömningar. De behöriga myndigheterna ska vidta alla rimliga åtgärder för att se till att personuppgifter som är felaktiga, ofullständiga, eller inaktuella inte överförs eller görs tillgängliga. Om det visar sig att felaktiga personuppgifter har överförts eller att uppgifterna olagligen har överförts ska mottagaren omedelbart underrättas om detta. I sådana fall ska personuppgifterna rättas eller raderas eller behandlingen begränsas i enlighet med artikel 16.

Artikel 8 anger att behandlingen är laglig endast om och i den mån den är nödvändig för de ändamål som anges i artikel 1.1 och som sker på grundval av unionsrätt eller medlemsstaternas nationella rätt. Den nationella rätt som reglerar behandling inom tillämpningsområdet för direktivet ska åtminstone precisera syftet med behandlingen, vilka personuppgifter som ska behandlas och behandlingens ändamål.

I artikel 9 anges särskilda villkor för behandling av uppgifter. De uppgifter som samlas in för de ändamål som anges i artikel 1.1 ska inte behandlas för andra ändamål än de som anges i den artikeln, såvida inte sådan behandling är tillåten enligt unionsrätten eller nationell rätt. När personuppgifter behandlas för andra ändamål ska EU:s dataskyddsförordning tillämpas, såvida inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten. Om behöriga myndigheter ges andra uppgifter än de som utförs för ändamål som anges i artikel 1.1 ska dataskyddsförordningen vara tillämplig på behandlingen för dessa ändamål, inklusive arkivändamål av allmänt intresse, för historiska eller vetenskapliga forskningsändamål eller för statistiska ändamål, såvida inte behandlingen utförs i en verksamhet som inte omfattas av unionsrätten.

Artikel 10 behandlar särskilda kategorier av personuppgifter. Det är endast tillåtet att behandla personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller politisk övertygelse eller medlemskap i fackförening, genetiska eller biometriska uppgifter samt uppgifter om hälsa, sexualliv eller sexuell läggning om det är absolut nödvändigt och under förutsättning att det finns lämpliga skyddsåtgärder för den registrerades rättigheter och friheter. Det krävs därutöver att behandlingen är tillåten enligt unionsrätten eller nationell rätt, att behandlingen sker för att skydda intressen av grundläggande betydelse för den registrerade eller annan fysisk person eller om behandlingen rör uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

I artikel 11 anges att beslut som enbart grundas på automatiserad behandling, t.ex. profilering, som har negativa rättsliga följder för den registrerade eller i betydande grad påverkar vederbörande ska förbjudas om de inte är tillåtna enligt unionsrätten eller nationell rätt. Det krävs vidare att det föreskrivs lämpliga skyddsåtgärder för den registrerades rättigheter och friheter, åtminstone till rätten till mänskligt ingripande från den personuppgiftsansvariges sida. Beslut som grundas på automatiserad behandling får inte grundas på de särskilda kategorier av personuppgifter som avses i artikel 10, såvida inte lämpliga skyddsåtgärder har vidtagits. Profilering som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter enligt artikel 10 ska förbjudas i enlighet med unionsrätten.

Kapitel 3 i direktivet handlar om den registrerades rättigheter. Av artikel 12 framgår bl.a. att den personuppgiftsansvarige ska vidta rimliga åtgärder för att tillhandahålla den registrerade viss information meddelanden i en koncis, begriplig och lättillgänglig form och på ett klart och tydligt språk. I artikel 15 anges att den registrerade ska ha rätt att få bekräftelse på om personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till viss information om behandlingen, t.ex. ändamålen med behandlingen och dess rättsliga grund.

Dataskyddsdirektivet innehåller i likhet med EU:s dataskyddsförordning även bestämmelser om konsekvensbedömning och förhandssamråd, dataskyddsombud, tillsyn och sanktionsavgifter samt skadestånd.

4.5 Brottsdatalagen

EU:s dataskyddsdirektiv genomförs i svensk rätt framför allt genom brottsdatalagen. Syftet med lagen är enligt 1 kap. 1 § andra stycket att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt. Brottsdatalagen är en ramlag som innehåller övergripande principer, riktlinjer och mål med behandlingen av personuppgifter vid brottsbekämpande myndigheter, utan att detaljreglera området. Lagen kompletteras av brottsdataförordningen som genomför vissa bestämmelser i direktivet.

I brottsdatalagens första kapitel finns allmänna bestämmelser. Av 1 kap. 3 § framgår att lagen gäller vid bl.a. sådan behandling av personuppgifter som är helt eller delvis automatiserad. Enligt 1 kap. 2 § gäller lagen vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Den gäller också vid behandling av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet.

Med behörig myndighet avses i det här sammanhanget, enligt 1 kap. 6 §, en myndighet som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verk-

ställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet, när myndigheten behandlar personuppgifter för ett sådant syfte. Brottsdatalagens tillämpningsområde knyts alltså både till vilket syfte som behandlingen av personuppgifter har och till att det är en behörig myndighet som utför behandlingen. Om en behörig myndighet behandlar personuppgifter i ett annat syfte än det lagen anger är det i stället EU:s dataskyddsförordning och kompletterande bestämmelser tillämpliga.

4.5.1 Grundläggande krav på personuppgiftsbehandling

I brottsdatalagens andra kapitel finns bestämmelser om grundläggande krav på personuppgiftsbehandling som direkt svarar mot de bestämmelser som finns i dataskyddsdirektivet. I 2 kap. 1 § anges de tillåtna rättsliga grunderna för att behandla personuppgifter. Enligt första stycket får personuppgifter behandlas om det är nödvändigt för att en behörig myndighet ska kunna utföra sin uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Bestämmelsen ger den yttre ramen för när det är tillåtet att behandla personuppgifter enligt lagen. Personuppgifter får bara behandlas om det är nödvändigt för att fullgöra en sådan uppgift.

I 2 kap. 3 § anges att personuppgifter bara får behandlas för särskilda, uttryckligen angivna och berättigade ändamål. Ändamålen med behandlingen måste bestämmas redan när personuppgifter behandlas första gången, eftersom det är i förhållande till ändamålen som det ska prövas om personuppgifterna som behandlas är adekvata och relevant för ändamålet med behandlingen och hur många personuppgifter som behöver behandlas. Ändamålet får inte vara så vagt eller omfattande att en prövning blir omöjlig i praktiken. Att ändamålet ska vara berättigat innebär att det måste finnas en koppling till de rättsliga grunderna.

Av 2 kap. 4 § framgår att innan personuppgifter får behandlas för ett nytt ändamål ska det säkerställas att det finns en rättslig grund enligt 1 § för den nya behandlingen och att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet. Enligt andra stycket behöver någon sådan prövning inte göras om skyldigheten att lämna uppgifter framgår av lag eller förordning.

2 kap. 6 och 7 §§ anges att personuppgifter ska behandlas författningsenligt och på ett korrekt sätt samt att uppgifterna ska vara korrekta och om nödvändigt uppdaterade. Uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet.

Personuppgifterna ska även, enligt 2 kap. 8 §, vara adekvata och relevanta i förhållande till ändamålen med behandlingen och fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till dessa ändamål.

Av 2 kap. 9 § framgår att olika kategorier av personuppgifter så långt det är möjligt ska särskiljas så att det framgår om personen är misstänkt, dömd för brott, brottsoffer eller någon annan som berörs av ett brott. Om det inte framgår av sammanhanget eller på annat sätt till vilken kategori en person hör, ska det tydliggöras genom en särskild upplysning.

I 2 kap. 10 § anges att personuppgifter som grundar sig på fakta så långt det är möjligt ska särskiljas från personuppgifter som grundar sig på personliga bedömningar.

Av 2 kap. 17 § första stycket framgår att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet. Av andra stycket i samma paragraf följer att bestämmelsen i första stycket inte hindrar att en behörig myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

Bestämmelser om behandling av känsliga personuppgifter finns i 2 kap. 11–14 §§. I 11 § första stycket slås fast att personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning inte får behandlas. Av andra stycket framgår att personuppgifter som behandlas dock får kompletteras med sådana känsliga personuppgifter, när det är absolut nödvändigt för ändamålet med behandlingen. Av 12 § framgår att biometriska och genetiska uppgifter endast får behandlas om det är särskilt föreskrivet och absolut nödvändigt för ändamålet med behandlingen.

4.5.2 Den personuppgiftsansvariges skyldigheter och säkerhet för personuppgifter

I brottsdatalagens tredje kapitel finns bestämmelser om den personuppgiftsansvariges skyldigheter. Av 3 kap. 1 § följer att den personuppgiftsansvarige är ansvarig för all behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar. Den personuppgiftsansvarige ska också enligt 3 kap. 2 §, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas (principen om ansvarsskyldighet).

I 3 kap. 3 och 4 §§ finns bestämmelser om inbyggt dataskydd respektive dataskydd som standard. Den personuppgiftsansvarige ska också enligt 3 kap. 6 §, se till att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

I 3 kap. 5 § finns en skyldighet för den personuppgiftsansvarige att säkerställa att det i automatiserade behandlingsystem förs loggar över personuppgiftsbehandling i den utsträckning det är särskilt föreskrivet. Av 3 kap. § brottsdataförordningen framgår att denna skyldighet omfattar behandlingar som innebär insamling, ändring, läsning, utlämning, överföring till tredjeland eller internationella organisationer, sammanföring och radering av personuppgifter. Loggarna över läsning och utlämning ska visa datum och tidpunkt för behandlingen och, så långt det är möjligt, vem som har läst eller lämnat ut personuppgifterna och vem som har fått ta del av personuppgifterna.

I 3 kap. 7 § första stycket finns bestämmelser om konsekvensbedömningar. Om en ny typ av behandling eller betydande förändringar av redan pågående behandling kan antas medföra särskild risk för intrång i den registrerades personliga integritet ska den personuppgiftsansvarige bedöma konsekvenserna för skyddet av personuppgifter. Bedömningen ska göras innan behandlingen påbörjas eller förändringen genomförs. Enligt skäl 58 i dataskyddsdirektivet bör konsekvensbedömningarna omfatta relevanta system och processer för behandling men inte enskilda fall.

Genom 3 kap. 9 § andra stycket brottsdataförordningen förtydligas att vid bedömningen av om typen av behandling innebär sådan risk att förhandssamråd ska äga rum ska ny teknik, nya rutiner eller nya förfaranden särskilt beaktas. Av förarbetena till brottsdatalagen framgår

följande. Förhandsamråd blir främst aktuellt när den personuppgiftsansvarige har gjort en konsekvensbedömning som visar att behandlingen innebär en särskild risk för intrång i registrerades personliga integritet. Vid förhandssamrådet bör den personuppgiftsansvarige redovisa vilka åtgärder som planeras för att minska risken. Det kan vara svårt för den personuppgiftsansvarige att på egen hand avgöra vilka åtgärder som är tillräckliga. Regeringen utesluter dock inte att vidtagna åtgärder från den personuppgiftsansvariges sida kan befria från skyldigheten. I vilken utsträckning förhandssamråd inte bör krävas för att den personuppgiftsansvarige har vidtagit åtgärder som minskat risken för intrång till en godtagbar nivå, bör enligt regeringen överlämnas åt rättstillämpningen att avgöra. Om förhandssamråd aktualiseras på grund av att typen av behandling i sig innebär särskild risk för intrång i registrerades personliga integritet är resultatet av konsekvensbedömningen enligt förarbetena inte avgörande för om förhandssamråd med tillsynsmyndigheten ska äga rum.[44]

Enligt 3 kap. 8 § brottsdatalagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada. Av förarbetena framgår bl.a. följande. Skydd mot obehörig eller otillåten behandling innebär att obehöriga personer ska vägras åtkomst till utrustning som används vid behandling, att obehörig läsning, kopiering, ändring eller radering av datamedier ska förhindras och att obehörig registrering av personuppgifter och obehörig kännedom om, ändring eller radering av lagrade personuppgifter ska förhindras. Åtgärder ska också vidtas i syfte att säkerställa att personer som är behöriga att använda ett it-system endast har tillgång till personuppgifter som omfattas av deras behörighet. Som exempel på organisatoriska säkerhetsåtgärder kan nämnas fastställandet av en säkerhetspolicy, kontroller och uppföljning av säkerheten, utbildning i datasäkerhet och information om vikten av att följa gällande säkerhetsrutiner[45]

Den personuppgiftsansvarige ska slutligen, enligt 3 kap. 3 § brottsdataförordningen, föra förteckning över de kategorier av personuppgiftsbehandlingar som denne ansvarar för. Förteckningen ska för varje kategori av behandling innehålla uppgifter om bl.a. den rättsliga

[44] Jfr prop. 2017/18:232, *Brottsdatalag*, s. 184.
[45] Prop. 2017/18:232, *Brottsdatalag*, s. 457.

grunden och ändamålen, vilka kategorier av tjänstemän som har tillgång till personuppgifterna och vilka kategorier av mottagare uppgifterna kan komma att lämnas ut till. Ytterligare uppgifter som ska finnas i förteckningen är vilka kategorier av registrerade som berörs av behandlingen samt – om det är möjligt – tidsfristerna för hur länge personuppgifter får behandlas och en allmän beskrivning av vilka säkerhetsåtgärder som har vidtagits.

4.5.3 Enskildas rättigheter

Brottsdatalagens fjärde kapitel innehåller bestämmelser om enskildas rättigheter. Av 4 kap. 1 § framgår att viss allmän information ska göras tillgänglig för den registrerade. Det handlar exempelvis om den personuppgiftsansvariges och dataskyddsombudets kontaktuppgifter samt information om kategorier av ändamål för behandlingen, rätten att begära information, rättelse eller radering och möjligheten att lämna in klagomål till tillsynsmyndigheten. Enligt förarbetena kan informationen göras tillgänglig på t.ex. den behöriga myndighetens webbplats.[46]

Av 4 kap. 2 § framgår att den personuppgiftsansvarige i ett enskilt fall ska lämna viss information till den registrerade, om det behövs för att han eller hon ska kunna ta till vara sina rättigheter. Av förarbetena framgår att det är fråga om personrelaterad information som på den personuppgiftsansvariges eget initiativ ska lämnas till den registrerade. Här framgår också att det normalt bör krävas att det är fråga om överträdelser av regelverket som kan föranleda skadeståndsansvar, allvarlig kritik eller ingripande från tillsynsmyndigheten eller någon liknande reaktion för att informationsskyldigheten ska inträda.[47]

Den personuppgiftsansvarige ska, enligt 4 kap. 3 §, till den som begär det utan onödigt dröjsmål lämna skriftligt besked om personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas, ska sökanden få del av dem och få viss i bestämmelsen uppräknad information.

I 4 kap. 9 och 10 §§ finns bestämmelser om den personuppgiftsansvariges skyldighet att på begäran av den registrerade rätta eller

[46] Prop. 2017/18:232, *Brottsdatalag*, s. 465.
[47] Se prop. 2017/18:232, *Brottsdatalag*, s. 465 f.

komplettera personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen samt i vissa angivna situationer radera personuppgifter.

4.5.4 Tillsyn och skadestånd

Som nämnts är IMY tillsynsmyndighet enligt den generella dataskyddsregleringen, och så även enligt brottsdatalagen.[48] Även Myndigheten för säkerhet och integritetsskydd[49] kan utöva tillsyn över vissa brottsbekämpande myndigheters personuppgiftsbehandling i vissa fall.[50]

Enligt 5 kap. 2 § brottsdatalagen ska tillsynsmyndigheten utöva allmän tillsyn över personuppgiftsbehandling inom lagens tillämpningsområde och handlägga klagomål från registrerade. Av 5 kap. 5–7 §§ framgår vilka befogenheter tillsynsmyndigheten har i tillsynsverksamheten. Undersökningsbefogenheterna består bl.a. i att tillsynsmyndigheten har rätt att av personuppgiftsansvariga få tillgång till alla personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen av personuppgifter samt säkerhets- och skyddsåtgärder, tillträde till lokaler som den personuppgiftsansvarige disponerar samt tillgång till utrustning och andra medel för behandling av personuppgifter. De förebyggande befogenheterna innebär bl.a. att om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå den personuppgiftsansvarige att vidta åtgärder för att motverka den risken.

Tillsynsmyndigheten får också utfärda en skriftlig varning för att en planerad eller pågående behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning eller att den personuppgiftsansvarige på något annat sätt inte fullgör sina skyldigheter, får tillsynsmyndigheten utnyttja vissa korrigerande befogenheter. Dessa består bl.a. i att genom råd, rekommendationer eller påpekanden försöka förmå den personuppgifts-

[48] Se 2 a § förordning med instruktion för Integritetsskyddsmyndigheten.
[49] Myndigheten för säkerhet och integritetsskydd bytte namn den 1 mars 2026 och hette tidigare Säkerhets- och integritetsskyddsnämnden.
[50] Se 1 § lagen om tillsyn över viss brottsbekämpande verksamhet.

ansvarige att vidta åtgärder för att behandlingen ska bli författningsenlig, att förelägga den personuppgiftsansvarige att vidta åtgärder, att förbjuda fortsatt behandling om bristen är allvarlig eller att besluta om en administrativ sanktionsavgift.

Av 6 kap. 1 § brottsdatalagen framgår att en sanktionsavgift får tas ut av en personuppgiftsansvarig vid överträdelse av någon av brottsdatalagens bestämmelser om bl.a. rättsliga grunder eller ändamål, behandling för nya ändamål, uppgiftsminimering och lagringsminimering. Sådan avgift får även tas ut bl.a. om den personuppgiftsansvarige inte har använt sig av inbyggt dataskydd eller dataskydd som standard, begränsat tillgången till personuppgifter, gjort en konsekvensbedömning, genomfört ett förhandssamråd eller vidtagit lämpliga tekniska och organisatoriska åtgärder. En sanktionsavgift får också tas ut om en personuppgiftsansvarig inte följer tillsynsmyndighetens beslut om föreläggande eller förbud.

Av 6 kap. 3 § framgår att sanktionsavgifter vid överträdelser av bestämmelserna om begränsning av tillgången till personuppgifter, om konsekvensbedömning eller förhandssamråd eller dokumentation av personuppgiftsincidenter ska bestämmas till högst 5 miljoner kronor. Vid överträdelser av övriga sanktionerade bestämmelser ska avgiften bestämmas till högst 10 miljoner kronor.

Utöver sanktionsavgifterna kan även skadestånd komma i fråga. Enligt 7 kap. 1 § ska den personuppgiftsansvarige ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandling av personuppgifter i strid med den lagen, eller föreskrifter som har meddelats i anslutning till den, har orsakat.

4.5.5 Särskilda registerförfattningar

Utöver brottsdatalagen finns särskilda registerförfattningar med specialbestämmelser för myndigheter som behandlar personuppgifter på brottsdatalagens område. Dessa författningar tar hänsyn till de särskilda behov som dessa myndigheter har av att kunna behandla personuppgifter för att utföra sina arbetsuppgifter. Registerförfattningarna gäller utöver brottsdatalagen och innehåller preciseringar, undantag eller avvikelser från lagen.

Exempel på registerförfattningar på brottsdatalagens område är lagen (2018:1693) om polisens behandling av personuppgifter inom

brottsdatalagens område, lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område och lagen (2018:1695) om Kustbevakningens behandling av personuppgifter inom brottsdatalagens område.

4.6 Polisens brottsdatalag

Lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område, även benämnd polisens brottsdatalag, gäller utöver brottsdatalagen vid behandling av personuppgifter i brottsbekämpande verksamhet vid Polismyndigheten, i viss utsträckning i brottsbekämpande verksamhet vid Ekobrottsmyndigheten samt vid Säkerhetspolisen i frågor som inte rör nationell säkerhet, om uppgifterna behandlas i brottsbekämpande syfte.

I lagens andra kapitel återfinns grundläggande bestämmelser om behandling av personuppgifter. I 2 kap. 1 § anges att personuppgifter får behandlas om det är nödvändigt för att någon av de myndigheter som omfattas av lagen ska kunna utföra följande uppgifter:

1. förebygga, förhindra eller upptäcka brottslig verksamhet,
2. utreda eller lagföra brott,
3. verkställa uppbörd,
4. upprätthålla allmän ordning, eller
5. fullgöra förpliktelser som följer av internationella åtaganden

Förutsättningarna för att behandla personuppgifter i enlighet med lagen för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen där det framgår att innan personuppgifter får behandlas för ett nytt ändamål ska det säkerställas att det finns en rättslig grund för den nya behandlingen och att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet. I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning ska någon sådan prövning inte göras.

Behandling av känsliga personuppgifter regleras särskilt i 2 kap. 4–6 §§. Polismyndigheten och Säkerhetspolisen får behandla biometriska uppgifter om det är absolut nödvändigt för ändamålet med

behandlingen. Det ställs alltså striktare krav för sådan behandling än den generella behandlingen av personuppgifter enligt lagen.

Sökförbudet i 2 kap. 14 § brottsdatalagen hindrar inte att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott, uppgifter om verkställighet av påföljd eller uppgifter som beskriver en persons utseende används som sökbegrepp. Sökförbudet hindrar inte heller sökningar i syfte att få fram ett urval av personer grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller uppgifter som rör hälsa, sexualliv eller sexuell läggning, om sökningen görs i personuppgifter som inte har gjorts gemensamt tillgängliga i polisens datasystem.

Personuppgifter får enligt 2 kap. 7 § lämnas ut till Interpol, Europol eller en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol. Ett sådant utlämnande får ske endast om det är förenligt med svenska intressen och om mottagaren behöver uppgifterna för att utföra en uppgift som avses i 2 kap. 1 §.

Enligt 2 kap. 8 § har Polismyndigheten, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket, trots sekretessbestämmelser i offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 §, om den mottagande myndigheten behöver uppgifterna för ett syfte som anges i 1 kap. 2 § brottsdatalagen. Även Europeiska åklagarmyndigheten har rätt att ta del av sådana uppgifter. Bestämmelsen gäller inte uppgifter som behandlas i särskilda register enligt 5 kap. Samma myndigheter som nämns ovan har även rätt att ta del av uppgifter i biometriregister som förs enligt 5 kap., om den mottagande myndigheten behöver uppgifterna för ett syfte som anges i 1 kap. 2 § brottsdatalagen. Enligt 2 kap. 10 § har Migrationsverket rätt att ta del av uppgifter i biometriregister, om verket behöver uppgifterna för att kontrollera fingeravtryck som tagits där.

Enligt 2 kap. 13 § får uppgifter som tillhandahålls av transportföretag enligt 25 § polislagen behandlas för att förebygga, förhindra eller upptäcka brottslig verksamhet samt för att utreda eller förebygga brott. Sådana personuppgifter få endast i ett enskilt fall behandlas för nya ändamål enligt 2 kap. 4 eller 22 §§ brottsdatalagen. Av 2 kap. 14 § framgår att vid terminalåtkomst enligt 26 § polislagen får personuppgifterna inte ändras eller bearbetas på annat sätt.

Lagens tredje kapitel behandlar gemensamt tillgängliga uppgifter. Uppgifter som endast en särskilt avgränsad krets har rätt att ta del av anses inte som gemensamt tillgängliga. Kapitlet gäller inte när personuppgifter behandlas med stöd av 2 kap. 2 § brottsdatalagen.

Enligt 3 kap. 2 § får följande personuppgifter göras gemensamt tillgängliga:

1. Uppgifter som kan antas ha samband med misstänkt brottslig verksamhet, om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet.
2. Uppgifter som behövs för övervakningen av en person som
3. kan antas komma att begå brott för vilket det är föreskrivet fängelse i två år eller mer, och
4. är allvarligt kriminellt belastad eller kan antas utgöra ett hot mot andras personliga säkerhet.
5. Uppgifter som förekommer i ett ärende om utredning eller av lagföring av brott.
6. Uppgifter som förekommer i ett ärende om uppbörd.
7. Uppgifter som förekommer i ett ärende om kontaktförbud eller om personskydd.
8. Uppgifter som har rapporterats till Polismyndighetens ledningscentraler.
9. Uppgifter som behandlas i syfte att upprätthålla allmän ordning och säkerhet.
10. Uppgifter som behandlas i syfte att fullgöra internationella åtaganden, om det krävs för att den aktuella förpliktelsen ska kunna fullgöras.
11. Uppgifter som har samlats in genom kamerabevakning.

Dna-profiler får inte göras gemensamt tillgängliga. Att sådana uppgifter får behandlas i särskilda register följer av 5 kap. Tillgången till uppgifter som görs gemensamt tillgängliga med stöd av 3 kap. 2 § första stycket 2 ska begränsas till särskilt angivna tjänstemän som har till uppgift att arbeta med övervakningen. Information om att en person är föremål för övervakning får dock göras tillgänglig för

andra. Enligt 3 kap. § ska det framgå genom en särskild upplysning eller på något annat sätt om personuppgifter har gjorts gemensamt tillgängliga med stöd av 2 § första stycket 2 eller 6.

I 4 kap. finns bestämmelser om under hur lång tid personuppgifter får behandlas. Kapitlet gäller endast för automatiserad behandling. I 4 kap. § hänvisas till 2 kap. 17 § första stycket brottsdatalagen där det framgår att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

I 4 kap. 2 § anges att personuppgifter som inte har gjorts gemensamt tillgängliga inte får behandlas längre än ett år efter det att ärendet avslutades, om de behandlas i ett ärende, eller ett år efter det att de behandlades automatiserat första gången, om de inte kan hänföras till ett ärende. Detta gäller emellertid inte personuppgifter i ärenden om utredning av eller lagföring för brott.

Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott får, enligt 4 kap. 3 §, personuppgifter som finns i anmälan och som gjorts gemensamt tillgängliga inte längre behandlas för ändamål inom denna lags tillämpningsområde. Om en brottsanmälan i annat fall inte har lett till förundersökning eller annan motsvarande utredning, får personuppgifter som har gjorts gemensamt tillgängliga inte behandlas för ändamål inom lagens tillämpningsområde när åtal inte längre får väckas för brottet. Huvudregeln är alltså att uppgifter i en avskriven brottsanmälan ska kunna behandlas så länge det påstådda brottet inte är preskriberat. Fram till dess kan förundersökning inledas eller en nedlagd förundersökning återupptas, om det kommer fram nya omständigheter som kan leda till att brottet klaras upp. Om anmälan avskrivits på grund av att gärningen inte var ett brott får uppgifterna i anmälan inte behandlas vidare i den brottsutredande verksamheten.

Av 4 kap. 4 § framgår att om en förundersökning har lett till åtal eller annan domstolsprövning, får personuppgifter som finns i förundersökningen och som har gjorts gemensamt tillgängliga inte behandlas för ändamål inom lagens tillämpningsområde längre än fem år efter utgången av det kalenderår då domstolens avgörande fick laga kraft. Samma tidsperiod gäller för personuppgifter i en förundersökning som har lagts ner eller avslutats på annat sätt än genom åtal.

I lagen finns i övrigt bl.a. ytterligare bestämmelser om personuppgifter i ärende om uppbörd, övriga gemensamt tillgängliga uppgifter, rätt att meddela föreskrifter samt bestämmelser om register.

I mars 2026 tillsattes en utredning med uppdrag att se över Polismyndighetens behandling av personuppgifter.[51] Utredningen ska bl.a. undersöka i vilken dagens regelverk för behandling av personuppgifter på brottsdatalagens område försvårar en effektiv informationshantering inom myndighetens verksamhet och lämna förslag på hur personuppgifter kan behandlas på ett mer ändamålsenligt sätt.

4.7 Tullverkets behandling av personuppgifter inom brottsdatalagens område

Lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område gäller utöver brottsdatalagen när Tullverket i egenskap av behörig myndighet behandlar personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa uppbörd.

Regleringen liknar i stora delar motsvarande lag för Polismyndigheten. Utöver vad som anges för Polismyndigheten får Tullverket även lämna ut personuppgifter till en tullmyndighet eller kustbevakningsmyndighet inom Europeiska ekonomiska samarbetsområdet, under förutsättning att det är förenligt med svenska intressen.

I 2 kap. 10 § Tullverkets brottsdatalag anges att personuppgifter från transportföretag som lämnas till Tullverket enligt 7 kap. 12 § tullbefogenhetslagen får behandlas för att planera kontroller, välja ut kontrollobjekt och för att göra analyser som behövs för att uppdatera eller skapa nya kriterier som ska användas vid planering av kontroller eller urval av kontrollobjekt. Behandlingen ska ske som ett led i att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. Personuppgifterna får endast i ett enskilt fall behandlas för nya ändamål enligt 2 kap. 4 eller 22 §§ brottsdatalagen.

Enligt 11 § får Tullverket vid direktåtkomst enligt 7 kap. 12 § tullbefogenhetslagen inte ändra eller på annat sätt bearbeta uppgifterna. Av 12 § framgår att vid sökning i personuppgifter som avses i 10 § första stycket får namn, personnummer, samordningsnummer och

[51] Dir. 2026:17, *Polismyndighetens behandling av personuppgifter.*

andra liknande identitetsbeteckningar användas som sökbegrepp endast om uppgifterna avser en person som är eller har varit misstänkt för brott, är misstänkt för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 3 kap. 2 § första stycket 1 eller övervakas under de förutsättningar som anges i 3 kap. 2 § första stycket 2.

I 3 kap. 2 § anges vilka personuppgifter som får göras gemensamt tillgängliga. Enligt första stycket 1 gäller det uppgifter som kan antas ha samband med misstänkt brottslig verksamhet, om den misstänkta innefattar brott för vilket det är föreskrivet fängelse i ett år eller mer, eller om den misstänkta verksamheten sker systematiskt. I samma paragraf första stycket 2 anges att uppgifter som behövs för övervakningen av en person som kan antas komma att begå brott för vilket det är föreskrivet fängelse i två år eller mer och är allvarligt kriminellt belastad får göras gemensamt tillgängliga. I första stycket 3 anges vidare att uppgifter från transportföretag som behandlas enligt 2 kap. 10 § får göras gemensamt tillgängliga.

I 3 kap. 2 § tredje stycket anges att tillgången till uppgifter som görs gemensamt tillgängliga med stöd av första stycket 2 ska begränsas till särskilt angivna tjänstemän som har till uppgift att arbeta med övervakningen. Information om att en person är föremål för övervakning får dock göras tillgänglig för andra.

Enligt bestämmelsens fjärde stycke ska tillgången till uppgifter som görs gemensamt tillgängliga med stöd av första stycket 3 begränsas till särskilt angivna tjänstemän som har sådana uppgifter som anges i 2 kap. 10 § första stycket. Endast om det behövs i ett enskilt fall får uppgifterna göras tillgängliga för andra.

4.8 Säpodatalagen

4.8.1 Nuvarande reglering

EU:s dataskyddsförordning och dataskyddsdirektiv omfattar inte personuppgiftsbehandling som utförs som ett led i en verksamhet som inte omfattas av unionsrätten, såsom verksamhet rörande nationell säkerhet. Säkerhetspolisens personuppgiftsbehandling regleras i säpodatalagen[52] och förordningen (2019:1235) om Säkerhetspolisens behandling av personuppgifter. I april 2025 publicerades ett betän-

[52] Lag (2019:1182) om Säkerhetspolisens behandling av personuppgifter.

kande av Utredningen om Säkerhetspolisens informationshantering där det föreslås en reform av säpodatalagen.[53] I avsnitt 4.8.2 redogörs för de stora dragen i den föreslagna reformen.

Av 1 kap. 1 § säpodatalagen framgår att syftet med lagen är att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av personuppgifter och att säkerställa att Säkerhetspolisen kan behandla och utbyta personuppgifter på ett ändamålsenligt sätt.

Enligt 1 kap. 2 § gäller lagen vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet samt i tillämpliga delar vid Polismyndighetens behandling av personuppgifter när myndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen. Säkerhetspolisens verksamhet rör i princip uteslutande nationell säkerhet.

De tillåtna rättsliga grunderna för behandling av personuppgifter framgår av 2 kap. 1 §. Enligt bestämmelsen får personuppgifter behandlas om det är nödvändigt för att utföra en arbetsuppgift i vissa där angivna syften, t.ex. för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet, terrorbrott eller tryckfrihets- eller yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv. Personuppgifter får också behandlas bl.a. om det är nödvändigt för att utreda eller lagföra nyss nämnda brott, för att fullgöra uppgifter i samband med visst personskydd, uppgifter enligt säkerhetsskyddslagen (2018:585) eller uppgifter enligt utlännings- och medborgarskapslagstiftningen. Av bestämmelsen framgår också att de arbetsuppgifter som avses ska framgå av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift. Personuppgifter får även behandlas för att fullgöra förpliktelser som följer av internationella åtaganden.

Principen om ändamålsbegränsning kommer till uttryck i 2 kap. 3 §. Personuppgifter får inte behandlas för något ändamål som är oförenligt med det ändamål för vilket personuppgifterna ursprungligen behandlades. Principerna om laglighet, korrekthet, uppgifts- och lagringsminimering överensstämmer i princip med brottsdatalagens bestämmelser och finns i 2 kap. 6 och 8 §§ respektive 4 kap. 1 § säpodatalagen.

[53] SOU 2025:49, *Säkerhetspolisens behandling av personuppgifter*.

Principen om ansvarsskyldighet finns i 5 kap. 1 §. Bestämmelserna om inbyggt dataskydd, dataskydd som standard, loggning och tjänstemäns tillgång till personuppgifter finns i lagens 5 kap. 2–5 §§ respektive 4 kap. 5 § i tillhörande förordning. Bestämmelserna om konsekvensbedömningar och dess dokumentation samt förhandssamråd finns i lagens 5 kap. 6 § och 4 kap. 6 § i dess tillhörande förordning.

Bestämmelser om skyldigheten att vidta lämpliga tekniska och organisatoriska åtgärder finns i 5 kap. 7 § och skyldigheten att upprätta en förteckning över de kategorier av behandlingar m.m. som utförs finns i 4 kap. 4 § förordningen. Av 6 kap. 1 § säpodatalagen framgår att Säkerhetspolisen, på samma sätt som enligt brottsdatalagen, ska göra viss allmän information tillgänglig för den registrerade. I 6 kap. 2 § finns bestämmelser om den registrerades rätt till registerutdrag och i 6 kap. 6 och 7 §§ om den registrerades rätt att under vissa förutsättningar begära rättelse, komplettering eller radering av personuppgifter. Samtliga ovan nämnda bestämmelser motsvarar brottsdatalagens.

Både IMY och Myndigheten för säkerhet och integritetsskydd är tillsynsmyndigheter enligt säpodatalagen.[54] Av 7 kap. 1 § säpodatalagen framgår att den myndighet som utövar tillsyn enligt den lagen ska utöva allmän tillsyn över personuppgiftsbehandling och ge råd och stöd till Säkerhetspolisen om dess skyldigheter enligt lag eller annan författning vid förhandssamråd eller när det i övrigt är påkallat. Med undantag för sanktionsavgifter har tillsynsmyndigheten samma befogenheter som enligt brottsdatalagen, vilket framgår av 7 kap. 3–5 §§. I 8 kap. 1 § finns även en bestämmelse om skadestånd till den registrerade som motsvarar brottsdatalagens.

4.8.2 Ny säpodatalag

I maj 2023 beslutade regeringen att tillsätta en utredning med uppdrag att göra en översyn av de bestämmelser som reglerar Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet. I betänkandet[55], som publicerades i april 2025, konstateras att den nuvarande lagstiftningen inte är anpassad till Säkerhetspolisens verksamhet eller till dagens informationsmängder. Säkerhetspolisen intar en särställ-

[54] Jfr 2 a § förordning med instruktion för Integritetsskyddsmyndigheten och 1 § lagen om tillsyn över viss brottsbekämpande verksamhet.
[55] SOU 2025:49, *Säkerhetspolisens behandling av personuppgifter*.

ning inom brottsbekämpningen i och med uppdraget som nationell säkerhetstjänst. Brottsutredande verksamhet utgör endast en liten del av uppdraget. Trots de stora skillnaderna i myndigheternas uppdrag, mål och metoder har Säkerhetspolisen i stora delar identisk lagstiftning vad gäller behandling av personuppgifter som övriga brottsbekämpande myndigheter.

Den nuvarande säpodatalagen medför att varje enskild personuppgift ska granskas och bedömas för sig för att få behandlas. Det innebär att Säkerhetspolisen avstår från att hämta in uppgifter som i och för sig behövs för verksamheten. I betänkandet belyses ett flertal tydliga begränsningar i nuvarande regelverk: krav på konkret behov och ändamål för varje enskild personuppgift, krav på att alla känsliga personuppgifter ska identifieras och prövas för sig, för kort längsta tid för behandling med hänsyn till myndighetens uppdrag samt begränsad möjlighet att behandla referensdatabaser eller utveckla moderna tekniska verktyg såsom AI.

I betänkandet föreslås att proportionalitetsprincipen ska införas som grundläggande krav, dvs. varje behandlingsåtgärd måste vara proportionerlig i förhållande till ändamålet och intrånget i den enskildes fri- och rättigheter. Reglerna för ändamål, behov och behandlingstider bör göras mer flexibla för att bättre motsvara hur en underrättelse- och säkerhetstjänst faktiskt fungerar. Även till synes perifer information ska kunna sparas över tid när den förekommer i relevanta sammanhang, eftersom sådan information kan visa sig avgörande för att upptäcka säkerhetshot.

Lagen ska ha en teknikneutral utformning som möjliggör användning av moderna tekniker samtidigt som riskerna med dessa begränsas genom robusta skyddsmekanismer.

Tillsynen ska vara systemorienterad snarare än att utövas av behandlingen av enskilda personuppgifter. Detta ger en mer effektiv och realistisk tillsyn av stora informationsmängder.

Som ett komplement till säpodatalagen föreslås en särskild lag anpassad för behandling av stora informationsmängder. Lagen innebär ett proportionerligt undantag från vissa dataskyddsprinciper, vilket bedöms nödvändigt för att skydda nationell säkerhet. Säkerhetspolisen ges ökade möjligheter att behandla stora mängder information och även uppgifter som inte direkt behövs för uppdraget men som förekommer i sammanhang som är befogade att behandla.

I betänkandet införs begreppet *inledande behandling*, vilket exempelvis avser insamling och inhämtning. Det ställs lägre krav på för inledande behandling än annan behandling. Efter den inledande behandlingen regleras hur uppgifterna ska *granskas* för att säkerställa att de får fortsätta behandlas enligt högre krav. Fortsatt behandling får ske om det behövs för ett särskilt, uttryckligt angivet och berättigat ändamål. Kraven på adekvans, relevans och uppgiftsminimering bibehålls, men tillämpas inte före det att uppgifterna kunnat granskas.

Teknikutveckling tillåts uttryckligen som ändamål för personuppgiftsbehandling, men uppgifter som samlats in enbart för detta ändamål får inte användas operativt. Automatiserat beslutsfattande förbjuds om det har betydande påverkan på den enskilde.

För att motverka riskerna med utökade möjligheter att behandla personuppgifter föreslås förstärkta mekanismer för tillsyn och kontroll med omfattande krav på förhandsbedömning av domstol när det gäller framtagning av uppgifter som är registrerade i en särskild uppgiftssamling. Tillsynsmyndigheterna ges även utökade befogenheter och resurser, vilket bidrar till att upprätthålla rättssäkerheten och det allmänna förtroende för Säkerhetspolisens personuppgiftsbehandling.

4.9 Behandling av personuppgifter vid Försvarsmakten

Syftet med lagen (2021:1171) om behandling av personuppgifter vid Försvarsmakten är enligt 1 kap. 1 § att säkerställa att Försvarsmakten kan behandla personuppgifter på ett ändamålsenligt sätt och att skydda fysiska personers grundläggande fri- och rättigheter i samband med sådan behandling. Enligt 1 kap. 2 § gäller lagen vid Försvarsmaktens behandling av personuppgifter i verksamhet som rör Sveriges försvar och säkerhet samt internationellt försvars- och säkerhetsarbete.

I lagens andra kapitel uppställs grundläggande krav på behandlingen av personuppgifter. Enligt 2 kap. 1 § får personuppgifter bara behandlas för särskilda, uttryckligt angivna och berättigade ändamål och de får inte behandlas för något ändamål som är oförenligt med det ändamål som de ursprungligen behandlades för.

I 2 kap. 2 § anges att Försvarsmakten får behandla personuppgifter om det är nödvändigt för att planera, förbereda och genomföra verksamhet som rör Sveriges försvar och säkerhet, eller internationellt

försvars- och säkerhetsarbete. Försvarsmaktens uppgift att bedriva sådan verksamhet som anges i första stycket ska följa av lag, förordning, kollektivavtal eller annat avtal, eller ett särskilt beslut där regeringen har gett myndigheten i uppdrag att utföra uppgiften.

I 2 kap. 3–4 §§ berörs personuppgiftsbehandlingen inom försvarsunderrättelverksamheten. Personuppgifter får behandlas i Försvarsmaktens försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet. De uppgifter som Försvarsmakten har fått tillgång till i sådan verksamhet får fortsätta behandlas i den verksamheten, om det behövs för att fullgöra den. Detta gäller dock endast om inte något annat följer av denna lag eller en förordning som regeringen har meddelat i anslutning till lagen.

Personuppgiftsbehandlingen inom den militära säkerhetstjänsten regleras i 2 kap. 5–8 §§. Personuppgifter får behandlas i Försvarsmaktens militära säkerhetstjänst för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen, om det är nödvändigt för att klarlägga verksamhet som innefattar hot mot Sveriges säkerhet, eller vidta åtgärder för hindrar eller försvårar säkerhetshotande verksamhet. I 2 kap. 6 § anges närmare förutsättningar för personuppgiftsbehandlingen inom den militära säkerhetstjänsten.

Känsliga personuppgifter, dvs. uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller uppgifter som rör hälsa, sexualliv eller sexuell läggning, får enligt 2 kap. 15 § inte behandlas. När personuppgifter behandlas får de dock kompletteras med känsliga personuppgifter, om det är absolut nödvändigt med hänsyn till ändamålen med behandlingen. Enligt 2 kap. 17 § får känsliga personuppgifter och biometriska uppgifter användas som sökbegrepp om det är absolut nödvändigt med hänsyn till ändamålen med behandlingen.

I enlighet med 2 kap. 21 § får personuppgifter inte behandlas under längre tid än som behövs med hänsyn till ändamålen med behandlingen. Regeringen eller den myndighet som regeringen bestämmer kan meddela förskrifter om att personuppgifter får behandlas under endast viss tid eller fortsätta behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål.

I kap. 3–7 finns bestämmelser om gemensamt tillgängliga personuppgifter, skyldigheter som personuppgiftsansvarig, enskildas rättigheter, tillsyn samt skadestånd och överklagande.

5 Reglering av passageraruppgifter i brottsbekämpningen

5.1 Inledning

Under en längre tid har terrorism och våldsbejakande extremism utgjort ett hot mot säkerheten inom EU. Geopolitiska spänningar och digital utveckling har lett till att hoten har ökat i komplexitet.[1] Detsamma gäller för annan gränsöverskridande brottslighet.

En grundsten inom EU är den fria rörligheten för personer, varor, kapital och tjänster. Unionen är präglad av öppenhet och samarbete. EU:s öppna gränser underlättar emellertid även för kriminella att hitta det mest lönsamma landet att begå brott i samt att undvika lagföring för begångna brott. Den organiserade brottsligheten kan således välja de länder och rutter i EU som maximerar vinsterna och minimerar riskerna.[2] Kostnaderna för den organiserade brottsligheten uppskattas uppgå till minst en procent av EU:s totala BNP.[3]

Samarbetet mellan EU:s medlemsstater för att bekämpa gränsöverskridande brottslighet inleddes i blygsam skala på 1970-talet och har utökats efter hand. De allvarliga samhälleliga effekterna har medfört att kampen mot sådan brottslighet i dagsläget står högt upp på EU:s agenda.

Det framstår som oklart vad som fungerar väl på lång sikt. Olika strategier kan krävas för *akuta* brottsbekämpande insatser som leder till att någon lagförs och för *långsiktig* reducering av organiserad brottslighet som fenomen.[4] EU har under flera decennier initierat

[1] Europol, *European Union Terrorism Situation and Trend Report*, 2025.
[2] Svenska institutet för europapolitiska studier, *Gränsöverskridande organiserad brottslighet i EU*, 2024:3, s. 6.
[3] Svenska institutet för europapolitiska studier, *Gränsöverskridande organiserad brottslighet i EU*, 2024:3, s. 9.
[4] Svenska institutet för europapolitiska studier, *Gränsöverskridande organiserad brottslighet i EU*, 2024:3, s. 7.

en rad olika åtgärder, lagar, konventioner, byråer och organ just för att förenkla samarbetet över gränserna. Dessa initiativ utvärderas sällan och det är oklart vilka effekter det har på den organiserade brottsligheten.

EU har inte exklusiva befogenheter på området utan rättsväsendet anses vara en viktig nationell angelägenhet. Det sker dock en rad gränsöverskridande samarbeten och det finns lagstiftning som alla länder har antagit. En stor utmaning på området är att den organiserade brottsligheten är spänstig och snabb medan EU är byråkratiskt och kräver stor samstämmighet, vilket innebär en viss tröghet i systemet.[5]

En annan utmaning för både EU och de enskilda medlemsstaterna är skyddet för den personliga integriteten. All personuppgiftshantering på området innebär en avvägning mellan individens integritet och effektiv brottsbekämpning.

I detta avsnitt redogör vi för den befintliga lagstiftningen som rör passageraruppgifter i brottsbekämpningen, såväl i svensk som internationell rätt.

5.2 PNR-direktivet

5.2.1 Allmänt om direktivet

Den 27 april 2016 antog Europaparlamentet och rådet direktiv (EU) 2016/681 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet, i allmänhet benämnt som (PNR-direktivet).

PNR är en förkortning av den engelska benämningen *Passenger Name Record*. Detta översätts till svenska som passageraruppgiftssamling eller PNR-uppgifter. De uppgifter som avses är de personuppgifter som lämnas av passagerare och samlas in och sparas av lufttrafikbolag. Det rör sig om bl.a. passagerarens namn, resdatum, resväg, sittplats, bagage, kontaktuppgifter och betalningsmedel. Redan innan direktivet trädde i kraft samlade lufttrafikbolagen in sådana uppgifter om passagerarna för sina egna operativa och kommersiella syften. Direktivet ålägger inte lufttrafikbolagen någon skyldighet att samla

[5] Svenska institutet för europapolitiska studier, *Gränsöverskridande organiserad brottslighet i EU*, 2024:3, s. 7.

in uppgifter, utan reglerar skyldigheten för bolagen att överföra de redan insamlade uppgifterna till enheter för passagerarinformation i medlemsstaterna.

Syftet med direktivet är bl.a. att trygga säkerheten, skydda personers liv och säkerhet samt att inrätta en rättslig ram till skydd för PNR-uppgifter vid behöriga myndigheters behandling av uppgifterna. Direktivet utgör ett komplement till andra instrument i bekämpandet av gränsöverskridande brottslighet. Genom att behandla PNR-uppgifter ges brottsbekämpande myndigheter möjlighet att, utöver att identifiera sedan tidigare kända personer, även identifiera personer som tidigare varit okända men som efter en specifik analys av uppgifterna visar sig utgöra en potentiell risk.

5.2.2 Bakgrund

Under de senaste decennierna har terroristattentat lett till nya initiativ för att förbättra säkerheten. Samtidigt har den internationella organiserade brottsligheten ökat.[6] Terrorism och organiserad brottslighet inbegriper ofta internationella resor. Som en följd av detta har brottsbekämpande myndigheter i flera länder i allt större utsträckning börjat samla in och analysera uppgifter avseende resande i syfte att bekämpa terrorism och grov brottslighet.

PNR-uppgifter har använts i cirka 75 år, främst av tullmyndigheter men också till viss del av andra brottsbekämpande myndigheter.[7] I Sverige har uppgifterna använts av Tullverket på Arlanda sedan början av 1990-talet. Inledningsvis förekom endast manuell behandling av uppgifterna. I och med genomförandet av PNR-direktivet har PNR-uppgifter fått en betydligt större roll i brottsbekämpningen inom EU.

Många länder utanför EU har i dag särskilda system för inhämtande och analys av PNR-uppgifter. Efter terroristattentaten den 11 september 2001 antog USA lagstiftning som innebär att lufttrafikföretag med trafik till, från eller genom dess territorium ska tillhandahålla de amerikanska myndigheterna PNR-uppgifter. Flera andra länder har därefter infört liknande system.

[6] Europol, *European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime*, 2025.
[7] KOM (2010) 492 slutlig av den 21 september 2010, s. 2.

5.2.3 Innehåll

PNR-direktivet innehåller 22 artiklar fördelade över fyra kapitel. I artikel 1 anges syftet och tillämpningsområdet för direktivet. Artikelns andra punkt stadgar att PNR-uppgifter som samlas in i enlighet med direktivet endast får behandlas i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet.

Direktivet är bindande avseende flygningar utanför EU. Artikel 2 ger medlemsstaterna möjlighet att även tillämpa direktivet på flygningar inom EU. En medlemsstat som väljer en sådan tillämpning ska meddela detta till kommissionen. Det är även möjligt att endast tillämpa direktivet på valda flygningar inom EU. När en medlemsstat fattar ett sådant beslut ska den välja de flygningar som den anser vara nödvändiga för att efterfölja målen för direktivet. Medlemsstaten får när som helst besluta att ändra urvalet av flygningar inom EU.

I artikel 3 definieras centrala begrepp i direktivet. Med *lufttrafikföretag* menas ett företag med giltig operativ licens eller motsvarande som ger rätt att bedriva passagerarflygtrafik. Med *flygningar utanför EU* avses varje flygning som utförs av ett sådant lufttrafikföretag, med avgång från ett tredjeland och planerad landning på en medlemsstats territorium eller en flygning från en medlemsstats territorium med planerad landning i ett tredjeland. *Passagerare* är en person som transporteras eller ska transporteras med ett flygplan med lufttrafikföretagets godkännande. Ett sådant godkännande framgår av att personen står med på passagerarförteckningen.

Passageraruppgiftssamling eller *PNR-uppgifter* är en sammanställning av för resan nödvändiga uppgifter om varje enskild passagerare som gör det möjligt för lufttrafikföretaget att behandla och kontrollera reservationen för varje resa som bokas av en person eller för en persons räkning.

Enligt artikel 4 ska varje medlemsstat inrätta en myndighet eller en avdelning inom en myndighet med behörighet att bekämpa terroristbrott och grov brottslighet, vilken ska fungera som medlemsstatens enhet för passagerarinformation. Enheten för passagerarinformation, även kallad *PIU* efter engelskans *Passenger Information Unit*, ska ansvara för att samla in PNR-uppgifter från lufttrafikföretagen, lagra och behandla uppgifterna samt överföra uppgifterna eller resultatet av behandlingen av dem till behöriga myndigheter. Enheten för passa-

gerarinformation ska även utbyta uppgifter med andra medlemsstaters motsvarande enheter och med Europol.

I artikel 5 anges att medlemsstatens enhet för passagerarinformation ska utse ett dataskyddsombud som ska ansvara för övervakningen av behandlingen av PNR-uppgifter och för genomförandet av relevanta skyddsåtgärder. En registrerad har rätt att kontakta dataskyddsombudet i alla frågor som rör behandlingen av dennes PNR-uppgifter.

Artikel 6 rör behandlingen av PNR-uppgifter och ställer upp de tillåtna ändamål för vilka enheten för passagerarinformation får utföra sådan behandling. Enheten ska enbart behandla PNR-uppgifter för vissa uppräknade ändamål. Bland de tillåtna ändamålen kan nämnas att behandling är tillåten för att göra en bedömning av passagerare före deras beräknade ankomst till eller avresa från en medlemsstat, för att identifiera personer som de behöriga myndigheterna eller Europol behöver utreda ytterligare på grund av att dessa personer kan vara inblandade i terroristbrott eller grov brottslighet. Enheten för passagerarinformation ska vidare besvara en motiverad förfrågan från en behörig myndighet om att tillhandahålla och behandla PNR-uppgifter i specifika fall. Slutligen ska enheten för passagerarinformation analysera PNR-uppgifter för att uppdatera och skapa nya kriterier som ska användas vid de bedömningar som genomförs i syfte att identifiera personer som kan vara delaktiga i terroristbrott eller grov brottslighet.

En bedömning av en passagerare före planerad ankomst till eller avresa från en medlemsstat ska ske utifrån på förhand fastställda kriterier och på ett icke-diskriminerande sätt. Kriterierna måste vara riktade, proportionella och specifika. Dessa kriterier ska fastställas och regelbundet ses över av medlemsstatens enhet för passagerarinformation. Kriterierna får under inga omständigheter vara baserade på en persons ras, etniska ursprung, politiska åskådning, religiösa eller filosofiska övertygelse, fackföreningstillhörighet, hälsotillstånd, sexualliv eller sexuella läggning.

Den inledande behandlingen av PNR-uppgifter vid enheten för passagerarinformation sker automatiskt utifrån de fastställda kriterierna. Därefter ska dock de eventuella träffarna som tagits fram genom den automatiska behandlingen granskas individuellt med icke-automatiska metoder för att verifiera om en behörig myndighet behöver vidta åtgärder enligt nationell rätt.

Enligt artikel 7 ska varje medlemsstat fastställa en förteckning över de behöriga myndigheter som har befogenhet att begära eller

motta PNR-uppgifter från enheten för passagerarinformation för vidare granskning av informationen. Dessa myndigheter ska vara behöriga att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet. De svenska behöriga myndigheterna är enligt 3 § förordningen om flygpassageraruppgifter i brottsbekämpningen Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Tullverket och Försvarsmakten.

Artikel 8 berör lufttrafikföretagens skyldigheter när det gäller överföring av uppgifter. Företagen ska överföra PNR-uppgifter till databasen hos enheten för passagerarinformation i den medlemsstat på vars territorium flygningen kommer att avgå eller ankomma. Direktivet uppställer ingen skyldighet för lufttrafikföretagen att samla in viss information, utan överföringen av uppgifter sker under förutsättning att sådana uppgifter redan samlas in. I bilaga I till direktivet anges vilka PNR-uppgifter som ska överföras. Lufttrafikföretagen ska normalt överföra uppgifterna 24–48 timmar före flygningens planerade avgång samt omedelbart efter att gaten har stängts.

Formerna för utbyte av information mellan medlemsstaterna behandlas i artikel 9. När en person identifieras av en enhet för passagerarinformation i enlighet med artikel 6.2 ska alla relevanta och nödvändiga PNR-uppgifter eller resultaten av en eventuell behandling av dessa uppgifter översändas till motsvarande enheter i de andra medlemsstaterna. Överföring av uppgifter mellan medlemsstater kan ske självmant och på begäran. Villkoren för Europols åtkomst till PNR-uppgifter anges i artikel 10. När det gäller överföring av uppgifter till tredjeländer får detta ske endast under de förutsättningar som anges i artikel 11.

I artikel 12 anges att PNR-uppgifterna ska lagras hos enheten för passagerarinformation under en period på fem år efter överföringen till enheten i den medlemsstat på vars territorium flygningen ankom eller avgick. Därefter ska uppgifterna slutligt raderas. Efter sex månader ska alla PNR-uppgifter avidentifieras genom maskering av vissa uppräknade uppgifter som kan användas för att omedelbart identifiera de passagerare som uppgifterna avser. Vid utgången av sexmånadersperioden ska utlämnande av de fullständiga PNR-uppgifterna tillåtas endast om det rimligen kan anses vara nödvändigt för de ändamål som avses i artikel 6.2, och efter tillstånd från en rättslig myndighet eller en annan nationell myndighet som i enlighet med

nationell rätt är behörig att kontrollera om villkoren för tillgång är uppfyllda.

I svensk rätt regleras frågan om prövning av en rättslig eller annan myndighet i 4 kap. 11 § lagen om flygpassageraruppgifter i brottsbekämpningen. Där anges att om en förundersökning pågår ska en begäran från en behörig myndighet om att överföra behörighetsbegränsade uppgifter i deras helhet beslutas av en åklagare. I övriga fall, dvs. när en förundersökning inte pågår, krävs det att tillstånd har lämnats av Polismyndigheten.

Artikel 13 innehåller bestämmelser om skydd av personuppgifter. Medlemsstaterna ska föreskriva att alla passagerare vid all behandling av personuppgifter i enlighet med direktivet har rätt till samma skydd av sina personuppgifter, rätt till åtkomst, rättelse, radering och begränsning samt rätt till ersättning och tillgång till rättsmedel som fastställs i unionsrätten och nationell rätt och för genomförande av vissa artiklar i rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete. Vidare finns i artikel 13 dataskyddsbestämmelser om bl.a. förbud mot behandling av känsliga personuppgifter, regler om loggning, informationssäkerhet m.m.

Enligt artikel 14 ska medlemsstaterna fastställa regler om effektiva, proportionella och avskräckande sanktioner för överträdelse av nationella bestämmelser som antagits i enlighet med direktivet och vidta alla nödvändiga åtgärder för att se till att de genomförs. Det ska särskilt fastställas sanktioner mot lufttrafikföretag som inte översänder uppgifter i enlighet med artikel 8 i direktivet eller som inte översänder uppgifter i det fastställda formatet.

I artikel 15 anges att medlemsstaterna ska föreskriva att den nationella tillsynsmyndighet som avses i artikel 25 i rambeslut 2008/977/RIF ska ansvara för att ge riktlinjer för och övervaka tillämpningen av de bestämmelser som medlemsstaterna antar i enlighet med PNR-direktivet. Den nationella tillsynsmyndigheten ska utföra sina uppgifter i syfte att skydda grundläggande rättigheter i samband med behandling av personuppgifter. Tillsynsmyndigheten ska hantera klagomål från en registrerad och inom rimlig tid informera de registrerade om förloppet för och resultatet av dennes klagomål. Utöver detta ska tillsynsmyndigheten kontrollera att uppgiftsbehandlingen är laglig, genomföra utredningar, inspektioner och revisioner i enlighet med nationell rätt samt, på begäran, ge registrerade råd om

hur de kan utöva de rättigheter som fastställs i de bestämmelser som antas i enlighet med detta direktiv.

I svensk rätt är Integritetsskyddsmyndigheten, enligt 2 a § förordningen med instruktion för Integritetsskyddsmyndigheten, tillsynsmyndighet.

Direktivets tredje kapitel innehåller genomförandeåtgärder. Enligt artikel 16 ska all överföring av PNR-uppgifter från lufttrafikföretag till enheter för passagerarinformation göras med elektroniska medel som tillhandahåller tillräckliga garantier med avseende på den behandling som ska utföras. Gemensamma protokoll och understödda dataformat för detta ändamål ska antas av kommissionen. Enligt artikel 17 ska kommissionen biträdas av en kommitté.

Artikel 18–22 innehåller bestämmelser om införlivande, översyn, statistik, förhållande till andra bilaterala eller multilaterala avtal eller andra instrument samt ikraftträdande.

5.2.4 Överenskommelser i anledning av direktivet

PNR-direktivet ålägger lufttrafikföretag att överföra PNR-uppgifter för samtliga passagerare på flygningar som anländer från eller avgår till ett land utanför EU. Artikel 2 i direktivet ger medlemsstaterna möjlighet att på frivillig grund även tillämpa direktivet på flygningar inom EU. I deklarationen[8] som antogs av rådet i samband med antagandet av PNR-direktivet har Sverige och övriga medlemsstater förklarat att de, mot bakgrund av det aktuella säkerhetsläget i Europa, fullt ut kommer att utnyttja denna möjlighet.

I deklarationen har medlemsstaterna även förklarat att de, i enlighet med parlamentets önskemål, åtar sig att i enlighet med sin nationella lagstiftning och med förbehåll för parlamentsbehandling i vissa medlemsstater, utvidga insamlingen av PNR-uppgifter till att även omfatta aktörer som inte är lufttrafikföretag, t.ex. resebyråer och researrangörer som tillhandahåller reserelaterade tjänster, inklusive bokning av flygningar, för vilka sådana uppgifter samlas in och behandlas. Någon tidsgräns för när detta ska vara genomfört i nationell lagstiftning är inte angivet.

[8] Europeiska rådets uttalande avseende ärendet Utkast till Europaparlamentets och rådets direktiv om användning av passageraruppgiftssamlingar (PNR) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (första behandlingen), 7829/16 ADD 1, den 18 april 2016.

5.2.5 Kommissionens översyn av PNR-direktivet

Europeiska kommissionen publicerade den 24 juli 2020 en rapport med en översyn av PNR-direktivet.[9] Rapporten publicerades därmed innan PNR-domen meddelades i juni 2022. Det pågår en ny översyn av tillämpningen av direktivet som kommer att avslutas under 2026.

Rapporten publiceras i enlighet med artikel 19 i PNR-direktivet där det anges att kommissionen senast den 25 maj 2020 ska göra en översyn av samtliga delar av direktivet och överlämna och lägga fram en rapport för Europaparlamentet och rådet. Översynen skulle göras på grundval av information som medlemsstaterna tillhandahållit och bl.a. lägga särskild vikt vid efterlevnaden av de tillämpliga standarderna för skydd av personuppgifter, nödvändigheten och proportionaliteten i insamlingen och behandlingen av PNR-uppgifter samt längden på den period som uppgifterna lagras. Rapporten skulle också innefatta en översyn av nödvändigheten, proportionaliteten och ändamålsenligheten i att i direktivets tillämpningsområde inbegripa obligatorisk insamling och överföring av PNR-uppgifter avseende samtliga eller utvalda flygningar inom EU.

Mot bakgrund av den översyn som genomförs ska kommissionen om lämpligt lägga fram ett lagstiftningsförslag för Europaparlamentet och rådet i syfte att ändra direktivet.

I rapporten framförs att ett flertal länder, även länder utanför EU, under senare år har noterat värdet av att använda PNR-information som ett verktyg i brottsbekämpningen. Vid tiden för rapporten hade 24 medlemsstater till fullo genomfört direktivet i nationell rätt. En stor majoritet av medlemsstaterna hade etablerat fullt fungerande enheter för passagerarinformation, som i sin tur hade etablerat samarbeten med de behöriga myndigheterna och enheter för passagerarinformation i andra medlemsstater. Alla medlemsstater hade möjliggjort för de behöriga myndigheterna att begära information från enheten för passagerarinformation endast i syfte att hindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet.

Även om vissa medlemsstater inte fullt ut har genomfört direktivets krav på dataskydd pekar kommissionens analys på att medlemsstaterna generellt sett uppfyller kraven. Detta gäller både genomföran-

[9] Report from the Commission to the European Parliament and the Council On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, (SWD(2020) 128 final, den 24 juli 2020.

det i lagstiftningen och tillämpningen i praktiken. Kommissionen kommer att fortsätta övervaka följsamheten till direktivets krav och inleda rättsliga processer mot de medlemsstater som inte genomför direktivet eller inte lever upp till dess krav.

Samarbetet mellan enheterna för passagerarinformation och deras dataskyddsombud förefaller fungera väl. Dataskyddsombuden är värdefulla för det operativa arbetet som enheterna utför, särskild när det gäller övervakning av behandlingen av uppgifter, godkännande av förbestämda kriterier samt rådgivning angående dataskydd till personalen vid enheterna. I de flesta medlemsstater fungerar dataskyddsombuden som kontaktpunkt för enskilda som vill ha information om behandlingen av personuppgifter.

Översynen åskådliggör flera faktorer som bekräftar att insamlingen och behandlingen av PNR-uppgifter för de syften som anges i direktivet är nödvändig och proportionerlig. PNR-systemet har visat sig vara effektivt för att uppnå syftena, dvs. att skydda allmän säkerhet genom att förhindra, upptäcka, utreda och lagföra terroristbrott och annan grov brottslighet inom unionens territorium.

Enligt medlemsstaterna har behandlingen av PNR-information redan gett påtagliga resultat i kampen mot terrorism och brott. Medlemsstaterna har till kommissionen lämnat in bevis som illustrerar hur behandling av PNR-information har bidragit till identifiering av potentiella terrorister eller personer som är inblandade i andra kriminella aktiviteter, t.ex. narkotikasmuggling, sexuellt utnyttjande av barn, bortförande av barn och deltagande i organiserad brottslighet. I vissa fall har PNR-information lett till gripanden av personer som tidigare varit okända för brottsbekämpande myndigheter och möjliggjort ytterligare granskning av passagerare som tidigare inte hade uppmärksammats. Bedömningen av passagerare innan avgång eller ankomst har även inneburit att brott har kunnat förhindras. Nationella myndigheter understryker att dessa resultat inte hade kunnat uppnås utan PNR-information, genom att enbart använda andra verktyg som exempelvis API-information.

Utvärderingen visar att behandlingen av PNR-information om alla flygningar som korsar EU:s yttre gränser är strikt nödvändig för att uppnå direktivets mål.

PNR-direktivet förbjuder behandling av känsliga personuppgifter. Den information som behandlas rör en specifik aspekt av en persons privatliv, nämligen flygresor. Utöver detta innehåller direktivet strikta

regler för att ytterligare begränsa graden av inskränkning av grundläggande fri- och rättigheter till ett absolut minimum. De personuppgifter som överförs till behöriga myndigheter för vidare behandling avser en väldigt begränsad krets av enskilda personer.

Lagringen av PNR-information under fem år för alla passagerare är nödvändig för att uppnå målen avseende säkerhet och skydd för människor genom att beivra terroristbrott och annan grov brottslighet. Behovet att lagra uppgifter beror på PNR-systemets karaktär, dvs. att det är ett analytiskt verktyg som syftar till att både identifiera kända hot och att upptäcka okända risker. PNR-uppgifter används för att identifiera resmönster och för att göra kopplingar mellan kända och okända personer. Det ligger i sakens natur att det krävs långsiktig analys för att upptäcka sådana kopplingar. Det krävs vidare en tillräckligt omfattande databas för sådan analys.

Lagringen under fem år krävs också för att på ett effektivt sätt kunna utreda och lagföra terroristbrott och andra grova brott. En sådan process tar ofta månader, ibland år att genomföra. Detta bekräftas av medlemsstaterna som uppger att en femårsperiod är nödvändig ur operativ synvinkel. Skyddet för personuppgifter, t.ex. genom att behörighetsbegränsa uppgifterna, har visat sig vara tillräckligt robust för att förebygga missbruk.

Samarbetet och utbytet av PNR-uppgifter mellan medlemsstaternas enheter för passagerarinformation har varit en av de viktigaste aspekterna i direktivet. Överföringen av information efter en motiverad förfrågan från en annan medlemsstats enhet fungerar effektivt, medan överföring på en enhets egna initiativ är mindre vanligt förekommande. Detta beror på att överföring efter en begäran grundar sig på en klar och tydlig reglering. Direktivets reglering av överföring på en enhets initiativ är mindre tydlig och har lett till att sådana överföringar sker i begränsad omfattning.

En stor majoritet av medlemsstaterna har valt att utvidga PNR-systemet till att även omfatta flygningar inom EU. Eftersom denna tillämpning är så utbredd anser kommissionen att det inte är nödvändigt att göra sådan insamling obligatorisk.

Ett flertal medlemsstater har valt att tillämpa PNR-systemet även på andra transportmedel än flyg genom att införa sådan reglering i nationell rätt. En sådan reglering väcker juridiska, praktiska och operativa frågor och innan direktivets tillämpningsområde utökas till att gälla även andra transportmedel måste kommissionen genom-

föra en grundlig utvärdering av de eventuella konsekvenser som detta medför.

Kommissionens huvudsakliga slutsats i översynen är att direktivet och dess tillämpning har bidragit positivt i kampen mot terrorism och grov brottslighet. Det föreslås inga förändringar av direktivet utan fokus ligger i stället på att säkerställa att genomförandet och tillämpningen av direktivet sker på ett korrekt sätt.

5.3 Lagen om flygpassageraruppgifter i brottsbekämpningen

Den 1 augusti 2018 trädde lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen i kraft. Lagen genomför PNR-direktivet i svensk rätt.

Syftet med lagen är enligt 1 kap. 2 § att tillgodose behovet av tillgång till PNR-uppgifter i verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet och att skydda människor mot att deras personliga integritet kränks vid behandling av uppgifterna om dem.

Enligt 1 kap. 5 § får PNR-information endast behandlas i de syften som anges i 1 kap. 2 §, med två angivna undantag. Ett av undantagen regleras i 1 kap. 6 §, där det framgår att lagens bestämmelser om behandling av personuppgifter inte gäller för behöriga myndigheter i verksamhet som rör nationell säkerhet samt att enheten för passagerarinformation får behandla PNR-information när det är nödvändigt för att tillhandahålla uppgifter som behövs för sådan verksamhet.

Det andra undantaget behandlas i 5 kap. 3 § där det anges att om det har kommit fram uppgifter om ett annat brott än terroristbrottslighet eller annan allvarlig brottslighet i samband med en brottsbekämpande åtgärd som en behörig myndighet vidtar till följd av behandling av PNR-information, får informationen användas för att förhindra, utreda eller lagföra brottet.

I 2 kap. 7 § uppställs ett förbud mot att behandla PNR-uppgifter som utgör personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning.

Lagens andra kapitel behandlar lufttrafikföretagens skyldigheter med anledning av lagen. Enligt 1 § ska lufttrafikföretagen inför varje

flygning som ankommer till eller avgår från Sverige överföra PNR-uppgifter till enheten för passagerarinformation. PNR-uppgifter ska endast överföras i de fall lufttrafikföretagen samlar in uppgifterna som en del av sin normala verksamhet. Uppgifterna ska enlighet 2 § överföras 24–48 timmar före flygningens avgång samt omedelbart efter att gatens dörrar har stängts. Den senare överföringen får begränsas till uppdateringar och kompletteringar av de uppgifter som överfördes vid det första tillfället.

Enligt 3 § ska lufttrafikföretag på begäran av enheten för passagerarinformation överföra PNR-uppgifter även vid andra tidpunkter än de angivna, om enheten bedömer att det i ett enskilt fall är nödvändigt med tillgång till uppgifterna för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller annan allvarlig brottslighet.

I det tredje kapitlet finns bestämmelser om behandling av PNR-information vid enheten för passagerarinformation. Enligt 1–3 §§ ska PNR-uppgifter som har överförts från ett lufttrafikföretag bevaras i en databas vid enheten och det är enheten som ska behandla PNR-informationen i Sverige. Polismyndigheten är personuppgiftsansvarig för den behandling av personuppgifter som utförs vid enheten.

I 3 kap. 4 § anges de tillåtna ändamålen för behandling av PNR-uppgifter vid enheten vid passagerarinformation. Uppgifterna får endast behandlas för att

1. göra en förhandsbedömning av passagerare före deras beräknade ankomst till eller avresa från Sverige i syfte att välja ut personer som behöver utredas ytterligare av behöriga myndigheter eller Europol, på grund av att dessa personer kan vara inblandade i terroristbrottslighet eller annan allvarlig brottslighet,
2. fullgöra sina uppgifter att överföra PNR-information till behöriga mottagare eller tredjeländer, eller
3. göra analyser för att uppdatera eller skapa nya kriterier som ska användas vid förhandsbedömningar.

Enligt 3 kap. 5 § får PNR-uppgifter vid en förhandsbedömning jämföras med register eller andra uppgiftssamlingar som är relevanta för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet och behandlas enligt på

förhand utformade och fastställda kriterier som är riktade, proportionella och avgränsade och som inte grundar sig på känsliga uppgifter.

I 3 kap. 9–11 §§ regleras den tid under vilken PNR-uppgifter ska bevaras. PNR-uppgifter som behandlas vid enheten för passagerarinformation ska bevaras i fem år från det att de kommit in från ett lufttrafikföretag och därefter ska de förstöras. PNR-uppgifter som inte anges i bilagan till lagen eller som utgör känsliga personuppgifter ska omedelbart förstöras om de kommer in till enheten. Vissa uppräknade PNR-uppgifter ska behörighetsbegränsas sex månader efter att de har kommit in från ett lufttrafikföretag om de kan användas för att identifiera en person:

1. namn på passagerare,
2. antal passagerare som reser tillsammans,
3. adress och kontaktuppgifter,
4. alla former av betalningsinformation, inklusive faktureringsadress,
5. uppgifter om bonusprogram,
6. allmänna markeringar, och
7. uppgifter enligt punkt 18 i bilagan till lagen.

I 3 kap. 12–14 §§ finns bestämmelser om dataskyddsombud. Polismyndigheten ska utse ett dataskyddsombud för enheten för passagerarinformation. Dataskyddsombudet ska ha tillgång till alla uppgifter som behandlas vid enheten och ansvarar för att fullgöra de uppgifter som anges i 3 kap. 14 § brottsdatalagen. En enskild ska ha rätt att kontakta dataskyddsombudet i alla frågor som rör behandling av hans eller hennes PNR-uppgifter enligt lagen. Om dataskyddsombudet anser att den personuppgiftsansvarige bryter mot bestämmelser för behandling av PNR-uppgifter, ska han eller hon anmäla det till tillsynsmyndigheten.

I det fjärde kapitlet regleras överföring av PNR-information från enheten för passagerarinformation. Av 1 § framgår att enheten så snart som möjligt ska överföra PNR-information till en eller flera behöriga myndigheter för att en vidare granskning ska göras av PNR-information som har valts ut vid en förhandsbedömning, besvara en begäran från en behörig myndighet om att ta del av PNR-information, eller vidarebefordra PNR-information som har mottagits från en motsva-

rande enhet i en annan medlemsstat. Överföring av PNR-information till andra medlemsstater ska enligt 2 § ska ske så snart som möjligt för att en vidare granskning ska göras beträffande passagerare som har valts ut vid en förhandsbedömning, eller för att besvara en begäran från enheten i den andra medlemsstaten om att ta del av PNR-information. I 5 § finns motsvarande reglering av överföring av PNR-uppgifter till Europol. Överföring till tredjeland får ske under vissa förutsättningar som framgår av 7–8 §§.

Enligt 11 § får PNR-uppgifter som är behörighetsbegränsade enligt 3 kap. 11 § endast överföras i sin fullständiga form till behöriga mottagare eller ett tredjeland om det rimligen kan antas vara nödvändigt för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet. om en förundersökning pågår ska en begäran från en behörig myndighet om att få tillgång till fullständiga PNR-uppgifter beslutas av en åklagare. I annat fall krävs att tillstånd till överföringen har lämnats av Polismyndigheten.

Det femte kapitlet rör behöriga myndigheters behandling av PNR-information. Enligt 1 § ska en behörig myndighet som har mottagit PNR-information från enheten för passagerarinformation efter enhetens förhandsbedömning omedelbart förstöra informationen om den visar sig sakna betydelse för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet. Detsamma gäller enligt 2 § om myndigheten tar emot sådana känsliga personuppgifter som avses i 1 kap. 7 §.

PNR-uppgifter får inte behandlas i syfte att bekämpa andra brott än terroristbrott och grov brottslighet enligt definitionen i artikel 3.9 och bilaga II i PNR-direktivet. Enligt 5 kap. 3 § får dock uppgifter som kommit fram om andra brott i samband med en brottsbekämpande åtgärd som en myndighet vidtar till följd av behandling av PNR-information användas för att förhindra, utreda eller lagföra brottet, utöver vad som anges i 1 kap. 5 §.

I 5 kap. 3 § finns ett förbud mot beslut som har rättsliga följder för en person eller annars i betydande grad påverkar honom eller henne, som enbart grundas på en automatiserad behandling av PNR-uppgifter.

5.4 Polismyndigheten och Säkerhetspolisen

Sedan 1998 har Polismyndigheten rätt att få tillgång till uppgifter från transportföretag redan innan misstanke om ett visst konkret brott har uppstått. Detta regleras i 25 och 26 §§ polislagen (1984:387). I 25 § första och andra stycket anges att ett transportföretag som befordrar varor, passagerare eller fordon till eller från Sverige på begäran av Polismyndigheten eller Säkerhetspolisen skyndsamt ska lämna de aktuella uppgifter om ankommande och avgående transporter som företaget har tillgång till. Transportföretaget har endast skyldighet att lämna de uppgifter om passagerare som avser namn, resrutt, bagage och medpassagerare samt sättet för betalning och bokning. Polismyndigheten får begära uppgifter endast om uppgifterna kan antas ha betydelse för den brottsbekämpande verksamheten.

Syftet med regleringen är att polisen ska kunna identifiera och karaktärsbestämma hot mot samhället eller skaffa det underlag som behövs för att brott ska kunna förhindras. Tanken är inte att polisen ska begära att få ut andra uppgifter än sådana som transportföretaget är skyldiga att lämna ut. Det bör inte heller komma i fråga att begära uppgifter för att bekämpa rena bagatellbrott. Detta följer av proportionalitetsprincipen i 8 § polislagen.[10]

I 25 § tredje stycket anges att lufttrafikföretag som omfattas av skyldigheten att överföra uppgifter enligt lagen om flygpassageraruppgifter i brottsbekämpningen endast är skyldiga att lämna uppgifter i enlighet med första och andra styckena om de behövs i verksamhet som rör nationell säkerhet.

I 26 § framgår att transportföretagen får lämna uppgifter enligt 25 § på så sätt att de görs läsbara för Polismyndigheten eller Säkerhetspolisen genom terminalåtkomst. Detta får ske endast i den omfattning och under den tid som behövs för att kontrollera aktuella transporter.

Polismyndigheten och Säkerhetspolisen får inte ändra eller på annat sätt bearbeta eller lagra uppgifter som hålls tillgängliga på detta sätt. Uppgifter om enskilda som lämnats på annat sätt än genom terminalåtkomst ska omedelbart förstöras om de visar sig sakna betydelse för utredning eller lagföring av brott.

Regleringen är inte avsedd att tillåta någon systematisk kartläggning av resandeströmmar eller något generellt insamlande av uppgifter. Det är inte heller avsett att uppgifter om resande ska registreras, lagras eller

[10] Prop. 1996/97:175, *Ändringar i polislagen m.m.*, s. 67 f.

bearbetas på ett sådant sätt att nya personregister om resande skapas. Uppgifter som inhämtas genom uppkoppling till databaser via terminal anses således fortfarande tillhöra och förvaras hos transportföretaget.[11]

För det fall att uppgifterna anses ha betydelse för utredning eller lagföring får informationen sparas i enskilda brottsutredningar med stöd av bestämmelserna i polislagen.

5.5 Tullverket

Tullverkets befogenhet att inhämta vissa passageraruppgifter från transportföretag om uppgifterna kan antas ha betydelse för dess brottsbekämpande verksamhet infördes 1996. I dag finns regleringen i tullbefogenhetslagen (2024:710). Syftet med den nya lagstiftningen är bl.a. att göra regelverket mer enhetligt och ändamålsenligt.

I 7 kap. 12 § anges att om uppgifterna kan antas ha betydelse för Tullverkets brottsbekämpande verksamhet, får Tullverket begära att ett transportföretag som befordrar varor, passagerare eller fordon till eller från Sverige lämnar uppgifter om ankommande eller avgående transporter som företaget har tillgång till (bokningsuppgifter). Detta gäller även andra företag än transportföretag som får tillgång till transportföretagets bokningsuppgifter. I fråga om passagerare omfattas endast uppgifter om

- namn,
- födelsedatum,
- nationalitet,
- resrutt,
- bagage,
- medpassagerare,
- mobiltelefonnummer,
- e-postadress,
- betalningssätt, och
- bokningssätt.

[11] Jfr prop. 1995/96:166, *Tullens befogenheter vid den inre gränsen*, s. 81 ff.

Bestämmelsen gäller inte lufttrafikföretag som omfattas av skyldigheten att överföra uppgifter enligt lagen om flygpassageraruppgifter i brottsbekämpningen.

I jämförelse med 25 § polislagen har Tullverket möjlighet att begära ut ett bredare spektrum av uppgifter om passagerare. I november 2024 utökades omfattningen av sådana uppgifter till att även gälla födelsedatum, nationalitet, e-postadress och mobiltelefonnummer, under förutsättning att företaget har tillgång till dessa uppgifter.

Transportföretaget ska enligt 13 § skyndsamt lämna Tullverket de uppgifter som myndigheten begär enligt 12 §. Ett transportföretag får lämna uppgifter genom direktåtkomst. Tullverket får ta del av bokningsuppgifter genom direktåtkomst innan transporten har ankommit eller avgått. Tullverket får även ta del av sådana uppgifter under högst sex månader därefter, om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott.

Om ett transportföretag efter en begäran från Tullverket inte lämnar uppgifter får Tullverket enligt 14 § förelägga ett transportföretag att fullgöra sina skyldigheter enligt 12 och 13 §§. Ett beslut om föreläggande gäller omedelbart och får förenas med vite.

Kompletterande bestämmelser till tullbefogenhetslagen finns i tullbefogenhetsförordningen (2024:759). I 6 kap. 1 § anges att Tullverket får ingå en överenskommelse med ett transportföretag om direktåtkomst till företagets bokningsuppgifter under de förutsättningar som anges i 7 kap. 12 och 13 §§ tullbefogenhetslagen. Av 2 § framgår att utrustning som ger Tullverket tillgång till ett transportföretags bokningsuppgifter och handlingar med sådana uppgifter ska hanteras på sådant sätt att obehöriga inte får tillgång till dem.

I 6 kap. 3 § anges att information om innehållet i bokningsuppgifter som inhämtats med stöd av 7 kap. 12 § tullbefogenhetslagen får lämnas till andra tulltjänstemän, andra enheter inom Tullverket, Polismyndigheten, Kustbevakningen och Skatteverket, om uppgiften behövs i Tullverkets brottsbekämpande verksamhet för att klarlägga om brott eller brottslig verksamhet har förekommit, pågår eller planeras. Informationen får också lämnas till en utländsk myndighet eller en mellanfolklig organisation, om utlämnandet följer av en konvention som Sverige har tillträtt eller en överenskommelse som Sverige har ingått.

6 API-uppgifter och transportörsansvaret

6.1 Inledning

Med transportörsansvar avses att transportörer har vissa skyldigheter beträffande de personer som de transporterar till ett lands gräns. De kan också åläggas sanktioner om de inte uppfyller sina skyldigheter. Sverige har sedan anslutningen till den s.k. Chicagokonventionen på 1940-talet haft internationella åtaganden när det gäller transportörsansvaret. En central rättsakt avseende transportörsansvaret inom EU är API-direktivet, som uppställer en skyldighet för lufttrafikföretag att, på begäran, föra över förhandsinformation om passagerare till en medlemsstat. API står för *Advance Passenger Information*, dvs. förhandsinformation om passagerare. Huvudsakligen handlar transportörsansvaret inte om brottsbekämpning, utan om gränskontroll och reglerad invandring. I december 2024 antogs dock två nya API-förordningar; en som rör gränskontroll och olaglig invandring samt en som rör brottsbekämpning.

I detta avsnitt behandlas inledningsvis de internationella åtaganden som Sverige har på området. Därefter behandlas transportörsansvaret i EU-rätten, inklusive API-direktivet samt de föreslagna API-förordningarna. Slutligen redogör vi för Sveriges nationella lagstiftning på området.

6.2 Internationella åtaganden

6.2.1 Chicagokonventionen

Sverige är ansluten till 1944 års konvention angående internationell civil luftfart, den s.k. Chicagokonventionen. Konventionen kallas även Icao-konventionen efter *International Civil Aviation Organisation* som är ett specialorgan inom FN med uppgift att underlätta flygning mellan världens länder och bidra till flygsäkerhet. Konventionen reglerar internationell civil luftfart och syftar till att upprätthålla säkerhet under internationell lufttrafik och att underlätta och främja luftfarten. Så gott som alla länder har anslutit sig till konventionen. Sverige ratificerade konventionen den 7 november 1946 och den svenska luftfartslagstiftningen bygger i stora delar på konventionen.

I Chicagokonventionen förbinder sig de fördragsslutande staterna till samarbete för att säkerställa största möjliga likformighet i fråga om författningar, normer, tillämpningsförfaranden och organisation avseende luftfartyg, besättning, luftfartslinjer och markorganisation. I detta syfte tar ICAO fram internationella normer och rekommendationer, som tas in som Annex till konventionen.

I Annex 9 finns bl.a. internationella normer om transportörsansvar och behandlingen av API- och PNR-uppgifter. Artikel 3.34 ålägger flygtrafikföretagen att kontrollera att passagerare vid ombordstigningen har pass och tillstånd för transit och inresa. Enligt artikel 3.32 ska de fördragsslutande staterna och transportörerna samarbeta för att fastställa att de resedokument som visas upp är äkta och giltiga. Myndigheterna ska enligt artikel 5.3 och 5.4 utan dröjsmål informera transportören när en person nekas inresa och rådgöra med transportören angående möjligheter till återförande. Transportören ska därefter enligt artikel 5.11 återföra passageraren till den plats där han eller hon påbörjade sin resa eller till någon annan plats där vederbörande kan tas emot. Enligt artikel 5.10 får transportören inte hindras från att ta ut transportkostnaden från den avvisade personen. Återförandeplikten upphör enligt artikel 3.46 när personen tillåts resa in i landet.

I avsnitt 9 B av Annex 9 finns bestämmelser om API-information. Artikel 9.5 anger att de fördragsslutande staterna ska införa ett API-system. Av artikel 9.11–9.16 framgår bl.a. följande. De fördragsslutande staterna ska, så långt det är möjligt, minimera de operativa och administrativa bördorna för flygtrafikföretagen. Antalet överföringar

av API-uppgifter per flygning bör minimeras. Staterna bör vidare avstå från att använda sig av sanktioner mot flygtrafikföretag på grund av tekniska överföringsfel. Stater som kräver att information överförs elektroniskt ska inte därutöver kräva uppgifterna i pappersform. Det rekommenderas att API-systemet användas dygnet runt och det bör införas rutiner för att undvika avbrott i systemet.

6.2.2 FN:s resolution 2178

Den 24 september 2014 antog FN:s säkerhetsråd resolution 2178 (2014). Resolutionen är antagen i enlighet med kapitel VII i FN-stadgan och är därmed folkrättsligt bindande för alla medlemsstater.

I resolutionen anges att terrorism i alla dess former är ett hot mot internationell fred och säkerhet. Det uttrycks vidare en allvarlig oro över det akuta och växande hot som de personer utgör som reser till ett annat land för att delta i terroristhandlingar eller terroristträning, även när detta sker inom ramen för en väpnad konflikt. De bidrar enligt resolutionen till intensiteten och varaktigheten i konflikter och till att de blir mer svårlösta. Personerna uppges även kunna utgöra ett allvarligt hot mot bl.a. sina ursprungsländer och länderna de reser igenom och till.

I resolutionens paragraf 2 bekräftas att alla stater ska begränsa möjligheten för terrorister eller terroristgrupper att röra sig fritt över gränser genom effektiv gränskontroll samt kontroll av identitetshandlingar och resedokument. Medlemsstaterna uppmuntras att använda evidensbaserad riskbedömning av passagerare och kontrollförfaranden för resande, inklusive insamling och analys av resedata. Detta ska dock ske utan profilering utifrån stereotyper grundade på diskriminering, vilket är förbjudet enligt folkrätten.

I paragraf 9 uppmanas medlemsstaterna att kräva av lufttrafikföretag som bedriver verksamhet inom deras territorier att i förväg lämnar ut uppgifter om passagerare till behöriga nationella myndigheter för att upptäcka avresa från deras territorier eller försök till inresa till eller transitering genom deras territorier med civila luftfartyg.

6.3 Vissa EU-rättsliga åtaganden

6.3.1 Schengenkonventionen och direktivet om transportörsansvar

Sverige har EU-rättsliga åtaganden om transportörsansvar, bl.a. till följd av API-direktivet, som behandlas nedan i avsnitt 6.4.

Artikel 26 i Schengenkonventionen[1] och rådets direktiv om komplettering av bestämmelserna i den artikeln (direktivet om transportörsansvar[2]) behandlar transportörsansvaret. I artikel 26 i Schengenkonventionen anges att de avtalsslutande parterna, om inte annat följer av förpliktelser i samband med anslutning till Genèvekonventionen angående flyktingars rättsliga ställning (ändrad genom New York-protokollet), ska införa vissa bestämmelser på området. Bestämmelserna gäller en skyldighet för en transportör att kontrollera inresehandlingar och att ordna återresa för utlänningar som vägras inresa i en Schengenstat samt sanktioner mot den som befordrar utlänningar utan nödvändiga resehandlingar. Med transportör avses i Schengenkonventionen varje fysisk eller juridisk person som bedriver yrkesmässig persontrafik luft-, sjö- eller landvägen.

Syftet med direktivet om transportörsansvar är att harmonisera medlemsstaternas lagar om ekonomiska sanktioner mot transportörer som försummar sin kontrollskyldighet avseende inresehandlingar.

De förpliktelser som följer av artikel 26 i Schengenkonventionen och direktivet om transportörsansvar har Sverige uppfyllt genom bestämmelser i utlänningslagen (2005:716), se avsnitt 6.5.1.

6.3.2 Kodex om Schengengränserna

I den så kallade kodexen om Schengengränserna[3], även kallad gränskodexen, behandlas en unionskodex om gränspassager för personer. I bilaga VI till kodexen finns särskilda bestämmelser om de olika transportmedel som används för passage av de yttre gränserna. Befälhavaren vid privata flygningar från eller till tredjeländer ska före starten överlämna en allmän deklaration som bl.a. innehåller passagerarnas

[1] Konventionen om tillämpning av Schengenavtalet av den 14 juni 1985.
[2] Rådets direktiv 2001/51/EG av den 28 juni 2001 om komplettering av bestämmelserna i artikel 26 i konventionen om tillämpning av Schengenavtalet av den 14 juni 1985.
[3] Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016 om en unionskodex om gränspassage för personer (kodex om Schengengränserna).

identitet till gränskontrolltjänstemännen i destinationsmedlemsstaten och, i förekommande fall, i den medlemsstat där den första inresan äger rum. När privatflyg från ett tredjeland på väg till en medlemsstat mellanlandar på andra medlemsstaters territorium, ska de behöriga myndigheterna i den medlemsstat där inresan sker utföra inresekontroller och fästa en inresestämpel på den allmänna deklarationen.

6.4 API-direktivet

Den 29 april 2004 antog Europeiska rådet direktiv 2004/82/EG om skyldighet för transportörer att lämna uppgifter om passagerare. Direktivet syftar till att förbättra gränskontrollerna och bekämpa olaglig invandring genom att ålägga transportörer att föra över förhandsuppgifter om passagerare till behöriga nationella myndigheter.

I artikel 3 föreskrivs att medlemsstaterna ska vidta de åtgärder som är nödvändiga för att ålägga transportörerna att, på begäran av de myndigheter som ansvarar för personkontrollen vid de yttre gränserna, senast vid slutet av incheckningen översända information om de passagerare som de kommer att befordra till ett godkänt gränsövergångsställe genom vilket personerna kommer att resa in på en medlemsstats territorium.

Informationen ska innehålla uppgifter om

- nummer på och typ av resehandling som används,
- nationalitet,
- fullständigt namn,
- födelsedatum,
- gränsövergångsställe för inresa till medlemsstaternas territorium,
- transportkod,
- avgångs- och ankomsttid för transporten,
- det totala antalet passagerare vid den transporten,
- ursprunglig ort för ombordstigning.

Överföringen av dessa uppgifter befriar inte transportörerna från de skyldigheter och det ansvar som följer av bestämmelserna i artikel 26 i Schengenkonventionen, kompletterade genom direktiv 2001/51/EG.

I artikel 4 regleras påföljder för transportörer som genom fel eller försummelse underlåtit att lämna uppgifter eller som lämnar ofullständiga eller felaktiga uppgifter. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att se till att påföljderna är avskräckande, effektiva och proportionella. Medlemsstaterna har möjlighet att välja att införa ett maximibelopp eller ett minimibelopp för sådana påföljder. Maximibeloppet får inte understiga 5 000 euro och minimibeloppet får inte understiga 3 000 euro.

Bestämmelsen hindrar inte att medlemsstaterna inför eller behåller andra påföljder gentemot transportörer som mycket allvarligt åsidosätter de skyldigheter som följer av bestämmelserna i direktivet. Sådana påföljder kan vara t.ex. körförbud, beslag och förverkande av transportmedel eller tillfälligt upphävande eller återkallande av den operativa licensen.

Enligt artikel 5 ska medlemsstaterna se till att det i deras lagar och andra författningar föreskrivs en rätt till effektiva rättsmedel för de transportörer mot vilka rättsliga åtgärder har vidtagits i syfte att ålägga dem påföljder.

Artikel 6 innehåller bestämmelser om behandling av uppgifter. De personuppgifter som ska överföras ska sändas till de myndigheter som ansvarar för genomförandet av personkontroller vid de yttre gränser som passeras när passagerarna reser in på en medlemsstats territorium. Syftet med detta är att underlätta gränskontrollerna för att mer effektivt kunna bekämpa den olagliga invandringen. De myndigheter som ansvarar för genomförandet av personkontroller vid de yttre gränserna ska spara uppgifterna i ett tillfälligt register. När passagerarna har rest in i landet ska de myndigheter som ansvarar för genomförandet av personkontroller vid de yttre gränserna radera uppgifterna inom 24 timmar efter översändandet, om inte uppgifterna behövs senare för att dessa myndigheter ska kunna utföra sina lagstadgade uppgifter enligt nationell lag och i enlighet med bestämmelser om uppgiftsskydd enligt dataskyddsdirektivet. Transportörer ska inom 24 timmar efter det att transportmedlet har anlänt enligt artikel 3.1 radera de personuppgifter som de har samlat in och översänt till gränskontrollmyndigheterna i enlighet med API-direktivet.

6.5 API-direktivet i svensk rätt

6.5.1 Utlänningslagen

API-direktivets bestämmelser om transportansvaret har bl.a. genomförts genom bestämmelser i 9, 12 och 19 kap. utlänningslagen. I 9 kap. 3 § anges att en transportör ska kontrollera att en utlänning som transportören transporterar till Sverige direkt från en stat som inte omfattas av Schengenkonventionen innehar pass och de tillstånd som krävs för att resa in i landet. Om det inte är obehövligt ska transportören även kontrollera att utlänningen har medel för sin hemresa.

Av 9 kap. 3 a § framgår att en transportör, som luftvägen ska transportera passagerare till Sverige direkt från en stat som inte tillhör EU och inte heller har slutit avtal om samarbete enligt Schengenkonventionen med konventionsstaterna, på begäran av Polismyndigheten ska överföra uppgifter om de ankommande passagerarna så snart incheckningen avslutats. De uppgifter som ska överföras är

1. nummer på och typ av resehandling som används,
2. medborgarskap,
3. fullständigt namn,
4. födelsedatum,
5. gränsövergångsstället för inresa,
6. transportkod,
7. avgångs- och ankomsttid för transporten,
8. det totala antalet passagerare vid transporten,
9. ursprunglig ort för ombordstigning.

Uppgifterna som samlas in ska enligt 9 kap. 3 b § sedan elektroniskt överföras till Polismyndigheten. Om det inte är möjligt att överföra uppgifterna elektroniskt ska de överföras på annat sätt. I 3 c § anges att bestämmelser om behandlingen av de uppgifter som överförts till Polismyndigheten finns i lagen om passagerarregister.

I 9 kap. 3 d § anges att en transportör som har överfört uppgifter enligt 3 a § inom 24 timmar efter det att transportmedlet har anlänt till gränsövergångsstället ska radera de insamlade och överförda uppgifterna.

Av 19 kap. 5 § framgår att en transportör som inte fullgjort sin kontrollskyldighet enligt 9 kap. 3 § ska betala en särskild avgift. Undantag från skyldigheten att betala en särskild avgift görs dock om transportören visar att underlåtenheten inte beror på fel eller försummelse eller om det framstår som uppenbart oskäligt att ta ut avgiften. Enligt 19 kap. 6 § ska den särskilda avgiften för varje flygning som har gjorts utan att transportören har fullgjort sin uppgiftsskyldighet bestämmas till högst 46 000 kronor. Frågan om transportören ska betala en avgift prövas enligt 19 kap. 7 § av Polismyndigheten.

I 12 kap. 5 § regleras transportörers ansvar att ombesörja utlänningars återresa i vissa fall. Med transportör avses här ägare eller brukare av ett fartyg eller ett luftfartyg. En utlänning som har kommit till Sverige med ett fartyg eller ett luftfartyg direkt från en stat som inte omfattas av Schengenkonventionen och som har avvisats för att han eller hon saknar pass eller de tillstånd som krävs för att resa in i landet eller medel för sin hemresa, får som utgångspunkt föras tillbaka till fartyget eller luftfartyget eller sättas ombord på ett annat sådant med samma transportör.

I 19 kap. 2 § regleras transportörers kostnadsansvar om utlänningar saknar pass eller de tillstånd som krävs för inresa till Sverige eller medel för hemresan. Transportören är enligt denna bestämmelse normalt skyldig att ersätta staten för kostnader för utlänningens resa från Sverige samt resekostnaden för den bevakningspersonal som följer med.

6.5.2 Befälhavares skyldigheter

Befälhavaren på ett luftfartyg som kommer från en ort utanför Schengenstaterna ska enligt 6 kap. 8 § utlänningsförordningen (2006:97) före ankomst underrätta flygplatschefen om ankomsten. Flygplatschefen ska utan dröjsmål underrätta Polismyndigheten om ett luftfartyg kommer från eller avgår från en ort utanför Schengenstaterna. Underrättelseskyldigheten gäller inte för befälhavare på ett privatflyg. För en sådan befälhavare finns bestämmelser om underrättelseskyldighet i gränskodexen, se ovan under avsnitt 6.3.2.

6.5.3 Lagen om passagerarregister

I lagen (2006:444) om passagerarregister finns bestämmelser om behandlingen av de API-uppgifter som har överförts till Polismyndigheten enligt 9 kap. 3 b § utlänningslagen. I 1 § anges att Polismyndigheten med hjälp av automatiserad behandling ska föra ett register över sådana passagerare som avses i 9 kap. 3 a § utlänningslagen. Myndigheten är personuppgiftsansvarig för behandlingen av personuppgifter i registret.

Av 2 och 2 a §§ framgår att lagen kompletterar EU:s dataskyddsförordning och att vid behandling av personuppgifter enligt lagen gäller lagen med kompletterande bestämmelser till dataskyddsförordningen och föreskrifter som har meddelats i anslutning till den lagen, om inte annat följer av lagen om passagerarregister eller föreskrifter som har meddelats i anslutning till denna lag.

I 2 b § anges att när en behörig myndighet enligt 1 kap. 6 § brottsdatalagen behandlar personuppgifter enligt denna lag för syften som faller inom tillämpningsområdet för brottsdatalagen gäller den lagen och föreskrifter som har meddelats i anslutning till den, om inte annat följer av denna lag eller föreskrifter som har meddelats i anslutning till den.

Syftet med lagen anges i 4 §. Passagerarregistret ska föras för att underlätta verkställandet av personkontroller vid Sveriges gräns mot stater som inte tillhör EU och inte heller har träffat avtal om samarbete enligt Schengenkonventionen med konventionsstaterna.

Enligt 5 § får registret endast innehålla vissa uppräknade personuppgifter som har kommit in i enlighet med 9 kap. 3 a § utlänningslagen. Det rör sig exempelvis om fullständigt namn, medborgarskap och födelsedatum.

I 6–8 §§ regleras utlämnande av uppgifter och direktåtkomst. Personuppgifter ur passagerarregistret ska lämnas ut på begäran av Säkerhetspolisen och Tullverket för sådan verksamhet som anges i 4 §. Säkerhetspolisen får för sådan verksamhet ha direktåtkomst till personuppgifterna i registret. Personuppgifter ur passagerarregistret får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

I 9 § anges att en uppgift i passagerarregistret ska raderas 24 timmar efter överföringen till Polismyndigheten. Om uppgifter i registret behövs för att Polismyndigheten, Säkerhetspolisen eller Tullverket ska

kunna verkställa personkontroller enligt 4 §, får uppgifterna i registret dock stå kvar till dess att myndighetens kontroller är slutförda.

6.6 Nya API-förordningar

Den 19 december 2024 antogs två API-förordningar som berör brottsbekämpning[4] och gränskontroll.[5] Syftet med förordningarna är att ersätta API-direktivet och ytterligare harmonisera insamlingen och behandlingen av passageraruppgifter som används i gränskontroll och brottsbekämpning. API-lagstiftningen moderniseras så att den överensstämmer med annan EU-lagstiftning samt internationella regelverk. Enligt Europeiska kommissionen har API-direktivet inte lett till en tillräckligt systematisk och harmoniserad insamling och användning av API-uppgifter.

Förordningarna utvidgar insamlingen av API-uppgifter från flygtransportörer, t.ex. genom att fler typer av uppgifter samlas in och att fler flygrutter omfattas av insamlingen. Uppgiftsinsamlingen automatiseras i högre grad. Bestämmelser om dataskydd har uppdaterats för att ligga i linje med EU:s övriga dataskyddslagstiftning. Flygtransportörer åläggs en skyldighet att överföra API-uppgifter till en central router som förvaltas av eu-Lisa.[6] Förordningarna ska tillämpas två år från den dag då routern tas i drift med avseende på API-uppgifter och fyra år från den dag då routern tas i drift med avseende på PNR-uppgifter. En del artiklar tillämpas emellertid sedan den 28 januari 2025 och ytterligare en del artiklar ska tillämpas från den dag då routern tas i drift.

Eftersom rättsakterna är EU-förordningar är de efter ikraftträdandet till alla delar bindande och direkt tillämpliga i alla medlemsstater. Det innebär att förordningarna ska tillämpas direkt av nationella myndigheter på samma sätt som lagar och andra nationella föreskrifter.

[4] Europaparlamentets och rådets förordning (EU) 2025/13 av den 19 december 2024 om insamling och överföring av förhandsinformation om passagerare för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet, och om ändring av förordning (2019/818).
[5] Europaparlamentets och rådets förordning (EU) 2025/12 av den 19 december 2024 om insamling och överföring av förhandsinformation om passagerare för att förbättra och underlätta in- och utresekontroller vid de yttre gränserna, om ändring av förordningarna (EU) 2018/1726 och (EU) 2019/817 och om upphävande av rådets direktiv 2004/82/EG.
[6] eu-Lisa är Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa.

Av motiveringen till förordningarna framgår att det sedan 2004 råder global enighet om att API-uppgifter inte bara är ett viktigt instrument för gränsförvaltning, utan också ett viktigt verktyg för brottsbekämpande ändamål, framför allt för att bekämpa grov brottslighet och terrorism. FN:s säkerhetsråd har i resolutioner sedan 2014 vid upprepade tillfällen efterlyst inrättande och globalt införande av API- och PNR-system för brottsbekämpande ändamål.[7]

6.6.1 API-förordning för brottsbekämpning

Europeiska kommissionens rapport[8] om översynen av PNR-direktivet visar att kampen mot grov brottslighet och terrorism i EU blir avsevärt effektivare när de behöriga brottsbekämpande myndigheterna behandlar API- och PNR-uppgifter tillsammans. Det innebär att PNR-uppgifter som samlas in av lufttrafikföretag i deras normala affärsverksamhet och överförs till behöriga brottsbekämpande myndigheter kompletteras med en skyldighet för lufttrafikföretagen att samla in och överföra API-uppgifter. Den kombinerade användningen av API-uppgifter och PNR-uppgifter gör det möjligt för de behöriga nationella myndigheterna att bekräfta passagerarnas identitet och förbättrar PNR-uppgifternas tillförlitlighet avsevärt.

En kombinerad användning av uppgifter före ankomst gör det möjligt för brottsbekämpande myndigheter att göra en bedömning och en närmare granskning endast av de personer som på grundval av objektiva bedömningskriterier och metoder mest sannolikt utgör ett hot mot säkerheten. Detta underlättar alla andra passagerares resor och minskar risken för att passagerare vid ankomsten utsätts för de behöriga myndigheternas granskning på grundval av godtyckliga faktorer.

EU:s nuvarande rättsliga ram reglerar användningen av PNR-uppgifter för att bekämpa grov brottslighet och terrorism, men däremot inte detsamma för API-uppgifter. Sådana uppgifter kan endast begäras avseende flygningar från tredjeland, vilket leder till en säkerhetslucka, framför allt när det gäller flygningar inom EU. Enheterna för passagerarinformation får de mest effektiva operativa resultaten på flygningar där både API- och PNR-uppgifter samlas in.

[7] FN:s säkerhetsråds resolutioner 2178(2014), 2309(2016), 2396(2017) och 2482(2019).
[8] Europeiska kommissionen, *Arbetsdokument från kommissionens avdelningar som åtföljer rapporten om översynen av direktiv 2016/681*, SWD(2020)128 final.

Den nuvarande ordningen innebär således att brottsbekämpande myndigheter inte kan dra nytta av resultaten av den kombinerade behandlingen av API- och PNR-uppgifter om flygningar inom EU. Reformen av API-systemet syftar till att täppa till denna lucka.

De föreslagna reglerna om insamling och överföring av API-uppgifter i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet är anpassade till de tillämpliga regler för behandling av PNR-uppgifter som fastställs i PNR-direktivet och tar hänsyn till de tolkningar som EU-domstolen har gjort i sin praxis, t.ex. PNR-domens uttalanden om flygningar inom EU.

Förordningen har nära samband med PNR-direktivet och bör tolkas som ett komplement till direktivet. Avsikten är att API-uppgifter samlas in och överförs i enlighet med de särskilda kraven i förordningen, t.ex. när det gäller i vilka situationer och på vilket sätt detta ska göras. Efter överföringen av API-uppgifter till en enhet för passagerarinformation är reglerna för enhetens efterföljande behandling av API-uppgifter de som fastställs i PNR-direktivet. Därmed är t.ex. reglerna i PNR-direktivet om ändamål med behandlingen, lagringstid, radering, informationsutbyte, medlemsstaternas överföring till tredjeländer och bestämmelser om skydd av personuppgifter tillämpliga även vad avser de insamlade API-uppgifterna.

Innehåll

De tre inledande artiklarna i förordningen om API-uppgifter i brottsbekämpningen berör syftet och tillämpningsområdet för förordningen, samt innehåller definitioner av centrala begrepp. I syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet fastställs i förordningen regler om lufttrafikföretags insamling av API-uppgifter om flygningar utanför EU och utvalda flygningar inom EU, lufttrafikföretags överföring av API-uppgifter till routern samt överföring av uppgifter från routern till enheterna för passagerarinformation. Förordningen är tillämplig på lufttrafikföretag som utför reguljära eller icke-reguljära flygningar utanför EU eller flygningar inom EU.

Förordningens andra kapitel rör insamling, överföring, lagring och radering av API-uppgifter. Enligt artikel 4 ska lufttrafikföretag samla in API-uppgifter om passagerare och besättningsmedlemmar på flyg-

ningar inom och utanför EU. I artikel 4.2 preciseras vad API-uppgifterna ska bestå av. Uppgifterna ska vara korrekta, fullständiga och aktuella. Uppgifterna ska i första hand samlas in med automatiserade metoder och de ska föras över till routern på elektronisk väg. Överföring ska ske både vid incheckning och omedelbart efter det att gaten stängs.

I artikel 5 anges att lufttrafikföretagen ska överföra krypterade API-uppgifter till routern på elektronisk väg så att de kan översändas till enheten för passagerarinformation.[9] API-uppgifterna för passagerare ska överföras vid tidpunkten för incheckningen, dock tidigast 48 timmar före flygets angivna avgångstid, och för alla passagerare som stigit ombord omedelbart efter att gaten stängts, dvs. när passagerarna har stigit ombord och det inte längre är möjligt för passagerare att stiga ombord eller lämna luftfartyget. För besättningsmedlemmar ska API-uppgifter överföras omedelbart efter att gaten stängts.

Enligt artikel 6 ska lufttrafikföretagen, under en period på 48 timmar från den tidpunkt då routern tar emot de API-uppgifter som överförts till den, lagra de API-uppgifter som de samlat in i enlighet med artikel 4. Efter utgången av denna period ska de omedelbart och permanent radera sådana API-uppgifter. Detta påverkar dock inte lufttrafikföretagens möjlighet att lagra och använda uppgifterna när det är nödvändigt för deras normala affärsverksamhet.

Artikel 12 behandlar översändande av API-uppgifter och andra PNR-uppgifter från routern till enheterna för passagerarinformation. Routerna ska översända sådana uppgifter till enheterna för passagerarinformation i den medlemsstat på vars territorium flygningen kommer att landa eller från vars territorium flygningen kommer att avgå, eller bådadera om det rör sig om en flygning inom EU. Uppgifterna ska översändas omedelbart och på ett automatiserat sätt, utan att på något sätt ändra innehållet. När det gäller flygningar inom EU ska routern dock översända API-uppgifter och andra PNR-uppgifter endast avseende de flygningar som ingår i den förteckning som medlemsstaten har upprättat över utvalda flygningar inom EU. En sådan förteckning ska upprättas av varje enskild medlemsstat och senast den dag då förordningen börjar gälla lägga till de utvalda flygningarna eller rutterna i routern.

[9] I den svenska översättningen av artikel 5 i API-förordningen för brottsbekämpning anges att lufttrafikföretagen ska överföra krypterade API-uppgifter till routern på elektronisk väg så att de kan översändas till *de behöriga gränsmyndigheterna*. Detta är en felaktig översättning; det korrekta är att uppgifterna ska överföras till enheten för passagerarinformation.

I artikel 13 anges att medlemsstaterna får tillämpa PNR-direktivet och därmed denna förordning på alla flygningar inom EU endast i situationer med ett verkligt och aktuellt eller förutsebart terroristhot, på grundval av ett beslut som grundar sig på en hotbedömning, som är tidsbegränsat till vad som är absolut nödvändigt och som kan bli föremål för effektiv prövning av en domstol eller ett oberoende förvaltningsorgan vars beslut är bindande. I avsaknad av ett sådant terroristhot ska medlemsstaterna göra ett urval av flygningar. Bedömningen som ligger till grund för urvalet ska utföras på ett objektivt, vederbörligen motiverat och icke-diskriminerande. I bedömningen ska beaktas endast kriterier som är relevanta för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet som har en objektiv koppling, inbegripet en indirekt koppling, till lufttransport av passagerare. Medlemsstaterna ska endast välja ut flygningar inom EU som har anknytning till bl.a. vissa rutter, resmönster eller flygplatser med avseende på vilka det finns indikationer på terroristbrott eller grov brottslighet och vilka motiverar behandling av API-uppgifter och andra PNR-uppgifter. Urvalet av flygningar ska begränsas till vad som är absolut nödvändigt för att uppnå målen i PNR-direktivet och i denna förordning.

6.6.2 API-förordning för gränskontroll

Syftet med förslaget till förordning är att förbättra och effektivisera kontrollerna vid EU:s yttre gränser, vilket i praktiken är Schengens yttre gräns, samt att motverka olaglig invandring. Den föreslagna förordningen kommer att ersätta API-direktivet i detta avseende. Den senaste utvärderingen av API-direktivet visade att de nationella myndigheterna inte alltid använder API-uppgifter på ett konsekvent sätt även när medlemsstaterna begär API-uppgifter. API-uppgifter gör det möjligt för gränskontrolltjänstemän att på förhand kontrollera passagerarnas identitet och deras resehandlingars giltighet mot de databaser som föreskrivs i kodexen om Schengengränserna. Alla medlemsstater använder dock inte denna möjlighet till förhandskontroll.

I API-direktivet anges endast begränsade kriterier för insamling, överföring och behandling av uppgifter när de gäller de flygningar som omfattas av insamlingen, de uppgiftselement som ska samlas in eller metoderna för att samla in data. Kriterierna är inte heller anpas-

sade till utvecklingen av internationella standarder och riktlinjer om insamling av API-uppgifter. Detta leder till mycket olikartade rutiner, vilket inte bara hämmar in- och utresekontrollernas ändamålsenlighet och effektivitet, utan också utgör en ytterligare börda för lufttrafikföretag som måste uppfylla olika krav beroende på de sträckor på vilka de transporterar passagerare och den medlemsstat som begär API-uppgifter. Att anpassa insamlingen och överföringen av API-uppgifter till dessa internationella standarder för API-uppgifter skulle säkerställa att luftfartsindustrin uppfyller API-kraven.

För att användningen av API-uppgifter ska vara effektiv krävs att de är korrekta, fullständiga och aktuella. I dagsläget händer det att identitetsuppgifter inte är tillförlitliga och verifierade. I sådana fall ger korskontroller i databaser inga tillförlitliga operativa resultat. Ofullständiga, inkorrekta eller föråldrade API-uppgifter som överförs till nationella myndigheter kan leda till kryphål i de typer av kontroller som gränsmyndigheterna kan utföra och i slutändan påverka resenärer som kan bli föremål för felaktiga och onödiga kontroller. I den nuvarande API-ramen föreskrivs inte vilka metoder som ska användas för att samla in API-uppgifter från resenärerna. I motsats till manuellt inmatad information skulle automatiserad insamling av uppgifter leda till mindre kvalitetsproblem och en mer ändamålsenlig och effektiv användning av API-uppgifter, vilket också skulle minska den tid som de behöriga gränsmyndigheterna lägger ned på sina kontakter med lufttrafikföretagen.

Översynen av det nuvarande systemet för insamling och överföring av API-uppgifter innebär en möjlighet att förbättra förvaltningen av de yttre gränserna och bekämpa olaglig invandring.

Innehållet i den föreslagna förordningen är i stora delar identiskt med förslaget om en API-förordning avseende brottsbekämpning. Av artikel 1 framgår att syftet med denna förordning är att förbättra och främja in- och utresekontrollernas ändamålsenlighet och effektivitet vid de yttre gränserna och att bekämpa olaglig invandring. I samma artikel anges att förordningen innehåller regler om överföring av API-uppgifter från routern till de behöriga gränsmyndigheterna, till skillnad från API-förordningen avseende brottsbekämpning som innehåller regler om överföring till enheterna för passagerarinformation.

7 PNR-domen

7.1 Inledning

Den 21 juni 2022 meddelade EU-domstolen dom i mål nr C-817/19, *Ligue des droits humains mot Conseil des ministres*. Den ideella organisationen Ligue des droits humains hade väckt talan vid den belgiska författningsdomstolen om ogiltigförklaring av den belgiska lagstiftningen genom vilken PNR-direktivet och API-direktivet genomförts i belgisk rätt. Författningsdomstolen vände sig till EU-domstolen och begärde ett förhandsavgörande avseende bl.a. giltigheten av PNR-direktivet och huruvida den belgiska lagstiftningen är förenlig med unionsrätten.

EU-domstolen konstaterar inledningsvis att PNR-direktivet enligt allmänna tolkningsprinciper och så långt det är möjligt ska tolkas på ett sätt som inte påverkar dess giltighet och i överensstämmelse med primärrätten i dess helhet, däribland bestämmelserna i EU-stadgan. När en bestämmelse i unionens sekundärrätt kan tolkas på flera sätt ska en tolkning som gör bestämmelsen förenlig med primärrätten ges företräde framför en tolkning som gör bestämmelsen oförenlig med primärrätten. Vid en sådan tolkning bedömer domstolen att det inte har kommit fram någon omständighet som kan påverka direktivets giltighet.

I domen uttalas vidare följande. Luftfartsföretagens överföring av PNR-uppgifter till enheten för passagerarinformation, övervakningen av villkoren för lagring och användning av uppgifterna samt eventuella överföringar till behöriga myndigheter eller Europol utgör betydande ingrepp i de rättigheter som garanteras i artikel 7 och 8 i EU-stadgan. Denna bedömning görs bl.a. mot bakgrund av att direktivet syftar till att införa ett system för övervakning som är kontinuerlig och systematisk och inte riktad samt att systemet innefattar automatiserad utvärdering av personuppgifter för samtliga personer som

använder sig av lufttransporter. Frågan är om dessa ingrepp är motiverade.

De rättigheter som slås fast i artikel 7 och 8 i EU-stadgan är inte absoluta, utan de ska betraktas i förhållande till deras funktion i samhället. Varje begränsning av dessa rättigheter ska vara föreskriven i lag och förenlig med det väsentliga innehållet i fri- och rättigheterna. Begränsningarna ska vara proportionerliga, dvs. endast göras om de är nödvändiga och faktiskt svarar mot ett mål av allmänt samhällsintresse som erkänns av unionen eller av behovet av skydd för andra människors rättigheter och friheter.

7.2 Tillåtna ändamål för behandling av PNR uppgifter

Den hänskjutande domstolen ställde frågan om unionsrätten utgör hinder för en nationell lagstiftning som tillåter behandling av PNR-uppgifter som samlats in i enlighet med direktivet i syfte att följa upp underrättelse- och säkerhetstjänstens verksamhet. Med detta avses den verksamhet som bedrivs inom ramen för skyddet för nationell säkerhet.

EU-domstolen uttalade att i artikel 1.2 i PNR-direktivet anges uttryckligen att PNR-uppgifter som samlas in i enlighet med direktivet endast får behandlas för att beivra terroristbrott och grov brottslighet. Enligt domstolen framgår det tydligt att uppräkningen är uttömmande. I den mån den nationella lagstiftningen godtar att ett syfte med behandlingen är att följa upp underrättelse- och säkerhetstjänstens verksamhet riskerar lagstiftningen att inte respektera att uppräkningen är uttömmande. I den engelska versionen av PNR-domen anges det *monitoring activities*, vilket på svenska torde motsvara övervakande åtgärder snarare än uppföljande åtgärder.

Denna tolkning får enligt domstolen stöd i skäl 11 i PNR-direktivet där det anges att behandlingen av PNR-uppgifter ska stå i proportion till de särskilda säkerhetsmål som direktivet syftar till att uppfylla, och av artikel 7.4, där det framgår att PNR-uppgifter och resultatet av den behandling av dessa uppgifter som mottas av enheten för passagerarinformation endast får vidarebehandlas om det specifika syftet är att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet.

PNR-uppgifter får inte heller lagras i en databas som kan användas för andra ändamål än de som tillåts enligt direktivet, eftersom detta skulle innebära en risk för att uppgifterna används för andra ändamål.

EU-domstolen tydliggör sitt ställningstagande ytterligare genom att ange att unionsrätten utgör hinder för nationell lagstiftning som tillåter behandling av PNR-uppgifter som samlats in i enlighet med direktivet för andra ändamål än de som uttryckligen anges i artikel 1.2 i direktivet.

7.3 Lagringstid för PNR-uppgifter

Enligt artikel 12 i PNR-direktivet ska medlemsstaterna se till att PNR-uppgifter som lämnas av lufttrafikföretag till enheten för passagerarinformation lagras i en databas under en period på fem år efter överföringen. Vid utgången av en period på sex månader efter överföringen ska alla PNR-uppgifter avidentifieras genom maskering av vissa uppgifter som kan användas för att omedelbart identifiera de passagerare som uppgifterna avser. Efter fem år ska uppgifterna slutgiltigt raderas. Som skäl för regleringen anges att lagringstiden bör vara tillräckligt lång och stå i proportion till ändamålen med behandlingen av uppgifterna. Enligt EU-domstolen är lagringen således inte motiverad om det saknas ett objektivt samband mellan lagringen och de mål som eftersträvas med direktivet, dvs. bekämpande av terroristbrott och grov brottslighet som har ett åtminstone indirekt objektivt samband med lufttransport av passagerare.

EU-domstolen konstaterar i PNR-domen att det i enlighet med skäl 25 till direktivet ska göras åtskillnad mellan å ena sidan den inledande lagringstiden på sex månader och, å andra sidan, den efterföljande perioden upp till fem år. Efter den inledande perioden ska åtkomst till uppgifter som gör det möjligt att direkt identifiera den registrerade endast beviljas under mycket strikta och begränsade villkor. Ju längre tid PNR-uppgifterna lagras, desto allvarligare ingrepp innebär en behandling av uppgifterna.

När det gäller perioden från sex månader fram till femårsperiodens slut medför lagring av PNR-uppgifter avseende samtliga passagerare inneboende risker för oproportionerlig användning och missbruk, till följd av den stora mängd uppgifter som kan lagras kontinuerligt. Sådan lagring förefaller alltså, enligt EU-domstolen, inte vara begränsad

till vad som är strikt nödvändigt. I de fall där det kunnat fastställas objektiva omständigheter som gör det möjligt att anse att vissa passagerare skulle kunna utgöra en risk framstår lagring av deras uppgifter som tillåten även efter den inledande sexmånadersperioden. När det gäller flygpassagerare för vilka det inte föreligger objektiva omständigheter som visar att det finns en risk för terroristbrott eller grov brottslighet som har ett åtminstone indirekt objektivt samband med dessa passagerares flygresor tycks det inte vara motiverat att dessa uppgifter lagras.

Att kontinuerligt lagra PNR-uppgifter för samtliga passagerare efter den inledande sexmånadersperioden är alltså inte begränsat till vad som är strikt nödvändigt och lagringen är därmed inte proportionerlig. PNR-direktivet utgör således enligt EU-domstolen hinder för en nationell lagstiftning som föreskriver en generell lagringstid på fem år för PNR-uppgifter som tillämpas utan åtskillnad på alla flygpassagerare.

7.4 Flygningar inom EU

Artikel 2 i PNR-direktivet ger medlemsstaterna rätt att tillämpa direktivet på flygningar inom EU. Även om det inte finns någon skyldighet att tillämpa direktivet på detta sätt har de flesta medlemsstater valt att utnyttja denna möjlighet.

Tillämpningen av PNR-direktivet på flygningar inom EU aktualiserar den fria rörligheten för personer, vilken är en av de grundläggande friheterna på den inre marknaden. Enligt artikel 3.2 i Fördraget om Europeiska unionen ska unionen erbjuda sina medborgare ett område med frihet, säkerhet och rättvisa utan inre gränser. Den fria rörligheten ska garanteras, samtidigt som lämpliga åtgärder vidtas avseende kontroller vid yttre gränser samt förebyggande och bekämpande av brottslighet. Enligt artikel 67.2 i Fördraget om Europeiska unionens funktionssätt ska unionen säkerställa att det inte förekommer någon kontroll av personer vid de inre gränserna, och den ska utarbeta en gemensam politik för kontroll av de yttre gränserna. Detta gäller inte bara lufttransport utan även järnvägs-, land- och sjötransporter inom unionen.

En inskränkning i den fria rörligheten för personer kan vara motiverad om den grundar sig på objektiva hänsyn till allmänintresset

och står i proportion till det legitima syfte som eftersträvas med de nationella bestämmelserna.[1] En inskränkning måste vidare vara förenlig med de grundläggande rättigheter som uppställs i EU-stadgan.

I det aktuella målet ställdes frågan om unionsrätten ska tolkas så att den utgör hinder för en nationell lagstiftning som föreskriver ett system för överföring och behandling av PNR-uppgifter för flyg och transporter med andra transportmedel inom unionen – från, till eller via den medlemsstat som antagit lagstiftningen i fråga.

EU-domstolen tar därvid upp att nationell lagstiftning som missgynnar vissa medborgare i en medlemsstat endast på grund av att de har utnyttjat rätten att fritt röra sig och uppehålla sig i en annan medlemsstat utgör en inskränkning i de friheter som tillkommer varje unionsmedborgare enligt EU-stadgan.

En sådan lagstiftning som är aktuell i målet, där PNR-direktivet tillämpas på flygningar och annan transport inom EU, leder till systematisk och kontinuerlig överföring och behandling av PNR-uppgifter för varje passagerare som på dessa sätt förflyttar sig inom unionen. Detta utgör ett allvarligt ingrepp i de grundläggande rättigheter som garanteras i artikel 7 och 8 i EU-stadgan. Ingreppet blir ännu allvarligare om tillämpningen av detta system utvidgas till att omfatta andra transportmedel inom unionen. Sådana ingrepp kan även missgynna medborgare i de medlemsstater som antagit en sådan lagstiftning samt unionsmedborgare som förflyttar sig med dessa transportmedel inom unionen, till eller från medlemsstaterna som antagit sådan lagstiftning. Det kan följaktligen avhålla dem från att utöva sin rätt till fri rörlighet. Det innebär att den aktuella lagstiftningen medför en inskränkning i denna grundläggande frihet.

En inskränkning i den fria rörligheten för personer kan vara motiverad endast om den grundar sig på objektiva skäl och står i proportion till det legitima syfte som eftersträvas med de nationella bestämmelserna. En åtgärd är proportionerlig om den är ägnad att säkerställa att det eftersträvade målet uppnås och inte går utöver vad som är nödvändigt för att uppnå detta mål. En nationell bestämmelse som kan hindra personer från att utöva sin fria rörlighet kan bara anses motiverad om den är förenlig med de grundläggande rättigheter som garanteras i stadgan.

[1] Se t.ex. EU-domstolens dom den 5 juni 2018, *Coman m.fl. mot Inspectoratul General pentru Imigrari m.fl.*, mål nr C-673/16, p. 41.

EU-domstolen uttalar sig därefter om huruvida lagstiftningen är lämplig och nödvändig för att uppnå det eftersträvade målet att bekämpa terroristbrott och grov brottslighet. Det har framgått att användningen av PNR-uppgifter gör det möjligt att identifiera personer som inte tidigare har misstänkts delta i terroristbrott eller i grov brottslighet, och som bör undersökas närmare. Lagstiftningen framstår därför som lämplig för att nå det eftersträvade målet med att bekämpa terroristbrott och grov brottslighet.

Kravet att lagstiftningen ska vara strikt nödvändig gör sig i än högre grad gällande när PNR-direktivet tillämpas på andra transportmedel inom unionen. Unionsrätten utgör hinder för nationell lagstiftning som, i avsaknad av ett verkligt och aktuellt eller förutsebart terroristhot i den berörda medlemsstaten, föreskriver ett system för överföring och behandling av PNR-uppgifter för alla flygningar inom EU och transporter med andra transportmedel, i syfte att bekämpa terroristbrott och grov brottslighet. I en sådan situation ska tillämpningen av systemet begränsas till överföring och behandling av PNR-uppgifter avseende flygningar och/eller transporter gällande bl.a. vissa flyglinjer eller resmönster eller vissa flygplatser, järnvägsstationer eller hamnar för vilka det finns uppgifter som kan motivera en sådan tillämpning.

Det ankommer på den berörda medlemsstaten att välja ut de flygningar inom EU och/eller andra transporter med andra transportmedel inom EU för vilka sådana uppgifter förekommer. Det ska regelbundet göras en översyn av tillämpningen med hänsyn till utvecklingen av de villkor som motiverat urvalet för att säkerställa att tillämpningen av systemet alltid är begränsad till vad som är strikt nödvändigt. Unionsrätten utgör vidare hinder för en nationell lagstiftning som föreskriver ett system för överföring och behandling av uppgifter insamlade med stöd av PNR-direktivet i syfte att förbättra gränskontrollerna och bekämpandet av illegal invandring.

7.5 Prövning av domstol eller oberoende förvaltningsmyndighet

7.5.1 Förhandskontroll vid begäran om tillgång till PNR-uppgifter

I artikel 12.3 b i PNR-direktivet anges att utlämnande av fullständiga PNR-uppgifter, efter den inledande sexmånadersperioden, endast ska tillåtas om det rimligen kan antas vara nödvändigt för de ändamål som anges i artikel 6.2 b, och efter tillstånd från en rättslig myndighet eller en annan nationell myndighet som i enlighet med nationell rätt är behörig att kontrollera om villkoren för tillgång är uppfyllda, under förutsättning att dataskyddsombudet vid enheten för passagerarinformation informeras och att denne genomför en efterhandsutvärdering.

Utöver vad som anges i artikel 12.3 b ges inte någon ytterligare vägledning i direktivet avseende vilka krav som ställs på en rättslig eller annan myndighet som ska utföra förhandskontrollen av om PNR-uppgifter kan överföras efter den inledande sexmånadersperioden.

I PNR-domen aktualiserades frågan om artikel 12.3 b utgör hinder för en nationell lagstiftning som föreskriver att den myndighet som inrättats som enhet för passagerarinformation även är behörig nationell myndighet med befogenhet att godkänna utlämnande av PNR-uppgifter vid utgången av sexmånadersperioden som följer efter överföringen av uppgifter till enheten för passagerarinformation.

Enligt EU-domstolen likställs en rättslig myndighet och en annan nationell myndighet i detta sammanhang. Följaktligen måste den nationella myndighet som utför förhandskontrollen ha en nivå av oberoende och opartiskhet som är jämförbar med en rättslig myndighet.

Den nationella myndigheten, som i PNR-domen även benämns som en *oberoende administrativ enhet*, måste vara fristående i förhållande till den myndighet som begär tillgång till uppgifterna, för att säkerställa att den kan utövas sin kontroll på ett objektivt och opartiskt sätt och skyddas mot yttre påverkan. På det straffrättsliga området innebär kravet på oberoende särskilt att den myndighet som ska utföra förhandskontrollen inte får vara involverad i den aktuella brottsutredningen och dessutom måste ha en neutral ställning till parterna i det straffrättsliga förfarandet.

Artikel 4.1 och 4.3 i PNR-direktivet anger att enheten för passagerarinformation ska vara behörig myndighet när det gäller att beivra

terroristbrott och annan grov brottslighet. Personalen vid enheten kan vara tjänstemän som avdelats från de behöriga myndigheter som avses i artikel 7 i direktivet, vilket för med sig att enheten med nödvändighet tycks vara anknuten till dessa myndigheter. Enheten får vidare även behandla PNR-uppgifter och lämna ut resultaten av behandlingen till beställarmyndigheterna. Därmed kan enheten för passagerarinformation inte anses vara fristående i förhållande till dessa myndigheter och den har inte den oberoende ställning och opartiskhet som krävs för att utföra förhandskontrollen av om villkoren för utlämnande av samtliga PNR-uppgifter är uppfyllda.

EU-domstolen uttalar vidare att det i artikel 12.3 b inte finns något uttryckligt processuellt villkor om godkännande av en rättslig eller annan myndighet för det fall att förfrågan om utlämnande och utvärdering i efterhand av PNR-uppgifter lämnas in före utgången av sexmånadersfristen. I detta sammanhang ska skäl 25 i direktivet beaktas, av vilket det framgår att unionslagstiftaren avsåg att säkerställa högsta möjliga nivå av dataskydd när det gäller åtkomsten till PNR-uppgifter i en form som gör det möjligt att direkt identifiera den registrerade. Varje förfrågan om utlämnande och bedömning i efterhand förutsätter en sådan åtkomst till dessa uppgifter, oberoende av om förfrågan lämnas in före eller efter sexmånadersperioden efter överföringen av uppgifterna till enheten för passagearrinformation.

För att säkerställa att de grundläggande rättigheterna iakttas fullt ut är det väsentligt att utlämnande av PNR-uppgifter för bedömning i efterhand i princip, utom i vederbörligen motiverade brådskande fall, ska föregås av en förhandskontroll utförd antingen av domstol eller av en oberoende förvaltningsmyndighet. Beslutet ska fattas efter en motiverad begäran från de behöriga myndigheterna. I brådskande fall ska kontrollen genomföras utan dröjsmål. Kravet på förhandskontroll enligt artikel 12.3 b i PNR-direktivet för förfrågningar om utlämnande av PNR-uppgifter som getts in efter utgången av sexmånadersfristen efter överföring av uppgifterna till enheten för passagerarinformation ska således gälla i tillämpliga delar även för det fall att förfrågan om utlämnande ges in före utgången av denna frist.

7.5.2 Beslut om att tillämpa PNR-direktivet på samtliga flygningar inom EU

Som nämnts i avsnitt 7.4 ankommer det på den berörda medlemsstaten att välja ut de flygningar inom EU som PNR-direktivet ska tillämpas på. I detta sammanhang uttalar EU-domstolen att i en situation där det, på grundval av en medlemsstats bedömning, konstateras att det föreligger tillräckligt konkreta omständigheter för att medlemsstaten ska anses stå inför ett verkligt och aktuellt eller förutsebart terrorhot, tycks det inte gå utöver vad som är strikt nödvändigt att tillämpa PNR-direktivet på samtliga flygningar inom EU. Att det föreligger ett sådant hot är nämligen i sig ägnat att upprätta ett samband mellan överföring och behandling av de berörda uppgifterna och kampen mot terrorism.

Beslutet om att tillämpa direktivet på samtliga flygningar inom EU måste kunna bli föremål för effektiv kontroll antingen av en domstol eller av en oberoende förvaltningsmyndighet, vars avgörande har bindande verkan. Syftet med prövningen är att kontrollera om det föreligger skäl för utvidgad tillämpning av PNR-direktivet och att de villkor och garantier som måste ställas upp är uppfyllda. Tillämpningsperioden måste vara tidsmässigt begränsad till vad som är strikt nödvändigt men kan förlängas om hotet kvarstår.

Sammanfattningsvis uppställer således PNR-domen dels ett krav på att ett formellt beslut om utvidgad tillämpning av direktivet ska fattas, dels att ett sådant beslut ska kunna bli föremål för effektiv kontroll av en domstol eller en oberoende förvaltningsmyndighet.

7.6 Jämförelser med relevanta databaser

Enligt artikel 6.3 a får enheten för passagerarinformation, när den utför förhandsbedömningen enligt artikel 6.2 a, jämföra PNR-uppgifter med uppgifter i databaser som är relevanta för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet, inklusive databaser över personer eller föremål som är eftersökta eller finns uppförda på spärrlista, i enlighet med unionsbestämmelser eller internationella eller nationella bestämmelser som är tillämpliga på sådana databaser. Bestämmelsen i PNR-direktivet är genomförd i svensk rätt genom 3 kap. 5 § 1 lagen om flygpassageraruppgifter i brottsbekämpningen.

I PNR-domen tydliggörs hur denna bestämmelse ska tolkas. Även om det framgår av ordalydelsen i artikel 6.1 a i PNR-direktivet att databaser över personer eller föremål som är eftersökta eller finns uppförda på spärrlista ingår bland de ”databaser som är relevanta” och som avses i den bestämmelsen, preciserar den däremot inte vilka andra databaser som också skulle kunna vara ”relevanta” utifrån de mål som eftersträvas med direktivet. Bestämmelsen preciserar inte uttryckligen arten av de uppgifter som sådana databaser kan innehålla och deras förhållande med dessa mål, och det anges inte heller om PNR-uppgifterna bara får jämföras med databaser som förvaltas av myndigheter eller om de även kan jämföras med databaser som förvaltas av privatpersoner.

Vid första anblick skulle artikel 6.3 a kunna tolkas så att PNR-uppgifter kan användas som sökkriterier för att göra analyser utifrån olika databaser, inbegripet databaser som medlemsstaternas säkerhets- och underrättelsemyndigheter förvaltar och använder i syfte att uppnå andra mål än dem som avses i direktivet, och att sådana analyser kan ske i form av utvinning av data. Möjligheten att utföra sådana analyser och att jämföra PNR-uppgifter med sådana databaser skulle kunna ge flygpassagerarna en känsla av att deras privatliv är föremål för en form av övervakning. Även om den förhandsbedömning som föreskrivs i denna bestämmelse utgår från den relativt begränsade samling uppgifter som PNR-uppgifterna utgör, kan en sådan tolkning av artikel 6.3 a inte godtas, eftersom en sådan tolkning skulle kunna medföra ett oproportionerlig utnyttjande av dessa uppgifter som skulle göra det möjligt att fastställa en exakt profil av de berörda personerna enbart till följd av att de avser att resa med flyg.

Med hänsyn till att det är nödvändigt att iaktta de krav på klarhet och precision som krävs för att säkerställa skyddet av de grundläggande rättigheter som slås fast i artikel 7 och 8 i stadgan, är enheten för passagerarinformation skyldig att begränsa den automatiska behandling som föreskrivs i artikel 6.3 a i PNR-direktivet till att endast omfatta de databaser som denna bestämmelse gör det möjligt att identifiera. Även om hänvisningen till ”databaser som är relevanta” inte kan tolkas på ett tillräckligt klart och precist sätt vad gäller vilka databaser som avses, förhåller det sig annorlunda med hänvisningen till ”databaser över personer eller föremål som är eftersökta eller finns uppförda på spärrlista, i enlighet med unionsbestämmelser eller internationella eller nationella bestämmelser som är tillämpliga på sådana

databaser”. De sistnämnda databaserna är de enda databaser som enheten för passagerarinformation får jämföra PNR-uppgifter mot.

Vad gäller de krav som dessa databaser ska uppfylla, ska det påpekas att enligt artikel 6.4 i PNR-direktivet ska den förhandsbedömning som görs utifrån på förhand fastställda kriterier utföras enligt artikel 6.4 i direktivet, på ett icke-diskriminerande sätt. Dessa kriterier måste vara riktade, proportionella och specifika. Medlemsstaterna ska se till att kriterierna fastställs och regelbundet ses över av enheterna for passagerarinformation i samarbete med de behöriga myndigheter som avses i artikel 7. Kravet på att dess databaser ska vara icke-diskriminerande innebär bl.a. att uppgifter om personer som eftersöks eller som finns uppförda på en spärrlista bara får föras in i databaserna enligt objektiva och icke-diskriminerande kriterier som definieras i unionsbestämmelser eller nationella eller internationella bestämmelser som är tillämpliga på sådana databaser.

För att uppfylla kravet på att de på förhand fastställda kriterierna ska vara riktade, proportionella och specifika, ska databaserna dessutom användas i samband med bekämpningen av terroristbrott och grov brottslighet som har ett åtminstone indirekt objektivt samband med lufttransport av passagerare.

De databaser som används i enlighet med artikel 6.3 a i PNR-direktivet ska förvaltas av de behöriga myndigheter som avses i artikel 7 i direktivet eller, vad gäller EU-databaser och internationella databaser, användas av dessa myndigheter inom ramen för deras uppdrag att bekämpa terroristbrott och grov brottslighet. Så är fallet med databaser avseende de personer eller föremål som eftersöks eller som finns uppförda på en spärrlista.

7.7 Medlemsstaternas agerande efter PNR-domen

Eftersom många medlemsstater, precis som Sverige, fortfarande inte har avslutat arbetet med anpassningar av sina nationella regleringar till PNR-domen är det förenat med svårigheter att göra jämförelser med övriga medlemsstater. PNR-regelverket bygger på ett direktiv och det ursprungliga genomförandet kan därför skilja sig åt mellan medlemsstaterna, vilket ytterligare försvårar sådana jämförelser. Flera av de förändringar som har genomförts har därutöver skett genom ändrad praktisk hantering av PNR-uppgifter hos medlemsstaternas

respektive enheter för passagerarinformation. Information om sådana förändringar är regelmässigt inte offentlig, vilket innebär att det är vanskligt att få en överblick över hur medlemsstaterna har agerat sedan PNR-domen meddelades.

De lagstiftningsärenden som har initierats av flera medlemsstater för att förändra den nationella rätten i linje med PNR-domen befinner sig alltså i olika stadier, som i flera fall i dagsläget inte har lett till antagen lagstiftning. Några exempel kan dock nämnas.

Tyskland har genomfört flera förändringar i hanteringen av PNR-uppgifter. Detta har exempelvis skett genom att man har uppdaterat bedömningarna av om det finns en direkt eller indirekt koppling mellan PNR-uppgifterna och internationell flygtrafik och om det misstänkta brottet faller inom tillämpningsområdet för direktivet, dvs. om det rör sig om terrorism eller annan grov brottslighet. Det har upprättats en oberoende nationell tillsynsmyndighet som ger råd avseende och överser behandlingen av PNR-uppgifter samt en enhet, *Risk-Flow Unit*, som analyserar vilka riskrutter som ska tillgängliggöras inom PNR-systemet. Den generella lagringstiden för PNR-uppgifter som inte har gett upphov till någon träff har sänkts från fem år till sex månader.

Flera länder, t.ex. Finland, har inlett lagstiftningsärenden för att förändra den nationella lagstiftningen i enlighet med vad som anges i PNR-domen. I Polen lämnades i november 2025 ett lagförslag över till *Sejm*, det polska parlamentets underhus. Lagförslaget behandlar bl.a. hur PNR-uppgifter för flygningar inom EU får behandlas.

I Belgien görs numera en terrorhotbedömning av *Coordination Unit for Threat Analysis*, OCAD. I dagsläget gör OCAD bedömningen att terrorhotet är av sådant allvar att det berättigar till insamling och vidare behandling av PNR-uppgifter för samtliga flygningar inom EU. Belgien tillämpar även bedömningen av terrorhotet för att motivera att PNR-uppgifter lagras hos enheten för passagerar-uppgifter i fem år. Bedömningen ska senast den 12 oktober 2026 genomgå en översyn för att säkerställa att förutsättningarna för en sådan tillämpning fortfarande föreligger.

7.8 Diskussion efter PNR-domen

7.8.1 Europeiska dataskyddsstyrelsens uttalande

Europeiska dataskyddsstyrelsen (*European Data Protection Board*, EDPB) är ett organ inom EU med uppgift att se till att dataskyddsförordningen och dataskyddsdirektivet för brottsbekämpning tillämpas enhetligt inom hela unionen. Som ett led i detta arbete ger EDPB råd och avger yttranden till Europeiska kommissionen i frågor som rör skydd av personuppgifter. EDPB:s yttranden är inte bindande för medlemsstaterna.

Den 13 mars 2025 utfärdade EDPB ett uttalande[2] om tillämpningen av PNR-direktivet i ljuset av PNR-domen. Även om EDPB konstaterar att PNR-direktivets giltighet inte ifrågasattes av domstolen innebär domen att direktivet måste tolkas mer restriktivt än tidigare avseende skyddet för personuppgifter, särskilt när det gäller skyddet för personuppgifter som garanteras i artikel 7 och 8 i EU-stadgan. I detta avsnitt sammanfattas ett urval av de rekommendationer som EDPB ger i uttalandet.

Objektiv koppling

För att tillämpning av systemet som etablerats av PNR-direktivet ska vara tillåten krävs det att det finns en direkt eller indirekt koppling mellan transporten av passagerare och terroristbrott eller grov brottslighet. För att kunna konstatera att en sådan koppling föreligger måste det fastställas objektiva kriterier för hur PNR-uppgifter kopplas till bekämpandet av sådana brott. En direkt koppling avser brott som riktar sig mot flygtransporten av passagerare samt brott som begås under eller genom flygresan. En indirekt koppling täcker de situationer där det inte finns någon direkt koppling, men terroristbrott och grov brottslighet kan förhindras, upptäckas, utredas eller lagföras genom behandling av PNR-uppgifter.

Varje tillämpning av PNR-systemet måste kontrolleras för att utvärdera om det finns en objektiv koppling. För att minska allvaret i inskränkningen av skyddet för personuppgifter behöver en sådan analys ske så tidigt som möjligt i processen. När en person har iden-

[2] EDPB, *Statement 2/2025 on the implementation of the PNR Directive in light of CJEU Judgment C-817/19*, den 13 mars 2025.

tifierats i den inledande automatiska behandlingen ska enheten för passagerarinformation därefter genomföra en manuell granskning. Överföring av PNR-uppgifter till behöriga myndigheter får endast ske om det finns tillräckligt underlag för att skäligen misstänka att personen som identifierats genom den automatiska behandlingen är delaktig i terroristbrott eller grov brottslighet.

När det gäller begäran från behöriga myndigheter gör EU-domstolen åtskillnad mellan en begäran som rör terroristbrott och en begäran som rör annan grov brottslighet. När det rör annan grov brottslighet krävs det en betydligt mer djupgående analys av enheten för passagerarinformation för att fastställa att förfrågan bygger på tillräckliga skäl, dvs. att förfrågan är baserad på objektiva uppgifter som ger anledning att misstänka att en person är inblandad i grov brottslighet som har koppling till flygtransporten. Denna mer djupgående analys bör fastställas i enheten för passagerarinformations interna rutiner, bl.a. för att tillsynsmyndigheten ska kunna granska processen.

Flygningar inom EU

EDPB uttalar sig även om flygningar inom EU. En medlemsstat som vill utnyttja möjligheten att antingen tillämpa PNR-direktivet på samtliga eller vissa utvalda flyg inom EU måste säkerställa att tillämpningen är begränsad till vad som är strikt nödvändigt för att säkerställa unionens, eller åtminstone den enskilda medlemsstatens, säkerhet och således för att skydda människors liv och säkerhet. I en sådan bedömning ska det beaktas hur allvarligt intrång det innebär i de grundläggande rättigheterna i artikel 7 och 8 i EU-stadgan.

Om det finns ett terroristhot som är verkligt och aktuellt eller förutsebart får medlemsstaterna samla in PNR-uppgifter från alla flygningar inom EU, under en begränsad tid. Detta gäller dock endast om principerna om strikt nödvändighet och proportionalitet beaktas. Principerna ska respekteras både under tiden för tillämpningen och när det gäller omfattningen av tillämpningen, dvs. vilka flygningar som PNR-direktivet tillämpas på. Om hotet inte gäller vissa flygningar är det möjligt att tillämpningen på alla flyg inom EU inte är nödvändig och proportionerlig. Myndigheterna i respektive land är ansvariga för att göra denna bedömning.

Eftersom tillämpningen av PNR-systemet innebär allvarliga inskränkningar i grundläggande rättigheter måste alla omständigheter och bedömningar som rättfärdigar urvalet av vilka flygningar som ska omfattas av tillämpningen dokumenteras och kontinuerligt omprövas. Omprövningen bör ske åtminstone var sjätte månad. Om en medlemsstat har beslutat att samla in PNR-uppgifter för samtliga flyg inom EU på grund av ett terroristhot måste beslutet kunna bli föremål för effektiv kontroll av en domstol eller av en oberoende förvaltningsmyndighet, vars avgörande har bindande verkan.

Enskildas rättigheter och automatiserad behandling

Enskildas rättigheter i enlighet med artikel 13.1 i PNR-direktivet ska säkerställas genom att tillhandahålla så fullständig information som möjligt till de registrerade, samt genom att de registrerade ska ha möjlighet att ifrågasätta lagligheten av den automatiserade behandlingen och den efterföljande individuella bedömningen och få ta del av grunderna och bevisningen som ligger till grund för ett beslut i en rättslig process.

EDPB rekommenderar att de behöriga myndigheterna upprättar tydliga och detaljerade regleringar för hur avvägningen ska göras mellan de behöriga myndigheternas intressen och enskildas grundläggande rättigheter.

Förhandsgranskning

En domstol eller en oberoende administrativ enhet ska utföra förhandsgranskningen som krävs för att PNR-uppgifter ska lämnas ut från enheten för passageraruppgifter till en behörig myndighet efter den inledande sexmånadersperioden. Myndigheten som utför förhandsgranskningen bör inte vara en myndighet som är involverad i utredningen av det aktuella brottet. Det bör inte heller vara möjligt att överlämna förhandsgranskningen till en tjänsteman eller en enhet inom en myndighet som i sig inte är oberoende i relation till brottsutredningen.

EU-domstolen ställer upp ett flertal krav på den myndighet som ska göra förhandsgranskningen. Myndigheten ska

- kunna göra en avvägning mellan de olika intressena och rättigheterna i fråga,
- ha en ställning som innebär att den kan fullgöra sitt uppdrag på ett objektivt och opartiskt sätt,
- vara fri från yttre påverkan och neutral i förhållande till parterna,
- vara fristående i förhållande till den behöriga myndighet som begär tillgång till uppgifterna,
- inte vara involverad i den aktuella brottsutredningen.

EDPB understryker vidare att myndigheten som ska utföra förhandsgranskningen måste ha tillräckliga resurser vad gäller budget och personal samt ha tillräcklig kunskap om brottsbekämpning.

Lagringstid

I artikel 12 i PNR-direktivet anges att PNR-uppgifter ska sparas under en period på fem år. Detta är dock inte motiverat såvida om det saknas ett objektivt samband mellan lagringen av uppgifter och syftena med direktivet. Enligt EU-domstolen kan lagringstiden delas upp i två separata perioder, dels den inledande perioden på sex månader, dels den senare perioden upp till fem år räknat från överföringen till enheten för passagerarinformation. Efter den inledande sexmånadersperioden får PNR-information endast lagras i den mån det finns ett objektivt samband med syftena med behandlingen enligt PNR-direktivet och bara så länge det är nödvändigt och proportionerligt. Det är därmed inte tillåtet att uppställa en generell lagringsperiod på fem år. Bedömningen av om fortsatt lagring av uppgifter är nödvändig och proportionerlig ska ske kontinuerligt.

EDPB:s avslutande synpunkter

Så som PNR-direktivet tolkades och tillämpades innan PNR-domen innebar det inskränkningar av grundläggande rättigheter för miljoner människor inom EU. EU-domstolen har fastställt att tolkningen i delar

inte var förenlig med PNR-direktivet. Det understryker vikten av att medlemsstaterna följer kraven i direktivet i ljuset av PNR-domen.

Såvitt EDPB känner till har några medlemsstater börjat anpassa nationell rätt efter domen, men det behöver fortfarande genomföras förändringar på bred front i medlemsstaterna. Det är av vikt att medlemsstaterna anpassar tillämpningen av direktivet till den restriktiva tolkningen av direktivet som framgår av domen. Förändringarna bör dessutom genomföras skyndsamt.

7.8.2 Kommissionens diskussionspromemoria

Den 9 september 2022 publicerade Europeiska kommissionen en promemoria med syftet att diskutera konsekvenserna av PNR-domen samt att främja efterlevnaden av de uttalanden som domstolen gjorde i domen.[3]

I promemorian anger kommissionen att det finns starka skäl som talar för att även fortsättningsvis tillämpa PNR-direktivet på flygningar inom EU, även med beaktande av de begränsningar som domen innebär. Vissa medlemsstater har uppgett att ungefär tre fjärdedelar av arbetsbördan för deras enheter för passagerarinformation rör flygningar inom EU.

Att enbart tillämpa PNR-direktivet på vissa utvalda flygningar inom EU innebär ett flertal påtagliga nackdelar. I ljuset av detta bör gångbara alternativ som är förenliga med uttalandena i domen utforskas. Enligt domen får PNR-information samlas in avseende samtliga flygningar inom EU endast om det föreligger ett terroristhot. Ett sådant hot är emellertid svårt att kvantifiera och det är sällan begränsat till en specifik tidsperiod.

En tillräcklig begränsning av behandlingen av PNR-uppgifter skulle kunna uppnås genom en filtrering av PNR-uppgifter från alla flygningar inom EU genom en automatisk jämförelse med relevanta databaser. Felaktiga träffar skulle därefter raderas. Genom att endast behålla information avseende personer som redan eftersöks av brottsbekämpande myndigheter och eftersom det inte innebär ett urval genom förbestämda kriterier kan det argumenteras för att det inte tillämpas urskillningslöst på samtliga passagerare.

[3] Europeiska kommissionen, *Improving Compliance with the Judgement in Case C-817/19 – Ideas for Discussion*, 11911/22, den 9 september 2022.

Om insamlingen av PNR-information ska begränsas till ett visst urval av rutter eller flygplatser kommer urvalet över tid att förändras. Det innebär ett flertal utmaningar. Lufttrafikföretagen kommer att behöva identifiera de relevanta flygningarna och omedelbart aktivera och avaktivera överföringen av information. Vilka flygningar som är relevanta kan dessutom skilja sig från land till land och ett lufttrafikföretag som är verksamt i flera olika medlemsstater kommer därmed behöva förhålla sig till ett flertal olika riktlinjer avseende urvalet av flygningar

Eftersom urvalet av flygningar kommer att variera över tid innebär det vidare att arbetsbördan för medlemsstaternas enheter för passagerarinformation kommer att variera. Det medför ekonomiska utmaningar avseende bemanning och övriga resurser. Vidare innebär ett urval av flygningar att potentiella terrorister och andra brottslingar kommer att försöka tillskansa sig information om processen för att välja ut relevanta flygningar.

Ett alternativ för att minska påverkan på brottsbekämpningen är att sållningen av information sker hos enheten för passagerarinformation i stället för hos lufttrafikföretagen. Det kräver att enheten för passagerarinformation omedelbart och utan att behandla uppgifterna raderar de uppgifter som rör flygningar eller flygplatser som inte vid tidpunkten har valts ut för behandling. Fördelen med detta är att det inte innebär några förändringar för lufttrafikföretagen samt att det aktuella urvalet av flygningar inte avslöjas för flygindustrin.

Ett annat alternativ är att riskbedömningen görs på europeisk nivå i stället för nationell samt att medlemsstaterna samarbetar avseende riskbedömningen. För detta krävs att metoden för riskbedömning harmoniseras inom unionen, alternativt att medlemsstaterna har kännedom om varandras riskbedömningar.

Artikel 9 i direktivet möjliggör utbyte av PNR-information mellan medlemsstater. Sådant informationsutbyte initieras antingen av enheten för passagerarinformation i enlighet med artikel 6.2 eller genom en motiverad begäran från en annan medlemsstats enhet för passagerarinformation. Artikel 2 anger att, för det fall att en medlemsstat beslutar att tillämpa direktivet på flygningar inom EU, ska alla bestämmelser i direktivet gälla för flygningar inom EU som om de vore flygningar utom EU. PNR-domen synes inte förändra denna syn på tillämpningsområdet för direktivet. Det kan därmed diskuteras huruvida det är möjligt för enheten för passagerarinformation att dela PNR-

information och resultatet av behandlingen av sådan information med en annan medlemsstat, även om informationen rör flygningar inom EU som den andra medlemsstaten inte inkluderat i dess eget urval av flygningar inom EU.

7.8.3 Medlemsstaternas synpunkter på kommissionens promemoria

Medlemsstaterna gavs möjlighet att besvara de frågeställningar som kommissionen tog upp diskussionspromemorian och den 26 oktober 2022 publicerades dessa svar.[4]

Många av medlemsstaterna uttrycker en oro över de negativa konsekvenser för brottsbekämpningen som PNR-domen medför. Det finns risk för att möjligheten att bekämpa terrorism och grov brottslighet kraftigt beskärs om anpassningarna till uttalandena i domen blir alltför långtgående. Medlemsstaterna efterfrågar ett samarbete mellan staternas respektive enheter för passagerarinformation inom ramen för EU-samarbetet för att i så stor utsträckning som möjligt begränsa de negativa konsekvenserna av PNR-domen.

Begränsningar avseende flygningar inom EU

PNR-uppgifter från flygningar inom EU har hittills utgjort en stor andel av de uppgifter som behandlas vid enheterna för passagerarinformation. Österrike har beslutat att inte samla in uppgifter för flygningar inom EU, vilket har lett till att deras enhet för passagerarinformation behandlar 66 procent färre uppgifter än tidigare. Flera medlemsstater uppger att en majoritet av uppgifterna som behandlas avser sådana flygningar. I Finland uppgår sådan behandling till cirka 75 procent av all behandling vid enheten och enstaka år till över 80 procent.

Enligt medlemsstaterna innebär begränsningen av insamlingen som uppställs i PNR-domen ett flertal nackdelar. Med tanke på de informationsluckor som uppstår när det saknas information kan den befintliga PNR-informationen inte utvärderas och analyseras på det sätt som krävs. Österrike exemplifierar detta med ett fall där en med-

[4] Europeiska kommissionen, *Improving Compliance with the Judgement in Case C-817/19 – comments from Member States*, 12856/22, den 26 oktober 2022.

lem av al-Qaida enligt uppgift skulle resa från en annan medlemsstat till Österrike. Verifieringen av huruvida personen faktiskt gick ombord på planet kunde inte ske med PNR-uppgifter, eftersom sådana saknades. Det krävdes i stället alternativa, mer resurs- och tidskrävande, metoder för en verifiering som inom PNR-system hade kunnat ske nästan omedelbart.

Många medlemsstater för fram att tillämpningen av PNR-direktivet på samtliga flygningar inom EU bidrar väsentligt till säkerheten inom unionen. Om detta begränsas innebär det en stor risk för att potentiella terrorister inte kommer att kunna identifieras, vilket underminerar den interna säkerheten.

Danmark anser att potentiella terrorister och andra brottslingar snabbt kommer att hitta och utnyttja informationsluckorna, dvs. de rutter som inte övervakas, för att undvika gränskontroll och övervakning. Att avgöra vilka rutter som ska bevakas kommer att försvåra arbetet mot oförutsedda terrorbrott. Enheten för passagerarinformation kommer i stället för att arbeta proaktivt, så som fallet är i dagsläget, tvingas bli mer reaktiv. Den danska Polismyndigheten ser inget lämpligt eller användbart alternativ för minimeringen av behandling av PNR-information för flygningar inom EU.

Estland ser ingen möjlighet att ens utesluta delar av insamlingen av PNR-information för flygningar inom EU. De flesta passagerare som kommer till Estland kommer från flygplatser i Europa. Det går inte att på förväg veta vilken rutt eller vilket flygbolag som kommer att användas av kriminella organisationer.

Flera medlemsstater för fram att det behövs en koordinerad insats på EU-nivå för att upprätthålla ett effektivt PNR-system och begränsa de negativa effekterna som PNR-domen kan medföra. Litauen anser att det skyndsamt behövs ny unionslagstiftning avseende behandling av PNR-uppgifter för flygningar inom EU.

Urval av flygningar inom EU

Enligt PNR-domen får PNR-information inte samlas in för samtliga flygningar inom EU, såvida det inte finns ett konkret och aktuellt eller förutsebart terrorhot. I avsaknad av ett sådant hot måste i stället ett urval av t.ex. rutter och flygplatser göras. Medlemsstaterna är överens

om att det av säkerhetsskäl inte är gångbart att avslöja detta urval för lufttrafikföretagen.

Enligt Danmarks polismyndighet vore att informera lufttrafikföretagen om vilka rutter som bevakas likvärdigt med att publicera polisen aktiviteter och information på internet. Informationen får i sådana fall ses som offentliga uppgifter. Finland uppger att det skulle stå i strid med nationell lagstiftning att på detta sätt avslöja taktiska och tekniska metoder som används av brottsbekämpande myndigheter. Även Sverige har fört fram att det inte är möjligt att avslöja något om bedömningskriterierna eller vilka metoder som används. Det troliga resultatet av ett sådant system är att behöriga myndigheter helt enkelt skulle sluta använda PNR-uppgifter. Sammanfattningsvis är medlemsstaternas uppfattning att urvalet av rutter och flygplatser som omfattas av insamlingen av PNR-uppgifter måste lösas på ett sätt som gör att informationen om bedömningen inte når lufttrafikföretagen.

Det har även förts fram att ett stort framsteg med PNR-direktivet var att man lämnade konceptet *risk routes*, dvs. att endast vissa rutter ansågs innebära en förhöjd risk för terroristbrott och annan grov brottslighet. Att gå tillbaka till ett sådant system vore ett steg tillbaka i det förflutna. Enligt Spanien är det endast möjligt att får ett mönster av brottslig aktivitet genom att analysera samtliga flygningar inom EU. En lösning vore att analysera samtliga data och därefter radera allt som inte resulterar i en träff. Det är, enligt Spanien, inte en idealisk lösning, men den går att acceptera om det är det närmaste man kan komma att behålla all information avseende flygningar inom EU. Om PNR-domen däremot tolkas bokstavligt kommer det bli nästintill omöjligt att genomföra polisarbete.

Ett urval av flygningar kommer även att medföra kostnader. Det finns i dag ingen teknisk lösning för att automatiskt radera vissa flygningar från enheten för passagerarinformations databas eftersom det hittills inte har behövts. Att koppla på nya flygbolag och nya rutter till PNR-systemet är också tidskrävande; i många fall tar det flera månader. Rutter ändras också frekvent.

Ett förslag som förs fram är att uppgifter avseende flygningar som inte för tillfället bevakas ska raderas omedelbart när de kommer in till enheten för passagerarinformation. Det går visserligen att tolka PNR-domen som att även själva översändandet av PNR-uppgifter från lufttrafikföretagen till enheten för passagerarinformation utgör

behandling av uppgifterna. Det krävs dock vidare analys om huruvida en radering av uppgifter som inte ska vidarebehandlas utgör en så pass begränsad behandling att den ligger inom de ramar som PNR-domen ställer upp.

Lagringstid

Det finns en viss oro bland medlemsstaterna att en begränsning av hur lång tid PNR-uppgifter får lagras hos enheten för passagerarinformation kommer att leda till försämrade möjligheter att hindra, upptäcka, utreda och lagföra terroristbrott och annan grov brottslighet. Ungern anser att lagringstiden bör fortsätta vara fem år och att distinktionen mellan de inledande sex månaderna och den längsta lagringstiden om fem år inte är realistisk. Utredningar tar ofta flera månader och ibland flera år.

Även Rumänien för fram att PNR-information bör sparas så länge det är nödvändigt för att uppnå målen med direktivet avseende terroristbrott och annan grov brottslighet. Den föreslagna perioden om sex månader är alldeles för begränsad. Det hör till sakens natur att utredning och åtal av terroristbrott kan ske först efter att brottet har begåtts och unionslagstiftarens intention var att säkerställa möjligheten att begära information även efter utgången av de inledande sex månaderna. Rumänien ger stöd till idén att all PNR-information ska samlas in och bevaras i fem år, men att informationen ska behandlas selektivt, baserat på riskbedömningar framtagna av de behöriga myndigheterna.

Det råder i stort sett konsensus bland medlemsstaterna att en begränsning av lagringstiden för PNR-uppgifter leder till omfattande svårigheter i brottsbekämpningen. Det efterfrågas en lösning som innebär att information kan lagras så länge som möjligt, samtidigt som skyddet för personuppgifter garanteras.

Prövning av domstol eller oberoende myndighet

Enligt ett flertal medlemsstater framgår det tydligt av PNR-domen att beslut att tillämpa direktivet på flygningar inom EU måste kunna bli föremål för prövning av en domstol eller av en oberoende myndighet. Det är värt att notera att en sådan myndighet inte bedriver verk-

samhet dygnet runt, vilket kan leda till ytterligare fördröjning av beslutet. Detta kan påverka skyndsamma förfrågningar negativt.

Finland för fram att domen ställer upp tydliga krav, men den lämnar ansvaret för hur kraven ska uppfyllas till medlemsstaterna. Det är medlemsstaterna som ska se till att målen uppfylls genom lagstiftning.

Kroatien anser att det inte är en idealisk lösning att en medlemsstat ska rättfärdiga bedömningen av ett terroristhot inför en domstol. Ett sådant hot är svårt att kvantifiera och det är sällan begränsat till en viss tidsperiod.

8 Förändringar av svensk rätt i ljuset av PNR-domen

8.1 Utgångspunkter

Vårt uppdrag i den här delen är att se över den svenska regleringen som genomför PNR-direktivet. EU-domstolen gör i PNR-domen ett flertal uttalanden som kräver anpassningar av svensk lagstiftning. Det gäller t.ex. insamlingen av passageraruppgifter från flygningar inom EU och lagringstiden för PNR-uppgifter vid enheten för passagerarinformation.

PNR-direktivets genomförande i Sverige och övriga medlemsstater har haft en positiv effekt på möjligheterna att bekämpa terrorism och grov brottslighet.[1] Vår utgångspunkt är att så långt det är möjligt bibehålla de brottsbekämpande myndigheternas tillgång till ändamålsenliga och effektiva verktyg. Samtidigt måste EU-rättens företräde respekteras och det grundläggande skyddet för enskildas personliga integritet, rätt till respekt för privatliv samt skydd av personuppgifter säkerställas. I och med EU-rättens företräde samt utredningens direktiv att ta ställning till vilka förändringar av den svenska regleringen som behöver göras med anledning av EU-domstolens praxis har vi inte analyserat nollalternativet, dvs. att inte genomföra de förändringar som EU-rätten kräver.

[1] Report from the Commission to the European Parliament and the Council On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, (SWD(2020) 128 final, den 24 juli 2020, s. 6–7.

8.2 Flygningar inom EU

Förslag

Det ska föras in ett nytt kapitel, 3 a, i lagen om flygpassageraruppgifter i brottsbekämpningen som behandlar flygningar inom EU. Om inte annat anges i kapitlet ska alla bestämmelser i lagen även gälla för flygningar inom EU.

Huvudregeln ska vara att PNR-uppgifter som avser flygningar inom EU omedelbart ska anonymiseras efter den inledande förhandsbedömningen som utförs av enheten för passagerarinformation.

Beslut om undantag från denna huvudregel ska få fattas om det föreligger ett verkligt och aktuellt eller förutsebart terroristhot mot Sverige. Vid sådana förhållanden får PNR-uppgifter som avser samtliga flygresor inom EU undantas från anonymisering. Om det inte föreligger något sådant hot ska beslut få fattas om ett urval av flygningar som undantas från anonymisering av passagerarnas PNR-uppgifter.

8.2.1 Tillämpning av PNR-direktivet på flygningar inom EU

Artikel 2.1 i PNR-direktivet ger medlemsstaterna möjlighet att besluta att tillämpa direktivet på flygningar inom EU. I svensk rätt har ett sådant beslut fattats genom bestämmelsen i 2 kap. 1 § lagen om flygpassageraruppgifter i brottsbekämpningen där det anges att lufttrafikföretag ska överföra PNR-uppgifter till enheten för passagerarinformation inför varje flygning som ankommer till eller avgår från Sverige. Det görs således i svensk rätt ingen skillnad mellan flygningar inom EU eller till eller från ett tredjeland.

I artikel 2.3 i direktivet anges att en medlemsstat får besluta att endast tillämpa direktivet på valda flygningar inom EU. När en medlemsstat fattar ett sådant beslut ska den välja de flygningar som den anser vara nödvändiga för att efterfölja målen för detta direktiv. Medlemsstaten får när som helst besluta att ändra urvalet av flygningar inom EU. I direktivet finns det inga bestämmelser beträffande formerna för ett beslut om urval av flygningar.

Sverige har tillsammans med övriga medlemsstater förklarat att de fullt ut kommer att utnyttja möjligheten att tillämpa direktivet på flygningar inom EU.[2] Till följd av detta har det inte införts regler i svensk rätt om formerna för ett beslut om urval av flygningar inom EU.

Inte heller i PNR-domen ges det vägledning i frågan. EU-domstolen uttalar att det är medlemsstaterna som har rätt att besluta om att tillämpa direktivet på utvalda flygningar. Det ankommer på medlemsstaterna att bedöma hoten knutna till terroristbrott och grov brottslighet. Möjligheten att utvidga tillämpningen av systemet som inrättats genom PNR-direktivet ska under alla omständigheter utövas med full respekt för de grundläggande rättigheter som garanteras i artikel 7 och 8 i EU-stadgan. Medlemsstaterna har en skyldighet att kontrollera att utvidgningen verkligen är nödvändig och proportionerlig för att uppnå de mål som anges i artikel 1.2 i direktivet.

I domen anges att behandlingen av PNR-uppgifter från flygningar inom EU ska vara *strikt nödvändig*. Uttrycket är emellertid inte etablerat i svensk lagstiftning. I författningsförslagen används i stället uttrycket *absolut nödvändig*. Avsikten är att uttrycken ska ha samma innebörd. Med strikt eller absolut nödvändig avser vi att bedömningen ska föregås av noggranna överväganden kring behov och att tillämpning ska ske restriktivt.

Genomgående i domen anges att det är *medlemsstaten* som har möjlighet att besluta om urval av flygningar inom EU. Som nämnts ovan är det även vad som anges i artikel 2.3 i direktivet. Vår utgångspunkt är därmed att medlemsstaterna är fria att bestämma formerna för att besluta om att tillämpa direktivet på samtliga flygningar inom EU samt att besluta om ett urval av flygningar inom EU.

Frågan är därmed vilken myndighet, eller enhet inom en myndighet, som lämpligen bör fatta sådana beslut. Enligt PNR-domen ska bedömningen av om PNR-systemet får tillämpas på samtliga flygningar inom EU baseras på om det finns ett verkligt och aktuellt eller förutsebart terroristhot mot medlemsstaten. I avsaknad av ett sådant hot får ett urval göras av flygningar för vilka det finns indikationer som kan motivera en sådan tillämpning. I den senare bedömningen kan alltså även risken för grov brottslighet beaktas. Eftersom prövningarna till viss del skiljer sig åt hanterar vi dem var för sig.

[2] Europeiska rådets uttalande avseende ärendet Utkast till Europaparlamentets och rådets direktiv om användning av passageraruppgiftssamlingar (PNR) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (första behandlingen), 7829/16 ADD 1, den 18 april 2016.

8.2.2 Beslut om att tillämpa PNR-direktivet på samtliga flygningar inom EU

Förslag

Säkerhetspolisen ska fatta beslut om att tillämpa PNR-direktivet på samtliga flygningar inom EU. Ett sådant beslut ska ha en giltighetstid om högst ett år. Inför beslutet kan Säkerhetspolisen vid behov inhämta synpunkter från Försvarsmakten och andra myndigheter. Beslutet ska gälla omedelbart och expedieras till enheten för passagerarinformation.

Den myndighet som ska besluta om att tillämpa PNR-direktivet på samtliga flygningar inom EU bör dels ha insyn i PNR-systemet, dels besitta kunskap om hotet om terrorism mot Sverige. De myndigheter som har insyn i PNR-systemet och därmed i första hand bör övervägas som beslutsmyndighet är Polismyndigheten genom enheten för passagerarinformation, samt övriga myndigheter som är behöriga enligt 3 § förordningen om flygpassageraruppgifter i brottsbekämpningen, dvs. Säkerhetspolisen, Ekobrottsmyndigheten, Tullverket och Försvarsmakten. Av dessa är det framför allt Säkerhetspolisen och Försvarsmakten som arbetar mot terrorism och därmed har den kompetens som krävs för att bedöma om det föreligger ett konkret terroristhot mot Sverige.

Säkerhetspolisen förfogar över beslutet om vilken terrorhotnivå på en femgradig skala som föreligger i Sverige. Ett sådant beslut baseras till stor del på den bedömning som Nationellt centrum för terrorhotbedömning, NCT, gör. NCT är en permanent arbetsgrupp med personal från Försvarets radioanstalt, FRA, Militära underrättelse- och säkerhetstjänsten, MUST, samt Säkerhetspolisen. Redan i dag hanterar således Säkerhetspolisen den mycket känsliga information som ligger till grund för bedömningen av terrorhot mot Sverige. Relevant information kommer även från och delas med FRA och MUST. Säkerhetspolisens beslut om terrorhotnivå och det material som ligger till grund för detta är relevant även för bedömningen av terrorhot inom ramen för PNR-systemet. Det rör sig emellertid om två olika bedömningar och bedömningen av terrorhotet inom PNR-systemet måste inte nödvändigtvis knytas till en viss nivå på den femgradiga skalan för terrorhot mot Sverige.

I avsnitt 8.3 föreslår vi att beslutet om att tillämpa PNR-systemet på samtliga flygningar inom EU ska prövas av Försvarsunderrättelsedomstolen. I dagsläget prövar Försvarsunderrättelsedomstolen ansökningar om tillstånd till signalspaning. Det finns emellertid förslag på att utöka domstolens verksamhetsområde. Även dessa beskrivs mer ingående i avsnitt 8.3. Enligt ett förslag[3] ska Försvarsunderrättelsedomstolen pröva frågor om tillstånd till framtagning från särskilda uppgiftssamlingar efter ansökan av Säkerhetspolisen. Tidigare har det även diskuterats om Försvarsunderrättelsedomstolen är lämplig som överprövningsinstans avseende beslut om nationell säkerhetslagring.[4] Även sådana beslut ska enligt förslaget fattas av Säkerhetspolisen.

Ett eventuellt utökande av Försvarsunderrättelsedomstolens verksamhet bör göras med försiktighet. Domstolen har sedan den inrättades 2009 prövat ansökningar från Försvarets radioanstalt och därigenom skapat och utvecklat rutiner för samarbetet som möjliggör en effektiv och rättssäker hantering av målen och de känsliga uppgifter som förekommer i dem. Att upprätta ett samarbete med en ny myndighet är tids- och resurskrävande. Att Säkerhetspolisen även i andra sammanhang diskuteras som beslutsinstans talar för att välja en sådan lösning avseende det nu aktuella beslutet.

Till följd av detta, särskilt med beaktande av att Säkerhetspolisen redan i dag förfogar över beslutet om terrorhotnivå i Sverige, anser vi att Säkerhetspolisen är ett lämpligt val av beslutsinstans. För att beslutsunderlaget ska bli så heltäckande som möjligt kan Säkerhetspolisen inför beslutet vid behov inhämta synpunkter från Försvarsmakten och andra myndigheter.

För att en inskränkning i grundläggande rättigheter ska anses vara proportionerligt måste det i nationell lagstiftning föreskrivas klara och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt anges minimikrav, så att personer vars personuppgifter berörs har tillräckliga garantier för att uppgifterna på ett effektivt sätt är skyddade mot riskerna för missbruk. Lagstiftningen ska vara rättslighet bindande enligt nationell rätt och i synnerhet ange under vilka omständigheter och på vilka villkor en åtgärd

[3] SOU 2025:49, *Säkerhetspolisens behandling av personuppgifter*, s. 618–620.
[4] Se SOU 2023:22, *Datalagring och åtkomst till elektronisk information*, s. 203–205 samt Försvarsunderrättelsedomstolens remissvar till betänkandet.

avseende behandling av sådana uppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strängt nödvändigt.[5]

När det gäller hemliga tvångsmedel finns det ett krav på förutsebarhet. Det innebär inte att den enskilde ska kunna förutse när t.ex. polisen kommer att avlyssna dennes kommunikationer och anpassa sig därefter. Däremot ska det finnas klara och detaljerade regler som beskriver i vilka situationer och under vilka förutsättningar som myndigheterna får använda tvångsmedel. Reglerna måste vara så klara och detaljerade att medborgarna skyddas från godtyckliga övervakningsåtgärder.[6]

Kraven på förutsebarhet och tydlighet som ställs på en reglering av under vilka omständigheter som hemliga tvångsmedel får användas gör sig inte gällande på samma sätt för en reglering av behandlingen av PNR-uppgifter från samtliga flygningar inom EU. Det för med sig svårigheter att i lagtext definiera vilka företeelser som kan komma att utgöra ett tillräckligt allvarligt terrorhot för att motivera insamling av passageraruppgifter från samtliga resor inom EU. Europadomstolen har tydliggjort att de hot som finns mot t.ex. nationell säkerhet kan variera och vara svåra att i förväg definiera.[7] Det är därför inte lämpligt att i författning precisera vilka omständigheter som ska föreligga för att terrorhotet ska anses vara tillräckligt allvarligt. Det ankommer på Säkerhetspolisen att, på ett så komplett underlag som möjligt, avgöra om det finns tillräckligt konkreta omständigheter för att anse att det finns ett verkligt och aktuellt eller förutsebart terrorhot mot Sverige. Förutsättningarna för när tillämpning av PNR-systemet på PNR-uppgifter från samtliga flygningar inom EU ska vara tillåten bör alltså inte vara mer konkretiserade i författning än att beslut om att enheten för passagerarinformation får behandla PNR-information i sin fullständiga form för samtliga flygningar inom EU får fattas om det föreligger ett verkligt och aktuellt eller förutsebart terroristhot mot Sverige.

Tillämpningsperioden för ett beslut om att tillämpa PNR-direktivet på samtliga flygningar inom EU måste vara begränsad till vad som är absolut nödvändigt, men den kan förlängas om hotet kvarstår. Det bör därför föreskrivas en längsta tid som beslutet får gälla. Denna tid bör dock inte var alltför kort. De förhållanden som legat till grund för bedömningen att Sverige står inför ett allvarligt hot om terro-

[5] EU-domstolens dom den 20 september 2022, *Tyskland mot SpaceNet AG m.fl.*, förenade målen 793/19 och 794/19, p. 69.
[6] SOU 2018:61, *Rättssäkerhetsgarantier och hemliga tvångsmedel*, s. 78.
[7] SOU 2018:61, *Rättssäkerhetsgarantier och hemliga tvångsmedel*, s. 79.

rism ändras vanligtvis inte särskilt snabbt. Vi föreslår därför att beslutet ska få gälla i högst ett år. Därefter har Säkerhetspolisen möjlighet att fatta ett nytt beslut, under förutsättning att villkoren för ett sådant beslut är uppfyllda.

Om säkerhetssituationen förändras och bedömningen görs att det finns ett verkligt och aktuellt eller förutsebart terrorhot mot Sverige är det av stor vikt att åtgärder kan vidtas med kort varsel. För att ge bästa möjliga förutsättningar för myndigheterna att agera i en sådan situation bör beslutet att tillämpa PNR-direktivet på samtliga flygningar gälla omedelbart och expedieras till enheten för passagerarinformation.

Ett beslut om att tillämpa PNR-direktivet på samtliga flygningar inom EU måste kunna bli föremål för kontroll av en domstol eller av en oberoende förvaltningsmyndighet. I avsnitt 8.3 lägger vi fram våra argument för att det är Försvarsunderrättelsedomstolen som ska genomföra en sådan kontroll.

8.2.3 Beslut om urval av flygningar

Förslag

Beslut om urval av flygningar inom EU som undantas från anonymisering av passagerarnas PNR-uppgifter omedelbart efter förhandsbedömningen ska fattas av enheten för passagerarinformation. Inför beslutet ska enheten inhämta och beakta synpunkter från de behöriga myndigheterna. Urvalsbeslutet ska regelbundet omprövas för att säkerställa att tillämpningen av systemet på flygningarna alltid är begränsat till vad som är absolut nödvändigt.

Undantag från huvudregeln om anonymisering får även göras för PNR-uppgifter från flygningar där det förekommer personer som efter förhandsbedömningen behöver utredas ytterligare av behöriga mottagare eller Europol. Dessa uppgifter får fortsatt behandlas av enheten för passagerarinformation för att fullgöra sina uppgifter.

I avsaknad av ett verkligt och aktuellt eller förutsebart terroristhot ska det göras en bedömning av om, och i så fall vilka, flygningar inom EU som ska kontrolleras i enlighet med PNR-systemet. I en sådan

bedömning ska både hotet om terrorism och risken för annan gränsöverskridande grov brottslighet beaktas. Medan bedömningen av terroristhotet kräver specialiserad, djup sakkunskap och tillgång till känsliga uppgifter kräver bedömningen av risken för grov brottslighet i stället en bredare kunskapsbas. Den generella grova brottsligheten är mer omfattande och mångfacetterad till sin karaktär än terroristbrottsligheten.

I de nya API-förordningen för brottsbekämpning regleras motsvarande möjlighet att göra ett urval av flygningar inom EU. I artikel 13 anges att i avsaknad av ett verkligt och aktuellt eller förutsebart terroristhot ska medlemsstater som tillämpas PNR-direktivet och följaktligen API-förordningen på flygningar inom EU välja ut sådana flygningar inom EU enligt resultatet av en bedömning som utförts på grundval av vissa krav. Bedömningen ska utföras på ett objektivt, vederbörligen motiverat och icke-diskriminerande sätt i enlighet med artikel 2 i PNR-direktivet. Det är endast tillåtet att beakta kriterier som är relevanta för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet som har en objektiv koppling, inbegripet en indirekt koppling, till lufttransport av passagerare. Kriterierna får inte enbart bygga på de grunder som anges i artikel 21 i EU:s rättighetsstadga med avseende på passagerare eller passagerargrupper. I bedömningen får endast användas information som kan utgöra stöd för en objektiv, vederbörligen motiverad och icke-diskriminerande bedömning.

På grundval av bedömningen ska medlemsstaterna välja ut flygningar inom EU som har anknytning till bl.a. vissa rutter, resmönster eller flygplatser med avseende på vilka det finns indikationer på terroristbrott och grov brottslighet och vilka motiverar behandling av API-uppgifter och andra PNR-uppgifter. Urvalet av flygningar ska begränsas till vad som är absolut nödvändigt för att uppnå målen i PNR-direktivet och API-förordningen.

Enligt artikel 13.7 i API-förordningen för brottsbekämpning ska medlemsstaterna, i enlighet med artikel 2 i PNR-direktivet, regelbundet och minst var tolfte månad se över sin bedömning av urvalet för att ta hänsyn till förändringar i de omständigheter som motiverade urvalet och för att säkerställa att det fortsatt begränsas till vad som är absolut nödvändigt.

Samtliga behöriga myndigheter arbetar mot gränsöverskridande grov brottslighet och beslutsmyndigheten bör också beakta samtliga

behöriga myndigheters perspektiv. Som nämnts ovan finns det ett etablerat samarbete mellan enheten för passagerarinformation och de behöriga myndigheterna. Genom det samarbetet finns det en bred och samlad kompetens när det gäller grov brottslighet, samt specialiserad kunskap om terrorism. Det förefaller därmed mest lämpligt att Polismyndigheten, genom enheten för passagerarinformation, utses till beslutsmyndighet. För att dra nytta av den expertis och erfarenhet som finns ska enheten i beslutsprocessen inhämta och beakta synpunkter från de behöriga myndigheterna.

I likhet med beslutet om att tillämpa PNR-direktivet på samtliga flygningar inom EU måste urvalet begränsas till vad som är absolut nödvändigt. En sådan bedömning kan resultera i att många eller inga rutter väljs bort. Enheten för passagerarinformation ska således löpande ompröva urvalet och endast vidarebehandla PNR-uppgifter från de flygningar där sådan behandling är motiverad.

8.2.4 När ska ett urval av flygningar göras?

I situationen där det inte finns något verkligt och aktuellt eller förutsebart terroristhot mot Sverige måste det göras ett urval av vilka flygningar som ska omfattas av tillämpningen av PNR-direktivet. I PNR-domen anges att tillämpningen ska begränsas till *överföring och behandling* av PNR-uppgifter avseende vissa flyglinjer. Domstolen gör således skillnad på den överföring som lufttrafikföretagen genomför och den behandling som sedan sker vid enheten för passagerarinformation och sedermera eventuellt vid behöriga myndigheter.

Frågan är om både överföringen av uppgifter och den senare behandlingen av uppgifter måste begränsas till ett visst urval eller om det gäller den sammantagna överföringen *och* behandlingen. Domstolen tar i detta sammanhang upp att det inte är begränsat till vad som är strikt nödvändigt att utan åtskillnad tillämpa *det system* som har inrättats genom PNR-direktivet på flygningar inom EU. Detta talar för att det är den sammantagna överföringen och behandlingen som ska begränsas, inte överföringen och behandlingen var för sig.

Det framgår inte av direktivet eller av PNR-domen hur ett beslut om urval av flygningar ska fattas och det är därmed upp till medlemsstaterna att bestämma detta. Beslutsordningen för urval av flygningar måste uppfylla de krav som EU-rätten ställer, samtidigt som brotts-

bekämpande myndigheters möjlighet att fullgöra sina uppgifter beskärs i så liten mån som möjligt. Nedan redovisar vi våra överväganden i detta avseende.

Urval bör inte göras hos lufttrafikföretagen

Ett tillvägagångssätt för att begränsa överföringen av PNR-uppgifter från lufttrafikföretag till enheten för passagerarinformation är att meddela lufttrafikföretagen vilka flygningar som för tillfället ska kontrolleras. Detta medför dock betydande säkerhetsrisker. Information om vilka flygningar som kontrolleras avslöjar vilka bedömningar som svenska myndigheter har gjort avseende terroristhot och annan allvarlig brottslighet inom unionen. Informationen är mycket känslig och den måste därför hållas inom en begränsad krets och kan inte delas till lufttrafikföretagen.

Om informationen skulle läckakan det leda till att potentiella terrorister och andra kriminella snabbt anpassar sina resmönster. PNR-systemet riskerar då att bli i det närmaste verkningslöst som verktyg mot terrorism och annan grov brottslighet.

Ett sådant tillvägagångssätt skulle även innebära en större administrativ börda för lufttrafikföretagen. Situationen avseende hotbilden mot Sverige kan snabbt förändras, och därmed även bedömningen av vilka flygningar som ska omfattas av skyldigheten att föra över PNR-uppgifter. Att ”koppla på” en ny rutt tar tid och kräver att resurser avsätts hos lufttrafikföretagen. En sådan tröghet i systemet kan vidare innebära stora konsekvenser med tanke på säkerhetsriskerna det medför. Lufttrafikföretagen skulle vidare kunna ställas inför en situation där samtliga medlemsstater inför ett liknande system, men gör olika bedömningar avseende vilka flygningar som ska kontrolleras. Resultatet av detta kan bli att lufttrafikföretagen ska översända PNR-information till samtliga medlemsstater, men att listan över utvalda flygningar skiljer sig från land till land. Ett sådant system riskerar att, utöver de tekniska utmaningarna, medföra betydande administrativa kostnader för lufttrafikföretagen.

Sammanfattningsvis anser vi att ett tillvägagångssätt för urval av flygningar inom EU där flygbolagen meddelas vilka flygningar som omfattas av urvalet inte är ett gångbart alternativ, särskilt med beaktande av de säkerhetsmässiga risker som det medför. Lufttrafikföre-

tagen ska därmed fortsätta översända PNR-uppgifter till enheten för passagerarinformation för samtliga flygningar inom EU. En sådan tillämpning ligger i linje med vad som framgår i API-förordningen avseende brottsbekämpning och bör inte anses stå i strid med de uttalanden som EU-domstolen gjort i PNR-domen. Det kräver emellertid att ett urval av flygningar i stället görs senare i processen.

Urval bör göras efter överföring till enheten för passagerarinformation

Eftersom lufttrafikföretagen även fortsättningsvis ska översända PNR-uppgifter för samtliga flygningar inom EU till enheten för passagerarinformation måste vissa uppgifter, baserat på urvalet av flygningar, därefter raderas eller åtminstone anonymiseras. Vi anser att det räcker med att PNR-uppgifterna anonymiseras för att leva upp till kraven som ställs i PNR-direktivet och uttalandena i PNR-domen. I avsnitt 8.8 lägger vi fram våra resonemang i denna fråga.

Frågan är i vilken fas av processen som anonymisering måste ske. Enligt PNR-domen får systemet som har inrättats genom PNR-direktivet inte tillämpas på samtliga flygningar inom EU. Vad som avses med PNR-systemet klargörs varken i direktivet eller domen. Det får dock anses avse insamlingen och den därefter följande behandlingen av PNR-uppgifter för de syften och under den tidsperiod som anges i direktivet. Det förefaller därmed stå klart att uppgifter som för tillfället inte omfattas av urvalet av flygningar måste begränsas beträffande den behandling som utförs och/eller den tidsperiod som uppgifterna lagras.

I sammanhanget bör den nya API-förordningen för brottsbekämpningen beaktas. Inom API-systemet ska lufttrafikföretagen översända API-uppgifter till en central router som administreras av eu-Lisa. Från routern skickas sedan API-uppgifterna vidare till medlemsstaternas respektive enhet för passagerarinformation. Det skickas emellertid endast information avseende utvalda flygningar. Vilka rutter som väljs ut är upp till den enskilda medlemsstaten. Enheten för passagerarinformation behandlar alltså inte på något sätt API-uppgifter från flygningar som inte har valts ut för insamling. Att det nya API-systemet har inrättats på detta sätt innebär inte att slutsatsen kan dras att enheten för passagerarinformation inte alls får behandla uppgifter såvida de inte kommer från utvalda flygningar. API-systemet bygger

på upprättandet av en central router som fungerar som en mellanhand mellan lufttrafikföretagen och enheten för passagerarinformation. Det förefaller naturligt att information från flygningar som inte har valts ut inte översänds från routern till enheten. På sikt kommer routern även användas för PNR-systemet, men i dagsläget måste begränsningen av behandlingen av information från ej utvalda flygningar således ske på något annat sätt, under ett annat skede i processen.

En möjlig begränsning av behandlingen av PNR-information som härrör från flygningar inom EU som har diskuterats[8] är att omedelbart radera uppgifterna när de kommer in till enheten för passagerarinformation. Radering sker då på samma sätt som radering av känsliga uppgifter i enlighet med artikel 13.4 i direktivet. Av artikeln följer att även om behandling av sådana uppgifter är förbjuden står det inte i strid med direktivet att enheten för passagerarinformation mottar sådana, under förutsättning att de omedelbart raderas. Eftersom enheten för passagerarinformation har tekniska förutsättningar att omedelbart radera känslig information bör skyldigheten att radera PNR-uppgifter för vissa flygningar vara möjlig att uppfylla med befintliga tekniska lösningar.

Om uppgifter som hänför sig till flygningar som för tillfället inte valts ut för kontroll kommer in till enheten och därefter omedelbart raderas eller anonymiseras, bör hanteringen inte stå i strid med direktivet, även med beaktande av de uttalanden som gjorts i PNR-domen. En nackdel med ett sådant alternativ är att det inte sker någon förhandsbedömning enligt artikel 6.2 a i direktivet och 3 kap. 4 § 1 lagen om flygpassageraruppgifter som syftar till att identifiera personer som behöver undersökas närmare av behöriga myndigheter. Kända potentiella terrorister eller andra brottslingar kommer således inte att flaggas i systemet. Det bör därför övervägas om en inledande behandling, varigenom slagningar görs mot relevanta databaser, följt av omedelbar anonymisering av de PNR-uppgifter som inte ger träff och som inte härrör från en flygning som inte ingår i urvalet av flygningar, ligger inom ramarna för vad direktivet och EU-stadgan tillåter.

En möjlig tolkning av PNR-domen är att sådan ytterligare behandling som en förhandsbedömning innebär inte är tillåten. PNR-uppgifterna har i sådant fall översänts från lufttrafikföretagen, tagits emot av enheten för passagerarinformation samt behandlats genom slag-

[8] Se t.ex. Europeiska kommissionens promemoria samt medlemsstaternas synpunkter som redovisas i avsnitt 7.8.2–3.

ningar mot relevanta databaser. I och med en sådan process har flera delar av de olika element som utgör PNR-systemet tillämpats på uppgifterna. Uppgifterna som inte ger någon träff kommer emellertid att anonymiseras direkt efter förhandsbedömningen och blir därmed inte föremål för den kontinuerliga behandling som sker genom vidare lagring samt övrig behandling som kan ske under lagringstiden. Detsamma gäller för träffar som efter manuell behandling visar sig vara falska. En mycket stor andel, över 99,9 procent, av PNR-uppgifterna för flygningar inom EU som inte ingår i urvalet av flygningar kommer därmed att anonymiseras inom mycket kort tid från att de kom in till enheten för passagerarinformation. Uppgifter som anonymiseras efter den inledande förhandsbedömningen kan dessutom inte bli föremål för en begäran om tillgång till uppgifterna från de behöriga myndigheterna. Med tanke på den kraftigt begränsade behandlingen av PNR-uppgifter, både vad gäller lagringstid och vilken typ av behandling som utförs, anser vi att ett sådant tillvägagångssätt inte står i strid med uttalandena i PNR-domen.

PNR-information för personer som efter förhandsbedömningen behöver utredas ytterligare av behöriga myndigheter eller Europol ska få fortsatt behandlas vid enheten för passagerarinformation för de ändamål som anges i 3 kap. 4 § 2 och 3, även för det fall att det flyg som personen reste med inte omfattas av urvalet av flygningar. Detsamma bör gälla för samtliga PNR-uppgifter från flyg där det förekommer sådana personer.

Detta tillvägagångssätt innebär att de brottsbekämpande myndigheterna förlorar möjligheten att följa resvägar för personer som vid en förhandsbedömning inte ger någon träff, men som senare visar sig vara av intresse. När en person för första gången uppmärksammas av brottsbekämpande myndigheter finns det således ingen data för förfluten tid avseende personens resor inom EU. Detta försvårar myndigheternas arbete mot terrorism och grov brottslighet. Vidare får det antas att potentiella terrorister och andra brottslingar kommer att verka för att i så stor utsträckning som möjligt ta reda på vilka flygningar som är utvalda av olika medlemsstater, för att på så vis kunna undvika dessa sträckor.

Med tanke på den påtagligt negativa effekten på brottsbekämpningen detta alternativ kan antas ha kan det ifrågasättas om tillämpningen ligger i linje med vad som anges i artikel 2.3 i PNR-direktivet. Av bestämmelsen framgår att när en medlemsstat beslutar att tillämpa

direktivet på valda flygningar inom EU, ska den välja de flygningar som den anser vara nödvändiga för att efterfölja målen för direktivet. Det kan argumenteras för att PNR-systemet, för att uppnå målen med direktivet och för att det inte ska vara verkningslöst, kontinuerligt måste tillämpas på samtliga flygningar inom EU.

Den rättsliga grunden för PNR-domens begränsning av behandling av PNR-uppgifter beträffande flygningar inom EU är att behandlingen på ett otillbörligt sätt inskränker de grundläggande fri- och rättigheter som följer av artikel 7 och 8 i EU-stadgan. EU-stadgan tillhör EU:s primärrätt och har i kraft av denna egenskap företräde framför PNR-direktivet, som tillhör sekundärrätten. Den begränsning som uppställs i PNR-domen, med grund i EU-stadgan, har alltså företräde framför en bedömning att begränsningarna medför att målet med PNR-direktivet delvis inte kan uppnås. Det är vidare EU-domstolen som är den yttersta uttolkaren av EU-rätten. Att PNR-domen begränsar möjligheten att uppnå målen med PNR-direktivet kan alltså inte användas som argument för att inte genomföra de förändringar av nationell rätt som PNR-domen kräver.

Bland vissa länder har det efter PNR-domen diskuterats en ändrad lagringstid för PNR-uppgifter från flygningar inom EU. Enligt vår mening är det inte förenligt med uttalandena i PNR-domen, och därmed inte förenligt med EU-stadgan, att behandla inkomna PNR-uppgifter för samtliga flygningar inom EU utöver den inledande förhandsbedömningen. Sådan fortsatt lagring och annan behandling skulle innebära att PNR-systemet till fullo tillämpas på uppgifterna. Genom att utesluta vidare behandling av uppgifter som inte ger någon träff, efter manuell behandling radera falska träffar, samt genom att förkorta lagringstiden från upp till fem år till att endast lagras fram till att förhandsbedömningen har genomförts har behandlingen begränsats vad gäller systematiken och kontinuiteten på ett sätt som vi anser ligger i linje med PNR-domen.

8.3 Prövning av beslut om utvidgad tillämpning av PNR-direktivet

Förslag

Försvarsunderrättelsedomstolen ska utses till prövningsinstans för beslut om att tillämpa PNR-direktivet på samtliga flygningar inom EU. Ett sådant beslut ska underställas Försvarsunderrättelsedomstolen utan onödigt dröjsmål och senast inom en vecka från det datum då det fattades och ha en giltighetstid om ett år. Domstolens avgörande ska expedieras till Säkerhetspolisen och enheten för passagerarinformation.

Försvarsunderrättelsedomstolen får besluta att ett underställt beslut tills vidare inte ska gälla.

PNR-domen slår fast att ett beslut om att tillämpa direktivet på samtliga flygningar inom EU måste kunna bli föremål för effektiv kontroll, antingen av en domstol eller av en oberoende förvaltningsmyndighet. Avgörandet ska ha bindande verkan och syftet är att kontrollera om det finns förutsättningar för en sådan tillämpning. Kravet på effektiv kontroll nämns i samband med beslut om att tillämpa direktivet på *samtliga* flygningar inom EU. Något liknande krav ställs inte upp avseende beslut om att tillämpa direktivet på ett *urval* av flygningar.

Frågan är vilken domstol eller myndighet som ska genomföra denna kontroll. Eftersom kravet på ett formellt beslut om utvidgad tillämpning av PNR-direktivet till att omfatta även flygningar inom EU introducerades i och med PNR-domen finns det inga bestämmelser, vare sig i direktivet eller i svensk rätt, om den rättsliga prövningen av ett sådant beslut.

I detta sammanhang utvecklar EU-domstolen inte vilka krav som ställs på domstolen eller den oberoende förvaltningsmyndigheten som ska genomföra prövningen. Begreppen som används – *domstol eller oberoende förvaltningsmyndighet* – är dock desamma som används avseende förhandskontrollen vid en begäran om tillgång till PNR-uppgifter. I det sammanhanget anger EU-domstolen att myndigheten ska förfoga över alla befogenheter och lämna alla nödvändiga garantier för att säkerställa en avvägning mellan de olika intressena och rättigheterna i fråga. Myndigheten måste ha en ställning som innebär att den kan fullgöra sitt uppdrag på ett objektivt och opartiskt sätt,

och den måste därför vara fri från all yttre påverkan. Detta krav på oberoende innebär att myndigheten måste vara fristående i förhållande till den som begär tillgång till uppgifterna, så att myndigheten kan utöva sin kontroll utan yttre påverkan. När det gäller prövningen av ett beslut om utvidgad tillämpning av direktivet finns det emellertid ingen begäran om tillgång till uppgifter. Det bör dock anses stå klart att myndigheten som ska pröva beslutet om urval av flygningar som fattas av Säkerhetspolisen ska vara fristående i förhållande till enheten för passagerarinformation samt de behöriga myndigheterna.

Enligt nuvarande rättsordning fattar åklagare beslut om tillgång till PNR-uppgifter under pågående förundersökning. Även om åklagaren har ett nära samarbete med Polismyndigheten i brottsutredningar får åklagaren anses vara fristående och oberoende i detta sammanhang då det inte rör någon specifik brottsutredning. Själva sakfrågan, dvs. att bedöma ett eventuellt terroristhot, är dock främmande för åklagare. Till skillnad från frågan om tillgång till PNR-uppgifter bär den inga likheter med t.ex. beslut om användande av tvångsmedel i en brottsutredning. Sammantaget anser vi inte att det är lämpligt att åklagare prövar beslutet om utvidgad tillämpning av PNR-direktivet.

Ett annat alternativ är att allmän domstol eller allmän förvaltningsdomstol utses till prövningsinstans. Domstolarna är fristående och oberoende i förhållande till enheten för passagerarinformation och de behöriga myndigheterna. Genom ett domstolsförfarande säkerställs en rättssäker och gedigen prövning av beslutet och det finns kapacitet att fatta beslut inom rimlig tid. Domstolarna har visserligen erfarenhet av och kompetens att hantera nya, komplicerade frågor, men frågor om potentiella terroristhot framstår som främmande för både allmän domstol och allmän förvaltningsdomstol. Vid en prövning av ett beslut av den karaktär som det är fråga om behöver domstolen vidare beakta information som är mycket känslig ur säkerhetssynpunkt. Även med beaktande av att man inom en domstol kan avgränsa vilken personal som får ta del av känsliga uppgifter innebär detta vissa säkerhetsrisker.

Mot bakgrund av dessa argument anser vi att varken allmän domstol eller allmän förvaltningsdomstol är lämpliga som prövningsinstans för beslut om att tillämpa PNR-direktivet på samtliga flygningar inom EU.

Vi anser att Försvarsunderrättelsedomstolen bör utses till prövningsinstans i den aktuella frågan. En sådan ordning medför de positiva

aspekter som nämns ovan i och med den domstolsprövning som det innebär. Enligt 4 a § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, signalspaningslagen, ska Försvarets radioanstalt ansöka om tillstånd för signalspaning hos Försvarsunderrättelsedomstolen. Tillstånd får enligt 5 § signalspaningslagen endast lämnas om uppdraget är förenligt med lagen (2000:130) om försvarsunderrättelseverksamhet och signalspaningslagen, om syftet med inhämtningen inte kan tillgodoses på ett mindre ingripande sätt, om uppdraget förväntas ge information vars värde är klart större än det integritetsintrång som inhämtning i enlighet med ansökan kan innebära, om de sökbegrepp som är avsedda att användas är förenliga med 3 §, och ansökan inte avser en viss fysisk person.

I betänkandet *Säkerhetspolisens behandling av personuppgifter*[9] har Försvarsunderrättelsedomstolen föreslagits som prövningsinstans för frågor om tillstånd till framtagning från särskilda uppgiftssamlingar. I betänkandet nämns att tanken på att utvidga domstolens uppdrag inte är ny. I samband med remitteringen av betänkandet *Datalagring och åtkomst till elektronisk information*[10] uppkom frågan om vilken instans som skulle ansvara för överprövning av Säkerhetspolisens beslut om nationell säkerhetslagring. I betänkandet föreslogs att en särskilt inrättad nämnd inom Säkerhets- och integritetsskyddsnämnden skulle stå för överprövningen. Försvarsunderrättelsedomstolen påtalade i sitt remissvar att sambanden mellan inre och yttre säkerhet är mer direkt än tidigare till följd av globaliseringen. Även inre hot mot den nationella säkerheten har ofta en internationell dimension. Försvarsunderrättelsedomstolen ansåg sig därför ha kompetens att bedöma hot mot den nationella säkerheten och att pröva integritetsskyddsaspekter, även vad gäller den nationella säkerhetslagringen. I samma ärende framhöll Åklagarmyndigheten att Försvarsunderrättelsedomstolen har betydande kunskaper när det gäller de aktuella frågorna om hot mot Sveriges säkerhet.

I betänkandet anges vidare att det historiskt har funnits en tveksamhet kring att blanda försvarsunderrättelseverksamhet (militär underrättelse, t.ex. signalspaning) med den nationella säkerhetstjänsten (Säkerhetspolisens verksamhet). Ambitionen har varit att hålla isär försvarsmyndigheternas arbete och Säkerhetspolisens uppdrag. Mandatet för försvarsunderrättelseverksamheten har emellertid över tid

[9] SOU 2025:49, *Säkerhetspolisens behandling av personuppgifter*, s. 618–620.
[10] SOU 2023:22, *Datalagring och åtkomst till elektronisk information*.

anpassats från kartläggning av ”yttre militära hot” till ”yttre hot”, vilket bl.a. innebär att även internationell terrorism och grov gränsöverskridande brottslighet med säkerhetspolitiska konsekvenser kan omfattas av försvarsunderrättelseverksamheten.

Försvarsunderrättelsedomstolen har erfarenhet och kompetens att bedöma frågor som rör yttre hot mot landet. Domstolen är också van att hantera skyddsvärda uppgifter med koppling till underrättelseinformation. Försvarsunderrättelsedomstolens ordförande utnämns efter prövning i Domarnämnden och domstolen består enligt 2 § lagen (2009:966) om Försvarsunderrättelsedomstol därutöver av en eller två vice ordförande samt minst två och högst sex särskilda ledamöter. Enligt 3 § ska ordföranden och vice ordförandena ska vara lagfarna med erfarenhet av tjänstgöring som domare. De särskilda ledamöterna ska tillgodose domstolens behov av kompetens rörande bl.a. underrättelseverksamhet och integritetsskydd. Det rör sig därmed om en begränsad krets av personer som kommer ta del av den känsliga information som de aktuella besluten innehåller.

I betänkandet *Säkerhetspolisens behandling av personuppgifter* föreslås en utökning av antalet ordinarie domare och särskilda ledamöter som får finnas i Försvarsunderrättelsedomstolen. Ett beslut om att tillämpa PNR-direktivet på samtliga flygningar inom EU kommer i normalfallet fattas högst en gång om året. Även om varje beslut kräver genomgång av komplex materia och en noggrann avvägning mellan de motstående intressena innebär det således inte någon påtaglig ökning av arbetsbördan för Försvarunderrättelsedomstolen.

Genom den verksamhet som domstolen bedriver finns det en gedigen kunskap om relevanta områden inom underrättelseverksamhet. Den kunskapen medför att domstolen även har goda förutsättningar att bedöma och värdera terroristhot. Domstolen har också erfarenhet av att regelmässigt beakta enskildas personliga integritet och göra avvägningar mellan säkerhetsintressen och andra motstående intressen. Sammantaget anser vi att starka skäl talar för att utse Försvarsunderrättelsedomstolen till prövningsinstans för beslut om att tillämpa PNR-direktivet på samtliga flygningar inom EU.

Enligt vårt förslag i avsnitt 8.2 ska beslut om utvidgad tillämpning av PNR-systemet på samtliga flygningar inom EU gälla omedelbart. Det bör därför införas en möjlighet för Försvarsunderrättelsedomstolen att besluta att det underställda beslutet, efter att det har kommit in till domstolen, tills vidare inte ska gälla. För att lämpliga åtgärder

snabbt ska kunna vidtas bör Försvarsunderrättelsedomstolens avgöranden i de aktuella målen expedieras till Säkerhetspolisen och till enheten för passagerarinformation.

8.3.1 Anhängiggörande av mål vid Försvarunderrättelsedomstolen

För att en prövning i Försvarsunderrättelsedomstolen ska komma till stånd behöver det finnas en ordning för att anhängiggöra målet vid domstolen. Exempel på sådana förfaranden är att anhängiggörandet sker genom överklagande eller genom underställning. Enligt allmänna förvaltningsrättsliga regler får ett beslut överklagas av den som det angår, om det gått honom eller henne emot.[11] När det gäller beslut om utvidgad tillämpning av PNR-direktivet står det inte omedelbart klart vem som beslutet angår. Det kan exempelvis argumenteras för att lufttrafikföretagen, som överför PNR-information till enheten för passagerarinformation, påverkas av ett beslut om att samla in PNR-information för samtliga flygningar inom EU. Så som vi har utformat vårt förslag ska emellertid lufttrafikföretagen fortsätta översända all PNR-information för samtliga flyg, både inom och utom EU, oavsett om det finns ett beslut om utvidgad tillämpning eller inte. Lufttrafikföretagen bör därmed inte ha talerätt avseende ett beslut av den här karaktären.

Enskilda personer vars PNR-information behandlas i PNR-systemet kan anses beröras av ett beslut om utvidgad tillämpning av PNR-direktivet. Ett sådant beslut innebär att vissa enskildas PNR-information kommer att behandlas i större utsträckning än de annars skulle. I dagsläget lagras cirka 130 miljoner bokningar i databasen vid enheten för passagerarinformation. Av dessa rör cirka 65 procent flygningar inom EU. Ett system där varje enskild person som berörs har möjlighet att överklaga beslutet riskerar alltså att leda till en mycket stor mängd mål vid Försvarsunderrättelsedomstolen. Det förefaller också olämpligt att enskilda kan bli part i mål vid Försvarsunderrättelsedomstolen. Till följd av detta anser vi att detta alternativ inte är en lämplig lösning.

Vi anser i stället att ett beslut om att tillämpa PNR-direktivet på samtliga flygningar inom EU som fattats av enheten för passagerar-

[11] 33 § andra stycket förvaltningsprocesslagen (1971:291).

information ska underställas Försvarsunderrättelsedomstolen. Med en sådan processordning säkerställs att samtliga sådana beslut blir föremål för en effektiv kontroll i domstol. Det innebär vidare att antalet mål som anhängiggörs vid domstolen begränsas till ett per år, med undantag för den osannolika händelseutvecklingen att fler än ett beslut fattas inom loppet av ett år. För att säkerställa att beslutet underställs domstolens prövning inom rimlig tid anser vi att det bör införas en bestämmelse som innebär att beslutet ska underställas utan onödigt dröjsmål och senast inom en vecka från det datum då beslutet fattades.

8.3.2 Förfarandet vid Försvarsunderrättelsedomstolen

Förslag

Vid handläggningen i Försvarsunderrättelsedomstolen ska de befintliga förfaranderegelna i lagen om Försvarsunderrättelsedomstol tillämpas, med undantag för att ett integritetsskyddsombud inte ska förordnas. Målen ska således avgöras efter sammanträde.

Integritetsskyddsombud

I mål hos Försvarsunderrättelsedomstolen som avser tillstånd till signalspaning förekommer ett integritetsskyddsombud som ska bevaka enskildas integritetsintresse i mål vid domstolen. Ombudet har rätt att ta del av det som förekommer i målet och att yttra sig. Det finns ingen möjlighet att överklaga Försvarsunderrättelsedomstolens avgöranden och integritetsskyddsombudens roll är således mer begränsad än offentliga ombud i som bevakar enskildas integritetsintressen när det gäller hemliga tvångsmedel.

Frågan om offentliga ombud har diskuterats i flera lagstiftningsprocesser. Lagstiftaren har tidigare, i frågor som rör tvångsmedel, ifrågasatt om en sådan kan fylla någon reell funktion eftersom denne inte kommer att kunna hämta upplysningar från den misstänkte eller från något annat håll. Det offentliga ombudet kommer att vara helt hänvisad till det material som åklagaren förebringar och möjligheterna att tillvarata den misstänktes och andras intressen är alltså inte bättre än beslutsorganets. Värdet skulle närmast ligga i möjligheten att över-

klaga i tveksamma fall. Det värdet är emellertid begränsat eftersom den lägre instansens avgöranden inte kan publiceras eller på annat sätt tjäna till vägledning utanför det enskilda fallet.[12] Ett system med ett offentligt ombud har också beskrivits som i det närmaste en skenprocess där några avgörande fördelar inte står att vinna.[13]

I senare förarbeten har i stället fördelarna med en ett oberoende ombud som bevakar enskildas intressen lyfts fram och offentliga ombud infördes i tillståndsprocessen för hemliga tvångsmedel. Enligt regeringen förstärks enskildas rättsskydd om det i processen tillkommer en person som särskilt har till uppgift att bevaka enskildas intressen och att lyfta fram omständigheter till skydd för den enskildas integritet. Genom införandet av ett system med offentliga ombud skapas ett slags kontradiktorisk process i ärenden om hemliga tvångsmedel. En sådan process ger bättre förutsättningar för en allsidig belysning av saken.[14]

I mål om tillstånd till signalspaning vid Försvarsunderrättelsedomstolen har en domstolsprövning med endast en sökande som part ansetts inte i tillräcklig grad motsvara den prövning som generellt sett förekommer vid domstolar. Systemet med integritetsskyddsombud utformades i huvudsak i enlighet med vad som gäller för offentliga ombud och infördes bl.a. för att ge prövningen en tydligare kontradiktorisk karaktär. Integritetsskyddets uppgift är inte att företräda det direkt motstående intresset vid prövningen av tillstånd till signalspaning. Det uppenbara motsatsförhållandet vid prövningen står nämligen inte mellan det allmänna och det enskilda, utan mellan olika direkta eller indirekta statsintressen. Det faller på sin egen orimlighet att ett integritetsskyddsombuds roll skulle bestå i att företräda en främmande makts intressen. Integritetsskyddsombudets uppgift måste i stället vara att på ett generellt plan företräda integritetsintresset i allmänhet.[15]

I betänkandet *Säkerhetspolisens behandling av personuppgifter* föreslås Försvarsunderrättelsedomstolen som prövningsinstans för Säkerhetspolisens ansökningar om tillstånd till framtagning av personuppgifter från särskilda uppgiftssamlingar. Enligt förslagen i betänkandet ska integritetsskyddsombudet i processen ersättas av tillsynsmyndig-

[12] Prop. 1988/89:124, *Om vissa tvångsmedel*, s. 53.
[13] SOU 1990:51, *Säkerhetspolisens arbetsmetoder, personalkontroll och meddelarfrihet*, s. 176.
[14] Prop. 2002/03:74, *Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering*, s. 22–23.
[15] Prop. 2008/09:201, *Förstärkt integritetsskydd vid signalspaning*, s. 74–75.

heten Säkerhets- och integritetsskyddsmyndigheten. En sådan lösning anses mer effektiv. Det förs även fram att betydande rättssäkerhetsvinster skulle kunna uppnås om tillsynsmyndigheten, som har förutsättningar att få kännedom om hur besluten verkställs även har en möjlighet att förmedla detta till domstolen. Generellt har en kontradiktorisk process stora fördelar i förhållande till ett rent ansökningsförfarande. En motpart som företräder andra intressen än sökanden berikar både det material som domstolen ska ta ställning till och den rättsliga diskussionen. Det finns goda skäl ge även en röst till samhällsintressen som indirekt eller direkt står i motsatsförhållande till de intressen som föranleder ansökningen. Ett offentligt ombud kan ges ett tydligt intresse att bevaka i processen, vilket inte på samma sätt låter sig göras för en annan myndighet under regeringen.

I betänkandet anges vidare att tillståndsförfarandet syftar till att bl.a. möjliggöra och samtidigt kontrollera införandet av ny teknik som skulle kunna utgöra en fri- och rättighetsrisk. Det pågår en mycket snabb och svårbedömd teknisk utveckling inom området. Det finns en risk att en allmän juridisk skicklighet inte längre är tillräckligt för att kunna göra välavvägda bedömningar i de frågor som avhandlas i en ansökan om tillstånd.[16]

När det gäller prövningen av ett beslut att tillämpa PNR-systemet på samtliga flygningar inom EU, som i sak handlar om en bedömning av terrorhotet mot Sverige, gör sig inte argument avseende den tekniska utvecklingen gällande så som i frågor om tillstånd till framtagning av personuppgifter från särskilda uppgiftssamlingar.

Ett beslut om att tillämpa PNR-systemet på samtliga flygningar inom EU påverkar enskildas grundläggande rättigheter och det kan ur det perspektivet argumenteras för att det bör finnas ett ombud som bevakar det intresset i processen. Som nämnts handlar dock sakfrågan om huruvida det finns ett verkligt och aktuellt eller förutsebart terrorhot mot Sverige. Om det finns ett sådant ska ett beslut fattas. I prövningen ingår således inte en proportionalitetsbedömning där man väger åtgärden mot det motstående intresset av personlig integritet. Att ett sådant beslut är proportionerligt om förutsättningarna är uppfyllda framgår redan av EU-domstolens praxis.

I en bedömning av om det föreligger att terrorhot mot Sverige kan ett integritetsskyddsombud inte bidra på ett meningsfullt sätt till materialet i processen och det framstår inte heller som att ombu-

[16] SOU 2025:49, *Säkerhetspolisens behandling av personuppgifter*, s. 636–637.

det skulle kunna bidra till den rättsliga diskussionen. Mot bakgrund av detta anser vi att det inte ska förordnas ett integritetsskyddsombud i mål som rör underställda beslut avseende tillämpningen av PNR-systemet på samtliga flygningar inom EU. I betänkandet som rör Säkerhetspolisens behandling av personuppgifter har det föreslagits att det i 5 § lagen om Försvarsunderrättelsedomstol anges att ett integritetsskyddsombud ska bevaka enskildas integritetsintresse i mål vid domstolen om tillstånd till signalspaning. Vi anser att en sådan lösning är att föredra framför att införa ett eller flera undantag i samma paragraf.

Sammanträde

För mål vid Försvarsunderrättelsedomstolen gäller delar av förvaltningsprocesslagen (1971:291). Rättegångsbalkens regler om muntlighet, omedelbarhet och koncentration gäller inte i förvaltningsprocessen som i stället som huvudregel tillämpar ett skriftligt förfarande. Regleringen i 12 § lagen om Försvarsunderrättelsedomstol om att mål ska avgöras efter sammanträde infördes bl.a. för att främja snabbheten i handläggningen.[17] Det finns även ett värde i att rättens ledamöter får en muntlig föredragning och ges möjlighet att ställa frågor om Säkerhetspolisens bedömning. Vi anser därför att det är lämpligt att samma förfarande tillämpas i mål som avser underställda beslut om utvidgad tillämpning av PNR-systemet. Även i övrigt bör förfaranderegelrna i lagen om Försvarsunderrättelsedomstol tillämpas.

8.4 Förhandskontroll vid begäran om tillgång till PNR-information

Förslag

Bestämmelserna om överföring av PNR-uppgifter i lagen om flygpassageraruppgifter ska förändras på så sätt att de även omfattar begäran om överföring av PNR-information i efterhand. Reglerna ska gälla begäran om överföring av PNR-information i efterhand oavsett om de är behörighetsbegränsade eller ej.

[17] Prop. 2008/09:201, *Förstärkt integritetsskydd vid signalspaning*, s. 74–75.

I artikel 12.3 i PNR-direktivet anges att vid utgången av den inledande sexmånadersperioden ska utlämnande av fullständiga PNR-uppgifter tillåtas endast om det rimligen kan antas vara nödvändigt för direktivets ändamål. Det krävs vidare tillstånd från en rättslig myndighet eller en annan nationell myndighet som i enlighet med nationell rätt är behörig att kontrollera om villkoren för tillgång är uppfyllda.

I svensk rätt har detta reglerats i 4 kap. lagen om flygpassageraruppgifter i brottsbekämpningen. I 11 § anges att PNR-uppgifter som är behörighetsbegränsade enligt 3 kap. 11 § endast får överföras i sin fullständiga form till behöriga mottagare om det rimligen kan antas vara nödvändigt. Om en förundersökning pågår ska en begäran från en behörig myndighet att få tillgång till fullständiga PNR-uppgifter beslutas av en åklagare. Om det inte pågår någon förundersökning krävs det att Polismyndigheten lämnar tillstånd till överföringen.

Varken i PNR-direktivet eller i svensk lagstiftning framgår att en begäran om tillgång till PNR-uppgifter under de inledande sex månaderna ska underställas en liknande prövning. Av PNR-domen framgår dock att så ska ske. EU-domstolen hänvisar till skäl 25 i direktivet, som avser att säkerställa högsta möjliga nivå av dataskydd när det gäller åtkomsten till PNR-uppgifter i en form som gör det möjligt att direkt identifiera den registrerade. En förfrågan om utlämnande och bedömning i efterhand förutsätter en sådan åtkomst, oberoende av när förfrågan lämnas in, dvs. före eller efter sexmånadersperiodens utgång. Utlämnande av PNR-uppgifter i efterhand ska alltså föregås av en förhandskontroll utförd av en domstol eller en oberoende förvaltningsmyndighet. Beslutet ska fattas efter en motiverad begäran från den behöriga mottagaren.

Den svenska regleringen behöver således ändras för att vara förenlig med uttalandena i PNR-domen, och därmed EU-rätten, avseende förhandskontrollen av en begäran om tillgång till PNR-uppgifter. Bestämmelserna om vilka myndigheter som ska pröva frågan om en begäran om tillgång till PNR-uppgifter ska därför inte längre gälla endast behörighetsbegränsade uppgifter, utan i stället gälla som en generell regel för alla förfrågningar om att ta del av PNR-information i efterhand. Bestämmelserna i 4 kap. 11 § första stycket lagen om flygpassageraruppgifter ska därför förändras på så sätt att de reglerar överföring av PNR-uppgifter till behöriga mottagare eller ett tredjeland, oavsett om de är behörighetsbegränsade eller ej.

Bestämmelsen omfattar i nuläget endast PNR-uppgifter och inte PNR-information. Med PNR-uppgifter avses inom ramen för PNR-systemet uppgifter om varje enskild passagerare som har lämnats vid bokning av en flygresa och vid incheckning. PNR-information är sådana PNR-uppgifter och resultatet av en enhet för passagerarinformations behandling av sådana uppgifter. Av artikel 6.2 b i PNR-direktivet framgår att enheten för passagerarinformation ska behandla PNR-uppgifter för att i enskilda fall besvara en förfrågan från de behöriga mottagarna om att tillhandahålla och behandla PNR-uppgifter i specifika fall och tillhandahålla de behöriga myndigheterna eller, när så är lämpligt, Europol, *resultaten* av sådan behandling. En överföring kan således utöver PNR-uppgifter även omfatta PNR-information. Motsvarande bestämmelse när det gäller en begäran från en enhet för passagerarinformation i en annan medlemsstat finns i artikel 9.2.

För att möjliggöra att även PNR-information överförs bör rubriken till och texten i 4 kap. 11 § lagen om flygpassageraruppgifter i brottsbekämpningen ändras för att återspegla detta.

Förhandskontroll behöver inte göras när enheten för passagerarinformation använder informationen för att fullgöra uppgifterna enligt 3 kap. 4 § 3 i lagen om flygpassageraruppgifter i brottsbekämpningen.

8.5 Prövning av begäran om tillgång till PNR-information

I enlighet med vårt förslag som läggs fram i avsnitt 8.4 kräver all begäran om tillgång till PNR-information ett godkännande, oavsett om begäran sker under den inledande sexmånadersperioden eller den efterföljande perioden upp till fem år. Enligt den nuvarande regleringen i 4 kap. 11 § lagen om flygpassageraruppgifter i brottsbekämpningen ska beslut om tillgång till fullständiga PNR- information fattas av en åklagare om det pågår en förundersökning, och av Polismyndigheten om det inte pågår någon förundersökning. Lagen stiftades innan PNR-domen meddelades och frågan är om svensk rätt i detta avseende är förenlig med de uttalanden som EU-domstolen gjorde i domen.

I PNR-domen anges att det är en domstol eller oberoende förvaltningsmyndighet som ska besluta om tillgång till PNR-uppgifter. Myndigheten ska förfoga över alla befogenheter och lämna alla nödvändiga garantier för att säkerställa en avvägning mellan de olika intressena

och rättigheterna i fråga. Myndigheten måste ha en ställning som innebär att den kan fullgöra sitt uppdrag på ett objektivt och opartiskt sätt, och den måste därför vara fri från all yttre påverkan. Detta krav på oberoende innebär att myndigheten måste vara fristående i förhållande till den som begär tillgång till uppgifterna, så att myndigheten kan utöva sin kontroll utan yttre påverkan. På det straffrättsliga området innebär kravet på oberoende att myndigheten dels inte får vara involverad i den aktuella brottsutredningen, dels att den ska ha en neutral ställning i förhållande till parterna i det straffrättsliga förfarandet.

För att bedöma om svensk rätt är förenlig med EU-rätten i ljuset av de uttalanden som gjorts i PNR-domen är det av vikt att beakta de resonemang som låg till grund för den nuvarande svenska lagstiftningen. I nedanstående avsnitt redogörs därför för förarbetena till den svenska regleringen.

8.5.1 Förarbeten till den svenska beslutsordningen

Under lagstiftningsarbetet[18] diskuterades vilken eller vilka myndigheter som skulle pröva en begäran från en behörig myndighet om att få tillgång till fullständiga PNR-uppgifter.

En förutsättning för överföring av PNR-uppgifter i sin fullständiga form är att det finns tillstånd till överföringen från en rättslig myndighet eller en annan nationell myndighet som i enlighet med nationell rätt är behörig att kontrollera om villkoren för tillgång är uppfyllda. I EU:s rättsakter för samarbete i rättsliga frågor används ofta begreppet rättslig myndighet, med vilket avses i första hand domstol eller, för svenska förhållanden, åklagare. PNR-direktivet öppnar även upp för att en annan nationell myndighet kan lämna behövligt tillstånd.

Vid tiden för lagstiftningen fanns det inget befintligt system med bevarande och tillgång till PNR-uppgifter i brottsbekämpningen och det fanns därmed inte någon ordning att ta avstamp i vid bedömningen av hur direktivets krav på tillstånd till utlämnande ska genomföras. Det konstaterades att det inte fanns någon myndighet som var självskriven för tillståndsgivningen.

[18] Detta avsnitt redogör för innehållet i prop. 2017/18:234, *Lag om flygpassageraruppgifter i brottsbekämpningen*, avsnitt 10.5.2 samt SOU 2017:57, *Lag om passageraruppgifter i brottsbekämpningen*, avsnitt 15.5.4.

I svensk rätt beror beslutsordningen på om det pågår en förundersökning. Om en sådan pågår ska en åklagare fatta beslut om tillgång till PNR-uppgifter. Åklagaren tar över ledningen av förundersökningen så snart någon skäligen kan misstänkas för brottet, eller om det annars är motiverat av särskilda skäl. Det framgår av PNR-direktivets skäl 25 att den maskering av PNR-uppgifter som ska ske efter sex månader syftar till att undvika oproportionerlig användning av uppgifterna. Åtkomst till fullständiga PNR-uppgifter ska därefter endast få ske under mycket strikta och begränsade villkor för att säkerställa högsta möjliga nivå av dataskydd. Samtidigt är förutsättningen för en överföring till behöriga myndigheter knuten till vad som kan antas vara nödvändigt för den brottsbekämpande verksamheten i fråga. Det är därför lämpligt att, i de fall en förundersökning har inletts, prövningen om det finns ett behov av full åtkomst till PNR-uppgifterna görs av någon som har relevant erfarenhet och kunskap för att bedöma behoven av uppgifterna i en förundersökning.

En svensk åklagare uppfyller rekvisiten för att vara en sådan rättslig myndighet som avses i artikel 12.3 b i direktivet. Det ingår i åklagarens ordinarie arbete som förundersökningsledare att fatta beslut om ingripande åtgärder på ett rättssäkert sätt och med beaktande av proportionalitetsprincipen. Det torde också vara förundersökningsledaren som, bättre än någon annan, kan bedöma om förutsättningarna för att få ut behörighetsbegränsade PNR-uppgifter är uppfyllda, dvs. om de kan antas vara nödvändiga för brottsutredningen och därmed utgöra en proportionerlig användning.

Eftersom åklagaren inte har någon roll i polisens allmänna underrättelsearbete får det anses vara mindre lämpligt att åklagaren beslutar om att hämta in fullständiga PNR-uppgifter som är behörighetsbegränsade när de behövs i underrättelseverksamhet. Inte heller domstolarna eller någon av de myndigheter som har till uppgift att utöva tillsyn över den brottsbekämpande verksamheten anses lämpliga att meddela tillstånd i dessa fall.

Det alternativ som återstår att överväga är därmed om frågan om tillstånd till en överföring kan beslutas av någon av de behöriga myndigheterna, PNR-direktivet föreskriver nämligen inte att det måste vara en oberoende myndighet som ska ge tillstånd, som alternativ till en rättslig myndighet, när det handlar om överföring av behörighetsbegränsade PNR-uppgifter.

I förarbetena görs vidare en jämförelse med det upphävda datalagringsdirektivet. En av bristerna med direktivet var avsaknaden av kontroll av en oberoende myndighet i förhållande till brottsbekämpande myndigheters tillgång till lagrade trafik- och lokaliseringsuppgifter.[19] Regeringen ansåg dock att det fanns väsentliga skillnader mellan användningen av datalagrad elektronisk kommunikation i brottsbekämpningen respektive användning av PNR-uppgifter. Regeringen ansåg vidare att det fanns goda skäl att inte dra så långtgående slutsatser av EU-domstolens avgöranden i datalagringsfrågorna att någon oberoende kontrollinstans måste ges i uppgift att godkänna överföring av behörighetsbegränsade PNR-uppgifter trots att detta inte är ett krav enligt PNR-direktivet.

Det bör vara tillräckligt att tillstånd till överföring av PNR-uppgifter i sin fullständiga form till behöriga myndigheter inhämtas från en behörig myndighet, som lämpligen är Polismyndigheten. Tillstånd bör inte kunna ges av någon som själv deltar i den verksamhet som har begärt ut informationen eller av någon som arbetar vid enheten för passagerarinformation. En begäran från andra medlemsstater och Europol bör behandlas på samma sätt som en begäran från svenska myndigheter utanför förundersökningsförfarandet, oavsett om uppgifterna begärs ut för att användas i en förundersökning eller i underrättelseverksamhet.

8.5.2 EU-domstolens yttrande avseende PNR-avtalet mellan EU och Kanada

Den 26 juli 2017 meddelade EU-domstolen ett yttrande[20] avseende ett föreslaget avtal mellan EU och Kanada beträffande överföring av PNR-uppgifter. Domstolen ansåg att avtalet, i dess dåvarande form, inte var förenligt med grundläggande rättigheter inom EU-rätten. Vissa delar av avtalet, särskilt vad avser lagringen och regleringen av tillgång till uppgifter, var inte tillräckligt begränsade till vad som är strängt nödvändigt för att uppnå målen att bekämpa terrorism och grov brottslighet.

[19] EU-domstolens domar den 21 december 2016, *Tele2 Sverige AB*, mål nr C-203/15 och *Watson m.fl.*, mål nr C-698/15.
[20] EU-domstolens yttrande 1/15, *Förslag till avtal mellan Kanada och Europeiska unionen*, den 26 juli 2017.

I yttrandet konstaterar EU-domstolen att det är väsentligt att användningen av lagrade PNR-uppgifter under flygpassagerares vistelse i Kanade i princip, utom i vederbörligen motiverade brådskande fall, är underkastad förhandskontroll av en domstol eller en oberoende myndighet och att beslutet fattas efter att behöriga myndigheter framställt en motiverad ansökan. I det planerade avtalet finns det inte något sådant krav på tillstånd från en domstol eller oberoende myndighet och under dessa omständigheter går avtalet utöver vad som är strängt nödvändigt.

8.5.3 Är den svenska beslutsordningen förenlig med PNR-domen?

Under pågående förundersökning

Den svenska lagstiftningen trädde i kraft innan PNR-domen meddelades. Lagstiftarens uppfattning var vid den tidpunkten att PNR-direktivet inte ställde upp något krav på att myndigheten som prövar ett beslut om tillgång till PNR-uppgifter ska vara oberoende. I PNR-domen slås det emellertid fast att så är fallet; det finns ett krav på oberoende som innebär att myndigheten måste vara fristående i förhållande till den som begär tillgång till uppgifterna. På det straffrättsliga området innebär kravet på oberoende att myndigheten inte får vara involverad i den aktuella brottsutredningen samt att den ska ha en neutral ställning i förhållande till parterna i det straffrättsliga förfarandet. Det finns därför anledning att ifrågasätta om den svenska regleringen uppfyller detta krav.

När det gäller en begäran om tillgång till PNR-uppgifter i en pågående förundersökning ska beslut fattas av en åklagare. Beslut att inleda förundersökning kan enligt 23 kap. 3 § rättegångsbalken, RB, fattas av Polismyndigheten, Säkerhetspolisen eller åklagare. Även Tullverket kan fatta beslut om inledande av förundersökning enligt 8 kap. 3 § tullbefogenhetslagen (2024:710). Åklagaren tar över ledningen för förundersökningen så snart någon skäligen kan misstänkas för brottet eller när det är motiverat av särskilda skäl, med undantag för förundersökningar avseende mindre allvarliga brott.

Enligt 23 kap. 4 § RB ska en förundersökning bedrivas objektivt. Vid förundersökningen ska förundersökningsledaren söka efter, ta till vara och beakta omständigheter och bevis som talar såväl till den

misstänktes fördel som till hans eller hennes nackdel. Förundersökningen ska bedrivas så att inte någon onödigt utsätts för misstanke eller orsakas kostnad eller olägenhet. Åklagaren åtnjuter vidare en självständig ställning gentemot utomstående.

Under en förundersökning kan en mängd olika mer eller mindre ingripande åtgärder vidtas. Vissa särskilt ingripande åtgärder regleras som straffprocessuella tvångsmedel i 24–28 kap. RB, t.ex. frågor om frihetsberövande, vissa andra begränsningar i rörelsefriheten, kvarstad, beslag, husrannsakan och kroppsbesiktning. I 27 kap. regleras hemliga tvångsmedel, t.ex. hemlig övervakning av elektronisk kommunikation.

Gemensamt för all tvångsmedelsanvändning enligt rättegångsbalken är att beslutsförfarandet är reglerat. Vid mer ingripande tvångsmedel är allmän domstol ensam behörig att fatta beslut. Åklagare har rätt att i vissa fall fatta interimistiska beslut i brådskande fall. Beträffande många andra åtgärder under pågående förundersökning finns det inte någon motsvarande reglering som den i rättegångsbalken för tvångsmedel. Detta gäller exempelvis vissa spanings- eller utredningsmetoder såsom infiltration eller provokation. När det gäller sådana metoder finns det i stället riktlinjer som har utfärdats av Åklagarmyndigheten.[21] Av dessa framgår bl.a. att beslut om användande av sådana metoder alltid ska fattas av den allmänna åklagare som är förundersökningsledare.

När det gäller åklagarens oberoende gentemot Åklagarmyndigheten skiljer sig Sverige från många andra europeiska länder. Svenska åklagare är självständiga i beslutsfattande och utövar myndighet på eget ansvar och i eget namn. Behörigheten följer direkt av författning och inte genom delegation från den åklagarmyndighet som de tjänstgör vid. Åklagarmyndigheten har som myndighet inte beslutanderätt i brottsmålsfrågor utan den rätten tillkommer de enskilda åklagarna. Det finns ett stort antal åtgärder och beslut som enbart får vidtas eller fattas av åklagare och inte av en åklagarmyndighet. En åklagarmyndighet har t.ex. inte rätt att utföra de åtgärder som ålagts åklagarna i rättegångsbalken och kan inte besluta om att en förundersökning ska inledas, hur förundersökningen ska bedrivas eller om åtal ska väckas. Det är frågor som endast kan avgöras och beslutas av en åklagare. Beslut som fattas av en åklagare kan bara överprövas i efterhand av en åklagare på en högre rättslig nivå, medan beslut som fattas av en

[21] Riksåklagarens riktlinjer, *Provokation och infiltration inom förundersökning*, RåR 2016:1.

åklagarmyndighet i stället prövas och överklagas på samma sätt som andra förvaltningsbeslut. En åklagarmyndighet kan alltså inte överpröva en åklagares beslut. Som nämnts anges det i PNR-domen att myndigheten som ska fatta beslut om tillgång till PNR-uppgifter inte får vara involverad i den aktuella brottsutredningen. Liknande resonemang läggs fram av EU-domstolen i målet *Prokuratuur*[22]. Domstolen ansåg att det fanns hinder mot en nationell lagstiftning som gav Åklagarmyndigheten, vars uppdrag är att leda förundersökningar och, i förekommande fall, väcka åtal i samband med ett senare förfarande, behörighet att ge offentliga myndigheter tillgång till trafik- och lokaliseringsuppgifter inom ramen för en brottsutredning. Detta gäller även med beaktande av att Åklagarmyndigheten enligt nationell rätt är skyldig att agera oberoende, endast är underställd lagen och under förundersökningen ska undersöka både sådana omständigheter som är till fördel och sådana som är till nackdel för den misstänkte. Ett sådant förfarande syftar icke desto mindre till att samla in bevisning och skapa erforderliga förutsättningar för en rättegång. Det är Åklagarmyndigheten som företräder det offentliga under rättegången och den är således även part i förfarandet. Domstolen ansåg därför att myndigheten inte uppfyller kravet att den inte får vara involverad i den aktuella brottsutredningen samt att den ska ha en neutral ställning i förhållande till parterna i det straffrättsliga förfarandet.

I svensk rätt är det den enskilde åklagaren, och inte Åklagarmyndigheten, som har ålagts att pröva en begäran om tillgång till PNR-uppgifter under pågående förundersökning. Det är således den enskilde åklagarens oberoende och neutrala ställning i förhållande till parterna i det straffrättsliga förfarandet som ska bedömas. Det är den enskilde åklagaren som leder förundersökningar, beslutar om åtgärder under förundersökningen, väcker åtal och för talan under den straffrättsliga processen. Med beaktande av detta är det svårt att se åklagaren som neutral till parterna i processen, eftersom åklagaren själv intar partsställning i rättegången. Detta gäller även om ett beslut om tillgång till PNR-uppgifter fattas av en annan åklagare än den som är eller sedermera blir involverad i processen. Mot bakgrund av det som angivits ovan står det klart att svensk lagstiftning måste ändras i detta avseende.

[22] EU-domstolens dom den 2 mars 2021, *Prokuratuur*, mål nr C-746/18, se p. 47.

Beslutsordning i andra fall

Om det inte pågår en förundersökning är det Polismyndigheten som ska lämna tillstånd till överföring av fullständiga PNR-uppgifter till den behöriga myndighet som begärt tillgång till uppgifterna. Polismyndigheten är själv en av de behöriga myndigheterna enligt 3 § förordningen om flygpassageraruppgifter i brottsbekämpningen. Med hänvisning till uttalandena i PNR-domen förefaller det uteslutet att en begäran från Polismyndigheten ska prövas av den egna myndigheten. Även i detta avseende behöver således svensk rätt ändras.

8.5.4 Våra överväganden och förslag

I förarbetena till den nuvarande regleringen konstateras att det inte finns någon myndighet som är självskriven för tillståndsgivningen.[23] Efter att ha uteslutit de behöriga myndigheterna samt, under pågående förundersökning, Åklagarmyndigheten som tillståndsgivare har detta konstaterande än mer bäring. Det återstår endast ett fåtal myndigheter som kan komma i fråga som tillståndsgivare.

Enheten för passagerarinformation bedriver verksamhet, tar emot och behandlar begäran om tillgång till PNR-information dygnet runt. För brottsbekämpande myndigheter är det av vikt att snabbt få tillgång till de begärda uppgifterna. Vår utgångspunkt är därför att den myndighet som ges uppgiften bör ha kapacitet att fatta beslut under dygnets alla timmar.

Under lagstiftningsarbetet diskuterades fyra olika existerande myndighetsorganisationer som framstår som tänkbara för uppgiften: domstolsväsendet, åklagarväsendet och de två tillsynsmyndigheter som har tillsyn över polisens behandling av personuppgifter, vilka i dagsläget är Integritetsskyddsmyndigheten, IMY, och Säkerhets- och integritetsskyddsnämnden, SIN. Det kan även övervägas om en särskild nämnd ska inrättas för att genomföra tillståndsprövningen eller om den bör förläggas till enheten för passagerarinformation. Vi har inte identifierat någon ytterligare myndighet som kan komma i fråga som tillståndsgivare.

IMY är den myndighet som utövar tillsyn över personuppgiftsbehandlingen enligt lagen om flygpassagerarinformation. Vi anser emellertid att det vore olämpligt att använda sig av samma myndighet

[23] Prop. 2017/18:234, *Lag om flygpassageraruppgifter i brottsbekämpningen*, s. 102.

för tillståndsgivningen som för tillsynen över arbetet inom enheten för passagerarinformation.

Vid SIN finns det visserligen en upparbetad organisation för att hantera sekretesskyddat material från förundersökningar och underrättelsearbete. SIN är däremot inte uppbyggd för att hantera frågor med mycket kort varsel. Det skulle också innebära ett nytt slags aktiv inblandning i myndigheters pågående verksamhet än vad nämnden har i dag. Sammantaget anser vi att det inte är lämpligt att göra SIN till tillståndsgivare för överföring av PNR-information.

Ett alternativ är att tillskapa en särskild nämnd som fattar beslut i frågor om tillgång till PNR-information. I nämnden skulle kunna ingå välmeriterade jurister och andra tjänstemän med bred sakkunskap. Det finns emellertid nackdelar med ett sådant system. Ett system med en nämnd skulle vara sårbart i och med att kan uppstå svårigheter att med kort varsel samla nämnden för föredragning och beslut. Dessutom riskerar antalet ärenden innebära att arbetet med att fatta beslut kräver heltidsarbete av ledamöterna. Det skulle innebära att det snarare tillskapas en ny myndighet än en särskild nämnd. Detta skulle även försvåra rekryteringen av ledamöter. Detta kompliceras ytterligare av förutsättningen att nämnden skulle ha beredskap dygnet runt.

Utöver det som nämnts ovan innebär tillskapandet av en särskild nämnd en kostsam lösning som tar tid att genomföra. Övervägande skäl talar därför mot ett införande av en nämnd som fattar beslut i dessa frågor.

Enheten för passagerarinformation hanterar i dagsläget de begäran om tillgång till PNR-uppgifter som kommer in till enheten och bedömer om det finns förutsättningar att lämna ut uppgifterna. Vid enheten finns det dessutom stor kunskap, kompetens och erfarenhet som är relevant för tillståndsprövningen. Utöver att enheten besitter rätt kompetens vore en sådan lösning även den minst kostsamma.

I förarbetena[24] till den svenska regleringen framgår att bestämmelsen om att utlämnande av avmaskerade PNR-uppgifter kräver tillstånd från en rättslig myndighet eller annan nationell myndighet inte fanns med i kommissionens förslag till PNR-direktiv från 2011, utan tillkom i de senare förhandlingarna. Enligt kommissionens förslag skulle tillgång till avmaskerade PNR-uppgifter endast kunna beviljas av chefen för enheten för passagerarinformation. Juster-

[24] SOU 2017:57, *Lag om flygpassageraruppgifter i brottsbekämpningen*, s. 295–296.

ingen i direktivet kan inte tolkas på annat sätt än att det har byggts in ett krav på något slag av tilläggskontroll av enhetens egen prövning av att förutsättningarna för överföring av avmaskerade PNR-uppgifter är uppfyllda. I betänkandet konstaterades därför att ett genomförande som innebär att chefen för enheten för passagerarinformation beslutar om överföringen inte uppfyller kravet på godkännande som föreskrivs i direktivet.

Det kan ifrågasättas om enheten för passagerarinformation kan anses vara tillräckligt fristående och oberoende gentemot resten av Polismyndigheten, som i egenskap av behörig myndighet framställer begäran om tillgång till PNR-uppgifter till enheten. Enheten för passagerarinformation är organisatoriskt inordnad som en sektion under Nationella gränspolisenheten, NGPE, som i sin tur ligger under Nationella operativa avdelningen, Noa, vid Polismyndigheten. Det är enhetschefen vid NGPE som tillsätter enheten för passagerarinformations enhetschef. Enheten har ingen egen anslagspost i regleringsbrevet och inte heller en budget som är fristående från Polismyndighetens. Enheten sitter i lokaler som även en begränsad krets av utomstående personal inom Polismyndigheten har tillgång till. Det finns ett eget diarium och ett eget it-system som endast enhetens medarbetare har tillgång till.

I förarbetena[25] till lagen om flygpassageraruppgifter diskuterades enheten för passagerarinformations organisation och självständighet. Det konstateras att hur enheten ska organiseras, bemannas och administreras m.m. bör överlåtas till Polismyndigheten att bestämma, lämpligen i samband med behöriga myndigheter. Enhetens självständighet diskuteras utifrån ett sekretessperspektiv, dvs. huruvida det finns någon sekretessgräns mellan enheten och Polismyndighetens övriga brottsbekämpande verksamhet. Enligt 8 kap. 2 § offentlighets- och sekretesslagen (2009:400), OSL, kan det finnas en sekretessgräns inom en myndighet, nämligen mellan olika verksamhetsgrenar, om de är att betrakta som självständiga i förhållande till varandra. Motsvarande bestämmelse finns i 2 kap. 8 § tryckfrihetsförordningen[26] där det anges att en handling blir allmän när den överlämnats mellan organ inom samma myndighetsorganisation. Det avgörande även i detta fall är att organen uppträder som självständiga i förhållande

[25] Prop. 2016/:234, *Lag om flygpassageraruppgifter i brottsbekämpningen,* s. 49 och SOU 2017:57, *Lag om flygpassageraruppgifter i brottsbekämpningen,* s. 170–174.
[26] Bestämmelsen återfinns numera i 2 kap. 11 § tryckfrihetsförordningen.

till varandra. Däremot behöver det inte vara fråga om olika verksamhetsgrenar. Om olika delar av en myndighets verksamhet har att tillämpa olika sekretessbestämmelser samt om det finns en organisatorisk åtskillnad och om verksamhetsdelarna har skilda syften eller funktioner som motiverar intern sekretess får de anses utgöra olika verksamhetsgrenar i OSL:s mening.

I förarbetena konstateras vidare att enheten för passagerarinformation kommer att vara en egen enhet men som sådan utgöra en del av Polismyndighetens brottsbekämpande verksamhet. När det gäller informationsöverföring inom Polismyndigheten synes den rådande uppfattningen vara att det inte förekommer sekretessgränser inom myndighetens brottsförebyggande och brottsutredande verksamhet. Trots att enheten för passagerarinformation kommer att organiseras skild från övrig verksamhet är det inte troligt att den kommer att organiseras så att den blir i tillräcklig grad självständig gentemot övrig brottsbekämpande verksamhet vid Polismyndigheten.

Utifrån vad som har redovisats ovan är vår bedömning att enheten för passagerarinformation i dagsläget inte åtnjuter en tillräckligt självständig och oberoende ställning i relation till resten av Polismyndigheten. Det finns sätt att öka självständigheten för ett organ inom en myndighet, t.ex. genom att frigöra budgeten från myndighetens, ha lokaler avskilda från resterande personal eller genom att enhetschefen tillsätts av och rapporterar till regeringen. Det finns exempel på detta inom Polismyndigheten genom Avdelningen för särskilda utredningar och Finanspolissektionen. Dessa avdelningar har genom lagstiftning tillförsäkrats en hög grad av autonomi, men det kan ifrågasättas om självständigheten gentemot Polismyndigheten lever upp till de krav som ställs i PNR-domen.

För att enheten för passagerarinformation skulle uppfylla kraven på självständighet krävs det att den slås fast i författning. I och med att enheten fortsatt kommer att vara placerad inom Polismyndigheten kvarstår det dock en viss osäkerhet om en sådan ordning kan leva upp till kraven i PNR-domen. Vi anser till följd av detta att det inte är lämpligt att enheten för passagerarinformation utses till prövningsinstans för begäran om tillgång till passageraruppgifter.

8.5.5 Ny beslutsordning under pågående förundersökning

Förslag

Om en förundersökning pågår ska en begäran från en behörig myndighet om att få tillgång till PNR-information i efterhand prövas av allmän domstol.

En begäran om tillgång till PNR-information i efterhand under en pågående förundersökning ska prövas av den domstol som anges i 19 kap. rättegångsbalken. En begäran som framställs av Försvarsmakten eller Säkerhetspolisen ska dock prövas av Stockholms tingsrätt.

Förfarandet i domstol ska vara skriftligt och i övrigt följa reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor. Bestämmelserna om offentligt ombud ska inte tillämpas. En begäran om tillgång till PNR-information ska handläggas skyndsamt.

Vårt förslag är att allmän domstol ska fatta beslut om tillgång till PNR-information under pågående förundersökning. Allmän domstol uppfyller kraven som PNR-domen ställer på att prövningen ska ske av en domstol eller en oberoende förvaltningsmyndighet. En prövning av om tillstånd ska medges för tillgång till PNR-information bär vissa likheter med ett beslut om hemliga tvångsmedel och allmän domstol har den kompetens som krävs för att göra de aktuella bedömningarna. Domstolen intar en neutral ställning gentemot parterna i det straffrättsliga förfarandet. Allmän domstol framstår som väl lämpad att genomföra tillståndsprövningen under pågående förundersökning.

En domstol har emellertid inte möjlighet att ha beredskap dygnet runt för att fatta de aktuella besluten. Det är inte heller tänkbart att ålägga en domstol skyldigheten att bedriva verksamhet dygnet runt. Att förlägga tillståndsprövningen till allmän domstol är således inte en optimal lösning, men enligt vår mening framstår den ändå som bättre än de alternativ som tidigare redovisats.

Om prövningen ska genomföras av allmän domstol kan detta regleras på olika sätt. Ett alternativ är att införa ett skyndsamhetskrav för domstolen att genomföra prövningarna, vilket innebär att en begäran om tillgång till PNR-information som kommer in efter kontorstid i

normalfallet kan hanteras nästkommande arbetsdag. Den uppenbara nackdelen med detta är att dröjsmålet fråntar brottsbekämpande myndigheter möjligheten att snabbt vidta åtgärder under en stor del av dygnet. Behovet av att snabbt kunna vidta åtgärder bör dock vara något mindre under pågående förundersökning än i underrättelseskedet. En förundersökning avser ett redan begånget brott, medan PNR-information i underrättelseskedet kan användas för att avvärja nära förestående brott. Det kan emellertid uppstå situationer där omedelbara åtgärder behöver vidtas även under en förundersökning, exempelvis om det finns indikationer på att en misstänkt planerar att lämna landet. Förundersökningar kan även avse perdurerande brott, dvs. brott som anses pågå under hela tiden som ett visst tillstånd varar.

En alternativ lösning är att enheten för passagerarinformation i brådskande fall medger tillgång till PNR-information till en behörig myndighet och i efterhand underställer beslutet till en domstol. Det sker då, i likhet med dagens system, en prövning innan PNR-information lämnas ut. Enligt vår bedömning i avsnittet nedan är en sådan ordning förenlig med relevant praxis från EU-domstolen och vi föreslår också i det avsnittet en sådan ordning. I och med detta undviks den huvudsakliga nackdelen med att utse allmän domstol till prövningsinstans.

Behörig domstol

En begäran om tillgång till PNR-information bär vissa likheter med användandet av hemliga tvångsmedel och det finns därför anledning att utgå från den regleringen när det gäller frågan om behörig domstol att pröva en begäran om tillgång till PNR-information. Under pågående förundersökning gäller reglerna i rättegångsbalken om laga domstol i brottmål. Enligt huvudregeln i 19 kap. 1 § är laga domstol rätten i den ort där brottet har begåtts. Ett brott anses ha begåtts på den ort där gärningsmannen handlade. Det framgår vidare att om ett brott har skett på svenskt fartyg eller luftfartyg är även rätten i den ort dit den misstänkte först ankommer eller där han eller hon gripits eller annars uppehåller sig behörig. Om det är ovisst var brottet har begåtts får åtal tas upp av rätten i någon av de orter där det kan antas ha skett eller i den ort där den misstänkte gripits eller annars uppe-

håller sig. Enligt 19 kap. 12 § gäller reglerna i kapitlet även i fråga om domstolarnas befattning med förundersökning och användande av tvångsmedel. En sådan fråga får tas upp även av rätten i en annan ort än som följer av reglerna i detta kapitel, om beslut i frågan bör fattas utan dröjsmål och utredningen inte innehåller säkerhetsskyddsklassificerade uppgifter enligt säkerhetsskyddslagen.

Hanteringen av beslut om tillgång till PNR-information kan till följd av omfattningen och skyndsamhetskravet bli betungande för en enskild domstol att hantera. Det förefaller därför lämpligt att tillämpa samma regler som gäller för hemliga tvångsmedel även för sådana beslut.

Förfrågningar från Försvarsmakten och Säkerhetspolisen

Det finns omständigheter som talar emot att handläggningen av en begäran från Försvarsmakten eller Säkerhetspolisen om tillgång till PNR-information under pågående förundersökning sprids ut över flera domstolar.

I 27 kap. 34 § rättegångsbalken anges att Stockholms tingsrätt får pröva frågor om tillstånd till vissa hemliga tvångsmedel, när det gäller vissa i paragrafen uppräknade brott. Bland de uppräknade brotten kan nämnas sabotage och terroristbrott, vilka ingår i brottskatalogen inom PNR-systemet. I förarbetena till regleringen i rättegångsbalken framgår bl.a. följande. När det gäller tvångsmedelsanvändning inom Säkerhetspolisens arbete för att förhindra terrorism finns det en kompetens som har byggts upp vid Stockholms tingsrätt. Särlösningar i syfte att kontrollera handläggningen av vissa typer av mål till vissa domstolar bör dock användas endast när starka skäl talar för det. Så kan t.ex. vara fallet när det finns behov av extra stor skyndsamhet eller annan kompetens beträffande en viss måltyp.[27]

När det gäller brott som faller inom ramen för Säkerhetspolisens verksamhet leds förundersökningarna av Åklagarkammaren för säkerhetsmål, oavsett var i landet gärningsorten bedöms vara eller var den misstänkte uppehåller sig. I de ärenden som Försvarsmakten och Säkerhetspolisen handlägger förekommer det mycket känsliga uppgifter och det råder stark sekretess. Det finns behov både av extra stor skyndsamhet och särskild kompetens på området. Genom att

[27] Prop. 2013/14:237, *Hemliga tvångsmedel mot allvarliga brott*, s. 161–164.

koncentrera prövningen till en specifik domstol skapas förutsättningar för en ökad specialisering. Det främjar både skyndsamheten i handläggningen och uppbyggnad av specialkompetens allt eftersom domstolen handlägger målen.

Under utredningen har Försvarsmakten och Säkerhetspolisen fört fram att det är lämpligt att samtliga begäranden om tillgång till PNR-uppgifter under pågående förundersökning som framställs av respektive myndighet prövas av Stockholms tingsrätt. I och med att Stockholms tingsrätt redan är forum för vissa frågor om hemliga tvångsmedel när det rör t.ex. sabotage och terroristbrott framstår det som lämpligt att den domstolen är forum även vid begäran om tillgång till PNR-information som framställs av Försvarsmakten och Säkerhetspolisen under pågående förundersökning.

Förfarandet i domstol

Det framgår inte i PNR-direktivet eller PNR-domen hur tillståndsförfarandet ska gå till. Det är således upp till de enskilda medlemsstaterna att fastställa nödvändiga regler för handläggningen av beslut om tillgång till PNR-information. För att användningen av PNR-information ska vara ändamålsenlig krävs det ett snabbt beslutsfattande. Det finns därmed behov av en mindre formbunden handläggning i domstol.

Vid prövningen av vissa hemliga tvångsmedel utses ett offentligt ombud och det hålls ett sammanträde. Ett system med offentligt ombud innebär att prövningen får en kontradiktorisk karaktär[28] och fyller en funktion som rättssäkerhetsgaranti. Ombuden har sin främsta betydelse vid vissa särskilt integritetskänsliga tvångsmedel som t.ex. hemlig kameraövervakning. Vid vissa tvångsmedel, t.ex. hemlig rumsavlyssning och hemlig kameraövervakning, finns det utrymme för stora variationer i integritetsutrymmet. Detta kan bero på hur platsen för tvångsmedlet väljs och avgränsas, på vilken kameravinkel som används eller på att villkor ställs på när avlyssning eller övervakning får ske. Offentliga ombud har däremot inte ansetts motiverat i ärenden om hemlig övervakning av elektronisk kommunikation eftersom sådan övervakning inte ger någon information om innehållet i den kommunikation som övervakas och att integritetsintrånget typiskt

[28] Prop. 2008/09:201, *Förstärkt integritetsskydd vid signalspaning*, s. 70.

sett är avsevärt mindre när detta tvångsmedel används. Det finns därför mera sällan utrymme för att ifrågasätta eller diskutera utformningen av ett sådant tillstånd.[29]

Frågan om offentligt ombud diskuteras även i en proposition avseende polisens användning av AI i för ansiktsigenkänning i realtid.[30] Regeringen anför att det integritetsintrång som användning av tekniken kan medföra är mindre än jämfört med hemliga tvångsmedel. Integritetsintrånget begränsas också av de höga krav som föreslås i lagen om hur och när AI-system får användas och av rättssäkerhetsgarantier som säkerställer att intrånget i den personliga integriteten inte blir större än vad som kan godtas enligt regeringsformen, Europakonventionen, barnkonventionen och EU:s rättighetsstadga. Sammantaget anser regeringen att det inte bör införas ett krav på medverkan av offentliga ombud vid domstolens handläggning av ärenden om tillstånd att använda AI-system för ansiktsigenkänning i realtid. En följd av detta är att handläggningen också kan vara skriftlig.[31]

De uppgifter som kan utgöra PNR-uppgifter framstår som mindre känsliga ur integritetsperspektiv än både de uppgifter som behandlas inom ramen för hemlig elektronisk kommunikation och inom AI-system för ansiktsigenkänning. Känsliga personuppgifter får inte behandlas inom PNR-systemet och de uppgifter som faktiskt får behandlas rör förhållandevis neutrala uppgifter som t.ex. namn, kontaktuppgifter och bagageinformation. De offentliga ombudens medverkan i ärenden i domstol bör koncentreras till ärenden där behoven och funktionen av detta har visat sig vara starka.

Sammantaget bedömer vi att domstolens handläggning av en begäran om tillgång till PNR-information ska ske utan att ett offentligt ombud utses samt att handläggningen ska vara skriftlig. När det gäller övriga förfaranderegler ska rättegångsbalkens regler om handläggning vid domstol av frågor om tvångsmedel i brottmål gälla för förfarandet, t.ex. regler om rättens sammansättning och om överklagande.

Med tanke på att brottsbekämpande myndigheters behov av PNR-information ofta är tidskänsligt bör det i lagen föreskrivas att en begäran om tillgång till PNR-information ska handläggas skyndsamt.

[29] Prop. 2013/14:237, *Hemliga tvångsmedel mot allvarliga brott*, s. 120–121.
[30] Prop. 2025/26:150, *Polisens användning av AI för ansiktsigenkänning i realtid*.
[31] Prop. 2025/26:150, *Polisens användning av AI för ansiktsigenkänning i realtid*, s. 69.

8.5.6 Ny beslutsordning i andra fall

Förslag

Om det inte pågår en förundersökning ska en begäran om tillgång till PNR-information i efterhand prövas av åklagare.

Vårt förslag är att åklagare ska fatta beslut om tillgång till PNR-information i andra fall än under pågående förundersökning. En svensk åklagare uppfyller rekvisiten för att vara en sådan rättslig myndighet som avses i artikel 12.3 b i) i PNR-direktivet och har utöver detta erfarenhet och kapacitet att fatta beslut inom korta tidsramar. Åklagaren har en lagstadgad objektivitetsplikt även i de fall beslut fattas utanför en förundersökning enligt 23 kap. 4 § tredje stycket rättegångsbalken, vilket innebär att såväl omständigheter som talar för och som talar emot att en viss person är inblandad i brottslig verksamhet ska beaktas och att åklagaren inte får låta sig vägledas av andra intressen än de som de har i uppdrag att tillgodose.

Argumenten för att underkänna åklagaren som prövningsinstans i förundersökningsskedet gör sig inte gällande på samma sätt i underrättelseskedet. I den senare situationen finns det i regel inget konstaterat brott och det finns således ingen misstänkt. I Prokuratuur-målet[32] anger EU-domstolen att på det straffrättsliga området innebär kravet på oberoende att den myndighet som ska utföra förhandskontrollen dels inte får vara involverad i den aktuella brottsutredningen, dels ska ha en neutral inställning i förhållande till parterna i det straffrättsliga förfarandet. Så är inte fallet med en åklagarmyndighet som leder utredningsförfarandet och, i förekommande fall, väcker åtal för det allmännas räkning.

Som nämnts ovan finns det i underrättelseskedet i regel inget konstaterat brott och en begäran om tillgång till PNR-information är inte en del av en brottsutredning. En åklagare som fattar beslut gör det inte heller som ett led i ett utredningsarbete, såsom är fallet under en pågående förundersökning. Vid en jämförelse med syftena som anges i artikel 1 i PNR-direktivet och 1 kap. 1 § lagen om flygpassageraruppgifter i brottsbekämpningen avser behandlingen i det har skedet snarare att förebygga och förhindra terroristbrott och annan grov brottslighet än att upptäcka, utreda och lagföra sådan brottslighet.

[32] EU-domstolens dom den 2 mars 2021, *Prokuratuur*, mål nr C-746/18, p. 51 och 58.

Det finns dock vissa skäl som talar emot att ge åklagare en roll i underrättelseverksamheten. I regel deltar en åklagare inte i sådan verksamhet, utan i stället sker åklagarinträde först i samband med att förundersökning för ett konkret brott har inletts och någon är skäligen misstänkt för brottet. Det framstår som främmande att en åklagare skulle delta i den löpande underrättelseverksamheten. Om åklagaren har en central roll i underrättelseskedet genom att pröva begäran om tillgång till PNR-information kan det dessutom ge anledning att ifrågasätta åklagarens ställning och beslut om det senare blir fråga om en förundersökning och åtal där åklagaren intar partsställning. Åklagare har emellertid ansetts vara oberoende i förhållande till polisen när hemliga tvångsmedel används inom ramen för lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.[33]

Av de lösningar som är både praktiskt genomförbara och förenliga med EU-domstolens praxis anser vi att den lämpligaste är att beslut om tillgång till PNR-information i andra fall än under pågående förundersökning ska fattas av åklagare. Av naturliga skäl kan en begäran från Ekobrottsmyndigheten inte prövas av en åklagare anställd vid den myndigheten.

Till följd av att medlemsstaterna har införlivat PNR-direktivet på olika sätt i nationell rätt och att olika tolkningar av PNR-domen förekommer finns det en risk att det uppstår situationer där en annan medlemsstat eller tredjeland kräver godkännande från en oberoende myndighet vid vissa förfrågningar i Sverige trots att detta inte krävs i svensk rätt. För dessa fall är det lämpligt att införa en ventil, dvs. en möjlighet att i särskilda situationer kunna inhämta godkännande från åklagare eller domstol beroende på ärenden. Utan en sådan möjlighet riskerar Sverige att inte kunna samarbeta fullt ut med vissa medlemsstater eller tredjeländer.

[33] Prop. 2023/24:117, *Preventiva tvångsmedel för att förebygga och förhindra allvarliga brott*, s. 74–75.

8.5.7 Begäran från behörig mottagare utanför Sverige eller från tredjeland

Förslag

Om en begäran om tillgång till PNR-information i efterhand framställs av en behörig mottagare utanför Sverige eller från ett tredjeland ska beslut om tillgång fattas av åklagare, oavsett om begäran sker under pågående förundersökning eller i annat fall. Det ska därför anges att det endast är förundersökningar enligt rättegångsbalken som prövas av allmän domstol.

Om en rättslig prövning redan har genomförts av en domstol eller oberoende förvaltningsmyndighet i medlemsstaten varifrån begäran har inkommit ska ingen motsvarande prövning genomföras av en svensk åklagare. Detsamma gäller om begäran har inkommit från ett tredjeland som har slutit avtal med EU om överföring och behandling av passageraruppgifter.

Utöver de i svensk rätt utsedda behöriga myndigheterna kan det till enheten för passagerarinformation komma in en begäran om tillgång till PNR-information i efterhand från behöriga mottagare i ett annat land. Det kan vara en enhet för passagerarinformation i en annan medlemsstat, en behörig myndighet i en annan medlemsstat, Europol eller ett tredjeland. Enligt kommissionen följer det av ordalydelsen och logiken i PNR-direktivet och PNR-domen att det bör vara en myndighet i medlemsstaten som tar emot begäran som gör prövningen av om tillgång till uppgifter ska medges, och inte av den stat som framställer begäran.[34]

I praktiken går det till på olika sätt. I vissa fall, t.ex. vid begäranden från Tyskland eller Belgien, där det finns oberoende myndigheter som prövar en begäran om tillgång till uppgifter, finns det ett beslut om godkännande fogat till begäran. I andra fall finns det inte ett sådant beslut. Den svenska lagstiftningen bör vara anpassad till att kunna hantera både situationen där det finns ett medföljande beslut om godkännande av utlämnande av uppgifter, och där det inte finns ett sådant beslut.

[34] Europeiska kommissionen, *Report of the 14th Meeting on the Application of the PNR-directive*, 30 januari 2024, s. 5.

Av artikel 12.3 i PNR-direktivet följer att en begäran från en enhet för passagerarinformation till en enhet i en annan medlemsstat ska genomgå en rättslig prövning. Artikeln genomförs i svensk rätt genom 4 kap. 11 § lagen om flygpassageraruppgifter i brottsbekämpningen. I förarbetena till bestämmelsen framförde regeringen att bestämmelsen, dvs. artikel 12.3 i direktivet, är generellt formulerad och att det inte framgår att den endast är tillämplig vid överföring till någon särskild mottagare. Att bestämmelsen är tillämplig på andra medlemsstaters enheter för passagerarinformation och behöriga myndigheter framgår av artikel 9.2 sista meningen och artikel 9.3. bestämmelsen i svensk rätt ska därför vara tillämplig på samtliga behöriga mottagare och tredjeländer.[35]

I förarbetena framgår vidare att när det gäller en begäran från andra medlemsstater och Europol om att få ut behörighetsbegränsade PNR-information hade det i och för sig varit tänkbart att den svenska enheten för passagerarinformation skulle kunna godta ett beslut från en utländsk domstol eller annan rättslig myndighet som tillåtit inhämtningen i en brottsutredning. Eftersom det är oklart vilken information som kommer att bifogas en begäran bör dock enligt regeringens mening en begäran från andra medlemsstaters enheter och Europol behandlas på samma sätt som en begäran från svenska myndigheter utanför förundersökningsförfarandet. Detta innebär att oavsett om uppgifterna begärs ut för att användas i en förundersökning eller i underrättelseverksamhet så ska Polismyndigheten ge tillstånd till utlämnandet. Detsamma gäller när det kan bli aktuellt att lämna ut behörighetsbegränsade PNR-information i sin fullständiga form till ett tredjeland.[36]

När det inte har skett någon rättslig prövning innan begäran kommer in till enheten för passagerarinformation måste en sådan göras av en svensk myndighet för att uppfylla kravet enligt artikel 12.3 i PNR-direktivet. När det gäller underrättelseskedet bör prövningen, precis som vid en begäran från en svensk behörig myndighet, göras av åklagare. Så bör även kunna ske under pågående förundersökning. En svensk åklagare är inte involverad i förundersökningen i ett annat land och har alltså en neutral ställning gentemot parterna i ett sådant straffrättsligt förfarande. Det förefaller därför lämpligt att åklagare fattar beslut, oavsett om förundersökning pågår eller inte. För att

[35] Prop. 2017/18:234, *Lag om flygpassageraruppgifter i brottsbekämpningen*, s. 101.
[36] Prop. 2017/18:234, *Lag om flygpassageraruppgifter i brottsbekämpningen*, s. 105.

klargöra detta bör det i 4 kap. 11 § andra stycket lagen om flygpassagerarinformation förtydligas att beslut ska fattas av allmän domstol om en begäran sker under en pågående förundersökning enligt rättegångsbalken. På så sätt görs en avgränsning mot förundersökningar i andra länder. Att åklagare fattar beslut när det inte pågår en förundersökning följer redan av det tredje stycket.

När en rättslig prövning redan har genomförts i medlemsstaten från vilket begäran framställs kan det ifrågasättas om det bör göras ytterligare en prövning av en svensk myndighet. Enligt vår mening framstår det inte som lämpligt att myndigheter i olika länder överprövar varandras beslut. Det går inte heller att utläsa av PNR-direktivet eller PNR-domen att det skulle krävas sådana dubbla prövningar. Det bör därför införas en bestämmelse i 4 kap. med innebörden att vid en begäran från en behörig mottagare i en annan medlemsstat som har föregåtts av en rättslig prövning av tillgången till PNR-uppgifter ska det inte fattas något beslut enligt tredje stycket.

Överföring av PNR-information till en myndighet i ett tredjeland regleras i 4 kap. 7 § lagen om flygpassageraruppgifter i brottsbekämpningen. En sådan överföring får endast göras under förutsättning att överföringen omfattas av ett beslut om adekvat skyddsnivå, tillräckliga skyddsåtgärder eller ett undantag för särskilda situationer enligt 8 kap. 1 § första stycket 3 brottsdatalagen, att överföringen är nödvändig för att bekämpa terroristbrottslighet eller annan allvarlig brottslighet, och att tredjelandet har godtagit att uppgifterna får vidareföras till ett annat tredjeland endast om det är absolut nödvändigt för att bekämpa sådan brottslighet och efter det att ett uttryckligt medgivande till vidareöverföringen har inhämtats från enheten för passagerarinformation.

I 8 kap. 3–4 § brottsdatalagen anges bl.a. att personuppgifter får överföras till ett tredjeland om Europeiska kommissionen har beslutat att det finns en adekvat nivå för skyddet av personuppgifter i tredjelandet. Om det inte finns något sådant beslut får uppgifterna ändå överföras om skyddsåtgärder för personuppgifterna har fastställts i ett avtal som ger tillräckliga garantier för skydd för den registrerade eller om myndigheten som uppgifterna ska överföras till på annat sätt garanterar tillräckligt skydd för dem.

EU har slutit avtal om överföring och behandling av passageraruppgifter med ett flertal länder, bl.a. USA och Kanada. Det pågår även processer för att sluta avtal med fler länder, bl.a. Norge och Schweiz.

Ett avtal ska följa de EU-rättsliga bestämmelserna om behandling av personuppgifter och utgör ett sådant avtal som avses i 8 kap. 4 § 1 och som ger tillräckliga garantier till skydd för den registrerade. En begäran från ett sådant land bör därför kunna behandlas på samma sätt som en begäran från en behörig mottagare i en medlemsstat i frågan om en rättslig prövning ska genomföras i Sverige, dvs. att en sådan ska genomföras endast om det inte gjorts i landet från vilken begäran har inkommit.

Enheten för passagerarinformation hanterar i dagsläget inte begäranden från tredjeländer som saknar avtal med EU. Regleringen bör dock omfatta även eventuella sådana förfrågningar. Även om det i den begärande statens rättsordning finns reglerat en ordning för att pröva tillgången till PNR-uppgifter är det svårt att ur ett svenskt och EU-rättsligt perspektiv överblicka vad en sådan hypotetisk prövning innefattar. Det finns även en risk att den begärande statens rättsliga system inte uppfyller vissa grundläggande krav på rättssäkerhet. En begäran från ett tredjeland som saknar avtal med EU bör därför alltid föregås av en prövning av svensk åklagare.

8.5.8 Rättslig prövning vid avsaknad av efterfrågad PNR-information

Förslag

Vid en begäran om tillgång till PNR-information ska det endast ske en rättslig prövning av allmän domstol eller åklagare om den efterfrågade PNR-informationen finns hos enheten för passagerarinformation.

Det framgår inte av PNR-direktivet eller av den svenska lagstiftningen om tillgång till PNR-information ska ha medgetts av en domstol eller annan myndighet innan en sökning på den efterfrågade informationen får göras av enheten för passagerarinformation. Det finns dessutom olika uppfattningar om frågan bland EU:s medlemsstater. Så som PNR-systemet hittills har tillämpats har det inte varit en relevant fråga, eftersom PNR-uppgifter har samlats in från samtliga flygningar, både inom och utom EU. Det har krävts beslut om tillgång till uppgifter som är behörighetsbegränsade, vilket är enkelt att kon-

statera eftersom det sker efter sex månader. De begränsningar av PNR-systemet som vi föreslår kommer att innebära att en behörig mottagare eller tredjeland som begär information från enheten för passagerarinformation inte alltid vet om uppgifterna finns hos enheten.

För att kunna genomföra en välgrundad bedömning av om PNR-information ska lämnas ut bör prövningsinstansen ha tillgång till informationen. Det framstår dessutom som att det finns en stor risk för resursslöseri om en rättslig prövning ska genomföras även när det visar sig att det inte finns någon information att lämna ut. Mot bakgrund av detta bör det i 4 kap. anges att en prövning av allmän domstol eller åklagare endast ska ske om den efterfrågade PNR-informationen finns hos enheten för passagerarinformation. Av detta följer att enheten måste genomföra en manuell analys och validering av eventuellt rätt information för att kunna konstatera att informationen finns hos enheten innan begäran underställs rätt prövningsinstans.

8.5.9 Särskilt om brådskande fall

Förslag

Vid fara i dröjsmål ska enheten för passagerarinformation medge tillgång till PNR-information för behöriga mottagare utan föregående förhandskontroll. Detsamma ska gälla för en begäran från ett tredjeland som har slutit avtal med EU om överföring och behandling av passageraruppgifter.

Om sådan tillgång har medgetts ska enheten för passagerarinformation underställa begäran till prövningsinstansen utan onödigt dröjsmål och senast inom 24 timmar.

Om den behöriga myndigheten inte längre har skäl för behandlingen av PNR-informationen ska behandlingen omedelbart upphöra. Om förhandskontrollen innebär att begäran om tillgång till PNR-information nekas ska behandlingen av uppgifterna omedelbart upphöra.

När det gäller brådskande fall finns det ingen särskild reglering, vare sig i PNR-direktivet eller i lagen om flygpassageraruppgifter i brottsbekämpningen. I PNR-domen anges att utlämnande av PNR-information för en bedömning i efterhand i princip, *utom i vederbörligen motiverade brådskande fall*, ska föregås av en förhandskontroll utförd antingen av domstol eller av en oberoende förvaltningsmyndighet. Därefter anges att i vederbörligen motiverade brådskande fall ska kontrollen genomföras utan dröjsmål. Det är inte helt tydligt hur dessa uttalanden ska tolkas.

EU-domstolen hänvisar i samma punkt till domstolens yttrande angående PNR-avtalet mellan EU och Kanada.[37] I yttrandet anger domstolen att det är väsentligt att användningen av lagrade PNR-uppgifter under flygpassagerarnas vistelse i Kanada i princip, utom i vederbörligen motiverade brådskande fall, är underkastad förhandskontroll av en domstol eller en oberoende myndighet. Detta anges i flera punkter i domen och det nämns inte att någon förhandskontroll måste ske utan dröjsmål.

I PNR-domen hänvisas vidare till EU-domstolens dom i målet *Commissioner of An Garda Síochána m.fl.*[38] Målet rörde tillämpningen av direktivet om integritet och elektronisk kommunikation.[39] En fråga i målet berörde tillgången till lagrade uppgifter som polisen inkommit med inom ramen för en utredning. Även på detta område är tillgången till lagrade uppgifter underkastad en förhandskontroll av en domstol eller av en oberoende myndighet som fattar beslut efter att en myndighet har framställt en motiverad begäran om tillgång. En sådan förhandskontroll ska ske innan tillgång ges till de berörda uppgifterna, utom i vederbörligen motiverade brådskande fall. I sådana fall ska kontrollen genomföras utan dröjsmål. En sådan senare kontroll uppnår nämligen inte det mål som eftersträvas med en förhandskontroll, det vill säga att tillgång till de aktuella uppgifterna beviljas utöver vad som är strängt nödvändigt. En efterhandskontroll kan inte ersätta kravet på en oberoende och, förutom i vederbörligen motiverade brådskande fall, på förhand utförd prövning.

[37] EU-domstolens yttrande 1/15 *Förslag till avtal mellan Kanada och Europeiska unionen*, den 26 juli 2017, se särskilt p. 202 och 208.
[38] EU-domstolens dom den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, mål nr C-140/20, se särskilt p. 102, 106 och 110.
[39] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation.

Liknande resonemang lades även fram i målet *Prokuratuur*[40] vid EU-domstolen. En fråga i målet rörde om det finns hinder mot nationell lagstiftning som ger Åklagarmyndigheten behörighet att ge offentliga myndigheter tillgång till trafik- och lokaliseringsuppgifter inom ramen för en brottsutredning. Domstolen anger att det är väsentliga att behöriga nationella myndigheters tillgång till de lagrade uppgifterna är underkastad förhandskontroll av en domstol eller oberoende myndighet, och att domstolen meddelar sitt avgörande eller myndigheten antar sitt beslut till följd av att dessa myndigheter har framställt en motiverad begäran inom ramen för exempelvis ett förfarande för förebyggande, avslöjande eller lagföring av brott. I vederbörligen motiverade fall som ställer krav på skyndsamhet ska denna kontroll ske utan dröjsmål.

Domstolen uttalar sig vidare i frågan om avsaknaden av en oberoende myndighets kontroll kan avhjälpas genom att en domstol utför en senare kontroll av lagligheten av en nationell myndighets tillgång till trafik- och lokaliseringsuppgifter. Den oberoende kontrollen ska emellertid ske innan tillgång till uppgifterna beviljas, förutom i vederbörligen motiverade fall då denna kontroll ska ske utan dröjsmål. En senare kontroll kan inte uppnå det mål som eftersträvas med en förhandskontroll, det vill säga förhindra att det beviljas tillgång till de aktuella uppgifterna utöver vad som är strikt nödvändigt.

Även om det i EU-domstolens praxis anges att en senare kontroll inte kan uppnå det mål som eftersträvas med en förhandskontroll framgår det emellertid genomgående att en kontroll ska göras innan tillgång till uppgifter beviljas, förutom i vederbörligen motiverade brådskande fall. För att ytterligare utröna EU:s uppfattning i frågan kan en parallell dras till AI-förordningen[41] som trädde i kraft den 1 augusti 2024. Syftet med förordningen är att förbättra den inre marknadens funktion och främja användningen av artificiell intelligens, AI, samtidigt som en hög skyddsnivå säkerställs för hälsa, säkerhet och grundläggande rättigheter. I förordningen regleras bl.a. användning av biometrisk fjärridentifiering för brottsbekämpande ändamål. För att det ska vara tillåtet krävs enligt artikel 5.3 i förord-

[40] EU-domstolens dom den 2 mars 2021, *Prokuratuur,* mål nr C-746/18, p. 51 och 58.
[41] Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 3000/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

ningen ett förhandstillstånd från en rättslig myndighet eller en oberoende administrativ myndighet vars beslut är bindande i den medlemsstat där användningen ska äga rum. Ett sådant tillstånd ska utfärdas efter en motiverad begäran. I vederbörligen motiverade brådskande situationer får dock användningen av ett sådant system påbörjas utan tillstånd, förutsatt att ett sådant tillstånd begärs utan oskäligt dröjsmål och senast inom 24 timmar. Om ett sådant tillstånd nekas ska användningen stoppas med omedelbar verkan och alla uppgifter samt resultat och utdata som rör denna användning förstöras och raderas.

I AI-förordningen är det således tydligt att i brådskande fall får användning av tekniken inledas innan ett förhandstillstånd har meddelats. Förordningen trädde i kraft under 2024, dvs. efter EU-domstolens uttalanden i de ovan redovisade målen. Enligt vår uppfattning talar detta för att EU-domstolens uttalanden kan tolkas som att, i vederbörligen motiverade brådskande fall, får tillgång till information medges innan en prövning har kunnat genomföras av prövningsinstansen.

Användningen av PNR-information är inte sällan tidskänslig. Det kan handla om att snabbt lokalisera en misstänkt gärningsperson som är i färd med att begå ytterligare brott eller är på väg att lämna landet. Ungefär en fjärdedel av de begäranden om tillgång som kommer in till enheten för passagerarinformation sker utanför normal kontorstid. Det finns således ett behov av att, i vissa fall, få tillgång till PNR-information innan en förhandskontroll har kunnat genomföras. Sådan behandling av PNR-information ska begränsas till situationer där ändamålet med användningen riskerar att gå förlorad om den brottsbekämpande myndigheten avvaktar förhandskontrollen. Ju mer angeläget det är att lokalisera den aktuella personen, desto större bör utrymmet vara att få tillgång till PNR-information utan tillstånd.

Inom PNR-systemet framställer de behöriga myndigheterna en begäran om tillgång till PNR-information till enheten för passagerarinformation. I brådskande fall kommer således enheten för passagerarinformation att medge tillgång till PNR-uppgifter innan förhandskontrollen. Om sådan tillgång har medgetts ska en begäran om tillstånd översändas till prövningsinstansen utan onödigt dröjsmål. En frist om 24 timmar, så som anges i AI-förordningen, framstår som lämplig. Om begäran om tillgång till PNR-information nekas av prövningsinstansen ska behandlingen av uppgifterna upphöra med omedelbar verkan. Behandlingen ska också upphöra innan förhands-

kontrollen är genomförd om det inte längre finns skäl för behandlingen. Det är enheten för passagerarinformation som ansvarar för att en begäran om tillgång till PNR-information underställs rätt prövningsinstans.

Vid en begäran om tillgång till PNR-information i brådskande fall har enheten för passagerarinformation således till uppgift att bedöma om syftet med begäran är att behandla uppgifterna i enlighet med något av de tillåtna ändamålen i enlighet med 1 kap. 5 § lagen om flygpassageraruppgifter i brottsbekämpningen, dvs. att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet. Enheten ska dessutom bedöma om tillgången till uppgifterna utan föregående förhandskontroll är motiverad.

Det är sannolikt att en betydande andel av de aktuella ärendena kommer att kräva tillgång till PNR-information innan en förhandskontroll har kunnat genomföras av en rättslig instans. Det kan argumenteras för att det integritetsskydd som en förhandskontroll innebär riskerar att delvis förlora sin funktion till följd av detta. Tillgången till PNR-information ska emellertid fortfarande prövas av åklagare eller domstol, om än i efterhand. Om förhandskontrollen resulterar i att tillgång nekas ska dessutom PNR-informationen omedelbart raderas av den behöriga myndighet som medgetts tillgång till dem. Detsamma gäller om den behöriga myndigheten bedömer att det inte längre finns skäl att behandla uppgifterna. De negativa effekterna för skyddet för den personliga integriteten bör därför bli godtagbar.

Med hänsyn till vikten av att brottsbekämpande myndigheter, när det är motiverat, skyndsamt får tillgång till PNR-information anser vi att fördelarna med en sådan reglering väger tyngre än effekterna för enskildas personliga integritet och skyddet för personuppgifter. Det ligger även i linje med våra direktiv där det anges att brottsbekämpande myndigheters tillgång till flygpassageraruppgifter ska upprätthållas i möjligaste mån. Vårt förslag är således att tillgång till PNR-information i efterhand i brådskande fall får medges utan föregående förhandskontroll. Sådan tillgång får endast medges om ändamålet med användningen riskerar att gå förlorad om den brottsbekämpande myndigheten avvaktar förhandskontrollen. Den behöriga myndigheten ska i begäran om tillgång till PNR-information motivera varför tillgång ska medges innan en förhandsprövning har genomförts.

Samma reglering bör gälla för begäranden från behöriga mottagare i andra medlemsstater och från tredjeländer som har slutit avtal med EU om överföring och behandling av passageraruppgifter. I de fall där tillstånd nekas av åklagare har ett sådant beslut emellertid inte bindande verkan för en myndighet utanför Sveriges gränser. Det finns således inte någon möjlighet för svenska myndigheter att se till eller kontrollera att behandlingen avslutas omedelbart. Det kan därmed ifrågasättas om det är meningsfullt att genomföra en sådan prövning. För att uppfylla de krav som EU-rätten ställer måste dock en sådan prövning genomföras. Även om svenska myndigheter inte kan kontrollera verkställigheten av beslutet kan den behöriga mottagaren eller tredjelandet informeras om beslutet som åklagaren har fattat.

I avsnitt 8.5.7 har vi behandlat möjligheten att medge tillgång till PNR-information till tredjeländer som inte har slutit avtal med EU och föreslagit att sådan tillgång aldrig kan medges utan föregående prövning av svensk åklagare. Med samma resonemang som förs fram där kan sådan tillgång inte heller i brådskande fall medges utan föregående prövning.

Användningen av begreppet *vederbörligen motiverade brådskande fall* har behandlats i propositionen om polisens användning av AI för ansiktsigenkänning i realtid. Regeringen anför att begreppet är ovanligt i svensk författning och det föreslås i stället att begreppet *fara i dröjsmål* ska användas.[42] Fara i dröjsmål används i rättegångsbalken, t.ex. i 27 kap. 19 c §. För att undvika begreppsförvirring och behålla enhetlighet bör fara i dröjsmål användas även i lagen om flygpassageraruppgifter i brottsbekämpningen.

8.6 Jämförelse med relevanta databaser

Förslag

Vid en förhandsbedömning får PNR-uppgifter jämföras med en uppgiftssamling över personer eller föremål som är eftersökta eller finns uppförda på en spärrlista samt med register eller andra uppgiftssamlingar som är relevanta för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet.

[42] Prop. 2025 /26:150, *Polisens användning av AI för ansiktsigenkänning i realtid*, s. 79.

Med relevanta register och uppgiftssamlingar avses sådana som förvaltas av de behöriga myndigheterna eller, när det gäller EU-databaser och internationella databaser, används av de behöriga myndigheterna för de angivna syftena.

En jämförelse får endast göras om registrets eller uppgiftssamlingens innehåll och syfte har ett objektivt samband med terroristbrottslighet eller annan allvarlig brottslighet som har ett direkt eller indirekt samband med transport av flygpassagerare.

Av 3 kap. 4 § 1 lagen om flygpassageraruppgifter i brottsbekämpningen framgår bl.a. att enheten för passagerarinformation får behandla PNR-uppgifter som har överförts från ett lufttrafikföretag för att göra en förhandsbedömning av passagerare före deras beräknade ankomst till eller avresa från Sverige i syfte att välja ut personer som behöver utredas ytterligare av behöriga myndigheter eller Europol, på grund av att dessa personer kan vara inblandade i terroristbrottslighet eller annan allvarlig brottslighet. I 3 kap. 5 § anges att vid en förhandsbedömning får PNR-uppgifter jämföras med register eller andra uppgiftssamlingar som är relevanta för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet och behandlas enligt på förhand utformade och fastställda kriterier som är riktade, proportionella och avgränsade och som inte grundas på känsliga personuppgifter. Den svenska regleringen avseende jämförelse med relevanta databaser genomför artikel 6.3 a i PNR-direktivet.

I förarbetena[43] till den svenska regleringen konstaterades att direktivet inte anger vilka databaser eller register som får användas vid förhandsbedömningen, men att det innehåller en generell begränsning av vilka typer av uppgiftssamlingar som PNR-uppgifterna kan jämföras med. Medlemsstaterna får dock själva bestämma vilka uppgiftssamlingar som ska användas. Vid tiden för lagstiftningen stod det inte heller klart vilka register eller uppgiftssamlingar som PNR-uppgifterna kommer att jämföras med vid enheten för passagerarinformation.

Det konstateras vidare att vissa uppgiftssamlingar som kan bli aktuella för jämförelser kan innehålla uppgifter om personer som inte faller inom direktivets tillämpningsområde eftersom de t.ex. är misstänkta för annat slags eller lindrigare brottslighet. En automatisk

[43] SOU 2017:57, *Lag om flygpassageraruppgifter i brottsbekämpningen*, s. 231–232.

sökning i dessa uppgiftssamlingar skulle kunna innebära att PNR-uppgifter leder till träffar avseende sådan brottslighet som inte omfattas av direktivet. Dock kan en träff avseende exempelvis ett lindrigare brott, en person som är försvunnen eller ett dokument som är stulet, leda till andra antaganden och annan information, som i sin tur leder till misstanke om inblandning i grov brottslighet eller terroristbrottslighet. Sökningarna i de olika databaserna bör därför inte begränsas till att omfatta endast sådana brott som avses i direktivet.

I PNR-domen tydliggörs hur artikel 6.3 a i direktivet ska tolkas. Artikeln skulle kunna tolkas så att PNR-uppgifterna kan användas som sökkriterier för att göra analyser utifrån olika databaser, inbegripet databaser som medlemsstaternas säkerhets- och underrättelsemyndigheter förvaltar och använder i syfte att uppnå andra mål än dem som avses i direktivet, och att sådana analyser kan ske i form av utvinning av data. Möjligheten att utföra sådana analyser och att jämföra PNR-uppgifter med sådana databaser skulle kunna ge flygpassagerarna en känsla av att deras privatliv är föremål för en form av övervakning. En sådan tolkning av artikeln kan enligt EU-domstolen dock inte godtas eftersom det skulle kunna medföra ett oproportionerligt utnyttjande av dessa uppgifter som skulle göra det möjligt att fastställa en exakt profil av de berörda personerna enbart till följd av att de avser att resa med flyg.

Databaserna som används i enlighet med artikeln ska förvaltas av de behöriga myndigheterna eller, när det gäller EU-databaser och internationella databaser, användas av dessa myndigheter inom ramen för deras uppdrag att bekämpa terroristbrott och annan grov brottslighet. För att uppfylla kravet på att de på förhand fastställda kriterierna ska vara riktade, proportionella och specifika ska databaserna dessutom användas i samband med bekämpningen av sådana brott som har ett åtminstone indirekt objektivt samband med lufttransport av passagerare. Hänvisningen i artikel 6.3 a i direktivet till databaser som är relevanta kan inte tolkas på ett tillräckligt klart och precist sätt avseende vilka databaser som avses. Däremot förhåller det sig annorlunda med hänvisningen till databaser över personer eller föremål som är eftersökta eller finns uppförda på spärrlista, i enlighet med unionsbestämmelser eller internationella eller nationella bestämmelser som är tillämpliga på sådana databaser. De sistnämnda databaserna är därför de enda databaser som enheten för passagerarinformation får jämföra PNR-uppgifter mot.

Mot bakgrund av uttalandena i PNR-domen behöver svensk rätt förtydligas. Bestämmelsen i 3 kap. 5 § lagen om flygpassageraruppgifter i brottsbekämpningen är baserad på artikel 6.3 a i direktivet och kan enligt PNR-domen inte tolkas på ett tillräckligt klart och precist sätt. Uttalandet om att de i artikel 6.3 i direktivet uppräknade databaserna är de enda databaser som PNR-uppgifter får jämföras mot ska inte tolkas som att samtliga andra databaser utesluts. För att en databas ska få användas inom PNR-systemet måste den dock uppfylla kraven på tydlighet som ställs i PNR-domen. Kraven som ställs på en databas måste således förtydligas i svensk rätt. Enligt vår uppfattning är de krav som PNR-domen ställer på en relevant databas följande.

1. Hänvisningen till databaser ska kunna tolkas på ett tillräckligt klart och precist sätt när det gäller vilka databaser som avses.
2. Databaserna ska vara icke-diskriminerande, vilket innebär att uppgifter om personer som eftersöks eller som finns uppförda på en spärrlista bara får föras in i databaserna enligt objektiva och icke-diskriminerande kriterier som definieras i unionsbestämmelser eller nationella eller internationella bestämmelser som är tillämpliga på sådana databaser.
3. Databaserna ska användas i samband med bekämpningen av terroristbrott och grov brottslighet som har ett åtminstone indirekt objektivt samband med lufttransport av passagerare.
4. Databaserna ska förvaltas av de behöriga myndigheterna eller, när det gäller EU-databaser och internationella databaser, användas av dessa myndigheter inom ramen för deras uppdrag att bekämpa terroristbrottslighet och annan grov brottslighet.

Enligt vår mening kan punkterna 3 och 4 genomföras genom tillägg i 3 kap. 5 § lagen om flygpassagerarinformation i brottsbekämpningen. Bestämmelsens första stycke ska kompletteras med att PNR-uppgifter vid en förhandsbedömning får jämföras med register eller andra uppgiftssamlingar över personer eller föremål som är eftersökta eller finns uppförda på en spärrlista.

För att den befintliga bestämmelsen i första stycket ska vara förenlig med PNR-domens uttalanden bör det införas förtydliganden av vad som avses med relevanta register och uppgiftssamlingar. Sådana

register och uppgiftssamlingar ska förvaltas av de behöriga myndigheterna. När det gäller EU-databaser och internationella databaser ska de användas av de behöriga myndigheterna för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet.

Ett register eller en uppgiftssamling ska användas i samband med bekämpningen av terroristbrottslighet eller annan allvarlig brottslighet som har ett åtminstone indirekt objektivt samband med transport av flygpassagerare. Det EU-rättsliga kravet på ändamålsbegränsning innebär att det måste finnas ett angivet och berättigat ändamål för behandling av personuppgifter. Det sägs emellertid inte i PNR-domen att det uttryckligen måste framgå att ändamålet med behandlingen av uppgifterna i databasen är att bekämpa sådan brottslighet eller att databasen endast får användas mot sådan brottslighet. Det är generellt sett inte lämpligt att i författning peka ut vilka databaser som används i samband med bekämpning av de aktuella brottstyperna eftersom detta kan förändras över tid. Som exempel på databaser som är stabila över tid kan dock nämnas Schengen Information System, SIS, och Nationellt efterlysta personer och U-boken, Nepu. Bedömningen av om en databas används för att bekämpa terroristbrottslighet och annan allvarlig brottslighet bör således göras i varje enskilt fall. Redan med dagens lagstiftning krävs det att en databas ska vara relevant för den aktuella brottsbekämpningen. En sådan relevant databas är t.ex. Tullverkets underrättelseregister. Förtydligandet av vad som avses med relevanta register eller andra uppgiftssamlingar bör därmed inte medföra några större förändringar i tillämpningen.

Genom förtydligandet kan hänvisningen till databaser tolkas på ett tillräckligt klart och precist sätt och regleringen ligger därmed i linje med EU-domstolens uttalanden. Vilka faktiska databaser som används i tillämpningen av PNR-systemet kommer även fortsättningsvis bestämmas av enheten för passagerarinformation i samråd med de behöriga myndigheterna. I lagen om flygpassageraruppgifter används begreppen register eller annan uppgiftssamling i stället för databaser, vilket är det begrepp som används i PNR-domen. För att undvika begreppsförvirring förespråkar vi att den svenska regleringen behåller begreppen register eller annan uppgiftssamling.

När det gäller punkt 2 har det i svensk rätt inte införts en motsvarighet till vad som anges PNR-direktivets artikel 6.4 beträffande att en förhandsbedömning ska utföras på ett icke-diskriminerande

sätt. Det finns emellertid inga indikationer på att de databaser som används vid förhandsbedömningen inte uppfyller kravet på icke-diskriminering som ställs upp i direktivet och förtydligas i PNR-domen. Det följer även av 1 kap. 9 § regeringsformen att en myndighet inte ska utföra sitt arbete på ett diskriminerande sätt. Det saknas därför anledning att särskilt ange detta kriterium i lagen om flygpassageraruppgifter i brottsbekämpningen.

8.7 Lagringstid

Förslag

Huvudregeln ska vara att PNR-uppgifter som behandlas vid enheten för passagerarinformation bevaras i sin fullständiga form i sex månader från att de kommit in från ett lufttrafikföretag. Därefter ska de anonymiseras.

Undantag från huvudregeln får göras om det finns någon omständighet som visar att det föreligger en risk för terroristbrott eller annan allvarlig brottslighet som har ett direkt eller indirekt samband med en passagerares flygresor. I sådana fall ska PNR-uppgifterna från sådana flygresor behörighetsbegränsas efter sex månader.

Samtliga uppgifter ska förstöras fem år från att de kommit in från ett lufttrafikföretag.

Bedömning

Under utredningen har ett annat möjligt alternativ för bedömningen av lagringstiden diskuterats. Huvudregeln ska även här vara att PNR-uppgifter bevaras i sin fullständiga form i sex månader. I likhet med förslaget ovan ska undantag göras om det finns någon omständighet som visar att det föreligger en risk för terroristbrott eller allvarlig brottslighet som har ett direkt eller indirekt samband med en passagerares flygresor. Utöver detta ska dessutom samtliga PNR-uppgifter efter sex månader behörighetsbegränsas i stället för att anonymiseras om det anses föreligga ett verkligt och aktuellt eller förutsebart terrorhot mot Sverige. Enligt våra förslag i avsnitt 8.2.2 får Säkerhetspolisen fatta beslut om

att PNR-uppgifter från samtliga flygningar inom EU får samlas in vid ett sådant terrorhot. De behörighetsbegränsade PNR-uppgifterna ska då få lagras hos enheten för passagerarinformation i upp till fem år. I ett särskilt yttrande lägger experter från Polismyndigheten, enheten för passagerarinformation, Säkerhetspolisen, Försvarsmakten, Tullverket samt Ekobrottsmyndigheten fram ett alternativt förslag i linje med denna bedömning.

I artikel 12 i PNR-direktivet anges att PNR-uppgifter som lämnas av lufttrafikföretag ska lagras i en databas vid enheten för passagerarinformation under en period om fem år efter överföringen till enheten. Efter sex månader ska alla PNR-uppgifter avidentifieras genom maskering av vissa uppgifter. I svensk rätt finns motsvarande bestämmelser i 3 kap. 9 och 11 §§ lagen om flygpassageraruppgifter i brottsbekämpningen.

I PNR-domen uppställs vissa begränsningar av den generella lagringstiden om fem år. Lagring av samtliga PNR-uppgifter under de inledande sex månaderna går inte utöver vad som är strikt nödvändigt. För den efterföljande perioden upp till fem år finns det emellertid enligt EU-domstolen inneboende risker för oproportionerlig användning och missbruk, till följd av den stora mängd uppgifter som kan lagras kontinuerligt.

För de passagerare för vilka varken förhandsbedömningen enligt artikel 6.2 a i PNR-direktivet, eventuella kontroller som utförts under de inledande sex månaderna, eller någon annan omständighet har visat att det föreligger objektiva omständigheter som visar att det föreligger en risk för terroristbrott eller annan grov brottslighet, tycks det inte föreligga något samband mellan PNR-uppgifterna och målet med direktivet som motiverar att dessa uppgifter lagras. Att kontinuerligt lagra PNR-uppgifter för samtliga passagerare efter den inledande sexmånadersperioden förefaller således inte vara begränsat till vad som är strikt nödvändigt. PNR-direktivet och EU-stadgan utgör alltså hinder för nationell lagstiftning som föreskriver en generell lagringstid på fem år för PNR-uppgifter, om lagringstiden tillämpas utan åtskillnad på alla flygpassagerare.

Det står klart att den svenska regleringen i detta avseende inte är förenlig med uttalandena som EU-domstolen gör i PNR-domen. En generell lagringstid om fem år för PNR-uppgifter står i strid med

artikel 12.1 i PNR-direktivet jämförd med artikel 7, 8 och 52.1 i EU-stadgan.

För att den svenska lagstiftningen inte ska stå i strid med EU-rätten måste den stipulerade lagringstiden modifieras. För flygpassagerare som inte har flaggats vare sig i den inledande förhandsbedömningen enligt artikel 6.2 a i PNR-direktivet eller i eventuella kontroller som utförts under de inledande sex månaderna ska PNR-uppgifterna anonymiseras efter sex månader. Om det föreligger någon objektiv omständighet som innebär att det finns en risk för terroristbrott eller annan grov brottslighet som har ett direkt eller indirekt samband med en passagerares flygresa ska uppgifterna fortsatt lagras hos enheten för passagerarinformation i upp till fem år och behörighetsbegränsas enligt 3 kap. 11 § lagen om flygpassagerarinformation i brottsbekämpningen. Om det bedöms att det finns ett samband mellan en viss passagerares flygresa och en risk för brottslighet bör detta innebära att det finns ett, åtminstone indirekt, samband även för övriga passagerare på samma flygning. Det är av vikt för den fortsatta analysen att undersöka eventuella kopplingar mellan den identifierade personer och övriga resenärer på flyget. PNR-uppgifterna för samtliga resenärer på en sådan flygning får således undantas från anonymisering och i stället behörighetsbegränsas efter sex månader. Sådana uppgifter får således bevaras hos enheten för passagerarinformation i upp till fem år. Detta innebär att 3 kap. 11 § behöver modifieras på så sätt att det framgår att PNR-uppgifterna ska behörighetsbegränsas efter sex månader, under förutsättning att de inte ska anonymiseras enligt 3 kap. 9 §.

I avsnitt 8.8 lägger vi fram våra resonemang som ligger till grund för bedömningen att uppgifterna ska anonymiseras i stället för att raderas.

Den föreslagna regleringen innebär ett större skydd för personuppgifter som översänds till enheten för passagerarinformation. Personer som inte har något samröre med terrorism eller grov brottslighet kommer inte längre ha sina personuppgifter lagrade hos enheten för passagerarinformation under hela femårsperioden. För personer som reser regelbundet kan detta innebära att personuppgifterna lagras under kortare tidsperioder i stället för att lagras kontinuerligt utan avbrott.

Det är inte ovanligt att personer uppmärksammas av brottsbekämpande myndigheter först efter att den inledande sexmånadersperioden

har löpt ut. Utredningsarbete avseende exempelvis terroristbrott tar tid och kopplingar mellan personer ådagaläggs inte alltid omedelbart efter en flygresa eller under de nästkommande sex månaderna. Genom att anonymisera PNR-uppgifter på det sätt som föreslås kommer möjligheterna att utreda begångna brott och förhindra planerade brott att kraftigt försämras. Det kommer även att innebära svårigheter för myndigheterna att kartlägga terroristverksamhet och kriminella nätverk. För att svensk rätt ska vara förenlig med EU-rätten måste dock en sådan begränsning av lagringstiden införas.

Under utredningen har en alternativ tolkning av EU-domstolens uttalanden om lagringstiden förts fram av experter från de behöriga myndigheterna och enheten för passagerarinformation. Tolkningen, som framgår i det särskilda yttrande som fogats till betänkande, innebär att en generell och odifferentierad lagringstid i mer än sex månader kan motiveras av en verklig, aktuell och förutsägbar risk för att Sverige utsätts för terrorbrott och annan allvarlig brottslighet. Ett sådant hot kan utgöra en sådan annan omständighet som, utöver vad som kommer fram under förhandskontrollen eller andra eventuella kontroller som utförts under den inledande sexmånadersperioden, visar att det föreligger en risk för terroristbrott eller annan allvarlig brottslighet.

En sådan tolkning kan under vissa förutsättningar innebära att PNR-uppgifter får lagras betydligt längre än de föreslagna sex månaderna. Ur ett brottsbekämpande perspektiv vore det en påtaglig fördel att kunna behandla uppgifterna under längre tid.

8.7.1 Lagring av resultatet av behandling av PNR-uppgifter

Bedömning

Resultat från en förhandsbedömning ska få bevaras så länge de bakomliggande PNR-uppgifterna inte har raderats eller anonymiserats. Denna tolkning ryms inom nuvarande utformning av bestämmelsen i förordningen om passageraruppgifter och det krävs därför ingen författningsändring.

I 9 § lagen om flygpassageraruppgifter i brottsbekämpningen framgår att resultatet av en behandling av PNR-uppgifter inte får behandlas under längre tid än vad som behövs för att kunna informera behöriga mottagare om resultatet. Om resultatet inte behöver granskas vidare av en behörig mottagare får resultatet ändå behandlas om syftet är att fortsättningsvis undvika motsvarande felaktiga träffar. Behandlingen av resultatet ska dock upphöra senast i samband med att PNR-uppgifterna ska förstöras. Bestämmelsen genomför artikel 12.5 i PNR-direktivet.

I förarbetena diskuterades om bestämmelsen i direktivet skulle kunna tolkas som att en positiv träff från en förhandsbedömning bara får sparas tills den har sänts vidare till en eller flera behöriga myndigheter och eventuellt en enhet för passagerarinformation. Eftersom en behörig myndighet kan komma att återrapportera att även en annan behörig mottagare bör informeras om träffen bör dock en möjlighet finnas för enheten att behålla resultatet en viss tid efter att en träff har skickats till en behörig myndighet för vidare granskning. Artikeln bör därför tolkas på så sätt att ett resultat ska förstöras så snart det inte längre behövs för att informera myndigheter och eventuellt andra medlemsstater. Falska träffar bör däremot få bevaras som längst till dess att de bakomliggande PNR-uppgifterna har raderats.[44]

Resultatet av en behandling av PNR-uppgifter innehåller information om varför träffen är intressant. Sådan information behöver kunna delges till behöriga myndigheter samt finnas tillgänglig för dataskyddsombud som ska granska personuppgiftsbehandlingen vid enheten för passagerarinformation.

I artikel 12.5 i direktivet nämns inte tillgängligheten för dataskyddsombud som en grund för att spara de aktuella uppgifterna. Så som direktivet har genomförts och tillämpats hittills har detta inte heller haft samma betydelse som det har i och med förslagen om att lagringstiden begränsas såtillvida att det uppställs vissa krav för att få bevara PNR-uppgifter längre än sex månader. För att kunna bedöma om personuppgiftsbehandlingen är författningsenlig och korrekt bör dataskyddsombudet kunna ta del även av resultaten av en behandling av PNR-uppgifter.

Hur lång tid som behövs för att kunna informera behöriga mottagare om resultatet preciseras inte i 9 § i förordningen eller i PNR-direktivet. Information om en träff kan meddelas en behörig mottagare

[44] Prop. 2017/18:234, *Lag om flygpassageraruppgifter i brottsbekämpningen*, s. 77.

direkt efter att förhandsbedömningen har genomförts. Informationen kan även meddelas vid ett senare tillfälle, om det framkommer skäl att delge den med en viss behörig mottagare, t.ex. genom återrapportering från en behörig myndighet som meddelats om träffen. Enligt vår mening kan det finnas behov av att informera behöriga mottagare om resultatet av en behandling av PNR-uppgifter även bortom den tidpunkt som diskuteras i förarbetena. Sådant behov kan finnas så länge PNR-uppgifterna bevaras hos enheten för passagerarinformation. Regleringen för träffar bör således ligga i linje med regleringen för falska träffar, dvs. att resultat från en förhandsbedömning får bevaras så länge de bakomliggande PNR-uppgifterna inte har raderats eller anonymiserats. Först då upphör behovet av att kunna informera behöriga myndigheter om träffen. Detta är en tolkning som ryms inom nuvarande utformning av 9 § förordningen om passageraruppgifter och det krävs därför ingen författningsändring i det avseendet.

8.8 Radering eller anonymisering?

I tidigare avsnitt har vi föreslagit att PNR-uppgifter under vissa förutsättningar ska anonymiseras. Ett alternativ till detta hade varit att i stället radera uppgifterna.

Grunden för de begränsningar av tillämpningen av PNR-systemet som PNR-domen innebär är att behandlingen av personuppgifter riskerar att kränka de grundläggande rättigheterna som ställs upp i artikel 7 och 8 i EU-stadgan och som rör rätten till privat- och familjeliv och skydd för personuppgifter. En grundförutsättning för att en viss behandling ska kunna kränka någon av dessa rättigheter är att de uppgifter som behandlas på något sätt går att koppla till en viss person. Behandling av uppgifter som inte utgör personuppgifter kan inte innebära en inskränkning i de rättigheter som skyddas genom de nämnda bestämmelserna.

Med anonymisering avses en process som gör det nära nog omöjligt att identifiera en enskild person utifrån uppgifterna. Detta kan exempelvis ske genom att identifierande information som t.ex. namn eller personnummer raderas eller genom att individuella uppgifter aggregeras för att användas för statistiska ändamål. När uppgifter har anonymiserats utgör de inte längre personuppgifter. Till följd av detta är inte heller bestämmelser till skydd för personuppgifter

tillämpliga. Eftersom all koppling till en särskild individ har tagits bort går det inte heller att återupprätta kopplingen mellan de anonymiserade uppgifterna och individen. Anonymisering ska särskiljas från pseudonymisering, som innebär behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

Uppgifter som i sig inte är personuppgifter kan emellertid få karaktär av personuppgifter om den personuppgiftsansvarige gör dessa tillgängliga för andra personer som förfogar över medel som med rimlig sannolikhet skulle kunna göra det möjligt att identifiera den registrerade. Det gäller t.ex. om den som får tillgång till uppgifterna har lagliga möjligheter att från någon annan erhålla kompletterande information som gör det möjligt att identifiera en specifik person.[45] För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel, som t.ex. utgallring, som, antingen av den personuppgiftsansvarige eller av en annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att fastställa om hjälpmedel med rimlig sannolikhet kan komma att användas för att identifiera den fysiska personen bör man beakta samtliga objektiva faktorer, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten som den tekniska utvecklingen.[46]

För att anse att en faktisk anonymisering av PNR-uppgifter har skett måste det således göras en bedömning av enheten för passagerarinformation och de behöriga myndigheternas möjligheter att med hjälp av uppgifterna och de möjligheter som står myndigheterna till buds att återskapa kopplingen till en identifierbar fysisk person. En sådan bedömning är vansklig att göra i ett inledande skede av lagstiftningsprocessen. Med tanke på den tekniska utvecklingen samt potentiella förändringar av brottsbekämpande myndigheters rätt att ta del

[45] EU-domstolens dom den 4 september 2025, *Europeiska datatillsynsmannen mot Gemensamma resolutionsnämnden*, mål nr C-413/23 P.
[46] Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG, skäl 16.

av och behandla uppgifter bör anonymiseringen av PNR-uppgifter inte regleras i detalj i lagtext. Det bör räcka med att i lagtext ange att anonymisering ska ske under vissa förutsättningar. Tillämpningen överlåts till enheten för passagerarinformation som åläggs att genomföra anonymiseringen på det sätt som krävs för att uppnå kraven som ställs på en sådan process.

Med de anonymiserade uppgifterna i PNR-systemet kommer det inte gå att koppla en viss individ till en viss resa. Trots detta finns det ett värde i att behålla uppgifterna i anonymiserad form i databasen vid enheten för passagerarinformation. Med hjälp av uppgifterna går det fortfarande att analysera reseflöden och resmönster. Uppgifterna är även användbara i arbetet med att uppdatera eller skapa nya kriterier som ska användas vid förhandsbedömningen enligt 3 kap. 4 § 3 lagen om flygpassageraruppgifter i brottsbekämpningen.

Mot bakgrund av att anonymiserade uppgifter kan vara användbara för brottsbekämpningen samt att behandlingen av sådana uppgifter vid enheten för passagerarinformation inte riskerar att inskränka några grundläggande rättigheter anser vi att anonymisering av PNR-uppgifter är ett lämpligt alternativ i de situationer där uppgifter annars skulle raderas innan den maximala lagringstiden om fem år har löpt ut.

8.9 Tillåtna ändamål med behandling av PNR-uppgifter

Förslag

1 kap. 6 § andra stycket lagen om flygpassageraruppgifter i brottsbekämpningen som berör behandling av personuppgifter i verksamhet som rör nationell säkerhet ska upphävas.

I artikel 1.2 i PNR-direktivet anges att PNR-uppgifter som samlas in i enlighet med direktivet endast får behandlas i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet i enlighet med artikel 6.2 a, b och c. I lagen om flygpassageraruppgifter i brottsbekämpningen regleras detta i 1 kap. 5 §. I 6 § andra stycket samma kapitel anges vidare att enheten för passagerarinformation får behandla PNR-information när det är nödvändigt för att tillhandahålla uppgifter som behövs för sådan verksamhet.

I PNR-domen förtydligas det vilka ändamål för behandling av PNR-uppgifter som är tillåtna. EU-domstolen hänvisar till direktivets bestämmelse och anger att det framgår tydligt av ordalydelsen att uppräkningen av de mål som eftersträvas med behandlingen av PNR-uppgifter enligt PNR-direktivet är uttömmande. Detta får, enligt EU-domstolen, ytterligare stöd av skäl 11 i direktivet, enligt vilket behandlingen av PNR-uppgifter ska stå i proportion till de särskilda säkerhetsmål som direktivet syftar till att uppfylla och av artikel 7.4 enligt vilken PNR-uppgifter och resultatet av behandling av dessa endast får vidare behandlas om det specifika syftet är att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott eller grov brottslighet. Den uttömmande karaktären av de ändamål som avses i artikel 1.2 innebär dessutom att PNR-uppgifter inte får lagras i en enda databas som kan användas för andra ändamål eftersom det skulle innebära en risk för att uppgifterna används för andra ändamål än vad som avses i artikel 1.2.

I förarbetena till den svenska regleringen förs det fram argumentation till stöd för att införa bestämmelsen om att PNR-uppgifter får behandlas i verksamhet som rör nationell säkerhet.[47] Regeringen ansåg att eftersom nationell säkerhet faller utanför EU:s kompetens bör enheten för passagerarinformation ges ett stöd för att kunna lämna ut PNR-information som behövs för sådan verksamhet. Enheten för passagerarinformation ska därför få behandla PNR-information när det är nödvändigt för att tillhandahålla uppgifter som behövs i verksamhet som rör nationell säkerhet. Det kan t.ex. handla om att förebygga högmålsbrott och brott mot Sveriges säkerhet i 18 eller 19 kap. brottsbalken, som inte faller in under definitionen av terroristbrottslighet eller annan grov brottslighet och därmed inte faller in under lagens tillämpningsområde.

Det framgår således att syftet med bestämmelsen i 1 kap. 6 § andra stycket bl.a. är att behandla PNR-uppgifter för att bekämpa brott som inte omfattas av PNR-systemets tillämpningsområde.

Det kan konstateras att frågan om nationell säkerhet ligger utanför EU:s kompetens, dvs. den är varje enskild medlemsstats eget ansvar. Det råder inget tvivel om att medlemsstaterna står fria att lagstifta om insamling av passageraruppgifter för att använda dessa i verksamhet som rör nationell säkerhet, under förutsättning att en sådan reglering är förenlig med allmänna rättsgrundsatser, internationella

[47] Prop. 2007/18:234, *Lag om flygpassageraruppgifter i brottsbekämpningen*, s. 44.

konventioner och övrig nationell rätt. I förevarande fall rör det dock behandling av PNR-uppgifter – uppgifter som har samlats in i enlighet med EU:s PNR-direktiv. PNR-systemet är inrättat i enlighet med ett EU-direktiv och det ligger inte utanför EU:s kompetens att bestämma hur uppgifter som samlats in i enlighet med ett EU-direktiv får och inte får användas. EU-domstolen är också mycket tydlig i frågan; listan över tillåtna ändamål med behandling av PNR-uppgifter som anges i direktivet är uttömmande. Det är svårt att tolka uttalandena i PNR-domen som att de angivna ändamålen är uttömmande såvida det rör verksamhet inom EU:s kompetens, men att det står medlemsstaterna fritt att inom systemet behandla PNR-uppgifter för att tillhandahålla uppgifter till verksamhet som ligger utanför EU:s kompetens. Enligt vår bedömning är det, i verksamhet som rör nationell säkerhet, tillåtet för enheten för passagerarinformation att behandla PNR-uppgifter eller resultatet av behandling av sådana uppgifter genom att tillhandahålla dem endast om det sker för de ändamål som framgår av PNR-direktivet.

De behöriga myndigheter som bedriver verksamhet som rör nationell säkerhet är Säkerhetspolisen och Försvarsmakten. För dessa myndigheter innebär den föreslagna förändringen en begränsning av för vilka ändamål som PNR-uppgifter får lämnas ut från enheten för passagerarinformation. Detta kan få konsekvenser för Sveriges säkerhet. Det bör emellertid understrykas att PNR-uppgifter även fortsättningsvis kommer kunna lämnas ut till verksamhet som rör nationell säkerhet, så länge det sker inom ramen för de tillåtna ändamålen. Exempelvis är det således tillåtet att behandla PNR-uppgifter för att bekämpa terrorism och sabotage, vilka också är frågor som kan röra Sveriges nationella säkerhet.

9 Trafikslagsneutral PNR-lagstiftning

Den alltmer komplexa hotbilden mot Sverige och Europa ställer högre krav på de brottsbekämpande myndigheternas förmåga att förutse och förhindra terrorism och annan allvarlig brottslighet. En central del i detta arbete är användningen av passageraruppgifter. Vårt uppdrag i denna del är att överväga om PNR-lagstiftningen, som i dagsläget endast omfattar flygtrafik, även bör omfatta andra trafikslag. Syftet med ett sådant system är att ge brottsbekämpande myndigheter motsvarande möjligheter att samla in uppgifter från t.ex. tåg, bussar och färjor. Skillnaderna mellan de olika trafikslagen har lett till svårigheter för brottsbekämpande myndigheter att kartlägga resvägen för kriminella som väljer att använda sig av flera olika transportmedel på vägen till eller från Sverige.

Det finns ett flertal olika parametrar att förhålla sig till när det gäller införandet av en trafikslagsneutral PNR-lagstiftning. Insamling av större mängder information kan utgöra ingrepp i de grundläggande rättigheter som fastställs i t.ex. EU:s rättighetsstadga. Avvägningar måste göras mellan syftet med lagstiftningen, dvs. att bekämpa terrorism och annan allvarlig brottslighet, och potentiella ingrepp i t.ex. rätten till respekt för sitt privatliv och rätten till skydd av personuppgifter.

Förändringar i lagstiftningen kan även ha påverkan på de transportbolag som omfattas. Om företagen åläggs ytterligare skyldigheter att tillhandahålla information till myndigheterna skulle det kunna leda till ökade kostnader för administration, samtidigt som ett enhetligt, automatiserat system också skulle kunna innebära att företagen får in färre begäranden om tillgång till passageraruppgifter med stöd av andra lagar, t.ex. polislagen och tullbefogenhetslagen. För att kunna bedöma lämpligheten av ett trafikslagsneutralt PNR-

system är det av vikt att analysera vad detta innebär för transportsektorn och i möjligaste mån inte påverka branschen negativt. Det framgår också av våra direktiv att fördelar med att ställa nya typer av krav på transportföretag inom fler trafikslag bör vägas mot nackdelar i form av minskad lönsamhet i berörda företag som i förlängningen kan innebära försämrad tillgänglighet på kommunikationer till och från Sverige.

Vi har vidare i uppdrag att se över den speciallagstiftning som gäller för brottsbekämpande myndigheter avseende möjligheten att begära in uppgifter från transportbolag. Detta innefattar dels att bedöma om dessa regleringar kan behållas för det fall att PNR-lagstiftningen görs trafikslagsneutral, dels att föreslå eventuella förändringar i lagstiftningen för att förbättra myndigheternas tillgång till uppgifter, oaktat om PNR-lagstiftningen görs trafikslagsneutral eller inte.

I de följande avsnitten analyseras förutsättningarna för en trafikslagsneutral PNR-lagstiftning övriga frågor som en sådan reglering aktualiserar samt frågor som rör brottsbekämpande myndigheters speciallagstiftning avseende användning av passageraruppgifter.

10 Pågående arbete inom EU

10.1 Etias

European Travel Information and Authorisation System, Etias, är ett initiativ från EU som syftar till att stärka de yttre gränserna och förbättra säkerheten inom Schengenområdet. Systemet föreslogs ursprungligen av Europeiska kommissionen 2016 och förordningen[1] antogs formellt 2018. Systemet börjar dock inte gälla förrän under det fjärde kvartalet 2026.

Systemet syftar till att identifiera personer som kan utgöra ett hot mot säkerheten, t.ex. kopplat till terrorism eller grov brottslighet, innan de anländer till EU:s yttre gränser. Detta sker genom att den sökandes uppgifter kontrolleras mot relevanta EU-databaser. Etias hjälper till att säkerställa att resenärer från visumfria länder följer reglerna för kortare vistelser och minskar risken för att personer stannar kvar illegalt. Vid behov kan systemet även användas för att flagga resenärer som kan utgöra en risk för epidemisk smitta.

10.1.1 Innehåll

Förordningen är tillämplig på tredjelandsmedborgare, under vissa förutsättningar som uppställs i artikel 2. I artikel 4 anges Etias syften, vilka bl.a. är att bidra till en hög säkerhet genom att göra en noggrann bedömning av säkerhetsrisker förknippade med sökande före deras ankomst till gränsövergångsställena vid de yttre gränserna i syfte att avgöra om det finns faktiska indikationer på, eller rimliga skäl på grundval av faktiska indikationer att anta, att personens vistelse

[1] Europaparlamentets och rådets förordning (EU) 2018/1240 av den 12 september 2018 om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias) och om ändring av förordningarna (EU) nr 1077/2011, (EU) nr 515/214, (EU) 2016/399, (EU) 2016/399, (EU) 2016/1624 och (EU) 2017/2226.

på medlemsstaternas territorium innebär en säkerhetsrisk. Systemet ska vidare bidra till att förebygga och förhindra illegal invandring, och skydda folkhälsan genom att göra en bedömning av om sökanden utgör en hög epidemirisk. Etias ska också öka in- och utresekontrollernas effektivitet, stödja syftet med *Schengen Information System,* SIS, avseende registreringar av tredjelandsmedborgare som har nekats inresa eller vistelse, samt bidra till att förebygga, förhindra, upptäcka och utreda terroristbrott eller andra grova brott.

Enligt artikel 5 ska Etias bestå av ett informationssystem, en centralenhet samt de nationella Etias-enheterna. Informationssystemet ska enligt artikel 6 utvecklas av eu-Lisa och ska uppfylla vissa i artikeln angivna krav. I artikel 7 anges att Etias centralenhet ska bedriva verksamhet dygnet runt alla dagar i veckan och att den bl.a. ska ansvara för att i de fall där den automatiserade behandlingen har gett en träff, kontrollera om sökandens personuppgifter motsvarar personuppgifterna för en person som gett upphov till träffen i Etias centrala system.

Varje medlemsstat ska enligt artikel 8 utse en behörig myndighet som ska fungera som den nationella Etias-enheten. Enheterna ansvarar bl.a. för att undersöka och besluta om ansökningar i resetillstånd i de fall där den automatiserade behandlingen har gett en träff och en manuell behandling av ansökan har inletts av Etias centralenhet. Sveriges nationella Etias-enhet kommer att vara Polismyndigheten.

I enlighet med artikel 9 inrättas Etias granskningsnämnd med en rådgivande funktion inom Europeiska gräns- och kustbevakningsbyrån och Europol. Granskningsnämnden ska höras av Etias centralenhet när det gäller definition, fastställande, förhandsbedömning, genomförande, efterhandsutvärdering, översyn och radering av de särskilda riskindikatorer som anges i artikel 33. Granskningsnämnden ska också höras av medlemsstaterna när det gäller tillämpningen av Etias bevakningslista och av Europol när det gäller tillämpningen av Etias bevakningslista i enlighet med artikel 34. Nämnden ska även utfärda yttranden, riktlinjer, rekommendationer och bästa metoder för de ändamål för vilka nämnden kan höras.

Enligt artikel 10 inrättas Etias rådgivningsråd för grundläggande rättigheter. Det är en oberoende nämnd med en rådgivande och utvärderande funktion. Nämnden ska bestå av Europeiska gräns- och kustbevakningsbyråns ombud för grundläggande rättigheter, en företrädare för Europeiska gräns- och kustbevakningsbyråns rådgivande

forum för grundläggande rättigheter, en företrädare för Europeiska datatillsynsmannen, en företrädare för Europeiska dataskyddsstyrelsen och en företrädare för Europeiska unionens byrå för grundläggande rättigheter.

Etias rådgivningsnämnd för grundläggande rättigheter ska genomföra regelbundna utvärderingar och utfärda rekommendationer till Etias granskningsnämnd om inverkan på de grundläggande rättigheterna av behandlingen av ansökningar och genomförandet av artikel 33, särskilt när det gäller rätten till privatliv, skydd av personuppgifter och icke-diskriminering. Nämnden ska också stödja Etias granskningsnämnd i utförandet av dess uppgifter när den senare samråder med rådgivningsnämnden i särskilda frågor som rör grundläggande rättigheter, särskilt när det gäller rätten till privatliv, skydd av personuppgifter och icke-diskriminering.

Enligt artikel 13 ska åtkomst till Etias informationssystem endast beviljas vederbörligen bemyndigad personal vid Etias centralenhet och de nationella Etias-enheterna. Gränsmyndigheters åtkomst till Etias centrala system ska begränsas till sökningar för att kontrollera om en resenär som befinner sig vid ett gränsövergångsställe vid de yttre gränserna har resetillstånd och till de uppgifter som avses i artikel 47.2 a, c och d. Därutöver ska gränsmyndigheterna automatiskt informeras om vissa flaggningar och om skälen till dessa flaggningar. Om en fördjupad kontroll vid gränsen rekommenderas enligt en flaggning eller om ytterligare kontroller krävs inom ramen för en fördjupad kontroll, ska gränsmyndigheterna får åtkomst till Etias centrala system för att kontrollera vissa ytterligare uppgifter.

Transportörers åtkomst till Etias informationssystem ska begränsas till sökningar för att kontrollera om en resenär har resetillstånd.

Invandringsmyndigheters åtkomst till det centrala informationssystemet ska begränsas till sökningar för att kontrollera om en resenär som befinner sig på medlemsstatens territorium har resetillstånd och till vissa ytterligare uppgifter.

Varje medlemsstat ska utse de behöriga nationella myndigheterna och ska utan dröjsmål överlämna en förteckning över dessa myndigheter till eu-Lisa.

Artikel 14 behandlar icke-diskriminering och grundläggande rättigheter. En användares behandling av personuppgifter i Etias informationssystem får inte leda till att tredjelandsmedborgare diskrimineras på grund av kön, ras, hudfärg, etniskt eller socialt ursprung,

genetiska särdrag, språk, religion eller övertygelse, politiska eller andra åsikter, tillhörighet till en nationell minoritet, förmögenhet, börd, funktionshinder, ålder eller sexuell läggning. Behandlingen ska fullt ut respektera mänsklig värdighet och integritet samt grundläggande rättigheter, inbegripet rätten till respekt för privatlivet och skydd av personuppgifter. Särskild hänsyn ska tas till barn, äldre och personer med funktionshinder. Barnets bästa ska sättas i främsta rummet.

Artikel 15 innehåller praktiska bestämmelser om inlämning av en ansökan. Den sökande ska lämna in ansökan genom att fylla i ett elektroniskt ansökningsformulär i tillräckligt god tid före den planerade resan eller, om de redan befinner sig på medlemsstaternas territorium, innan giltighetstiden för ett befintligt resetillstånd som de innehar löper ut. Enligt artikel 17 ska alla sökande lämna in ett ifyllt ansökningsformulär tillsammans med en försäkran om att de lämnade uppgifterna är riktiga, fullständiga, korrekta och tillförlitliga samt en förklaring om att de utsagor som gjorts är tillförlitliga och sanningsenliga. I artikeln anges vidare vilka personuppgifter som ska anges i ansökningsformuläret, t.ex. namn, eventuella andra medborgarskap och resehandlingens typ, nummer och utfärdandeland.

Sökanden ska även besvara frågor om brottslighet, om han eller hon har vistats i ett visst krigs- eller konfliktdrabbat område under de senaste tio åren och i så fall när och i vilket land, om han eller hon har varit föremål för ett beslut om att lämna en medlemsstats territorium under de senaste tio åren.

Enligt artikel 20 ska ansökningsakterna behandlas automatiskt av Etias centrala system för att kontrollera träffar. Det centrala systemet ska granska varje ansökningsakt individuellt. Uppgifterna ska jämföras med uppgifterna i ett register, en akt eller en registrering i Etias centrala system, SIS, in- och utresesystemet, VIS[2], Eurodac[3], Europoluppgifter och Interpols[4] databaser SLTD[5] samt TDAWN[6].

Artikel 21 anger att om den automatiserade behandlingen enligt artikel 20.2–20.5 inte ger någon träff ska Etias centrala system automatiskt utfärda ett resetillstånd i enlighet med artikel 36 och underrätta sökanden i enlighet med artikel 38. Om behandlingen gett en

[2] *Visa Information System*.
[3] *European Asylum Dactoscopy*.
[4] I den svenska översättningen av Etias-förordningen anges att det är Europols databaser, men i samtliga andra språkversioner framgår att det är det Interpols databaser som avses, vilket också är det korrekta.
[5] *Stolen and Lost Travel Documents database.*
[6] *Travel Documents Associated with Notices database.*

eller flera träffar ska ansökan bedömas i enlighet med förfarandet i artikel 22. Om kontrollen enligt artikel 22 bekräftar att de uppgifter som registrerats i ansökningsakten motsvarar de uppgifter som gett en träff vid den automatiserade behandlingen enligt artikel 20.2–20.5, eller om det råder tvivel om sökandens identitet efter en sådan kontroll, ska ansökan behandlas i enlighet med förfarandet i artikel 26. Om den automatiserade behandlingen enligt artikel 20.3 visar att den sökande svarat jakande på någon av frågorna i artikel 17.4 och det inte förekommer någon annan träff ska ansökan skickas till den nationella Etias-enheten i den ansvariga medlemsstaten för manuell behandling i enlighet med artikel 26.

I artikel 22 anges att om den automatiserade behandlingen enligt artikel 20.2–20.5 ger upphov till en eller flera träffar ska Etias centrala system automatiskt konsultera Etias centralenhet. Om centralenheten konsulteras ska denna beviljas åtkomst till ansökningsakten och eventuella anknytande ansökningsakter samt till alla träffar som uppkommit vid den automatiserade behandlingen enligt artikel 20.2–20.5 och till de upplysningar som kartlagts av det centrala systemet. Centralenheten ska kontrollera om de uppgifter som har registrerats i ansökningsakten motsvarar en eller flera av de särskilda riskindikatorer som avses i artikel 33, uppgifterna i Etias centrala system, uppgifterna i ett av de genomsökta EU-informationssystemen, Europoluppgifterna eller uppgifterna i Interpols databaser SLTD eller TDAWN. Om uppgifterna inte motsvarar andra uppgifter och inga andra träffar uppkommit vid den automatiserade behandlingen enligt artikel 20.2–20.5 ska Etias centralenhet radera den felaktiga träffen från ansökningsakten och det centrala systemet ska automatiskt utfärda ett resetillstånd i enlighet med artikel 36.

Enligt artikel 26 ska ansökan behandlas manuellt av den nationella Etias-enheten om den automatiserade behandlingen som avses i artikel 20.2–20.5 gett en eller flera träffar. Den nationella enheten ska ha åtkomst till ansökningsakten och eventuella anknytande ansökningsakter samt till alla träffar som uppkommit vid den automatiserade behandlingen. Etias centralenhet ska informera den nationella enheten i den ansvariga medlemsstaten om huruvida en eller flera andra medlemsstater eller Europol konstaterats ha fört in eller tillhandahållit de uppgifter som gav upphov till träffen enligt artikel 20.2 eller 20.4. Artikel 26 reglerar vidare hur den nationella Etias-enheten ska agera beroende på vilken typ av träff uppgifterna har gett upphov till.

I artikel 33–35 regleras Etias sökregler och bevakningslista. Etias sökregler ska vara en algoritm som möjliggör profilering genom en jämförelse i enlighet med artikel 20 av de registrerade uppgifterna i en ansökningsakt i Etias centrala system med särskilda riskindikatorer som fastställs av Etias centralenhet. Riskindikatorerna handlar om säkerhetsrisker, risk för olaglig invandring eller höga epidemirisker. Bevakningslistan ska bestå av uppgifter om personer som misstänks ha begått eller deltagit i terroristbrott eller annat grovt brott eller personer för vilka det utifrån en allmän personbedömning finns faktiska indikationer på eller rimliga skäl att anta att de kommer att begå ett terroristbrott eller annat grovt brott. I artikel 34.4 framgår att bevakningslistan ska vara sammansatt av uppgifter som består av vissa angivna poster.

I artikel 36 anges att när prövningen av en ansökan visar att det inte finns några faktiska indikationer på, eller rimliga skäl på grundval av faktiska indikationer att anta, att en persons vistelse på medlemsstaternas territorium innebär en säkerhetsrisk, risk för olaglig invandring eller hög epidemirisk ska resetillstånd utfärdas av Etias centrala system eller den nationella Etias-enheten i den ansvariga medlemsstaten. Om det råder tvivel angående om det föreligger tillräckliga skäl att neka resetillstånd ska den nationella Etias-enheten i den ansvariga medlemsstaten ha möjlighet, även efter en intervju, att utfärda ett resetillstånd med en flaggning som innebär en rekommendation till gränsmyndigheterna att utföra en fördjupad kontroll.

Enligt artikel 37 ska resetillstånd nekas om sökanden använt en resehandling som har anmälts som förkommen, stulen, förskingrad eller ogiltig i SIS, om sökanden innebär en säkerhetsrisk, risk för olaglig invandring eller hög epidemirisk. Resetillstånd ska vidare nekas om sökanden är en person för vilken en registrering har införts i syfte att neka inresa och vistelse, om sökanden inte besvarar en begäran om ytterligare upplysningar eller handlingar inom vissa frister eller om sökanden inte inställer sig till en intervju.

Resetillstånd ska också nekas om det vid tidpunkten för ansökan finns rimliga och allvarliga skäl att ifrågasätta uppgifternas äkthet, tillförlitligheten vad gäller sökandens påståenden, de styrkande handlingar som sökanden lämnat in eller innehållets sanningshalt. Sökande som nekats resetillstånd har rätt att överklaga beslutet i den medlemsstat som fattade beslut om ansökan.

I artikel 41 anges bl.a. att resetillstånd ska återkallas om det framgår att villkoren för utfärdandet inte längre är uppfyllda. Återkallelse ska ske med hänvisning till ett eller flera av de skäl för att neka resetillstånd som anges i artikel 37.1. Även beslut om återkallelse kan överklagas i den medlemsstat som fattade beslut om ansökan.

Transportörers, gränsmyndigheters och invandringsmyndigheters användning av Etias regleras i artikel 45–49. Lufttrafikföretag, transportörer som bedriver sjötrafik och internationella transportörer som ansvarar för grupptransporter med buss ska sända en förfrågan till Etias informationssystem för att kontrollera att tredjelandsmedborgare som omfattas av kravet på resetillstånd innehar ett giltigt sådant.

Gränsmyndigheter med behörighet att utföra in- och utresekontroller vid gränsövergångsställen vid de yttre gränserna i enlighet med Schengens gränskodex ska söka i Etias centrala system med de uppgifter som finns i resehandlingens maskinläsbara fält.

Medlemsstaternas invandringsmyndigheter ska ha åtkomst till Etias centrala system för att kunna kontrollera eller verifiera att villkoren för inresa till eller vistelse på medlemsstatens territorium är uppfyllda och för att kunna vidta lämpliga åtgärder i detta avseende.

I artikel 50–53 anges förfarande och villkor för åtkomst till Etias centrala system för brottsbekämpande ändamål. Medlemsstaterna ska utse de myndigheter som har rätt att begära sökning i de uppgifter som har registrerats i Etias centrala system i syfte att förebygga, förhindra, upptäcka eller utreda terroristbrott eller andra grova brott. Varje medlemsstat ska vidare utse en central åtkomstpunkt som ska ha åtkomst till Etias centrala system. Den utsedda myndigheten och den centrala åtkomstpunkten får ingå i samma organisation om detta tillåts enligt nationell rätt, men den centrala åtkomstpunkten ska agera helt oberoende av de utsedda myndigheterna när den fullgör sina uppgifter enligt förordningen. Den centrala åtkomstpunkten ska vara åtskild från de utsedda myndigheterna och får inte ta emot instruktioner från dessa vad avser resultatet av verifieringen, som den ska utföra självständigt. Endast vederbörligen bemyndigad personal vid de centrala åtkomstpunkterna ska ha åtkomstbehörighet till Etias centrala system.

De utsedda myndigheterna får begära sökning i uppgifter i Etias centrala system om vissa villkor är uppfyllda. Det krävs att åtkomst för sökning är nödvändig för att förebygga, förhindra, upptäcka, eller utreda terroristbrott eller andra grova brott, att åtkomst för sökning

är nödvändig i ett särskilt fall samt att det finns bevis för eller rimliga skäl att anta att sökningen i uppgifter i Etias centrala system kommer att bidra till att brotten i fråga förebyggs, förhindras, upptäcks eller utreds, särskilt om det finns välgrundade skäl att tro att en person som misstänks för, har begått eller har utsatts för ett terroristbrott eller ett annat grovt brott ingår i en kategori av resenärer som omfattas av förordningen.

Enligt artikel 54 ska alla ansökningsakter lagras i Etias centrala system under resetillståndets giltighetstid eller under fem år från den dag då det sista beslutet att neka, ogiltigförklara eller återkalla resetillståndet fattades.

10.2 Entry Exit System

Det nya in- och utresesystemet *Entry Exit System*, EES, togs delvis i bruk den 12 oktober 2025. EES grundar sig på en EU-förordning[7] som ska införas successivt i alla länder i Schengenområdet. Förordningen är ett led i att vidareutveckla EU:s strategi för integrerad gränsförvaltning, bl.a. genom bättre användning av modern teknik för att förbättra förvaltningen av de yttre gränserna. På sikt kommer EES helt att ersätta dagens manuella stämpling av pass och göra det enklare att identifiera resenärer som försöker resa in eller ut från Schengenområdet under felaktig identitet eller med förfalskat pass samt personer som har vistats inom Schengenområdet längre än tillåten tid. Systemet kommer även att bidra till arbetet med att förebygga, upptäcka och utreda terroristbrott och annan allvarlig brottslighet.

10.2.1 Innehåll

Enligt artikel 1 i förordningen inrättas ett in- och utresesystem för registrering och lagring av datum, tidpunkt och plats för in- och utresa för tredjelandsmedborgare som passerar medlemsstaternas gränser vid vilka in- och utresesystemet har tagits i drift. Systemet är också

[7] Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017 om inrättande av ett in- och utresesystem för registrering av in- och utreseuppgifter och av uppgifter om nekad inresa för tredjelandsmedborgare som passerar medlemsstaternas yttre gränser, om fastställande av villkoren för åtkomst till in- och utresesystemet för brottsbekämpande ändamål och om ändring av konventionen om tillämpning av Schengenavtalet och förordningarna (EG) nr 767/2008 och (EU) nr 1077/2011.

till för beräkning av längden på tillåten vistelse, generering av varningar till medlemsstaterna när den tillåtna vistelsen har löpt ut samt registrering och lagring av datum, tidpunkt och plats för nekad inresa för tredjelandsmedborgare vars inresa för en kortare vistelse har nekats samt vilken myndighet i medlemsstaten som nekade inresan och skälen till nekad inresa.

I syfte att förebygga, förhindra, upptäcka och utreda terroristbrott eller andra grova brott fastställs i förordningen också de villkor enligt vilka utsedda myndigheter i medlemsstaterna och Europol kan få åtkomst till in- och utresesystemet för sökningar.

Enligt artikel 2 är förordningen tillämplig på tredjelandsmedborgare som beviljats inresa för en kortare vistelse till medlemsstaternas territorium och som underkastas in- och utresekontroller i enlighet med kodexen om Schengengränserna när de passerar de gränser vid vilka in- och utresesystemet har tagits i drift. Förordningen är vidare tillämplig vid inresa till och utresa från medlemsstaternas territorium på tredjelandsmedborgare som är familjemedlemmar till en unionsmedborgare som omfattas av rörlighetsdirektivet[8] eller till en tredjelandsmedborgare som i enlighet med en överenskommelse mellan å ena sidan unionen och dess medlemsstater och å andra sidan ett tredjeland åtnjuter fri rörlighet med unionsmedborgarnas, och inte innehar uppehållskort som avses i rörlighetsdirektivet eller uppehållstillstånd enligt förordningen om en enhetlig utformning av uppehållstillstånd för medborgare i tredjeland[9].

10.3 Europeiska kommissionens studier om sjöfart och landtransport

Den gränsöverskridande brottsligheten har under flera år ökat och omfattar t.ex. narkotikasmuggling, flyktingsmuggling, trafficking och ekonomisk brottslighet. I takt med denna utveckling har även intresset för att bekämpa denna typ av brottslighet ökat inom EU. 2019 uttryckte medlemsstaterna ett intresse för att utforska möjlig-

[8] Europaparlamentets och rådets direktiv 2004/38/EG av den 29 april 2004 om unionsmedborgares och deras familjemedlemmars rätt att fritt röra sig och uppehålla sig inom medlemsstaternas territorier och om ändring av förordning (EEG) nr 1612/68, och om upphävande av direktiven 64/221/EEG, 68/360/EEG, 72/194/EEG, 75/34/EEG, 75/35/EEG, 90/364/EEG, 90/365/EEG och 93/96/EEG.
[9] Rådets förordning (EG) nr 1030/2002 av den 13 juni 2002 om en enhetlig utformning av uppehållstillstånd för medborgare i tredjeland.

heterna att utvidga insamlingen av information från flyget till att även omfatta andra transportmedel. Nedan redovisas innehållet i två studier som genomförts på initiativ av Generaldirektoratet för migration och inrikes frågor, som är en avdelning inom Europeiska kommissionen. Studierna rör harmonisering av tillgången till reseinformation för land- och tågtransport[10] samt sjöfart[11].

10.3.1 Studien om land- och tågtransport

Under 2022 skedde det över 500 miljoner resor in i EU, varav en tredjedel av resorna företogs via landtransport. Samma år skedde över en miljard resor med landtransport över landsgränser inom EU, vilket vida överstiger de 300 miljoner resorna med flyg. Terrorister och andra brottslingar använder regelmässigt landtransport både för att ta sig in i EU och för att förflytta sig inom unionen. För att kunna kartlägga kriminella nätverk som opererar inom EU är det av vikt att förstå dessa resmönster.

Studien initierades för att utforska potentiella lösningar i kampen mot terrorism och annan grov brottslighet. Syftena med studien är följande.

- Utreda omfattningen av brottsligheten kopplad till resor via land och tåg över interna och externa gränser i EU/Schengen.
- Utvärdera de befintliga tillvägagångssätten som transportföretag och brottsbekämpande myndigheter använder för att samla in, överföra, behandla, dela, använda och lagra reseinformation.
- Identifiera de brister som finns för brottsbekämpande myndigheter i användningen av reseinformation för att bekämpa terrorism och annan grov brottslighet som sker med hjälp av gränsöverskridande resor.
- Utveckla möjliga åtgärder för att läka dessa brister, med hänsyn både till brottsbekämpande myndigheter och transportföretag.

[10] Europeiska kommissionen: Generaldirektoratet för migration och inrikes frågor, BearingPoint, ICF och Unisys, *Study on harmonising access to information related to cross-border travel taking place via road or rail, including obligations on transport operators and the use of such information for law enforcement purposes – Final Report*, november 2024.
[11] Europeiska kommissionen: Generaldirektoratet för migration och inrikes frågor, BearingPoint, ICF och Unisys, *Study on harmonising reporting obligations of travel data on maritime transport, with a view to use such data for law enforcement purposes – Final Report*, november 2024.

- Utvärdera rimligheten, proportionaliteten och tekniska aspekter avseende att samla in och behandla reseinformation.

Studien omfattar samtliga EU-länder för att säkerställa att de föreslagna åtgärderna är förenliga med EU-rätten, vilket särskilt inkluderar grundläggande rättigheter och dataskydd.

Landtransport spelar en stor roll i den gränsöverskridande brottsligheten och olika transportmedel används i olika utsträckning beroende på brottstyp. För illegal invandring används ofta buss eller taxi, medan narkotika- och migrantsmugglare oftare använder sig av lastbilar och andra privata fordon. Vid trafficking används ofta bussar och minibussar.

I avsaknad av statistik kring landtransportens betydelse för brottsligheten får brottsbekämpande myndigheter förlita sig på underrättelser och erfarenheter för att bedöma omfattningen och karaktären av det hot som brottsligheten utgör.

Reseinformation kan vara ett kraftfullt verktyg för brottsbekämpande myndigheter i att utreda, upptäcka, förhindra och analysera brott. Utvärderingen av API-direktivet visar att det tillför brottsbekämpningen stort värde att ta del av information från lufttrafikföretag för att kunna göra riskbedömningar och identifiera kriminella aktiviteter. Att ta del av information från boknings- och biljettsystem gör att brottsbekämpande myndigheter kan göra riskbedömningar i realtid och gör det möjligt att fånga upp en potentiell brottsling innan den korsat en gräns eller nått sin slutliga ankomstort.

Reseinformationen används även för att upptäcka brott genom att kartlägga misstänkta resmönster, t.ex. ovanliga resrutter eller frekvent användande av en avlägsen gränsövergång. Sådana tillvägagångssätt kan tyda på kriminell aktivitet, t.ex. smuggling eller trafficking. Brottsbekämpande myndigheter kan använda sådana uppgifter för att flagga potentiell kriminell aktivitet. Informationen kan också användas för att spåra hur en brottsling förflyttar sig och för att lokalisera stulna fordon.

I Finland och Estland har användandet av passagerarinformation från tågtrafiken enligt studien avsevärt förbättrat gränskontrollen, särskilt genom att förbättra kontrollen vid hållplatser där tågen stannar under en kort period. Det har möjliggjort tidig identifiering av efterlysta personer, terrorister och andra brottslingar. I Estland har det

varit särskilt effektivt för att identifiera resande utan visering eller uppehållstillstånd.

Identifierade problem

I studien identifieras fyra huvudsakliga problem med den befintliga insamlingen av reseinformation. Ett av dessa problem är att buss- och tågoperatörer, med mycket få undantag, inte har automatiserade system för att samla in och överföra passagerarinformation till myndigheterna. Brottsbekämpande myndigheter har inte tillgång till information om personer som korsar interna och externa gränser med olika former av landtransport. Bristen på data begränsar förmågan att identifiera brottslingar i tid och förmågan att göra de kopplingar mellan dem som krävs för att lösa ett brott. Till följd av avsaknaden av inre gränskontroll inom Schengen har brottsbekämpande myndigheter inte systematisk tillgång till information om brottslingar som rör sig över interna gränser. Vissa medlemsstater använder ett ANPR-system, *Automatic Number Plate Recognition*, vilket är ett system som automatiskt avläser registreringsskyltar och jämför dem med olika register. I Sverige används ett ANPR-system till exempel vid Öresundsbron. Generellt sett är detta dock inte en lösning på bristen på reseinformation som brottsbekämpande myndigheter har tillgång till.

Ett annat problem är att den reseinformation som finns inte behandlas systematiskt av brottsbekämpande myndigheter. Det finns nationella regleringar som hindrar den, för brottsbekämpande syften nödvändiga, behandlingen.

Ytterligare ett problem är att reseinformation inte når de brottsbekämpande myndigheterna i tid samt att informationen inte skickas till relevant myndighet. Exempelvis kan SIS användas för automatiska slagningar, men det klarar inte av de stora mängder slagningar som skulle behövas.

Slutligen är den information som samlas in av transportföretag och brottsbekämpande myndigheter av låg kvalitet. Den är ofta ofullständig och av varierande slag. Detta leder till falska positiva träffar, försämrad effektivitet för polisen och svårigheter med att verifiera någons identitet.

Potentiella lösningar

En potentiell reglering som läggs fram i studien är att det ska vara obligatoriskt för alla tågoperatörer att samla in API-uppgifter och/eller BRI-uppgifter, *Booking and Reservation Information*, för alla passagerare och besättning på långdistanståg som korsar interna gränser inom Schengen, samt att föra över uppgifterna till brottsbekämpande myndigheter och gränsmyndigheter. Detta liknar det system som Storbritannien använder för tågtrafiken till och från Schengenområdet och som Belgien använder för internationell tågtrafik.

Förslaget skulle förbättra tillgängligheten till den reseinformation som samlas in av operatörerna och underlätta för brottsbekämpande myndigheter att identifiera misstänkta personer som korsar gränser med tågtrafik. Genom att standardisera kraven på vilken information som ska samlas in förbättras även uppgifternas kvalitet och pålitlighet.

Det finns ett flertal problem med ett sådant system. Till skillnad från lufttrafikföretag och sjöfartsföretag är tågtrafikföretag inte skyldiga att samla in passagerarinformation enligt något internationellt regelverk, EU-rätt eller, i de flesta fall, nationell lagstiftning. Tågtrafikföretag är inte heller skyldiga att verifiera passagerarnas identitet innan ombordstigning. Sådana åtgärder är upp till de enskilda bolagen, som kan välja vilken information som samlas in av kommersiella och operationella skäl. Vissa tågtrafikföretag kräver inte att passagerarna ska ha en biljett för en specifik avgång. Många biljetter för gränsöverskridande resor har odaterade biljetter som kan utnyttjas under en begränsad tidsperiod. Vissa biljetter kräver inte att passageraren uppger något namn och andra kan köpas endast några minuter innan avgång. Bördan för tågtrafikföretagen att samla in information och i rätt tid översända den till berörd myndighet kan innebära både omfattande administration och få ekonomiska konsekvenser. Det går också att ifrågasätta proportionaliteten i åtgärden. Enligt Frontex[12] skulle uppskattningsvis 27,6 miljoner resenärer årligen påverkas.

De flesta tågtrafikföretag och tågstationer har inte de resurser eller den fysiska infrastruktur som krävs för att kunna verifiera passagerarnas identitet innan ombordstigning. Sådan verifiering skulle dessutom kräva att passagerarna filtreras beroende på slutdestination eftersom det på samma tåg kan resa personer vars slutdestination ligger både utom och inom landet från vilket tåget avgår. Det skulle sanno-

[12] EU:s gräns- och kustbevakningsbyrå.

likt krävas investeringar i infrastrukturen, samtidigt som en sådan verifiering går att undvika genom att köpa två eller fler separata biljetter. Verifiering av identitet på tågresor skulle sammantaget bli mycket kostsamt. Utgångspunkten är därför att identitetsuppgifterna inte kommer att verifieras innan avgång, vilket har negativ påverkan på uppgifternas användbarhet.

Liknande argument läggs fram avseende busstrafik. Bussbolag är inte skyldiga att samla in passageraruppgifter och inte heller skyldiga att verifiera passagerarnas identitet. Det krävs ytterligare resurser och fysisk infrastruktur för att införa ett sådant system.

Ett annat potentiellt policyförslag som läggs fram är att medlemsstaterna ska koppla sina respektive ANPR-system till SIS, vilket skulle underlätta lokaliseringen av fordon som används av kriminella. Det kräver ingen ytterligare insamling av data. I praktiken innebär förslaget att brottsbekämpande myndigheter genom automatiserad behandling ska göra en slagning på all insamlad data avseende registreringsnummer mot SIS-databasen, i vilken det kan finnas flaggade fordon. För att vara förenlig med uttalandena måste användandet av ANPR-information begränsat till vad som är strikt nödvändigt för att bekämpa terrorism och annan grov brottslighet och rikta sig mot särskilt brottsutsatta områden. Information som inte har någon koppling till brottslighet måste raderas omedelbart och lagringen av annan information ska vara begränsat i tid och omfattning. Även tillgången till ANPR-information ska vara strikt kontrollerad och begränsad till behörig personal vid brottsbekämpande myndigheter. För att förbättra användningen av ANPR-uppgifter föreslås att ett forum inrättas för utveckling av nationella strategier för brottsbekämpningen.

Slutsatserna i studien är bland annat att det finns en påtaglig lucka i information för landbaserat resande jämfört med flygresor. Även om vissa medlemsstater har vidtagit åtgärder är tillämpningen i de olika medlemsstaterna fragmenterat och ofullständigt. Utvecklingen av Entry Exit-systemet och ETIAS kommer innebära att en begränsad mängd information blir tillgänglig för brottsbekämpande myndigheter, men myndigheterna kommer fortfarande att ha begränsad eller ingen information om misstänkta personers resor över interna gränser inom EU. För effektiv brottsbekämpning krävs det mer information, samt en infrastruktur som gör det möjligt att ta del av informationen och dela den vidare inom kort tid från att den har samlats in.

10.3.2 Studien om sjöfart

Insamling och behandling av information om passagerare inom sjöfarten är inte reglerad på EU-nivå, men vissa medlemsstater har på olika sätt reglerat området inom nationell rätt. Både Europol och FN:s kontor för terrorismbekämpning har uppmärksammat att sjötransport används för gränsöverskridande brottslighet. Till exempel kommer knappt 70 procent av narkotikabeslagen som tullmyndigheter gör vid hamnar inom EU från fartyg som kommer från eller avgår till en hamn i ett tredjeland eller en annan medlemsstat.

Under 2022 reste cirka 350 miljoner passagerare med fartyg till hamnar inom EU. Antalet passagerare hade då inte återgått till nivåerna innan Covid-19-pandemin, då över 400 miljoner resor om året företogs. Under 2022 skedde drygt två tredjedelar av resorna inom EU. Under åren 2015–2022 företogs cirka 177 000 resor till eller från Sverige med sjötransport. Av dessa var det endast fem procent som avsåg resor utom EU. Sedan dess har rutterna förändrats, t.ex. genom att sträckan från Stockholm till Sankt Petersburg har lagts ned, vilket sannolikt har minskat andelen resor till eller från tredjeländer ytterligare.

Till följd av den minimala övervakning och kontroll som sker vid vissa gränsövergångar används sjöfart frekvent för att begå gränsöverskridande brott såsom narkotikasmuggling, vapensmuggling, trafficking och egendomsbrott. Allvarlig organiserad brottslighet har sedan länge utgjort ett påtagligt hot mot EU. Det sker enstaka samarbeten mellan medlemsstater inom ramen för EMPACT[13] med stöd av Europol. Två gånger per år får medlemsstaternas brottsbekämpande myndigheter information om passagerare och fordon från färjor. Myndigheterna får inte lagra informationen, utan den översänds till Europol för att göra slagningar i relevanta databaser, t.ex. EIS och EAS.[14] Om informationen ger träff informeras medlemsstaten som därefter kan vidta nödvändiga åtgärder. 2023 skedde ett sådant samarbete under tre dagar avseende sjöfartstrafiken i Sverige och Danmark. 25 000 passagerare och besättning samt 11 500 fordon kontrollerades, vilket resulterade i att 31 personer greps, att beslag gjordes av tio fordon och annan egendom (till ett värde av en miljard euro),

[13] European Multidisciplinary Platform Against Criminal Threats.
[14] Europol Information System och Europol Analysis System.

277 elcyklar och 500 000 euro i kontanter samt att 78 brott rapporterades.

Generellt sett saknar brottsbekämpande myndigheter den information som krävs för att fullgöra sina uppgifter. Särskilt saknas bokningsuppgifter, bagageinformation och information om fordon. Den information som myndigheterna har tillgång till håller ofta låg kvalitet och är opålitlig. Bristen på harmoniserade regler på nationell nivå innebär dessutom en onödig administrativ och ekonomisk börda för sjöfartsföretagen.

I studien läggs flera policyförslag fram. Ett förslag innebär att medlemsstaternas ska rekommenderas att harmonisera vissa aspekter av hur och vilken information som samlas in för gränsöverskridande sjöfart samt när den ska översändas till brottsbekämpande myndigheter. Rekommendationer som dessa är inte bindande och ges ut i enlighet med artikel 288 i Fördraget om Europeiska unionens funktionssätt. Syftet med förslaget är att slå fast när informationen ska överföras, vilket leder till bättre förutsättningar för brottsbekämpningen och högre grad av förutsebarhet för sjöfartsoperatörerna. Systematisk överföring av information innebär dessutom mindre administration för sjöfartsoperatörerna än ett system där myndigheter begär information i enskilda fall. Enligt studien kan tidsåtgången på detta sätt minskas med uppemot 97 procent. Det skulle också förbättra kvaliteten på den information som kommer brottsbekämpande myndigheter tillhanda och ge dessa tillräckligt med tid för att agera på den information som kommer in. Förslaget innebär visserligen en inskränkning i de grundläggande rättigheterna i artikel 7 och 8 i EU-stadgan, men dessa kan begränsas för att uppnå ett ändamål av allmänt intresse.

Ett annat förslag som läggs fram i studien innebär att brottsbekämpande myndigheter ska få tillgång till den information som redan översänds till respektive medlemsstats National Single Window, NSW. Detta kan ske antingen genom automatisk överföring på förhand eller genom begäran från myndigheterna. Detta har liknande konsekvenser som förslaget ovan i och med att det innebär mer och bättre information för myndigheterna, samtidigt som det leder till mindre administration för sjöfartsoperatörerna. Både från ett operativt och säkerhetsmässigt perspektiv framstår enheten för passagerarinformation som den lämpligaste mottagaren av informationen från sjöfartsoperatörerna.

I studien läggs ytterligare ett antal förslag fram. Generellt sett handlar förslagen om att ge bättre förutsättningar för brottsbekämpande myndigheter genom mer och bättre information, samtidigt som sjöfartsoperatörerna påverkas i så liten utsträckning som möjligt.

10.4 European Maritime Single Window environment

Genom en EU-förordning[15] införs en europeisk kontaktpunkt för sjöfart: *European Maritime Single Window environment*, EMSWe. Syftet med förordningen är att förbättra den europeiska sjöfartssektorns konkurrenskraft och effektivitet genom att minska den administrativa bördan och införa digitala komponenter och tjänster för att harmonisera de befintliga nationella systemen. Förordningen trädde i kraft den 15 augusti 2025, men det tekniska genomförandet i medlemsstaterna har försenats. I Sverige planeras införandet att ske under andra halvåret av 2027. Förordningen ersätter ett direktiv om rapporteringsformaliteter för fartyg[16]. EMSWe ska ersätta det nuvarande systemet *National Single Window*, NSW.

Enligt artikel 4 i förordningen ska varje medlemsstat inrätta en nationell kontaktpunkt för sjöfart genom vilken alla uppgifter som krävs för fullgörandet av rapporteringsskyldigheterna ska tillhandahållas vid ett tillfälle. I Sverige är den nationella kontaktpunkten Sjöfartsverket. Efter att fartygen har uppfyllt sin uppgiftsskyldighet genom att översända information till Sjöfartsverket, kan verket dela informationen vidare till myndigheter som har ansvar som kräver information från fartygen, t.ex. Kustbevakningen, Transportstyrelsen och Tullverket. Viss information kan även delas med hamnar, vilket inte har varit möjligt tidigare. Genom att minska dubbelrapporteringen minskas administrationen. Denna engångsprincip fastställs i artikel 8, där det anges att medlemsstaterna ska säkerställa att deklaranten uppmanas att tillhandahålla uppgifter enligt förordningen endast en gång per fartygsanlöp och att relevanta dataelement i EMSWe-datauppsättningen tillgängliggörs och återanvänds genom att tillgänglig-

[15] Europaparlamentets och rådets förordning (EU) 2019/1239 av den 20 juni 2019 om inrättande av en europeisk kontaktpunkt för sjöfart och om upphävande av direktiv 2010/65/EU.
[16] Europaparlamentets och rådets direktiv 2010/65/EU av den 20 oktober 2010 om rapporteringsformaliteter för fartyg som ankommer till och/eller avgår från hamnar i medlemsstaterna och om upphävande av direktiv 2002/6/EG.

göras för deklaranten för att de ska kunna fullgöra rapporteringsskyldigheterna vid ankomst till nästa hamn i unionen.

Tidigare har varje medlemsstat haft sina egna nationella system med olika krav. I och med EMSWe införs en gemensam datauppsättning, dvs. en standardiserad och komplett uppsättning information som fartyg måste rapportera när det anlöper en hamn inom EU. Gemensamma tekniska moduler gör att fartygets egna it-system kan kommunicera direkt med myndigheternas system i alla medlemsstater.

11 Reglering i utvalda EU-länder

Ett flertal länder har valt att inkludera andra trafikslag i PNR-lagstiftningen. Detta är en utveckling som har skett under senare år och det förefaller troligt att sådan insamling kommer att öka även framöver. Kommissionen konstaterade i en studie från 2024 att t.ex. tåg- och bussföretag samlar in passagerarinformation i varierande grad som en del av deras normala verksamhet. Det är däremot inte särskilt vanligt att informationen överförs till nationella myndigheter inom EU. I avsaknad av EU-rättsliga eller nationella skyldigheter får myndigheterna sällan tillgång till information på ett automatiskt sätt inom rimlig tid.[1]

Vid tiden för kommissionens studie var det endast Belgien och Estland som hade lagstiftning som tillät automatisk insamling, överföring och vidare behandling av information från t.ex. busstrafik. Implementeringen av busstrafik i Belgien inleddes i juni 2024. Sedan dess har omfattningen av insamlingen i EU ökat.

De vanligaste trafikslagen som inkluderas är tåg-, buss- och färjetrafik. I Belgien, Finland och Irland samlas PNR-uppgifter från samtliga dessa trafikslag in till enheten för passagerarinformation. I åtminstone Finland sker överföringen från färjor till enheten för passagerarinformation via NSW, dvs. det finns ingen direkt kontakt mellan färjorna och enheten. I Finland är dessutom flygplatserna och hamnarna bevakade med kameror som skickar information till enheten.

I andra länder är olika trafikslag inkluderade i PNR-systemet. Cypern, Estland, Grekland, Italien, Litauen, Rumänien, Slovenien, Tjeckien och Ungern har inkluderat någon kombination av andra trafikslag än flyg. Danmark, Finland, Irland och Nederländerna samlar dessutom in PNR-uppgifter från privatflyg. I Polen pågår en

[1] Europeiska kommissionen: Generaldirektoratet för migration och inrikes frågor, BearingPoint, ICF och Unisys, *Study on harmonising access to information related to cross-border travel taking place via road or rail, including obligations on transport operators and the use of such information for law enforcement purposes – Final Report*, november 2024, s. 30–32.

lagstiftningsprocess för att utöka tillämpningen av PNR-systemet till andra trafikslag.

12 Behöriga myndigheters behov av passageraruppgifter

12.1 Inledning

Det finns ett generellt behov för brottsbekämpande myndigheter att ta del av passageraruppgifter. Uppgifterna används till utredningar, underrättelsearbete, statistiska underlag, jämförelser och profilering. Inom brottsbekämpningen används de för att förebygga, förhindra, upptäcka, utreda och lagföra brottslighet.

Det är önskvärt ur ett brottsbekämpande perspektiv att myndigheterna får täckning på fler trafikslag och möjlighet att snabbt få tillgång till uppgifter för att hinna vidta åtgärder innan en person lämnar landet. Det är även viktigt att kunna genomföra regelsökningar för att hitta nya, tidigare okända personer som använder ett specifikt mönster för att ta sig in i landet. Parametrar som kan beaktas i en sådan regelsökning kan t.ex. vara en viss rutt, en viss tid, en viss storlek på bagaget, eller flera av dessa faktorer tillsammans.

En potentiell förbättring jämfört med nuvarande PNR-system är möjligheten att kunna göra integrerade regelsökningar i flera olika transportslag. Det skulle t.ex. gå att uppmärksamma personer som vid en viss tid åker en viss sträcka med tåg, för att sedan byta och åka en viss sträcka med flyg. På så sätt kan underrättelseinformation om vilka metoder som specifika kriminella organisationer använder sig av komma till användning för att identifiera personer av intresse. I dagsläget går det att göra regelsökningar avseende flygtrafiken men inte när det gäller andra trafikslag.

Frånvaron av heltäckande insamling av passageraruppgifter från andra trafikslag än flyg har gjort att *broken travel*, dvs. att genomföra en resa med flera olika trafikslag, har blivit effektivt och vanligt sätt att undvika eller minska myndigheternas kännedom om en persons

resor som företas i kriminellt syfte. För att komma åt detta krävs det insamling från flera olika datakällor.

I dagsläget samlas passageraruppgifter från gränsöverskridande resor med flyg, tåg, buss och färja in systematiskt. Insamlingen är dock endast heltäckande när det gäller utrikesflyg genom PNR-systemet. För flyg- och tågtrafik sker överföringen automatiskt från transportföretaget till ett program hos enheten för passagerarinformation. För färjetrafiken är överföringen manuell från företagen till en funktionsbrevlåda hos Polismyndigheten. När det gäller busstrafiken sker överföringen manuellt från en funktionsbrevlåda till ett program hos enheten för passagerarinformation.

Data inhämtas även på enskild basis från inrikestrafik. Då rör det sig om specifik inhämtning avseende en viss individ och inget systematiskt inhämtande av uppgifter.

12.2 Polismyndigheten

Polismyndigheten har ett omfattande behov av passageraruppgifter för att på ett effektivt sätt bekämpa terrorism och grov organiserad brottsligheten. Uppgifterna används för att identifiera misstänkta terrorister genom att matcha resmönster mot underrättelseinformation, vilket gör det möjligt att ingripa innan brott begås. Vidare kan uppgifterna användas för att lokalisera och gripa personer som är internationellt efterlysta eller som försöker undkomma lagföring i Sverige.

I förarbetena anförde regeringen beträffande 25 § polislagen bl.a. följande. Polisen har stor nytta av tillgång till uppgifter i transportföretagens bokningsregister i spaningsverksamheten. Redan innan lagändringen fanns det möjlighet att ta del av sådana uppgifter inom ramen för en förundersökning med stöd av rättegångsbalkens regler om beslag. Det fanns däremot inte någon motsvarande möjlighet under förspaningsstadiet. Förspaningen kan ha flera olika inriktningar, t.ex. kan den utövas i syfte att identifiera och karaktärsbestämma hot mot samhället som det är polisens uppgift att förebygga. Det kan t.ex. innebära en kartläggning av hur narkotika transporteras eller en beskrivning av strukturen av en viss organiserad brottslighet. Syftet med förspaningen kan också vara att ge polisen det underlag som behövs för att brott ska kunna förhindras. Sådan verksamhet

kan exempelvis bestå i att polisen inför ett större evenemang samlar in information som behövs för att insatserna ska kunna planeras. Sammanställning av sådan information kan vara avgörande för polisens möjlighet att förhindra att brott begås. Förspaningen kan också syfta till att ge kunskap om brottsliga aktiviteter. För samtliga dessa former av förspaning skulle polisen ha nytta av bokningsuppgifter hos transportföretagen.[1]

Genom att se vilka som bokar resor tillsammans kan polisen avslöja kopplingar inom organiserad brottslighet. Det kan t.ex. gå att identifiera nyckelpersoner som sällan själva hanterar narkotika eller vapen, men som är inblandad i sådan verksamhet. I utredningar av allvarliga brott används historiska passageraruppgifter för att knyta en misstänkt till en specifik plats vid en viss tidpunkt. Analys av resmönster med förutbestämda riskkriterier används för att upptäcka tidigare okända personer som uppvisar ett beteende som indikerar kopplingar till allvarlig brottslighet.

I nuläget, med ett PNR-system som endast omfattar flygtrafik, har polisen svårare att följa en misstänkt person som väljer att helt eller delvis resa med ett annat transportmedel. Med en mer heltäckande kontroll av gränsöverskridande resor skulle polisen ha större möjlighet att kartlägga en persons hela resväg. Det skulle även underlätta kartläggningen av hur kriminella nätverk transporterar vapen, narkotika och personer.

12.3 Tullverket

Tullverket har bl.a. i uppgift att övervaka och kontrollera trafiken till och från Sverige och tillse att bestämmelser om in- och utförsel av varor följs. Myndigheten har vidare i uppgift att förebygga, förhindra och upptäcka brottslighet i samband med in- och utförsel av varor och ingripa vid misstanke om brott, samt utreda och lagföra vissa brott i samband med detta. Varor kan vara illegala eller omfattas av särskilda restriktioner vid in- och utförsel, t.ex. narkotika, vapen, sprängämnen, läkemedel och stöldgods. För att effektivt förhindra smuggling krävs såväl möjlighet att upptäcka förbuds- eller restriktionsvaror liksom förmåga att ingripa, beslagta varorna och utreda brottsmisstankar. Tullverket ska också delta i det myndighetsgemen-

[1] Prop. 1996/97:175, *Ändringar i polislagen m.m.*, s. 67.

samma arbetet mot den grova och organiserade brottsligheten. Tullverket har därför fått brottsbekämpande befogenheter kopplade till in- och utförsel av vissa varor.

Tullverket har samlat in bokningsuppgifter sedan Sverige trädde in i EU 1995 då detta infördes som en kompensatorisk åtgärd för att möjliggöra ett selektivt och riskbaserat urval av passagerare, varor och fordon vid EU:s yttre gräns. Tullverkets regelverk om bokningsuppgifter har sedan dess återkommande ändrats i takt med ändrade behov.

Tullverkets befogenheter stärktes genom den nya tullbefogenhetslagen som trädde i kraft 2024. Syftet var bl.a. att bekämpa organiserad brottslighet. Smuggling av olagliga varor som narkotika och vapen har ofta koppling till kriminella nätverk. Genom kontrollverksamheten har Tullverket möjlighet att ingripa mot dessa brottsliga flöden i ett tidigt skede. Tullverkets strategiska inriktning är att fokusera på att hindra allvarlig brottslighet. För att kunna fullgöra hela kontrolluppdraget, och för att upptäcka den allvarliga brottsligheten, behöver Tullverket arbeta även mot överträdelser som initialt kan uppfattas som mindre allvarliga. Även s.k. myrtrafik och mindre allvarlig brottslighet har ofta kopplingar till mer allvarlig brottslighet i form av sprängningar och andra våldsdåd. Det är vidare inte ovanligt att smugglare delar upp varor i flera mindre sändningar. Detta kan Tullverket upptäcka med hjälp av bl.a. bokningsuppgifter från godstransporter. Genom att koppla ihop informationen med uppgifter om passagerare och transportmedel på en viss färjeavgång kan rätt kontrollobjekt identifieras på ett sätt som inte är möjligt endast med fysiska kontroller. Ett system med en ändamålsbegränsning som innebär att uppgifter endast får behandlas i syfte att bekämpa allvarlig brottslighet skulle således innebära en påtaglig begränsning för Tullverket att utföra sitt myndighetsuppdrag.

Enligt 2 kap. 10 § tullverkets brottsdatalag är ändamålet för insamlingen av bokningsuppgifter att dessa behövs för att planera och välja ut kontrollobjekt. Det finns inget krav på konkret misstanke om brottslig verksamhet vid insamling eller urvalsarbete, utan det räcker att uppgifterna kan antas ha betydelse för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda och beivra brott inom Tullverkets brottskatalog. Det innebär att Tullverket har rätt att samla in en omfattande mängd bokningsuppgifter med stöd av 7 kap. 12 § tulbefogenhetslagen.

Tullverkets riskanalyser behöver innefatta uppgifter om passagerare, fordon och varor. Möjligheten att samköra dessa olika typer av uppgifter är helt nödvändig för att Tullverket ska kunna uppfylla sitt brottsbekämpande uppdrag. Eftersom Tullverkets uppdrag avser brott som begås i varuflödet oavsett transportslag har myndigheten i sina riskanalyser och kontrollurval ett omfattande behov att kunna koppla samman information om passagerare med ett visst personligt transportmedel och i viss mån med uppgifter i tulldeklarationer. Detta är särskilt relevant för transportslag som transporterar såväl passagerare som gods och där ett transportmedel i sig är en del i brottslighetens utförande. En separation av uppgifter om passagerare från uppgifter om varor och fordon innebär denna förmåga till stor del går förlorad. Det har konstaterats att så har skett när det gäller flygtrafiken sedan införandet av PNR-systemet.

I förarbetena till tullbefogenhetslagen anfördes bl.a. följande.[2] Bokningsuppgifter används inom Tullverkets underrättelseverksamhet för att välja ut vilka objekt som ska tas ut för kontroll. Urvalet görs genom att de inkomna uppgifterna matchas mot redan kända objekt och s.k. riskprofiler, dvs. kriterier i fråga om exempelvis resmönster, betalningssätt och medpassagerare som kan motivera att ett visst objekt tas ut för kontroll.

Underrättelseverksamheten är central för att Tullverket ska kunna genomföra kontroller där riskerna för smuggling och undandragande av till, skatt och andra avgifter är som störst. Det är därför av stor vikt att Tullverket kan arbeta mer underrättelsebaserat, för att resurserna ska användas på mest effektiva sätt. I det arbetet är tillgång till information om varuflödet över gränserna och om resande nödvändig. Transportföretagens skyldighet enligt tullagen och inregränslagen att lämna bokningsuppgifter är väsentlig för underrättelseverksamheten och i förlängningen både för kontrollverksamheten och den brottsbekämpande verksamheten.

Brottsligheten har förändrats och blivit mer gränsöverskridande. Det förs in mer narkotika, vapen och explosiva varor över den svenska gränsen. Den organiserade brottsligheten har brett ut sig i samhället och blivit grövre. Därmed har också behovet av nya metoder för att upptäcka brottsligheten ökat. Genom att identifiera riskprofiler och kartlägga resmönster, betalningssätt och vilka som reser i sällskap samt

[2] Prop. 2023/24:132, *Ny tullbefogenhetslag*, s. 356–357.

transport- och varuflöden ökar möjligheterna att kunna avslöja brott och att upptäcka nya smugglingsmetoder.

12.4 Ekobrottsmyndigheten

Ekobrottsmyndigheten är en åklagarmyndighet med uppdrag att förebygga, upptäcka, utreda och lagföra ekonomisk brottslighet. Den ekonomiska brottsligheten kostar samhället miljarder i förlorade skatteintäkter och missbrukade bidrag. Det finns i dag en tydlig överlappning mellan den ekonomiska brottsligheten och den övriga organiserade brottsligheten.

Ärendena är ofta stora och innefattar komplicerade bolagsstrukturer. När det gäller den grova organiserade ekonomiska brottsligheten har i stort sett alla ärenden gränsöverskridande karaktär och i nästan samtliga ärenden används PNR-uppgifter. I regel gäller det historiska uppgifter men det sker även genom bevakning av misstänkta personer. Ekobrottsmyndigheten har därför behov av uppgifter som sträcker sig förhållandevis långt bak i tiden. Passageraruppgifter kan t.ex. användas för att jämföra en persons in- och utresor ur landet med tidpunkten för olika transaktioner på ett konto. Det är kombinationen av passageraruppgifter och annan information som tillsammans blir ett viktigt verktyg för att bekämpa den ekonomiska brottsligheten.

Inom den ekonomiska brottsligheten är det vanligt att de kriminella försöker distansera sig från den brottsliga verksamheten. Med hjälp av målvakter går det att undvika en direkt koppling till bolagen där den brottsliga verksamheten bedrivs. I och med den digitala utvecklingen går det att ytterligare distansera sig från brottsligheten genom att använda målvakternas e-legitimation. Brotten kan på så vis begås i Sverige även när de bakomliggande individerna befinner sig utomlands, vilket försvårar arbetet med lagföring i Sverige.

Penningtvätt är centralt inom ekonomisk brottslighet och den har ofta en internationell komponent. Ett nätverk av olika bolag kan användas för att slussa oredovisade intäkter från bolagen ut ur Sverige. Det kan ske en mängd transaktioner för att minska spårbarheten. Tillgång till passageraruppgifter innebär större möjligheter att koppla en viss person till de internationella bolag som används i ett sådant upplägg.

Genom analys av resmönster är det även möjligt att hitta nya tillvägagångsätt som de kriminella använder. Med hjälp av sådana analyser kan Ekobrottsmyndigheten utveckla strategier för att göra ekonomisk brottslighet svårare och mindre lönsamt. Sådan kartläggning blir mer kraftfull om tillgången till passageraruppgifter från andra trafikslag än flyg förbättras. Det skulle t.ex. innebära mer effektiv utredning av välfärdsbrott där kontroll av vistelseort är av stor vikt. Passageraruppgifter från tåg, färjor och bussar kan visa om en person som uppbär bidrag i Sverige i själva verket befinner sig utomlands under långa perioder.

12.5 Försvarsmakten

Av Försvarsmaktens myndighetsinstruktion[3] framgår att myndighetens huvuduppgift är att försvara Sverige och allierade stater mot ett väpnat angrepp med utgångspunkt i det kollektiva försvaret inom Nato. I 5 och 6 §§ anges att Försvarsmakten ska bedriva omvärldsbevakning och upptäcka, identifiera och förvarna om yttre hot mot Sverige och svenska intressen och bedriva försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet. Enligt 7 § ska Försvarsmakten leda och bedriva militär säkerhetstjänst i syfte att skydda de säkerhetsintressen som berör Försvarsmakten och dess tillsynsområde enligt säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2021:955).

Försvarsunderrättelseverksamheten ska bedrivas till stöd för svensk utrikes-, försvars- och säkerhetspolitik samt i övrigt för att kartlägga yttre hot mot landet. Försvarsunderrättelseverksamhet ska fullgöras genom inhämtning, bearbetning och analys av information enligt 1–2 §§ lagen om försvarsunderrättelseverksamhet. Försvarsunderrättelseverksamheten är ett led i Försvarsmaktens uppgifter att i hela konfliktskalan från fred till krig ge underlag för Försvarsmaktens beredskap, operativa verksamhet och förbandsproduktion samt för krigsorganisationens utveckling och materiella förnyelse.[4] Försvarsunderrättelseverksamheten ska också identifiera och redovisa eller ge förvarning om sådana förändringar i omvärldsläget som sedan kan

[3] Förordning (2024:1333) med instruktion för Försvarsmakten.
[4] Prop. 1999/2000:25, *Lag om försvarsunderrättelseverksamhet*, s. 14.

ligga till grund för politiska beslut om totalförsvarets anpassning på kort eller lång sikt.[5]

Den militära säkerhetstjänsten bedrivs genom säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signalskyddstjänst. Den syftar bl.a. till att förebygga, motverka och avvärja säkerhetshotande verksamhet. Den ska också klarlägga och analysera den säkerhetshotande verksamhetens mål, medel och metoder och utifrån hotbild och säkerhetshotande verksamhet vidta åtgärder för att säkerställa relevant skydd i form av informationssäkerhet, fysisk säkerhet och personalsäkerhet.

Vid implementeringen av PNR-direktivet i den svenska lagstiftningen gav regeringen uttryck för den stora betydelse som uppföljning av individer som reser in och ut ur Sverige har för flera verksamhetsområden kopplade till att förebygga, upptäcka och förhindra t.ex. terrorism och sabotageverksamhet.[6] Försvarsmakten har således verksamhetsuppgifter som är kopplade till att förebygga, upptäcka och förhindra t.ex. terrorism och den allvarliga brottslighet som framgår av bilaga II till PNR-direktivet och Försvarsmaktens behandling av PNR-uppgifter är i enlighet med ändamålen i direktivet. Regeringen konstaterade därför att Försvarsmakten uppfyller de krav som ställs i artikel 7.2 i PNR-direktivet på att ha verksamhetsuppgifter som är kopplade till att förebygga, upptäcka, och förhindra t.ex. terrorism och sabotageverksamhet. I ett större perspektiv har Försvarsmakten i ett framtida eventuellt beredskapsläge även till uppgift att hävda territoriell integritet där uppgifter om vissa in- och utresande individer blir relevant.

Försvarsmakten har behov av uppgifter om personer som reser in i landet för att kartlägga yttre hot mot landet och för att klarlägga och motverka säkerhetshotande verksamhet. Kartläggning av de yttre hoten sker utanför Sverige men när aktörerna reser in i landet behöver Försvarsmakten kunna indikera det säkerhetshot som en sådan närvaro innebär. Det kan exempelvis röra sig om risk för genomförande av sabotage eller industrispionage. Passageraruppgifter utgöra i sammanhanget en viktig informationsmängd för att Försvarsmakten ska kunna lösa sina myndighetsuppdrag, vilka det endast åligger Försvarsmakten att utföra. Bristande tillgång till för myndigheten nödvändiga

[5] Prop. 2020/21:224, *Behandling av personuppgifter vid Försvarsmakten och Försvarets radioanstalt*, s. 176.
[6] Prop. 2017/18:234, *Lag om flygpassageraruppgifter i brottsbekämpningen*, s. 84.

uppgifter om vilka som reser in i landet utgör därför en nationell sårbarhet.

Försvarsmaktens behov av passageraruppgifter, som regeringen fastslog i och med införandet av lagen om flygpassageraruppgifter i brottsbekämpningen, har förstärkts med anledning av rådande säkerhetspolitiska omvärldsläge, vilket har ökat bl.a. sabotagehotet mot Sverige. Det har därför blivit alltmer angeläget för Försvarsmakten att kunna indikera utländska säkerhetshotande aktörers försök att resa in i landet, ytterst för att kunna motverka säkerhetshotande verksamhet, som t.ex. terrorism eller sabotage. I närtid har främmande makt visat en ökande offensiv inställning när det gäller att planera och genomföra sabotage i länder inom EU och Nato. Sabotagehotet är som mest påtagligt när det gäller militärt och civilt stöd till Ukraina. Utöver det är infrastruktur, kommunikation och energiförsörjning de mest sannolika målen.

12.6 Säkerhetspolisen

Säkerhetspolisen har bl.a. i uppdrag att förebygga, förhindra och upptäcka brottslighet som innefattar terroristbrott och brott mot Sveriges säkerhet. För att kunna fullgöra sitt uppdrag har Säkerhetspolisen ett stort behov av tillgång till information. Tillgången till passageraruppgifter har ofta en avgörande betydelse för att effektivt föra underrättelsearbete och brottsutredningar framåt. Passageraruppgifter är effektiva för att identifiera hotaktörer och för att bekräfta eller avfärda annan underrättelseinformation. Uppgifterna är av särskild betydelse när det kommer till att avvärja terroristattentat eftersom det ger tydlig information om var en misstänkt person befinner sig. Genom tillgång till historiska uppgifter kan Säkerhetspolisen få information om misstänkta terrorister och andra hotaktörers resmönster. Det kan t.ex. handla om att få information om vilka hotaktörer som reser tillsammans eller till samma destination. Passageraruppgifter kan även ge Säkerhetspolisen viktig information om t.ex. betalningsuppgifter och telefonnummer som behövs i myndighetens brottsbekämpande verksamhet.

Det nuvarande PNR-systemet avser endast flygtrafik. Säkerhetspolisen har dock behov av att kunna följa en misstänkt passagerare som reser helt eller delvis med andra transportmedel än flyg. Med till-

gång till uppgifter från fler trafikslag skulle Säkerhetspolisens förmåga att kartlägga misstänkta personers hela resväg öka. Det skulle i sin tur öka förmågan att avvärja terroristhot och hot mot Sveriges säkerhet.

13 EU-domstolens praxis

13.1 Inledning

EU-domstolen har i ett flertal avgöranden berört rätten till respekt för privatliv och skydd av personuppgifter i förhållande till statlig övervakning och datalagring inom EU. Rättsutvecklingen har präglats av att EU:s rättighetsstadga har fungerat som det yttersta skyddet mot godtycklig övervakning.

Flera av målen handlar om insamling och lagring av trafik- och lokaliseringsuppgifter. Sådana uppgifter kan avslöja mycket känsliga detaljer om en persons privatliv, t.ex. sociala kontakter, politisk åskådning och uppgifter om någon hälsa. Att lagra sådana uppgifter har bedömts utgöra ett allvarligt intrång i den personliga integriteten. Generellt sett kan sägas att lagring av vissa uppgifter får ske under strikta krav på proportionalitet och nödvändighet.

De uppgifter som lagras inom ramen för PNR-systemet är inte av samma känsliga karaktär som trafik- och lokaliseringsuppgifter, vilket t.ex. påverkar bedömningen av om det är proportionerligt att använda uppgifter för mindre allvarliga brott. De principer som ställs upp i EU-domstolens avgöranden är emellertid giltiga i frågor som rör insamling, lagring och annan behandling av personuppgifter och vi har därför valt att redovisa några av dessa avgöranden nedan.

13.2 Digital Rights Ireland

I *Digital Rights*-målet[1] från 2014 ogiltigförklarade EU-domstolen det så kallade datalagringsdirektivet[2]. Huvudsyftet med direktivet var att harmonisera medlemsstaternas bestämmelser om de skyldigheter som leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät har att lagra vissa uppgifter som de genererat eller behandlat för att säkerställa att uppgifterna är tillgängliga för utredning, avslöjande och åtal av allvarliga brott, såsom brott med koppling till organiserad brottslighet eller terrorism.

Bland de uppgifter som lagras ingår en abonnents eller registrerad användares namn och adress, det uppringande telefonnumret, det uppringda telefonnumret och ip-adressen för internettjänster. Uppgifterna gör det i synnerhet möjligt att få kännedom om med vilken person en abonnent eller registrerad användare har kommunicerat och på vilket sätt, hur länge kommunikationen varat och från vilken plats kommunikationen har skett. De gör det dessutom möjligt att få kännedom om hur ofta abonnenten eller den registrerade användaren kommunicerat med vissa personer under en viss tidsperiod. Uppgifterna kan sammantagna göra det möjligt att dra mycket precisa slutsatser om personers privatliv, såsom deras vanor i vardagslivet, uppehållsorter och förflyttningar, aktiviteter de utövar samt deras umgängeskretsar.

För att fastställa om det skett ett ingrepp i den grundläggande rätten till respekt för privatlivet har det ingen betydelse om de uppgifter som avser privatlivet är av känslig art eller om de berörda har fått utstå eventuella olägenheter på grund av ingreppet. Att lagra uppgifter om en persons privatliv och kommunikationer utgör i sig ett ingrepp i de rättigheter som garanteras genom artikel 7 och 8 i EU-stadgan. De behöriga myndigheternas tillgång till uppgifterna utgör ytterligare ett ingrepp i dessa grundläggande rättigheter.

Varje begränsning av de rättigheter och friheter som erkänns i stadgan ska vara föreskriven i lag och förenlig med deras väsentliga innehåll. Begränsningar av dessa rättigheter och friheter får, med

[1] EU-domstolens dom den 8 april 2014, *Digital Rights Ireland Ltd mot Minister för Communications, Marine and Natural Resources m.fl.*, förenade målen nr C-293/12 och C-594/12.
[2] Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG.

beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller av behovet av skydd för andra människors rättigheter och friheter.

Bekämpandet av internationell terrorism i syfte att upprätthålla internationell fred och säkerhet utgör ett allmänt samhällsintresse som erkänns av unionen. Lagringen av de aktuella uppgifterna i syfte att eventuellt göra dem tillgängliga för behöriga nationella myndigheter svarar således mot ett mål av allmänt samhällsintresse. Det finns därmed anledning att kontrollera ingreppets proportionalitet.

Lagringen av uppgifter innebär att brottsbekämpande myndigheter får tillgång till ytterligare möjligheter att klara upp grova brott och de utgör i detta hänseende ett värdefullt verktyg i brottsutredningar. Lagringen av sådana kan därför anses vara ägnad att uppnå de eftersträvade målen. Ett sådant mål av allmänt samhällsintresse kan emellertid inte, trots dess grundläggande betydelse, i sig ensamt motivera att en sådan lagringsåtgärd ska anses vara nödvändig för att bekämpa grov brottslighet, organiserad brottslighet och terrorism. Skyddet av den grundläggande rätten till respekt för privatlivet kräver under alla omständigheter att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt. Unionslagstiftning måste därför förskriva tydliga och precisa bestämmelser som reglerar räckvidden och tillämpligheten av den aktuella åtgärden och som slår fast minimikrav, så att de berörda personerna har tillräckliga garantier som möjliggör ett effektivt skydd av deras personuppgifter mot riskerna för missbruk och otillåten tillgång eller användning. Sådana garantier är av än större betydelse när personuppgifterna är föremål för automatisk behandling och risken för otillåten tillgång till uppgifterna är stor.

Datalagringsdirektivet innebär att samtliga trafikuppgifter avseende fast och mobil telefoni, internetåtkomst, internetbaserad e-post och internettelefoni lagras. Direktivet omfattar således samtliga elektroniska kommunikationsmedel, vilkas användning är mycket utbredd och som är av växande betydelse i var och ens vardagsliv. Det omfattar dessutom samtliga abonnenter och registrerade användare. Direktivet medför således ett ingrepp i de grundläggande rättigheterna för nästintill hela Europas befolkning. Det görs alltså inte åtskillnader, begränsningar eller undantag utifrån syftet att bekämpa allvarliga brott. Direktivet gäller alltså även personer som inte ens indirekt be-

finner sig i en situation som kan föranleda lagföring. Syftet med direktivet är att bidra till bekämpandet av grov brottslighet, men det krävs inte något samband mellan de uppgifter som ska lagras enligt direktivet och ett hot mot den allmänna säkerheten.

Vidare innehåller direktivet inte de materiella och formella villkoren för behöriga myndigheters tillgång till uppgifterna och deras senare användning. Det framgår inte uttryckligen att tillgång till och senare användning av uppgifterna måste vara strängt begränsad till förebyggande och avslöjandet av noggrant avgränsade allvarliga brott eller till lagföringen av dessa brott. I synnerhet föreskrivs det inte heller något objektivt kriterium som gör det möjligt att begränsa antalet personer som är behöriga att få tillgång till och använda de lagrade uppgifterna till det antal som är strängt nödvändigt med hänsyn till det eftersträvade målet. Behöriga myndigheters tillgång till de lagrade uppgifterna är inte underkastad någon förhandskontroll utförd av en domstol eller en oberoende myndighet, vars beslut avser att begränsa tillgången till och användningen av uppgifterna till vad som är strängt nödvändigt för att uppnå det eftersträvade målet.

Ingreppet i de grundläggande rättigheterna enligt artikel 7 och 8 i EU-stadgan är långtgående och synnerligen allvarligt, utan att ingreppet är noggrant avgränsat genom bestämmelser som gör det möjligt att säkerställa att det verkligen är begränsat till vad som är strängt nödvändigt. Datalagringsdirektivet överskrider därmed de gränser som proportionalitetsprincipen ställer upp och är därför ogiltigt.

13.3 Tele2 Sverige och Watson m.fl.

De förenade målen *Tele2 Sverige* och *Watson m.fl.*[3] handlade också om datalagring i form av trafik- och lokaliseringsuppgifter avseende abonnenter och registrerade användare. Den nationella lagstiftningen föreskrev en generell och odifferentierad lagring av samtliga sådana uppgifter för samtliga abonnenter och registrerade användare avseende samtliga elektroniska kommunikationsmedel. Lagstiftningen ålade leverantörer av elektroniska kommunikationstjänster att systematiskt och kontinuerligt lagra dessa uppgifter, utan undantag. De uppgifter som leverantörerna var skyldiga att lagra är sådana som gör det möj-

[3] EU-domstolens dom den 21 december 2016, *Tele2 Sverige AB mot Post- och telestyrelsen* och *Secretary of State for the Home Department mot Watson m.fl.*, förenade målen nr C-203/15 och C-698/15.

ligt att spåra och identifiera en kommunikationskälla, identifiera målet för en kommunikation, identifiera kommunikationens datum, tidpunkt, varaktighet och typ, identifiera användarnas kommunikationsutrustning och identifiera lokalisering av mobil kommunikationsutrustning. Bland uppgifterna ingår abonnentens eller den registrerade användarens namn och adress, det uppringande telefonnumret, det uppringda numret och adressen för internettjänster.

EU-domstolen konstaterade att de uppgifter som lagras sammantaget kan göra det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter har lagrats, såsom deras vanor i vardagslivet, stadigvarande och tillfälliga uppehållsorter, dagliga förflyttningar och förflyttningar i övrigt, de aktiviteter de utövar, sociala relationer och de umgängeskretsar de rör sig i. Uppgifterna gör det alltså möjligt att kartlägga de berörda personerna på ett sätt som är lika känsligt ur integritetssynpunkt som själva innehållet i kommunikationerna.

Det ingrepp som en sådan lagstiftning utgör i de grundläggande rättigheterna enligt artikel 7 och 8 i EU-stadgan är långtgående och måste betraktas som synnerligen allvarligt. Den omständigheten att lagringen av uppgifterna och den senare användningen av dem sker utan att abonnenten eller den registrerade användaren är underrättad om detta kan ge de berörda personerna en känsla av att deras privatliv står under ständig övervakning. Även om lagstiftningen inte medger lagring av innehållet i kommunikationen, och därför inte kan kränka det väsentliga innehållet i dessa grundläggande rättigheter, skulle lagringen av trafik- och lokaliseringsuppgifter emellertid kunna inverka på användningen av elektroniska kommunikationsmedel och följaktligen på användarnas utövande av sin yttrandefrihet som garanteras i artikel 11 i stadgan.

Med hänsyn till det allvarliga ingreppet i de grundläggande rättigheterna som den nationella lagstiftningen utgör kan endast bekämpning av grov brottslighet motivera en sådan åtgärd. Även om syftet att bekämpa grov brottslighet är av allmänt samhällsintresse kan det emellertid inte, trots sin grundläggande betydelse, i sig ensamt motivera att en nationell lagstiftning som föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter ska anses nödvändig för detta ändamål. En sådan lagstiftning kräver inte något samband mellan de uppgifter som ska lagras och ett hot mot den allmänna säkerheten. Den är inte begränsad till lag-

ring av uppgifter avseende en viss tidsperiod, ett visst geografiskt område eller en viss krets av personer som på något sätt kan vara inblandade i ett allvarligt brott eller till personer beträffande vilka lagringen av uppgifter av andra skäl skulle kunna bidra till bekämpningen av brott. En sådan lagstiftning överskrider således gränserna för vad som är strängt nödvändigt och kan inte anses motiverad i ett demokratiskt samhälle.

Det finns däremot inte hinder för nationell lagstiftning som i förebyggande syfte tillåter en riktad lagring av trafik- och lokaliseringsuppgifter i syfte att bekämpa grov brottslighet, förutsatt att uppgifterna begränsas till vad som är strängt nödvändigt när det gäller vilka slags uppgifter som lagras, vilka kommunikationsmedel som avses, vilka personer som berörs och hur länge lagringen ska ske. För att uppfylla dessa krav måste lagstiftningen föreskriva tydliga och precisa bestämmelser som reglerar omfattningen och tillämpligheten av en sådan lagringsåtgärd och som slår fast minimikrav, så att de personer vars uppgifter har lagrats har tillräckliga garantier som möjliggör ett effektivt skydd av deras personuppgifter mot riskerna för missbruk. Vidare måste lagringen av uppgifterna alltid uppfylla objektiva kriterier som fastställer ett samband mellan de uppgifter som lagras och det eftersträvade syftet. I synnerhet måste villkoren vara sådana att de klart avgränsar åtgärdens omfattning och följaktligen den berörda personkretsen.

När det gäller avgränsningen av en åtgärd beträffande den personkrets och de situationer som kan komma att beröras anger domstolen att den nationella lagstiftningen ska grunda sig på objektiva omständigheter som kan avslöja en, åtminstone indirekt, koppling till grov brottslighet, på ett eller annat sätt bidra till att bekämpa grov brottslighet eller förhindra en allvarlig risk för den allmänna säkerheten.

Allmän tillgång till samtliga lagrade uppgifter, oberoende av om det finns någon koppling till det eftersträvade syftet är inte begränsat till vad som är strängt nödvändigt. Tillgång kan i princip bara beviljas i samband med bekämpning av brott och ska begränsas till uppgifter om personer som misstänks planera, begå eller ha begått ett allvarligt brott eller på något sätt vara inblandade i ett sådant brott. I särskilda fall, när vitala intressen för nationell säkerhet, försvar eller allmän säkerhet hotas av terrorism, skulle dock tillgång kunna ges även till uppgifter om andra personer när det finns objektiva omständigheter

som ger skäl att anta att de uppgifterna i ett konkret fall effektivt skulle kunna bidra till att bekämpa terrorism.

För att säkerställa att dessa villkor uppfylls fullt ut i praktiken är det väsentligt att behöriga nationella myndigheters tillgång till de lagrade uppgifterna i princip, utom i vederbörligen motiverade brådskande fall, är underkastad förhandskontroll av en domstol eller en oberoende myndighet och att domstolen meddelar sitt avgörande eller myndigheten fattar sitt beslut efter det att de behöriga myndigheterna har framställt en motiverad ansökan. Det krävs även att de behöriga myndigheterna som beviljats tillgång till lagrade uppgifter informerar de berörda personerna om detta, så snart en sådan upplysning inte längre riskerar att skada myndigheternas utredningar. Sådan information är nödvändig för att dessa personer ska kunna utöva sin rätt till rättslig prövning vid kränkning av deras rättigheter.

13.4 La Quadrature du Net

I målet *La Quadrature du Net* från 2020[4] uttalade sig EU-domstolen om datalagring och skydd för privatliv och personuppgifter. Enligt domstolen utgör EU-rätten, särskilt i form av EU-stadgan, hinder för nationell lagstiftning som kräver en generell och odifferentierad överföring eller lagring av trafik- och lokaliseringsuppgifter. Undantag från detta kan endast göras om det finns ett allvarligt hot mot den nationella säkerheten. Även under sådana omständigheter måste åtgärderna vara strikt nödvändiga och tidsbegränsade. Därutöver måste intrånget i de grundläggande rättigheterna vara proportionerligt i förhållande till det allmänna samhällsintresse som eftersträvas. Hänsyn ska alltså tas till hur allvarligt ingreppet är i de grundläggande rättigheterna och betydelsen av det mål av allmänt samhällsintresse som eftersträvas med begränsningen.

För att kravet på proportionalitet ska vara uppfyllt måste det i lagstiftning föreskrivas klara och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden. Det ska även anges minimikrav, så att de personer vars personuppgifter berörs har tillräckliga garantier för att uppgifterna på ett effektivt sätt är skyddade mot riskerna för missbruk. Lagstiftningen ska vara bindande

[4] EU-domstolens dom den 6 oktober 2020, *La Quadrature du Net m.fl. mot Premier ministre m.fl.*, förenade målen nr C-511/18, C-512/18 och C-520/18.

enligt nationell rätt och i synnerhet ange under vilka omständigheter och på vilka villkor en åtgärd avseende behandling av sådana uppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strikt nödvändigt. Behovet av sådana garantier är särskilt stort när personuppgifter är föremål för automatiserad behandling, särskilt när det föreligger en betydande risk för otillåten åtkomst till uppgifterna.

EU-domstolen uttalar vidare att omständigheten att en åtgärd har vidtagits för att skydda nationell säkerhet inte, trots att det ankommer på medlemsstaterna att definiera sina väsentliga säkerhetsintressen och att vidta de åtgärder som är nödvändiga för att säkerställa inre och yttre säkerhet, kan leda till att unionsrätten inte är tillämplig och befria medlemsstaterna från skyldigheten att iaktta unionsrätten.

I princip finns det inte hinder för en nationell lagstiftning som ger behöriga myndigheter rätt att ålägga leverantörer av elektroniska kommunikationstjänster att lagra trafik- och lokaliseringsuppgifter för samtliga användare av elektroniska kommunikationer under en begränsad tid, såvida det föreligger tillräckligt konkreta omständigheter för att anse att den berörda medlemsstaten står inför ett verkligt och aktuellt eller förutsebart hot mot nationell säkerhet. Förekomsten av ett sådant hot är ägnat att styrka att det finns ett samband mellan samtliga användare av elektroniska kommunikationer och hotet mot den nationella säkerheten.

Åläggandet att i förebyggande syfta lagra uppgifter som avser samtliga användare måste emellertid vara tidsmässigt begränsat till vad som är strängt nödvändigt. Om hotet kvarstår kan åläggandet för leverantörer förlängas, men varje åläggande får inte överskrida en förutsebar tidsrymd. En sådan lagring måste vara föremål för begränsningar och åtföljas av strikta garantier för att på ett effektivt sätt skydda de berördas personuppgifter från riskerna för missbruk. Lagringen får således inte vara systematisk.

Ett beslut om en generell och odifferentierad åtgärd för lagring av uppgifter måste kunna bli föremål för effektiv kontroll av en domstol eller en oberoende myndighet, vars avgörande har bindande verkan. Kontrollen ska ske i syfte att kontrollera om det föreligger ett hot mot den nationella säkerheten och att de villkor och garantier som måste ställas upp är uppfyllda.

När det gäller målet att förebygga, undersöka, avslöja och lagföra brott är det, i enlighet med proportionalitetsprincipen, endast bekämpning av grov brottslighet och förebyggande av allvarliga hot

mot allmän säkerhet som kan motivera allvarliga ingrepp i de grundläggande rättigheter som anges i artikel 7 och 8 i EU-stadgan. Endast ingrepp som inte är av allvarligt slag kan motiveras av målet att förebygga, undersöka, avslöja och lagföra brott i allmänhet.

13.5 Privacy International

I likhet med *La Quadrature du Net* handlade *Privacy International*[5] om behandling av trafik- och lokaliseringsuppgifter i syfte att skydda nationell säkerhet. Den inledande frågan i målet var om e-dataskyddsdirektivet[6] ska tolkas så att direktivets tillämpningsområde omfattar en nationell lagstiftning som ger en statlig myndighet rätt att ålägga leverantörer av elektroniska kommunikationstjänster att överföra trafik- och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna i syfte att skydda nationell säkerhet.

EU-domstolen uttalade att direktivet utesluter vissa av statens verksamheter, bl.a. på straffrättens område och verksamheter som avser allmän säkerhet, försvar och statens säkerhet. Sådana verksamheter kan endast bedrivas av staten eller statliga myndigheter och inte av enskilda. Eftersom det i direktivet anges att det ska tillämpas på behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom unionen, inbegripet allmänna kommunikationsnät som stöder datainsamling och identifieringsutrustning. Direktivet ska därför anses reglera verksamheten för leverantörer av sådana tjänster. Utlämnande av personuppgifter genom överföring, liksom lagring eller tillhandahållande på annat sätt av personuppgifter, utgör behandling i den mening som avses i direktivet och omfattas följaktligen av direktivets tillämpningsområde.

Enligt domstolens fasta praxis kan den omständigheten att en åtgärd har vidtagits för att skydda nationell säkerhet inte, trots att det ankommer på medlemsstaterna att definiera sina väsentliga säkerhetsintressen och att vidta de åtgärder som är nödvändiga för att säker-

[5] EU-domstolens dom den 6 oktober 2020, *Privacy International mot Secretary of State for Foreign and Commonwealth Affairs m.fl.*, mål nr C-623/17.
[6] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).

ställa inre och yttre säkerhet, leda till att unionsrätten inte är tillämplig och befria medlemsstaterna från skyldigheten att iaktta unionsrätten.

När medlemsstater däremot direkt genomför åtgärder som innebär undantag från konfidentialiteten vid elektronisk kommunikation, utan att ålägga tjänsteleverantörer av sådan kommunikation någon skyldighet att behandla uppgifter, omfattas skyddet av de berörda personernas uppgifter inte av direktivet, utan enbart av nationell rätt, med förbehåll för tillämpningen av dataskyddsdirektivet.

Den andra frågan som domstolen uttalade sig om var om EU-rätten utgör hinder för en nationell lagstiftning som ger en statlig myndighet rätt att ålägga leverantörer av elektroniska kommunikationstjänster att på ett generellt och odifferentierat sätt överföra trafikuppgifter och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna i syfte att skydda nationell säkerhet. Uppgifterna rör bl.a. namn, adress, telefonnummer och uppringt nummer. Utlämnandet av uppgifter genom överföring avser samtliga användare av elektroniska kommunikationsmedel, utan att det preciseras om överföringen ska ske i realtid eller i efterhand. När uppgifterna väl har överförts lagras de av säkerhets- och underrättelsetjänsterna och förblir tillgängliga för dem i deras verksamhet, i likhet med andra databaser som de har. I synnerhet kan uppgifter som samlas in på detta sätt och som är föremål för icke-konkret och automatiserad behandling och analys korskontrolleras mot andra databaser som innehåller olika kategorier av mängddata om personuppgifter eller lämnas ut utanför säkerhets- och underrättelsetjänsterna och till tredjeländer. Åtgärderna kräver inte förhandstillstånd från en domstol eller en oberoende förvaltningsmyndighet och de föranleder inte heller någon information till berörda personer.

Genom att anta e-dataskyddsdirektivet har unionslagstiftaren konkretiserat de rättigheter som är stadfästa i artikel 7 och 8 i EU:s rättighetsstadga, vilket innebär att användarna av elektroniska kommunikationsmedel i princip har rätt att förvänta sig att deras kommunikationer och därmed förbundna uppgifter förblir anonyma och inte kan registreras, såvida de inte har samtyckt till detta.

Direktivet medger emellertid en möjlighet att göra undantag från den principiella skyldigheten att garantera konfidentialiteten för personuppgifter när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för att skydda nationell säkerhet, försvaret och allmän säkerhet samt för förebyggande, undersök-

ning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem. Medlemsstaterna får för detta ändamål bland annat vidta lagstiftningsåtgärder som innebär att uppgifter får bevaras under en begränsad period när det är motiverat av ett av dessa skäl.

Utöver artikel 7 och 8 aktualiseras även artikel 11 i stadgan, som fastställer rätten till yttrandefrihet. Dessa rättigheter är emellertid inte absoluta, utan måste bedömas utifrån deras funktion i samhället. Det är enligt artikel 52.1 i stadgan tillåtet att begränsa utövandet av rättigheterna, under förutsättning att begränsningarna föreskrivs i lag, att de är förenliga med det väsentliga innehållet i dessa rättigheter och att de, med beaktande av proportionalitetsprincipen, är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller mot behovet av skydd för andra människors rättigheter och friheter. Undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt.

För att kravet på proportionalitet ska vara uppfyllt måste det i lagstiftning föreskrivas klara och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt anges minimikrav, så att de personer vars personuppgifter berörs har tillräckliga garantier för att uppgifterna på ett effektivt sätt är skyddade mot riskerna för missbruk. Denna lagstiftning ska vara rättsligt bindande enligt nationell rätt och i synnerhet ange under vilka omständigheter och på vilka villkor en åtgärd avseende behandling av sådana uppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strängt nödvändigt. Behovet av sådana garantier är särskilt stort när personuppgifter är föremål för automatiserad behandling, särskilt när det föreligger en betydande risk för otillåten åtkomst till uppgifterna. Dessa överväganden äger särskild giltighet när det är fråga om skyddet av den särskilda kategori av personuppgifter som utgörs av känsliga uppgifter.

Överföringen av trafik- och lokaliseringsuppgifter till tredje man utgör ett ingrepp i de grundläggande rättigheter som stadfästs i artikel 7 och 8 i stadgan, oavsett hur uppgifterna senare används. Det saknas betydelse om uppgifterna som avser privatlivet är av känslig art eller om de berörda har fått utstå eventuella olägenheter på grund av ingreppet. Det ingrepp som överföringen utgör måste betraktas som synnerligen allvarligt, bland annat med hänsyn till att den information som uppgifterna kan innehålla är känslig och i synnerhet till

att det utifrån uppgifterna är möjligt att kartlägga de berörda personerna, då sådan information är lika känslig som själva innehållet i kommunikationerna. Det kan dessutom ge de berörda personerna en känsla av att deras privatliv står under ständig bevakning. Med hänsyn till den stora mängden trafik- och lokaliseringsuppgifter som kan bli föremål för fortlöpande lagring medför omständigheten att leverantörer av elektroniska kommunikationstjänster lagrar dessa uppgifter i sig en risk för missbruk och olovlig åtkomst.

Eftersom en heltäckande tillgång till samtliga lagrade uppgifter, oberoende av om det finns någon koppling, ens indirekt, till det eftersträvade syftet, inte kan anses vara begränsad till vad som är strängt nödvändigt, måste en nationell lagstiftning som reglerar tillgång till trafik- och lokaliseringsuppgifter vara grundad på objektiva kriterier som avgör under vilka omständigheter och på vilka villkor behöriga nationella myndigheter ska ges tillgång till uppgifterna.

Överföringen av uppgifter sker på ett generellt och odifferentierat sätt och berör därför på ett allomfattande sätt samtliga personer som använder elektroniska kommunikationstjänster. Den är således även tillämplig på personer för vilka det inte finns något indicium som ger anledning att tro att deras beteende skulle kunna ha ett samband, inte ens indirekt eller avlägset, med målet att skydda den nationella säkerheten och, i synnerhet, utan att det har visats att det finns ett samband mellan de uppgifter som ska överföras och ett hot mot den nationella säkerheten.

En nationell lagstiftning som ålägger leverantörer av elektroniska kommunikationstjänster att genom generell och odifferentierad överföring lämnat ut trafik- och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna går således utöver vad som är strängt nödvändigt och kan inte anses vara motiverad i ett demokratiskt samhälle.

14 Central databas för passageraruppgifter

14.1 Inledning

När det gäller frågan om förbättring av brottsbekämpande myndigheters möjlighet att ta del av passageraruppgifter från andra transportmedel än flyg faller det sig naturligt att undersöka möjligheten att upprätta ett liknande system som för flygtrafiken. Ett sådant system innebär att vissa transportföretag åläggs en skyldighet att översända passagerarinformation till en central nod, där informationen läggs in i en databas. Ett antal behöriga myndigheter kan sedan begära tillgång till uppgifterna från den myndighet, eller enhet inom en myndighet, som administrerar den centrala databasen.

Det finns flera alternativ för hur ett sådant system kan se ut. Ett alternativ är att använda den befintliga databasen som används för flygtrafik vid enheten för passagerarinformation. Andra alternativ inkluderar att upprätta en separat databas vid enheten, eller att upprätta en ny databas vid en helt annan myndighet. De olika alternativen för med sig både för- och nackdelar och kräver olika mycket resurser och administration. Vår föresats är att analysera de olika alternativen och de konsekvenser som dessa medför.

14.2 Befintlig databas vid enheten för passagerarinformation

Vid enheten för passagerarinformation finns en befintlig databas som används för PNR-uppgifter från lufttrafikföretag. Ett potentiellt tillvägagångssätt för att förbättra tillgången till passageraruppgifter från andra transportslag för brottsbekämpande myndigheter är att uppgifterna översänds till enheten för passagerarinformation och lagras

i PNR-systemets databas. På så sätt görs regleringen av användandet av passageraruppgifter trafikslagsneutral.

Vid enheten för passagerarinformation finns ett etablerat system och relevant kompetens och erfarenhet samt den it-infrastruktur som krävs. Att lägga till andra transportslag i det befintliga systemet är det enklaste och minst kostsamma sättet att samla passagerarinformation i en central databas.

Om passageraruppgifter från övriga transportslag med denna lösning lagras tillsammans med PNR-uppgifter från flyget medför det vissa konsekvenser. Regelverket som gäller för PNR-systemet, dvs. den generella EU-rättsliga regleringen, PNR-direktivet och lagen om flygpassageraruppgifter i brottsbekämpningen, kommer att gälla även för de uppgifter som samlas in avseende andra transportslag. Vid tillämpning av de grundläggande rättigheterna enligt artikel 7 och 8 i EU:s rättighetsstadga gör det ingen skillnad om uppgifterna kommer från flygtrafik eller något annat transportmedel. Detta gäller emellertid för samtliga förslag som innebär att transportörerna åläggs att överföra alla passageraruppgifter, om än i något varierande grad.

PNR-direktivet och PNR-domen begränsar exempelvis vilka ändamål som uppgifterna hos enheten för passagerarinformation får användas för. Uppräkningen i artikel 1.2 i direktivet av tillåtna ändamål för behandling av PNR-uppgifter är uttömmande, vilket innebär att PNR-uppgifter som samlas in i enlighet med direktivet endast får behandlas i syfte att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet i enlighet med artikel 6.2 a, b och c. De passageraruppgifter som samlas in från andra transportslag än flyg samlas förvisso inte in i enlighet med direktivet, men bevaras i samma databas som uppgifterna från flygtrafik. Enligt PNR-domen innebär den uttömmande karaktären av de ändamål som avses i artikel 1.2 i direktivet även att PNR-uppgifter inte får lagras i en enda databas som kan användas för såväl dessa som andra ändamål. Anledningen till detta är att sådan lagring skulle innebära en risk för att uppgifterna används för andra ändamål än de som direktivet tillåter.

Att uppräkningen av de tillåtna ändamålen för behandling av PNR-uppgifter är uttömmande medför begränsningar för den generella brottsbekämpningen. PNR-direktivets bilaga II innehåller en uppräkning av vilka brott som omfattas av direktivets begrepp *grov brottslighet*. Utöver att räknas upp i bilaga II krävs det enligt artikel 3.9 i direktivet att brottet ska bestraffas med fängelse eller annan frihets-

berövande åtgärd i minst tre år enligt medlemsstatens nationella rätt. PNR-uppgifterna får således inte behandlas i syfte att bekämpa andra brott än de som uppfyller kriterierna i direktivet. Om passageraruppgifter från andra transportslag bevaras i samma databas som PNR-uppgifterna medför det att motsvarande ändamålsbegränsning kommer att gälla även för sådana passageraruppgifter. Denna begränsning är något som talar emot att passageraruppgifter från andra transportslag än flyg lagras i PNR-databasen.

Att ändamålen i PNR-direktivet är uttömmande påverkar även möjligheten för behöriga myndigheter att begära information rörande annan brottslighet med koppling till nationell säkerhet, i de fall de specifika brotten inte omfattas av direktivet. Med hänsyn till PNR-domen behöver den svenska lagstiftningen dock förhålla sig till detta. För att en nationell reglering avseende andra trafikslag inte ska omfattas av PNR-direktivets ändamålsbegränsning krävs det alltså en separat databas för en sådan insamling.

Det kan vidare konstateras att direktivet uppställer en snävare begränsning av vilka brott som får bekämpas genom behandling av PNR-uppgifter än den lagstiftning som finns för passageraruppgifter från andra trafikslag i dag, bl.a. eftersom insamlingen genom PNR-lagstiftningen per definition är mer omfattande. De brottsbekämpande myndigheterna har med befintlig lagstiftning olika möjligheter att använda passageraruppgifter i brottsbekämpningen. Denna inhämtning innebär att myndigheter kan begära in passageraruppgifter medan PNR-lagstiftningen ålägger transportörerna att föra över alla passageraruppgifter. Inhämtning inom ramen för PNR-systemet blir därmed mer heltäckande än inhämtning via polislagen och tullbefogenhetslagen. En nackdel med en sådan lösning är att PNR-lagstiftningen inte tillåter att andra än enheten för passagerarinformation har direkt tillgång till PNR-uppgifterna. För att andra myndigheter ska få tillgång till uppgifterna behöver de bemanna enheten med egen personal, koppla relevanta databaser till systemet enligt 3 kap. 4 § 1 eller begära tillgång till uppgifter enligt 3 kap. 4 § 2 lagen om flygpassageraruppgifter i brottsbekämpningen. Det finns därför ett behov av att komplettera ett trafikslagsneutralt PNR-system med ytterligare möjligheter för att använda passageraruppgifter i sin verksamhet.

Polislagen ger genom 25 § möjlighet för Polismyndigheten och Säkerhetspolisen att begära uppgifter om ankommande och avgående transporter från transportföretag. Polismyndigheten får begära sådana

uppgifter endast om de kan antas ha betydelse för den brottsbekämpande verksamheten. Det finns alltså ingen begränsning avseende vilken typ av brottslighet som det rör sig om, även om det inte bör komma i fråga att begära uppgifter för att bekämpa rena bagatellbrott. Tillämpningsområdet för 25 § polislagen för andra trafikslag än flyg, vilka inte påverkas av PNR-direktivet, är i det avseendet således större än vad som gäller för uppgifter som samlas in i enlighet PNR-direktivet.

Tullverkets möjligheter att begära in uppgifter från transportbolag regleras i 7 kap. 12 § tullbefogenhetslagen. Där anges att Tullverket får begära att ett transportföretag, som befordrar varor, passagerare eller fordon till eller från Sverige, lämnar uppgifter om ankommande eller avgående transporter som företaget har tillgång till, om uppgifterna kan antas ha betydelse för Tullverkets brottsbekämpande verksamhet. I 2 kap. 10 § Tullverkets brottsdatalag regleras för vilka närmare preciserade ändamål som Tullverket får samla in bokningsuppgifter och möjligheten att vidareanvända insamlade uppgifter för andra ändamål. Tullverket har dock rätt att använda bokningsuppgifter för att bekämpa samtliga brott som omfattas av Tullverkets brottskatalog. Tullverkets uppdrag och de brottstyper som omfattas av brottskatalogen förutsätter att uppgifter om varor och transportmedel samlas in, tillsammans med passageraruppgifter.

Enligt såväl polislagen som tullbefogenhetslagen finns en möjlighet att begära in uppgifter om varor och fordon. För de brottsbekämpande myndigheternas del är det helt nödvändigt att kunna koppla samman uppgifter om resande med deras varor och fordon. Alla dessa uppgifter kommer inte att ingå i en central databas vid enheten för passagerarinformation. Därmed kan en sådan databas inte fullt ut tillgodose myndigheternas behov av bokningsuppgifter. Det är därför centralt för deras verksamhet att möjligheterna att samla in bokningsuppgifter med stöd av tullbefogenhetslagen och polislagen kvarstår även för det fall att PNR-lagstiftningen görs trafikslagsneutral och PNR-uppgifter från fler trafikslag samlas i en central databas vid enheten för passagerarinformation.

PNR-domen innebär även vissa andra begränsningar av behandlingen av PNR-uppgifter som har redovisats i avsnitt 7 och 8. Det gäller t.ex. resor inom EU (avsnitt 8.2) och lagringstiden för PNR-uppgifter (avsnitt 8.7). Dessa begränsningar gör sig även gällande för andra passageraruppgifter som lagras i samma databas. För flyg-

trafiken utgör cirka 65 procent av flygningarna till eller från Sverige resor inom EU. För övriga trafikslag torde den andelen vara betydligt högre. Som exempel kan nämnas att det under åren 2015–2022 företogs cirka 177 000 passagerarresor till eller från Sverige med sjötransport, exklusive kryssningar, och av dessa var det endast fem procent som avsåg resor utom EU.[1]

Hur stor påverkan detta har i praktiken beror på hur stor andel av resorna som enheten för passagerarinformation får tillämpa PNR-systemet på. I en situation där terrorhotnivån berättigar till insamlande av passageraruppgifter från samtliga resor inom EU blir distinktionen mellan resor inom eller utom EU mindre avgörande. I avsaknad av ett verkligt och aktuellt eller förutsebart terrorhot ska det emellertid göras ett urval av resor, vilket, beroende på hur stort urvalet är, kan ha varierande påverkan på brottsbekämpningen. Ett sådant urval inom ramen för PNR-lagstiftningen kan potentiellt sett resultera i att alla resor omfattas av insamlingen av uppgifter.

Vissa administrativa åtgärder som krävs i PNR-systemet kommer att omfatta även de uppgifter som härrör från andra transportslag än flygtrafik. Ett beslut om att samla in och behandla passageraruppgifter från samtliga resor inom EU ska kunna bli föremål för en effektiv kontroll av en domstol eller en oberoende förvaltningsmyndighet. Detta har beskrivits i avsnitt 8.3. Att även passageraruppgifter från andra transportslag än flygtrafik ingår i databasen innebär emellertid ingen ytterligare arbetsbörda och det förändrar inte sakfrågan avseende en sådan prövning, dvs. om det finns ett verkligt och aktuellt eller förutsebart terrorhot mot Sverige.

En begäran om tillgång till PNR-uppgifter kommer precis som i det befintliga PNR-systemet för flygtrafik att behöva prövas genom en förhandskontroll i enlighet med våra förslag i avsnitt 8.5. Om en förundersökning pågår ska en begäran från en behörig myndighet om att få tillgång till PNR-uppgifter prövas av allmän domstol och i andra fall ska beslutet fattas av åklagare. Med fler trafikslag anslutna till PNR-systemet kommer sannolikt antalet sådana prövningar att öka.

En fördel med att föra in passageraruppgifter från andra trafikslag i den befintliga databasen är att mer data leder till mer effektiv brotts-

[1] Europeiska kommissionen: Generaldirektoratet för migration och inrikes frågor, BearingPoint, ICF och Unisys, *Study on harmonising reporting obligations of travel data on maritime transport, with a view to use such data for law enforcement purposes – Final Report*, november 2024, s. 8.

bekämpning. Det går att göra både djupare och bredare analyser med större datamängder. Ett sätt för kriminella att undvika upptäckt vid resande är så kallad *broken travel*, vilket innebär att en person på vägen till den slutliga destinationen reser med flera olika transportmedel. Med passageraruppgifter från fler trafikslag ökar möjligheterna att kartlägga en individs resväg markant. Det ökar också effektiviteten i regelsökningar om flera trafikslag integreras, dvs. sökningar som inte är baserade specifika individer utan i stället på resmönster som indikerar att en person kan vara av intresse för brottsbekämpande myndigheter. Det skulle t.ex. gå att uppmärksamma resenärer som vid vissa tider åker en viss sträcka med tåg för att sedan byta färdmedel och åka en viss sträcka med flyg.

En annan fördel med en trafikslagsneutral PNR-lagstiftning är att det fortsatt är kopplat till samma system som finns på internationell nivå, men för fler trafikslag. Om Sverige t.ex. inkluderar buss, tåg och färja i PNR-lagstiftningen går det att använda samma kanaler som i dag för att lägga bevakningar eller historiska sökningar från övriga EU-länder och tredjeländer som samlar in passageraruppgifter från fler trafikslag genom sin nationella lagstiftning. Ett sådant utbyte av uppgifter med andra länder är till gagn för brottsbekämpningen i Sverige, samtidigt som det stärker brottsbekämpningen globalt.

På sikt ska PNR-uppgifter som samlas in i enlighet med PNR-direktivet inte längre överföras till medlemsstaternas respektive enhet för passagerarinformation, utan i stället överföras till den router som administreras av eu-Lisa i enlighet med de nya API-förordningarna. PNR-uppgifterna kommer därefter under vissa förutsättningar föras över till enheten för passagerarinformation. Enheten kommer således även på sikt, efter att routern har tagits i bruk, ha kvar funktionen att lagra PNR-uppgifter i Sverige.

Sammanfattningsvis kan sägas att en modell där passagerarinformation från andra transportslag lagras i samma databas som PNR-uppgifter från flyget är den enklaste och minst kostsamma att genomföra, men att den också medför vissa begränsningar som har beskrivits ovan. Även om det är den minst kostsamma lösningen för ett centralt system för insamling kommer det krävas resurser och ta tid att förbereda insamlingen och upprätta kontakt och samarbete med trafikföretag. Det kan även krävas informationsinsatser och resurser för att svara på löpande frågor från de trafikföretag som åläggs en skyl-

dighet att överföra uppgifter. Detta gäller dock för ett sådant system oavsett vilken myndighet som ansvarar för databasen.

14.3 Separat databas vid enheten för passagerarinformation

En separat databas vid enheten för passagerarinformation dit passageraruppgifter från andra transportslag än flygtrafik översänds och lagras medför vissa skillnader gentemot en gemensam databas. Ett sådant system regleras inte av PNR-direktivet och vissa av de begränsningar som beskrivits ovan av PNR-systemet innebär gör sig inte gällande för en separat databas.

Eftersom databasen inte är upprättad i enlighet med, och därmed inte heller regleras av, PNR-direktivet finns det en större frihet att bestämma syftet med behandlingen av uppgifter i databasen. Ett av syftena kommer att vara att bekämpa terrorism och annan brottslighet. Med en separat databas har Sverige även möjlighet att bestämma att uppgifterna får användas i verksamhet som generellt rör nationell säkerhet, och inte bara sådan verksamhet som faller inom PNR-direktivets ändamålsbegränsning. Det innebär en förbättring av möjligheterna att använda passageraruppgifter från andra transportslag i verksamhet som rör nationell säkerhet jämfört med de ändamålsbegränsningar som följer av PNR-domen.

Ett grundläggande syfte med att inrätta en central databas med passageraruppgifter är att bekämpa terrorism och annan brottslighet. På detta område finns det reglering på EU-nivå i form av dataskyddsdirektivet, som ger verkan åt den grundläggande rätt till skydd för personuppgifter som fastställs i artikel 8 i EU:s rättighetsstadga i samband med behandling av personuppgifter som utförs av brottsbekämpande myndigheter. EU har således kompetens på området och den EU-rättsliga regleringen, i synnerhet EU:s rättighetsstadga, och EU-domstolens uttalanden måste beaktas.

Insamling av passageraruppgifter för andra trafikslag bär flera likheter med PNR-systemet för flygtrafik. De uppgifter som kommer att samlas in har samma karaktär som PNR-uppgifterna från flygtrafiken, även om de senare i många fall är mer omfattande än de uppgifter som kommer vara möjliga att samla in från andra trafikslag. Utgångspunkten är att insamlingen, i likhet med flygtrafiken, gäller

för samtliga gränsöverskridande resor som företas med utvalda trafikslag. Ändamålen med systemet är desamma som de som anges i PNR-direktivet, med tillägget att uppgifterna även får tillhandahållas till verksamhet som rör nationell säkerhet, utan ändamålsbegränsningen som direktivet fastställer. Skillnaderna mellan ett sådant system och PNR-systemet för flygtrafik kommer således att vara mycket små.

Vid tillämpningen av artikel 7 och 8 i EU:s rättighetsstadga har det ingen betydelse om de aktuella uppgifterna kommer från flygtrafik eller annan trafik. Det innebär exempelvis att uttalandena i PNR-domen, som har sin grund i stadgan, har bäring på lagringen och annan behandling av personuppgifter i databasen. De begränsningar som stadgan ställer upp, och vars tolkning framgår i PNR-domen, avseende resor inom EU och lagringstiden gäller även behandlingen av uppgifter i en separat databas vid enheten för passagerarinformation. Det gäller övriga konsekvenser avseende prövning av beslut om att samla in och behandla passageraruppgifter från samtliga flygningar inom EU samt förhandskontrollen vid en begäran om tillgång till passageraruppgifter.

Att ha en parallell databas medför större kostnader än att använda en redan befintlig databas. I likhet med att använda den befintliga databasen finns emellertid redan den kompetens, kunskap och it-infrastruktur som behövs vid enheten för passagerarinformation, vilket t.ex. innebär att behovet av fortbildning i ett inledande skede bör vara begränsad.

Tillgång till mer data innebär bättre förutsättningar för att bekämpa brott. Även om passageraruppgifterna för flygtrafik respektive andra trafikslag lagras i olika databaser bör det gå att kombinera uppgifter från de olika trafikslagen för att göra den analys som krävs. Det bör även vara tekniskt möjligt att göra regelsökningar som kombinerar flygtrafiken och något annat trafikslag. Sammantaget är en parallell databas för insamling av samtliga passageraruppgifter från andra trafikslag en mer kostsam lösning än att använda den befintliga PNR-databasen, samtidigt som det generellt sett innebär en påtaglig förbättring vad gäller tillgången till data jämfört med nuläget.

14.4 Databas vid annan myndighet

Att upprätta en databas för passageraruppgifter från andra trafikslag än flyg vid en annan myndighet än Polismyndighetens enhet för passagerarinformation innebär ett betydligt större projekt än att använda enhetens befintliga databas eller upprätta en ny databas inom enheten. Det kräver mer resurser och skulle ta betydligt längre tid än de tidigare beskrivna lösningarna. Även om det går att dra lärdom av enheten för passagerarinformations erfarenheter innebär en sådan lösning påtagligt större utmaningar än att använda den befintliga databasen eller en separat databas vid enheten för passagerarinformation. Under utredningen har två myndigheter identifierats som potentiellt kan ansvara för en sådan databas: Säkerhetspolisen och Tullverket.

14.4.1 Databas hos Säkerhetspolisen

Ett syfte med att upprätta en databas vid en annan myndighet är att kunna lagra passageraruppgifterna endast med ändamålet att främja nationell säkerhet och Säkerhetspolisen framstår som lämpligast att ansvara för en sådan databas. Eftersom medlemsstaterna enligt artikel 4.2 i Fördraget om Europeiska unionen har exklusiv kompetens avseende den nationella säkerheten skulle en sådan ordning till synes innebära att EU-rätten inte är tillämplig på behandlingen av uppgifter i databasen. Det skulle exempelvis kunna medföra en större frihet att lagra uppgifterna under längre tid än vad som tillåts inom PNR-systemet. Det finns dock flera problem med en sådan utgångspunkt.

Avsikten är att uppgifterna i databasen, även om det uttryckliga syftet med dem är att de ska användas i verksamhet som rör nationell säkerhet, även ska kunna begäras ut av andra myndigheter för att användas i brottsbekämpande syfte. Om ett sådant system införs får det betraktas som att syftet med behandlingen av uppgifterna i databasen även är brottsbekämpning som inte rör nationell säkerhet. I och med det blir det EU-rättsliga regelverket till stora delar tillämpligt och de begränsningar som nämnts ovan gör sig gällande även med denna lösning. EU:s rättighetsstadga och PNR-domens uttalanden om t.ex. resor inom EU och lagringstiden för uppgifterna kommer att gälla för de uppgifter som bevaras i databasen. Med en sådan lösning faller således de eftersträvade fördelarna med systemet ur ett brottsbekämpande och säkerhetsmässigt perspektiv bort.

Frågan om EU:s kompetens inom området nationell säkerhet har varit föremål för flera avgöranden från EU-domstolen. Några av dessa har beskrivits i avsnitt 13. I målet *La Quadrature du Net* uttalar domstolen att omständigheten att en åtgärd har vidtagits för att skydda nationell säkerhet inte innebär att unionsrätten inte är tillämplig och befriar medlemsstaterna från skyldigheten att iaktta unionsrätten, trots att det ankommer på medlemsstaterna att definiera sina väsentliga säkerhetsintressen och vidta de åtgärder som är nödvändiga för att säkerställa inre och yttre säkerhet.

Detta innebär att även om uppgifterna i databasen faktiskt bara skulle användas i syfte att främja nationell säkerhet, av myndigheter som har i uppdrag att bedriva sådan verksamhet, så kommer EU-rättsliga regleringar av behandlingen av personuppgifter att vara tillämpliga på ett sådant system. Det löser inte heller frågan om hur passageraruppgifter på ett bättre sätt kan användas för den generella brottsbekämpningen. En lösning med ett parallellt system, med en databas vid en annan myndighet än där personuppgifterna behandlas i brottsbekämpande syfte, framstår inte som eftersträvansvärt.

Sammantaget innebär en lösning med en central databas vid Säkerhetspolisen ett mycket resurs- och tidskrävande projekt. Det är vidare tveksamt om det medför några påtagliga fördelar jämfört med de tidigare redovisade alternativen med den befintliga eller en separat databas vid enheten för passagerarinformation. Mot bakgrund av detta anser vi inte att det är en lämplig lösning att upprätta ett system med en databas hos Säkerhetspolisen i syfte att användas i verksamhet som rör nationell säkerhet samt för att bekämpa terrorism och annan allvarlig brottslighet.

14.4.2 Databas hos Tullverket

Tullverket har sedan inträdet i EU bedrivit insamling av uppgifter från transportföretag om passagerare, varor och transportmedel och har nyligen fått utökande möjligheter att behandla sådana uppgifter. Det finns därför anledning att överväga om Tullverket bör få i uppgift att tillhandahålla passageraruppgifter även åt andra myndigheter. Myndigheten håller för närvarande på att utveckla en modernare lösning för insamling av uppgifter. Då myndigheten har samlat in bokningsuppgifter under lång tid har Tullverket redan etablerade

kontakter med berörda transportföretag och besitter den kompetens som krävs för sådant tillhandahållande.

För att Tullverkets brottsbekämpande förmåga inte ska försämras förutsätter detta att användningen av uppgifter får ske under samma förutsättningar som följer av nuvarande reglering i tullbefogenhetslagen och Tullverkets brottsdatalag. Tullverket samlar framför allt in uppgifterna i syfte att planera och välja ut kontrollobjekt i samband med in- och utförsel av varor. Det innebär bl.a. att uppgifterna måste få behandlas utan krav på konkreta misstankar om allvarlig brottslighet. Även om Tullverkets inhämtning är omfattande är den inte heltäckande så som PNR-systemets insamling. Regeringen har bedömt att detta innebär att ändamålsbegränsningen avseende allvarlig brottslighet inte behöver gälla för databasen.[2]

Även om de behöriga myndigheternas behandling av passageraruppgifter inom PNR-systemet sker i samma begränsade syfte, dvs. att bekämpa terrorism och annan allvarlig brottslighet, skiljer sig behoven åt från myndighet till myndighet. För att alla myndigheters behov ska tillgodoses krävs det att insamlingen är i det närmaste heltäckande. I jämförelse med andra alternativ där samtliga uppgifter samlas in framstår detta som en nackdel med denna lösning. Under utredningens gång har de övriga behöriga myndigheterna ställt sig tveksamma till om Tullverkets behov även täcker deras eget behov av uppgifter. Utifrån detta anser vi att denna lösning inte är lämplig att utreda vidare.

14.5 Ändamålsbegränsning

För det fall att det införs ett centralt system för insamling av passageraruppgifter som hålls separerat från PNR-databasen för flygtrafik, så som vi har beskrivit i avsnitt 14.3–4, finns det större frihet att bestämma syftena med behandling av uppgifter i databasen jämfört med PNR-systemet för flygtrafik. Det utgör en väsentlig skillnad mellan de olika systemen som är värd att belysa för att komma till en slutsats avseende vilka ändamål som en separat databas kan användas för. Till skillnad från PNR-systemet behöver ett sådant separat system inte nödvändigtvis begränsas till bekämpande av grov brottslighet så som den definieras i artikel 3.9 och bilaga II i PNR-

[2] Prop. 2023/24:132, *Ny tullbefogenhetslag*, s. 364.

direktivet utan det är möjligt att bestämma syftet till att inkludera även andra typer av brott. Det innebär visserligen ett vidare tillämpningsområde, men enligt praxis från EU-domstolen finns det vissa begränsningar avseende vilken brottslighet som får omfattas av ett liknande system. I ett flertal mål har domstolen uttalat att ett intrång i de grundläggande rättigheterna måste vara proportionerligt i förhållande till det allmänna säkerhetsintresse som eftersträvas.[3]

När det gäller målet att förebygga, undersöka, avslöja och lagföra brott är det, i enlighet med proportionalitetsprincipen, endast bekämpning av grov brottslighet och förebyggande av allvarliga hot mot allmän säkerhet som kan motivera allvarliga ingrepp i de grundläggande rättigheterna som anges i artikel 7 och 8 i EU-stadgan. Att bekämpa brott i allmänhet kan endast motivera sådana ingrepp som inte är av allvarligt slag. För att kravet på proportionalitet ska vara uppfyllt måste det i lagstiftning föreskrivas klara och tydliga bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden.

Insamling och lagring av samtliga passageraruppgifter från gränsöverskridande resor för flera olika trafikslag utgör ett allvarligt ingrepp i de grundläggande rättigheterna. Detta har även slagits fast i PNR-domen avseende flygtrafiken. I och med detta måste det göras en begränsning som innebär att passageraruppgifterna endast får användas för att bekämpa brottslighet av en viss allvarsgrad. Det finns i svensk rätt ingen generell definition av *grov brottslighet*, men generellt sett rör det sig om allvarliga brott som har en högre straffskala. Beteckningen ska i det här sammanhanget inte förväxlas med den svenska straffrättens indelning av brott i kategorierna ringa brott, brott av normalgraden och grovt brott. Snarare bör uttrycket jämställas med *allvarlig brottslighet*, vilket är det begrepp som används i lagen om flygpassageraruppgifter i brottsbekämpningen.

Att införa en brottskatalog så som i bilaga II till PNR-direktivet innebär att det är tydligt och förutsebart vilka brott som omfattas av tillämpningen av systemet. En sådan uppräkning riskerar emellertid att utelämna vissa brott som rimligen bör kunna bekämpas genom behandling av passageraruppgifter. Inom PNR-systemet är t.ex. mordbrand inte ett brott som omfattas av tillämpningen, trots att det utgör ett allvarligt brott med en straffskala om lägst två år och

[3] Se t.ex. EU-domstolens dom den 6 oktober 2020, *La Quadrature du Net m.fl. mot Premier ministre m.fl.*, förenade målen nr C-511/18, C-512/18 och C-520/18.

högst åtta års fängelse.[4] En fördel med att inte precisera vilka brott som omfattas är dessutom att allvarliga gärningar som kriminaliseras i framtiden kan omfattas av systemet utan att lagstiftningen behöver ändras. Vi förespråkar därför en bredare, mer generell definition av den aktuella brottsligheten. En sådan definition görs lämpligast genom en hänvisning till straffskalan. I PNR-direktivet har, utöver att brottet ska finnas med i uppräkningen i bilaga II, kravet ställts att brottet ska bestraffas med fängelse eller annan frihetsberövande åtgärd i minst tre år enligt en medlemsstats nationella rätt. I PNR-domen lägger domstolen inte fram några synpunkter på denna avgränsning av brottsligheten utan konstaterar att det i bilagan på ett tillräckligt klart och precist sätt fastställs vilka brott som kan utgöra grov brottslighet. Vi drar utifrån det slutsatsen att avgränsningen är förenlig med EU-rätten.

Även om PNR-systemets avgränsning kan vara vägledande utgör den inte en skarp gräns för hur Sverige i nationell rätt kan definiera allvarlig brottslighet. Den EU-rättsliga regleringen kan dessutom tillämpas olika beroende på vilka straffskalor för olika brott som föreskrivs i nationell lagstiftning. I svensk rätt finns det t.ex. ett flertal brott som har ett maximistraff om två år, såsom bedrägeri och urkundsförfalskning. Bedrägeri ingår i uppräkningen av brott i PNR-direktivets bilaga II. I bilagan nämns även förfalskning av administrativa dokument och handel med sådana förfalskningar, vilket går att jämföra med urkundsförfalskning. Dessa brott betraktas således som allvarliga inom ramen för PNR-direktivet, under förutsättning att nationell rätt föreskriver en straffskala där tre års fängelse ingår.

Att begränsa tillämpningen av det nationella systemet till att avse brott där två års fängelse ingår i straffskalan innebär att passageraruppgifter kommer att behandlas i bekämpandet av fler typer av brott än vad som kan ske inom PNR-systemet. Det innebär ett större ingrepp i de grundläggande rättigheterna, vilket påverkar bedömningen av om åtgärden är proportionerlig. Syftet med behandlingen är att bekämpa brott av en viss allvarsgrad, och åtgärden att sätta gränsen vid två år är ägnad att uppnå det målet i större utsträckning än om gränsen sätts vid tre år. Vi bedömer att nyttan med en sådan ordning väger tyngre än det ökade ingreppet i de grundläggande rättigheterna. I och med avgränsningen avseende straffskalan anser vi vidare att det framgår tydligt vilka brott som omfattas av tillämpningen, även

[4] 13 kap. 1 § brottsbalken.

i avsaknad av en uppräkning av specifika brott. De fördelar som en sådan lösning innebär väger enligt vår mening tyngre än fördelarna med en statisk brottskatalog.

I likhet med bestämmelsen i 5 kap. 3 § lagen om flygpassageraruppgifter i brottsbekämpningen bör det vara tillåtet att använda uppgifter om ett annat brott än terroristbrottslighet eller annan allvarlig brottslighet som har kommit fram i samband med att en behörig myndighet har vidtagit åtgärder till följd av behandling av passageraruppgifterna. Syftet med behandlingen får således inte vara något annat än att bekämpa terrorism och annan allvarlig brottslighet, men resultatet av behandlingen får användas även för att förhindra, utreda och lagföra annan, mindre allvarlig, brottslighet. I förarbetena till lagen om flygpassageraruppgifter i brottsbekämpningen ansåg regeringen att det i det här sammanhanget, med beaktande av integritetsintresset ställt mot intresset av en effektiv brottsbekämpning, inte bör ställas något krav på allvarlighetsgrad för att PNR-information ska få användas.[5] Av den generella proportionalitetsprincipen som kommer till uttryck i t.ex. 8 § polislagen följer emellertid att det inte bör komma i fråga att använda uppgifterna för att bekämpa rena bagatellbrott.

Vi drar således slutsatsen att om passageraruppgifter från andra trafikslag än flygtrafiken samlas in och behandlas i ett system som är separat från PNR-databasen är det möjligt att behandla uppgifterna för att bekämpa terroristbrott och annan allvarlig brottslighet, som definieras som brott där det ingår två års fängelse i straffskalan.

[5] Prop. 2017/18:234, *Lag om flygpassageraruppgifter i brottsbekämpningen*, s. 108–109.

15 Överväganden och förslag

15.1 PNR-lagstiftningen ska göras trafikslagsneutral

Förslag

PNR-lagstiftningen ska omfatta även andra trafikslag. Insamlingen av passageraruppgifter från samtliga trafikslag som omfattas av lagstiftningen ska göras av enheten för passagerarinformation och uppgifterna ska lagras i den befintliga databasen hos enheten.

I avsnitt 14 har för- och nackdelar med en trafikslagsneutral lagstiftning analyserats och olika alternativ för insamling av passageraruppgifter har lagts fram. Vi anser att behovet av en mer heltäckande insamling av passageraruppgifter för att främja det allmänna samhällsintresset att bekämpa terrorism och annan allvarlig brottslighet väger tyngre än det ingrepp i grundläggande rättigheter som en sådan insamling innebär. Det bör därför inrättas ett system för att på ett heltäckande och ändamålsenligt sätt samla in passageraruppgifter från andra trafikslag än flygtrafiken.

De alternativ för administrationen av en sådan databas som presenterats i avsnitt 14 och som framstår som lämpliga är att antingen använda den befintliga databasen eller en separat databas hos enheten för passagerarinformation. De två alternativen innebär lika omfattande insamling av uppgifter och samma ingrepp i den personliga integriteten. Fördelarna med en separat databas är att de tillåtna ändamålen för behandling av uppgifterna är mindre begränsade än inom PNR-systemet. Vi anser dock att fördelarna med att använda den befintliga databasen hos enheten för passagerarinformation väger tyngre. Det är t.ex. ett mindre kostsamt alternativ och det tar kortare tid att genomföra. I synnerhet talar möjligheten att utbyta passageraruppgifter med andra länder som har utökat PNR-systemet till att omfatta andra trafikslag

än flyg för en sådan lösning. Det gynnar inte bara brottsbekämpningen i Sverige utan även globalt. Mot bakgrund av detta förordar vi en sådan lösning.

15.2 Lagen om flygpassageraruppgifter i brottsbekämpningen ska tillämpas

Förslag

Lagen om flygpassageraruppgifter i brottsbekämpningen ska tillämpas även på passageraruppgifter från andra trafikslag. Lagen behöver därför modifieras för att vara anpassad till detta, bl.a. genom att den byter namn till lag om passageraruppgifter i brottsbekämpningen.

Hänvisningar till lagen om flygpassageraruppgifter i annan lagstiftning ska uppdateras till följd av att lagen byter namn.

I och med att passageraruppgifter från andra trafikslag kommer att lagras i samma databas som uppgifterna från flygtrafiken kommer de även att omfattas av samma regler. Det förefaller därför naturligt att tillämpa lagen om flygpassageraruppgifter i brottsbekämpningen även på dessa uppgifter, i stället för att stifta en ny lag för dessa uppgifter som i stort blir identisk med den befintliga lagen.

Detta kräver att lagen modifieras från att endast omfatta flygtrafik till att bli trafikslagsneutral. Vi föreslår därför att lagen ska byta namn till lagen om passageraruppgifter i brottsbekämpningen. Vissa begrepp, t.ex. lufttrafikföretag och flygresa, behöver ändras till transportföretag och resa. Hänvisningar till lagen om flygpassageraruppgifter i brottsbekämpningen i andra författningar, t.ex. polisens brottsdatalag och tullverkets brottsdatalag, behöver också uppdateras. Förändringen av lagen till att bli trafikslagsneutral kräver vidare justering i vissa avseenden. Dessa behandlas nedan.

15.2.1 Lagens innehåll

Förslag

Det ska anges att lagen innehåller bestämmelser om transportföretags överföring av PNR-uppgifter, utöver att den genomför PNR-direktivet.

Det ska anges att PNR-uppgifter även utgörs av uppgifter om varje enskild passagerare som har lämnats vid köp av biljett, utöver sådana uppgifter som har lämnats vid bokning av transport och vid incheckning.

I 1 kap. 1 § lagen om flygpassageraruppgifter i brottsbekämpningen anges lagens innehåll. Denna bestämmelse bör uppdateras så att det framgår att lagen inte endast genomför PNR-direktivet, som avser flygtrafik, utan att den även innehåller bestämmelser om transportföretags överföring av PNR-uppgifter. I bestämmelsen bör det vidare anges att PNR-uppgifter även utgörs av uppgifter om varje enskild passagerare som har lämnats vid köp av biljett, för att omfatta sådana resor som företas utan föregående reservation.

15.2.2 Definitionen av en medlemsstat

Förslag

Definitionen av en medlemsstat ska, när det gäller transporter med tåg, buss och färja, avse samtliga stater som är medlemmar i Europeiska unionen.

I 1 kap. 3 § definieras en medlemsstat som en stat som är medlem i Europeiska unionen och har antagit PNR-direktivet. Enligt definitionen av tredjeland i samma paragraf avses en stat som inte är en medlemsstat. Detta innebär att Danmark, som inte har antagit PNR-direktivet, inte betraktas som ett medlemsland inom ramen för PNR-systemet utan i stället som ett tredjeland.

I och med att fler trafikslag förs in i det svenska PNR-systemet bör detta uppdateras. Tåg-, buss- och färjetrafik regleras inte av PNR-direktivet och sådan trafik till och från Danmark bör inte behandlas

som transporter utanför EU. Definitionen av medlemsstat bör därför, när det gäller transporter med tåg, buss och färja, avse samtliga stater som är medlemmar i EU.

15.3 Förordningen om flygpassageraruppgifter i brottsbekämpningen

Förslag

Förordningen om flygpassageraruppgifter i brottsbekämpningen ska byta namn till förordningen om passageraruppgifter i brottsbekämpningen och vissa begrepp i förordningen behöver ändras för att spegla att regleringen är trafikslagsneutral.

Bestämmelsen i förordningen om att resultatet av en behandling av PNR-uppgifter inte får behandlas under längre tid än vad som behövs för att kunna informera behöriga mottagare om resultatet ska ändras så att den endast omfattar resultatet av en behandling av PNR-uppgifter som görs genom en förhandsbedömning.

Polismyndigheten ska bemyndigas att meddela närmare föreskrifter om hur transportföretag som bedriver tåg-, buss- eller färjetrafik ska överföra PNR-uppgifter till enheten för passagerarinformation.

Förordningen (2018:1181) om flygpassageraruppgifter i brottsbekämpningen behöver döpas om till förordningen om passageraruppgifter i brottsbekämpningen och vissa begrepp i förordningen kräver ändring för att spegla att regleringen är trafikslagsneutral.

I 9 § förordningen om flygpassageraruppgifter anges bl.a. att resultatet av en behandling av PNR-uppgifter inte får behandlas under längre tid än vad som behövs för att kunna informera behöriga mottagare om resultatet. Bestämmelsen genomför artikel 12.5 i PNR-direktivet. I artikel 12.5 anges dock att det endast är resultaten av den behandling som avses i artikel 6.2 a som omfattas av denna begränsning. Artikel 6.2 a rör förhandsbedömningen, dvs. en bedömning av passagerare före deras beräknade ankomst till eller avresa från den berörda medlemsstaten, för att identifiera personers om behöriga myndigheter eller Europol behöver utreda ytterligare. Artikel 12.5 omfattar således inte den behandling som görs enligt artikel 6.2 b

och c. 9 § förordningen om flygpassageraruppgifter ska därför ändras så att den endast avser resultatet av en behandling av PNR-uppgifter genom en förhandsbedömning enligt 3 kap. 4 § 1.

I 4 § i förordningen framgår att lufttrafikföretag ska överföra PNR-uppgifter i enlighet med ett genomförandebeslut av kommissionen. I genomförandebeslutet framgår vilka protokoll och format som ska användas vid överföringen. Regleringen är anpassad efter flygtrafiken och kan, om den implementeras även för andra trafikslag, innebära utmaningar för aktörer som inte använder de protokoll och format som föreskrivs i genomförandebeslutet. För att transportföretagen inte ska åläggas betungande pålagor bör kraven i 4 § inte omfatta transportföretag som bedriver tåg-, buss-eller färjetrafik. Polismyndigheten bör i stället bemyndigas att meddela föreskrifter om hur PNR-uppgifterna ska överföras, vilket omfattar reglering av vilka protokoll och format som ska användas för de aktuella trafikslagen. Polismyndigheten har redan i nuläget ett etablerat samarbete med transportföretagen och begär in uppgifter med stöd av 25 § polislagen. Det bör vara möjligt att genom det samarbetet arbeta fram lösningar för överföringen av uppgifterna även inom PNR-systemet som är ändamålsenlig för både transportföretagen och enheten för passagerarinformation. En reglering av godkända protokoll och format riskerar att landa i en mindre ändamålsenlig lösning än om enheten och transportföretagen gemensamt arbetar fram en modell för överföringen.

15.4 Påverkan på befintlig lagstiftning

Bedömning

Skyldigheten för transportbolag att på begäran lämna uppgifter till Polismyndigheten och Säkerhetspolisen enligt polislagen och till Tullverket enligt tullbefogenhetslagen ska kvarstå även efter införandet av en trafikslagsneutral PNR-lagstiftning.

Ett system med central insamling av passageraruppgifter kan få följdeffekter för den nu gällande lagstiftningen om brottsbekämpande myndigheters möjlighet att begära uppgifter från transportföretag.

Som redovisats i tidigare avsnitt innebär en bredare, systematisk insamling av passageraruppgifter att ändamålet med behandlingen

av uppgifterna begränsas till att bekämpa terroristbrott och grov brottslighet. I 25 § polislagen och 7 kap. 12 § tullbefogenhetslagen är kravet i stället att vissa uppgifter får begäras om de kan antas ha betydelse för den brottsbekämpande verksamheten. Om dessa bestämmelser kvarstår innebär det således att det är möjligt för t.ex. Polismyndigheten att, i stället för att begära tillgång till en specifik uppgift från den myndighet som handhar den centrala databasen, begära ut uppgiften direkt från ett transportföretag. På så vis skulle uppgiften kunna användas för att bekämpa andra brott än terroristbrott och grov brottslighet.

PNR-direktivet ställer inte upp några hinder för medlemsstaterna att inrätta ett liknande system för andra trafikslag. I skäl 33 anges att direktivet inte påverkar medlemsstaternas möjligheter att i enlighet med nationell rätt tillhandahålla ett system för insamling och behandling av PNR-uppgifter från bl.a. andra transportföretag än de som anges i direktivet, förutsatt att sådan nationell rätt är förenlig med unionsrätten. I skäl 36 anges att direktivet överensstämmer med principerna om dataskydd och dess bestämmelser är förenliga med rambeslut 2008/977/RIF[1] samt att för att direktivet inte ska inkräkta på proportionalitetsprincipen kommer dess bestämmelser i vissa fall vara strängare än motsvarande bestämmelser i rambeslutet. Som framgår i avsnitt 14.2–4 anser vi att våra förslag till ett centralt system för insamling av passageraruppgifter från andra trafikslag än flyg är förenliga med unionsrätten. Det står också klart att nuvarande bestämmelser i polislagen och tullbefogenhetslagen i och för sig är tillåtna enligt EU-rätten. Frågan är således om det finns några hinder mot att bibehålla befintlig lagstiftning samtidigt som ett trafikslagsneutralt PNR-system införs.

Frågan om hur PNR-direktivet påverkar den befintliga insamlingen av bokningsuppgifter från lufttrafikföretag diskuterades under lagstiftningsprocessen inför genomförandet av direktivet. Regeringen konstaterade då att direktivet inte uttryckligen utesluter att medlemsstaterna får behålla sina nationella system parallellt med det system som PNR-direktivet föreskriver. Samtidigt angavs att tanken bakom

[1] Rådets rambeslut av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete. Rambeslutet är inte längre i kraft utan har ersatts av Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

direktivet är att uppnå en enhetlig och rättssäker reglering inom EU av behandlingen av viss information som kan röra EU-medborgare. En ordning enligt vilken medlemsstaterna skulle kunna behålla sina nationella system vid sidan av det system som direktivet föreskriver skulle enligt regeringen därmed kunna motverka direktivets bakomliggande syften, dvs. att förbättra den inre säkerheten samtidigt som man upprätthåller skyddet för de överförda uppgifterna. Till följd av detta infördes det tillägg i polislagen, dåvarande tullagen och inregränslagen som anger att bestämmelserna om transportföretags skyldighet att överföra bokningsuppgifter inte ska gälla lufttrafikföretag som omfattas av skyldigheten att överföra uppgifter enligt den nya lagen.

När det gäller frågan om brott som rör nationell säkerhet ansåg regeringen att det inte kan anses vara rimligt att myndigheterna genom den nya lagen ska få en sämre förmåga att bekämpa brott som rör nationell säkerhet än vad de har i dag. Befintliga regler i nämnda lagar behölls därför i verksamhet som rör nationell säkerhet.[2]

Denna hantering av den dåvarande regleringen i polislagen och tullagen när PNR-direktivet genomfördes i svensk rätt talar i någon mån för att en trafikslagsneutral PNR-lagstiftning bör medföra att aktuella bestämmelser i polislagen och tullbefogenhetslagen tas bort. En sådan slutsats är dock inte given.

Den insamling av passageraruppgifter som vi föreslår sker i enlighet med nationell rätt och till skillnad från PNR-systemet för flygtrafiken finns det inte någon underliggande rättsakt på EU-nivå för det specifika systemet att förhålla sig till, även om vissa bestämmelser i PNR-direktivet kommer att påverka behandlingen även av de uppgifter som kommer från andra trafikslag.

Eftersom insamlingen av passageraruppgifter inte sker i enlighet med direktivet är alltså inte direktivets bestämmelser till fullo tillämpliga på behandlingen av uppgifterna. Den nationella rätten behöver inte heller förhålla sig till de mål eller syften som ligger till grund för PNR-systemet, även om den nationella lagstiftningen självklart ska vara förenlig med den generella unionsrätten.

EU-domstolen har i flera fall behandlat frågan om proportionalitet vid insamling av en stor mängd uppgifter i brottsbekämpande syfte och för verksamhet som rör nationell säkerhet. EU-domstolen har däremot inte behandlat frågan om ett parallellt system för begäran

[2] Prop. 2017/18, *Lag om flygpassageraruppgifter i brottsbekämpningen*, s. 45–46.

om passageraruppgifter från trafikföretag, vid sidan om ett centralt system för systematisk insamling i likhet med PNR-direktivet. Domstolens uttalanden om proportionalitet och begränsningar av ändamålet med behandling av personuppgifter gäller således den behandling som sker inom ramen för ett sådant system. Det är förenat med svårigheter att utifrån EU-domstolens praxis dra säkra slutsatser om i vilken utsträckning det är tillåtet enligt EU-rätten att inrätta ett sådant parallellt system. En grund för att inte tillåta sådan parallell insamling vid genomförandet av PNR-direktivet var att uppnå en enhetlig och rättssäker reglering inom EU av hanteringen av information som kan röra EU-medborgare och för att genom ett utvecklat samarbete förbättra möjligheterna att bekämpa allvarlig brottslighet. Om medlemsstaterna skulle behålla sina nationella system vid sidan av det system som direktivet föreskriver skulle det motverka direktivets bakomliggande syften. När det gäller insamling av passageraruppgifter från andra trafikslag än flyget gör sig inte dessa argument gällande på samma sätt. Det finns ingen EU-rättslig reglering som harmoniserar sådan insamling. Ett nationellt system behöver således inte anpassas för att uppnå enhetlighet inom unionen. Vissa länder samlar in andra passageraruppgifter, och med dessa skulle således ett utbyte av uppgifter kunna ske. Grunden för detta är dock inte en EU-rättslig reglering, utan samarbete medlemsstaterna emellan.

Det bör också framhållas att insamling av passageraruppgifter från fler trafikslag till en central databas väsentligt skiljer sig åt från aktuella bestämmelser i polislagen och tullbefogenhetslagen. I det första fallet handlar det om en automatisk insamling av samtliga passageraruppgifter till och från landet, oavsett om de har kopplingar till t.ex. ett begånget brott, vilket kan motiveras med att uppgifterna endast får användas i den brottsbekämpande verksamheten om det rör särskilt allvarliga brott. I det andra fallet handlar det i stället om att en brottsbekämpande myndighet behöver få ut vissa uppgifter från ett transportföretag. Det kan ifrågasättas om det är rimligt att t.ex. Polismyndigheten i ett sådant fall inte ska ha möjlighet att få tillgång till uppgifterna. Detta gäller särskilt som det kan handla om brottsmisstankar avseende brott som är allvarligt, även om det inte når upp till nivån som gör det möjligt att få ut uppgifterna från PNR-databasen. Att de olika lagstiftningarna har överlappande men också delvis olika syften talar också mot att de befintliga bestämmelserna i polislagen och tullbefogenhetslagen bör tas bort. T.ex. syftar bestämmelsen i

tullbefogenhetslagen också till kontroll av införsel av varor. Bokningsuppgifter, däribland uppgifter om passagerare, används inom Tullverkets underrättelseverksamhet för att planera kontroller, välja ut vilka objekt som ska tas ut för kontroll och göra analyser som behövs för att uppdatera eller skapa nya kriterier som ska användas vid planering av kontroller eller urval av kontrollobjekt. Om befogenheterna enligt tullbefogenhetslagen togs bort skulle det försvåra Tullverkets kontrollverksamhet. Detta visar också att även om det finns likheter mellan ett centralt system för insamling av uppgifter och myndigheternas enskilda insamling kan det inte betraktas som parallella system med samma syfte som tillämpas i olika stor skala.

Om möjligheten att i enskilda fall begära in uppgifter från trafikföretag tas bort innebär det att myndigheterna får en sämre förmåga att bekämpa brott som inte omfattas av PNR-direktivets tillämpningsområde. Det kan av ovan nämnda skäl ifrågasättas om en sådan konsekvens är rimlig. Tillgång till uppgifter i syfte att bekämpa mindre allvarlig brottslighet är dessutom ett värdefullt verktyg för att bekämpa även den allvarliga brottsligheten. Inte sällan leder brottsutredningar som initialt avser mindre allvarlig brottslighet till information som är användbar även för att förebygga, förhindra, upptäcka, utreda och lagföra allvarlig brottslighet. Det finns således även en risk att möjligheterna att uppnå målen att bekämpa terroristbrott och annan allvarlig brottslighet påverkas negativt. Vidare kan det ifrågasättas om det är tänkt att den EU-rättsliga regleringen ska innebära att medlemsstaterna ställs inför ett val att antingen införa ett centralt system med insamling av en stor mängd uppgifter som endast får användas i syfte att bekämpa allvarlig brottslighet och terrorism, eller ett mer splittrat system där myndigheter begär tillgång till enstaka uppgifter för att bekämpa brott i allmänhet.

Med beaktande av de skillnader gentemot PNR-systemet för flygtrafik som ett nationellt system innebär samt av att det inte framstår som rimligt att myndigheternas möjligheter att bekämpa mindre allvarlig brottslighet försämras och att även möjligheterna att bekämpa allvarlig brottslighet annars skulle försämras anser vi att det är lämpligt och proportionerligt att behålla den lagstiftning som ställer upp skyldigheter för transportföretag att på begäran av vissa myndigheter lämna uppgifter om transporter om uppgifterna kan antas ha betydelse för den brottsbekämpande verksamheten.

15.4.1 Lufttrafikföretagens skyldigheter enligt polislagen och tullbefogenhetslagen

Förslag

Skyldigheten för transportföretag att på begäran lämna uppgifter om transporter till Polismyndigheten och Säkerhetspolisen respektive Tullverket ska även omfatta lufttrafikföretag som omfattas av skyldigheten att överföra uppgifter enligt lagen om flygpassageraruppgifter i brottsbekämpningen.

Med tanke på att det enligt vårt förslag ovan fortsatt ska finnas en skyldighet för transportföretag att lämna uppgifter till vissa myndigheter bör det övervägas om det undantag som gäller för lufttrafikföretag bör kvarstå. I 25 § tredje stycket polislagen och 7 kap. 12 § andra stycket tullbefogenhetslagen anges att skyldigheten att lämna uppgifter om transporter inte omfattar lufttrafikföretag som omfattas av skyldigheten att överföra uppgifter enligt lagen om flygpassageraruppgifter i brottsbekämpningen. I avsnittet ovan redogjorde vi för resonemangen i förarbetena avseende dessa undantag.

PNR-direktivets bakomliggande syften är att förbättra den inre säkerheten genom bekämpning av terroristbrott och annan brottslighet samtidigt som skyddet för PNR-uppgifterna upprätthålls. Vi anser inte att möjligheten att få tillgång till uppgifter om flygtransporter även vid sidan om PNR-systemet, för delvis andra ändamål, motverkar dessa syften. Tvärtom bör sådan tillgång innebära bättre förutsättningar att bekämpa brott, vilket är ett led i att förbättra den inre säkerheten.

När det gäller syftet att upprätthålla skyddet för de uppgifter som behandlas kan det konstateras att PNR-direktivet visserligen uppställer striktare regler än vad som annars gäller för personuppgiftsbehandlingen i brottsbekämpande verksamhet. I andra sammanhang, dvs. all annan brottsbekämpning, anses dock övriga dataskyddsregelverk i form av dataskyddsdirektivet och dess genomförande i svensk rätt utgöra ett fullgott dataskydd. Vi anser att så bör vara fallet även avseende de nu aktuella uppgifterna. Det förefaller därför inte heller som att ett nationellt system vid sidan om PNR-systemet motverkar direktivets syfte att upprätthålla dataskyddet.

Det finns redan i nu gällande lagstiftning möjligheter för myndigheter att ta del av uppgifter om transporter vid sidan om PNR-systemet. Det går t.ex. att inom ramen för en förundersökning inhämta uppgifter med stöd av rättegångsbalkens regler om beslag. I 9 kap. 3 a–f §§ utlänningslagen regleras transportörsansvaret som innebär att transportörer under vissa förutsättningar ska överföra uppgifter om ankommande passagerare på begäran av Polismyndigheten. Flera av de typer av uppgifter som ska överföras enligt utlänningslagen är också sådana uppgifter som överförs inom PNR-systemet. Enligt lagen (2006:444) om passagerarregister ska Polismyndigheten med hjälp av automatiserad behandling föra ett register av passagerare som avses i 9 kap. 3 a § utlänningslagen.

Det är alltså inte uteslutet att i enstaka fall hämta in uppgifter vid sidan om PNR-lagstiftningen. Inhämtningen enligt utlänningslagen sker i annat syfte än PNR-lagstiftningen, men inhämtningen enligt rättegångsbalken sker i brottsbekämpande syfte. Inhämtning enligt polislagen och tullbefogenhetslagen har visserligen ett brottsbekämpande syfte, men det skiljer sig ändå mot PNR-systemet, som endast riktar sig mot terroristbrott och annan allvarlig brottslighet.

Argumenten angående övriga trafikslag om att det inte är rimligt att bekämpningen av mindre allvarlig brottslighet försämras till följd av inrättande av ett centralt system för insamling av PNR-uppgifter gör sig gällande även för flygtrafiken. Även bedömningen av proportionaliteten med parallell insamling är densamma för flygtrafiken. För att svensk rätt ska bli enhetlig när det gäller tillgången till uppgifter från olika trafikslag anser vi därför att skyldigheten för transportföretag att på begäran lämna uppgifter om transporter till Polismyndigheten och Säkerhetspolisen enligt 25 § tredje stycket polislagen och till Tullverket enligt 7 kap. 12 § andra stycket tullbefogenhetslagen även ska gälla för lufttrafikföretag som omfattas av skyldigheten att överföra uppgifter enligt lagen om flygpassageraruppgifter i brottsbekämpningen. Det innebär att bestämmelserna i respektive lagstiftning som har begränsat sådan insamling ska tas bort.

I den bestämmelse som tas bort i polislagen, dvs. 25 § tredje stycket, framgår att lufttrafikföretag endast är skyldiga att lämna uppgifter i enlighet med första och andra styckena om de behövs i verksamhet som rör nationell säkerhet. Att bestämmelsen tas bort innebär ingen förändring i sak vad avser denna skyldighet.

16 Transportföretagens roll

16.1 Inledning

Den huvudsakliga fördelen ur ett brottsbekämpande perspektiv med en central insamling av passageraruppgifter är att brottsbekämpande myndigheter får tillgång till en stor mängd information. Ett sådant system kräver att transportföretagen åläggs en skyldighet att översända passageraruppgifter till myndigheten som handhar den centrala databasen. Detta ger upphov till ett flertal frågeställningar, t.ex. om vilka aktörer, resor och uppgifter som ska omfattas av uppgiftsskyldigheten, ökad administration för transportföretagen och vem som ska ansvara för den tekniska infrastrukturen som krävs för ett sådant centraliserat system. Nedan beskriver vi dessa frågeställningar och ger förslag på lagtekniska lösningar.

16.2 Varierande förutsättningar för transportföretag

En utmaning med att införa ett system för flera trafikslag är de vitt skilda förutsättningar som kan gälla för olika företag och olika trafikslag. När det gäller internationell tågtrafik utgörs en stor majoritet av resorna av resor mellan Malmö och Köpenhamn. På den sträckan kör Öresundståg cirka 80 turer per dygn. Under 2024 företogs ungefär 40 000 sådana passagerarresor per dygn, vilket är den hittills högsta noterade nivån. I övrigt trafikeras de internationella sträckorna till Norge av SJ, SJ Norge och Vy Norge. Tågresor mot Tyskland och andra länder i centrala Europa går via Köpenhamn och erbjuds av SJ och Snälltåget.

SJ är ett statligt ägt reseföretag som har knappt 7 000 anställda och omsätter över åtta miljarder kronor om året. Vy Norge är det norska nationella järnvägsföretaget och är den största landbaserade transportkoncernen i Norden. Utöver tågtrafik bedriver Vy även busstrafik

och godstransport. Snälltåget är ett svenskt privat tågbolag som bedriver persontrafik med fokus på långdistans- och nattåg inom Sverige och internationellt. Bolaget har knappt 100 anställda och en omsättning om cirka 280 miljoner kronor om året.

Inom den internationella busstrafiken finns det ett fåtal stora bolag som dominerar marknaden, och många mindre bolag som främst erbjuder charter- och gruppresor. Det största bolaget på marknaden är FlixBus som erbjuder resor till en majoritet av länderna i Europa. Bolaget har över 2 500 destinationer i 36 länder. Som kontrast till detta finns det ett flertal mindre bolag som drivs som familjeföretag med ett mindre antal avgångar och betydligt färre anställda. Som exempel kan nämnas Westin Buss med cirka 40 anställda och Ellenius Buss AB med drygt 50 anställda. Dessa bolag, och flera andra mindre bolag som agerar på den internationella bussmarknaden, omsätter 50–100 miljoner kronor om året.

Även inom den internationella passagerartrafiken inom sjöfarten är skillnaderna mellan olika operatörer stora. Marknaden domineras av ett fåtal stora aktörer, t.ex. Stena Line och Tallink Silja Line. Stena Line transporterade 2024 totalt över sex miljoner passagerare och omsatte cirka 19,5 miljarder kronor. Mindre aktörer som Polferries AB Sverige, som mellan Sverige och Polen trafikerar linjerna Ystad till Swinoujscie och Nynäshamn till Gdansk, har en årsomsättning om 28 miljoner kronor.

Det står således klart att de ekonomiska och administrativa förutsättningarna för aktörer inom gränsöverskridande passagerartrafik skiljer sig åt. Det är av vikt att beakta dessa skillnader i analysen av frågor som aktualiseras med en trafikslagsneutral PNR-lagstiftning.

16.3 Vilka trafikslag ska omfattas?

Förslag

Transportföretag som bedriver passagerartrafik med tåg, buss eller färja ska inför varje resa som ankommer till eller avgår från Sverige överföra PNR-uppgifter till enheten för passagerarinformation.

De trafikslag som främst bör övervägas är gränsöverskridande resor med buss, färja och tåg. Tillsammans med flygtrafiken står dessa färdmedel för i princip alla kommersiella resor till och från Sverige. Ett system som omfattar samtliga dessa transportmedel skulle därför bli i stort sett heltäckande och försvåra för kriminella att genom *broken travel* resa in och ut ur Sverige obemärkt. Om något av dessa trafikslag utelämnas innebär det en lucka som inte täpps till och myndigheterna förlorar möjligheten att följa hela resvägen. Det kan därutöver leda till att kriminella i högre utsträckning väljer det transportmedel som inte omfattas av PNR-lagstiftningen för att transportera t.ex. vapen, narkotika eller efterlysta personer. Olika skyldigheter för transportbolag beroende på vilken typ av transportmedel som används riskerar även att skapa en ojämn administrativ börda för aktörer som agerar på samma marknad, dvs. den gränsöverskridande passagerartrafiken. Vi anser därför att transportföretag som bedriver gränsöverskridande passagerarresor med tåg, buss eller färja ska omfattas av skyldigheten att föra över PNR-uppgifter om sådana resor till enheten för passagerarinformation.

16.3.1 Särskilt om färjetrafiken

Bedömning

Överföring av PNR-uppgifter från färjetrafik bör ske via EMSWe.

Som nämnts ovan sker det inom färjetrafiken redan rapportering av uppgifter till Sjöfartsverkets NSW, som på sikt kommer att ersättas av EMSWe. För såväl rederierna som bedriver passagerartrafik med färja som för enheten för passagerarinformation förefaller det mer praktiskt om uppgiftsöverföringen sker via MSW/EMSWe, i stället för direkt från fartygen till enheten för passagerarinformation. Ett av huvudsyftena med utvecklingen av EMSWe är engångsprincipen som framgår av artikel 8 i EMSWe-förordningen[1], dvs. att uppgifter endast ska tillhandahållas en gång per fartygsanlöp.

Rapporteringsskyldigheten enligt EMSWe-förordningen följer av unionsrätten, andra internationella rättsliga instrument samt rap-

[1] Europaparlamentets och rådets förordning (EU) 2019/1239 av den 20 juni 2019 om inrättande av en europeisk kontaktpunkt för sjöfart och om upphävande av direktiv 2010/65/EU.

porteringsskyldigheter som följer av nationell lagstiftning och nationella krav. Sverige har således möjlighet att i nationell rätt ställa upp rapporteringsskyldigheter som blir gällande enligt förordningen. I skäl 14 i förordningen anges att det är nödvändigt att inrätta en heltäckande EMSWe-datauppsättning för att EMSWe ska kunna fungera. Datauppsättningen bör omfatta alla uppgifter som nationella myndigheter eller hamnoperatörer kan begära i administrativa eller operativa syften när ett fartyg anlöper en hamn. Enligt skäl 16 i förordningen bör rapporteringsskyldigheterna i unionens rättsakter och internationella rättsakter samt hänvisningar till relevanta kategorier av rapporteringsskyldigheter på nationell nivå förtecknas i bilagan till förordningen. Samtliga rapporteringsskyldigheter sammanställs på så vis till en EMSWe-datauppsättning som gäller vid fartygsanlöp inom hela unionen. Samtliga uppgifter om passagerare som är aktuella att samla in inom ramen för den svenska PNR-regleringen ingår redan i den befintliga datauppsättningen som kommer att användas inom EMSWe.

I artikel 1 i EMSWe-förordningen anges att syftet med förordningen är att inrätta ett ramverk för en europeisk kontaktpunkt för sjöfart med harmoniserade gränssnitt för att underlätta elektronisk överföring av uppgifter i samband med rapporteringsskyldigheter för fartyg som ankommer till, uppehåller sig i och avgår från en hamn i unionen. Det framgår dock inte av förordningen om det finns några ändamålsbegränsningar avseende behandlingen av de uppgifter som omfattas av rapporteringsskyldigheten och som således översänds till EMSWe. I artikel 5.4 anges att medlemsstaterna ska säkerställa att erforderliga uppgifter når de myndigheter som ansvarar för tillämpningen av lagstiftningen i fråga, och att den begränsas till var och en av dessa myndigheters behov. Det anges ingen begränsning av vilka myndigheter som avses eller för vilket syfte myndigheterna ska ha behov av uppgifterna. Däremot krävs det naturligtvis att uppgifterna behandlas i enlighet med EU-rättsliga regler om personuppgiftsbehandling.

Passageraruppgifter från det nuvarande systemet, NSW, används i stor utsträckning av brottsbekämpande myndigheter inom unionen. Enligt en studie av kommissionen får knappt 58 procent av brottsbekämpande myndigheter i medlemsstaterna uppgifter från sjöfarten

via NSW, jämfört med cirka 21 procent direkt från operatörerna.[2] Det förefaller således okontroversiellt att uppgifter som översänds via NSW används för brottsbekämpande syften. Eftersom ett huvudsyfte med EMSWe är att genomföra engångsprincipen framstår det som sannolikt att så kommer ske även efter att EMSWe tas i drift.

I kommissionens studie diskuteras tillvägagångssättet att låta brottsbekämpande myndigheter ta del av passageraruppgifter via NSW. En sådan lösning innebär inte några ytterligare skyldigheter för rederier att samla in information. Eftersom antalet enskilda begäranden om uppgifter från myndigheter skulle minska innebär det dessutom troligen minskad administration och därmed minskade kostnader för rederierna. För brottsbekämpande myndigheter kan det innebära en initial kostnad men på sikt minskar administrationen, vilket leder till minskade kostnader. Sammantaget kan en sådan lösning innebära positiva ekonomiska effekter.

Eftersom PNR-systemet för flygtrafik har visat påtagliga resultat i bekämpandet av terrorism och annan allvarlig brottslighet kan det antas att systematisk tillgång till information från färjetrafik skulle förbättra effektiviteten i brottsbekämpningen.

Vidare anges i studien att enheten för passagerarinformation utses till mottagare av informationen är mest lämpligt utifrån ett ekonomiskt och säkerhetsmässigt perspektiv, och för att bäst säkerställa skyddet för grundläggande rättigheter.

Om brottsbekämpande myndigheter ges direkt åtkomst till NSW aktualiseras de grundläggande rättigheterna i artikel 7 och 8 i EU:s rättighetsstadga. Ingreppet i rättigheterna skulle dock vara acceptabelt eftersom det sker i syfte att bekämpa terrorism och allvarlig brottslighet. Ingreppet är proportionerligt så länge de rättssäkerhetsgarantier som krävs enligt PNR-domen tillämpas. Vid sådana förhållanden kan PNR-direktivet och dataskyddsdirektivet ge ett fullgott skydd för personuppgifterna. Detta talar ytterligare för att enheten för passagerarinformation bör vara mottagare av uppgifterna, eftersom de då omfattas av PNR-systemets regelverk. Det innebär

[2] Europeiska kommissionen: Generaldirektoratet för migration och inrikes frågor, BearingPoint, ICF och Unisys, *Study on harmonising reporting obligations of travel data on maritime transport, with a view to use such data for law enforcement purposes – Final Report*, november 2024, s. 29.

också att en sådan lösning inte har någon negativ påverkan på den fria rörligheten för unionsmedborgare enligt artikel 45 i stadgan.[3]

Frågan om uppgifter från färjetrafiken kan skickas till enheten för passagerarinformation handlar om den praktiska hanteringen av överföringen av uppgifter och inte om huruvida det är möjligt att uppställa en skyldighet för operatörer att föra över uppgifter. Att så är fallet har konstaterats i tidigare avsnitt. Överföring av uppgifter till enheten för passagerarinformation via NSW, och sedermera via EMSWe, förefaller vara det lämpligaste sättet att genomföra överföringen, både för rederierna och för enheten och i förlängningen för brottsbekämpande myndigheter. I och med att uppgifter från NSW används av andra medlemsstater i brottsbekämpande syfte, att kommissionen har konstaterat att det är ett potentiellt tillvägagångssätt för att tillgängliggöra passageraruppgifter samt med beaktande av EMSWe:s engångsprincip anser vi att inhämtningen av passageraruppgifter från färjetrafiken bör ske via EMSWe när systemet tas i bruk i Sverige. Det går emellertid inte att säkerställa att detta är möjligt förrän rapporteringsskyldigheten förs in i bilagan till EMSWe-förordningen. För att detta ska göras måste rapporteringsskyldigheten dessförinnan regleras i nationell rätt.

Osäkerheten angående om det går att använda EMSWe för att ge enheten för passagerarinformation tillgång till passageraruppgifter har betydelse för vissa praktiska frågor kring regleringen. För det fall att det inte är möjligt att använda EMSWe måste tidpunkten för överföring av uppgifter från fartygen regleras, i likhet med 2 kap. 2 § lagen om flygpassageraruppgifter i brottsbekämpningen. Om det går att använda EMSWe för överföringen regleras dock tiden för överföring av EU-rättsliga bestämmelser och ska inte regleras i svensk rätt. Det är således inte möjligt att stifta lag som är anpassad både för situationen där EMSWe används och inte används. Vi bedömer att det sannolikt är möjligt att använda EMSWe för överföringen av passageraruppgifter till enheten för passagerarinformation. Vi kommer därför att utforma förslagen avseende färjetrafiken med denna utgångspunkt.

[3] Europeiska kommissionen: Generaldirektoratet för migration och inrikes frågor, BearingPoint, ICF och Unisys, *Study on harmonising reporting obligations of travel data on maritime transport, with a view to use such data for law enforcement purposes – Final Report*, november 2024, s. 77–82.

16.4 Vilka företag ska omfattas av uppgiftsskyldigheten?

Förslag

De företag som omfattas av uppgiftsskyldigheten är transportföretag som har giltig operativ licens, tillstånd, certifikat eller motsvarande som ger rätt att mot ersättning utföra transporter av passagerare med tåg, buss eller färja, utöver redan gällande skyldighet vid transport med flygplan. Skyldigheten gäller företag som i sin normala verksamhet samlar in och behandlar PNR-uppgifter i ett elektroniskt system för hantering av reservationer och biljettköp.

I lagen om flygpassageraruppgifter i brottsbekämpningen uppställs en skyldighet för lufttrafikföretag att överföra vissa PNR-uppgifter till enheten för passagerarinformation. Lufttrafikföretag definieras i 1 kap. 3 § som ett företag som har operativ licens eller motsvarande som ger rätt att mot ersättning utföra lufttransporter av passagerare, och som i sin normala verksamhet samlar in och behandlar PNR-uppgifter i ett elektroniskt system för hantering av reservationer.

För att anpassa regleringen till att omfatta övriga trafikslag bör det genomgående i lagstiftningen anges att den gäller transportföretag i stället för lufttrafikföretag samt transporter i stället för lufttransporter. Frågan är om definitionen av lufttrafikföretag bör modifieras för att passa även företag som bedriver passagerartrafik med tåg, buss och färja.

För att bedriva busstrafik till, från och/eller genom andra EU-länder krävs det tillstånd. Bestämmelser som sådan trafik finns i Europaparlamentets och rådets förordning (EG) nr 1073/2009 av den 21 oktober 2009 om gemensamma regler för tillträde till den internationella marknaden för persontransporter med buss och om ändring av förordning (EG nr 561/2006). Samtliga transportföretag som utför internationella persontransporter med buss ska ha ett s.k. gemenskapstillstånd som beviljas av Transportstyrelsen. Det krävs även särskilda tillstånd beroende på vilken typ av trafik som bedrivs, t.ex. linjetrafik, speciell linjetrafik, beställningstrafik och cabotagetrafik. Det finns en nordisk överenskommelse om att ett färdbladshäfte inte behöver medföras i fordonen vid tillfällig busstrafik mellan

Sverige, Danmark, Finland och Norge. Även vid sådana transporter måste det dock finnas ett gemenskapstillstånd för persontransporter.

Det krävs även tillstånd för att bedriva busstrafik utanför EU. För internationell linjetrafik krävs det tillstånd i samtliga länder längs linjesträckningen. I Sverige ser Transportstyrelsen till att samtliga tillstånd kommer in från berörda länder. För att bedriva beställningstrafik, dvs. tillfällig trafik, till länder utanför EU krävs, utöver gemenskapstillstånd, ofta också ett kontrolldokument. Det förekommer även att det beslutas om bilaterala transporttillstånd som medger en transport tur och retur mellan Sverige och en annan stat.

När det gäller tågtrafik krävs det olika typer av tillstånd beroende på var trafiken ska bedrivas. Om trafiken ska ske på järnvägsinfrastruktur som ingår i det europeiska järnvägssystemet krävs det ett gemensamt säkerhetsintyg som i Sverige beviljas av Transportstyrelsen. För viss typ av trafik behövs det endast ett nationellt trafiksäkerhetstillstånd. Det gäller trafik som endast ska bedrivas på järnvägsnät som är funktionellt åtskilda från den svenska delen av EU:s järnvägssystem och endast är avsedda för persontransport i lokal-, stads- eller förortstrafik, privatägda järnvägsnät som ägaren eller en operatör använder för sin godsverksamhet eller för icke-kommersiell persontrafik, eller järnvägsnät som är avsedda att enbart användas för lokala eller historiska ändamål eller turiständamål.

Undantag från kravet på tillstånd gäller t.ex. museiföreningar som bedriver museitrafik och vars huvudsakliga syfte är att bedriva kulturhistorisk verksamhet, järnvägsföretag som utför viss järnvägstrafik, men i syfte att utföra underhåll på infrastrukturen och fordonstillverkare som provkör fordon.

Regler om fartyg som används till sjöfart inom Sveriges sjöterritorium och svenska fartyg som används till sjöfart utanför sjöterritoriet finns i fartygssäkerhetslagen (2003:364). I 1 kap. 4 § finns en uppräkning av ett antal certifikat och dokument som enligt 2 kap. 3 § krävs för ett fartyg, t.ex. fartcertifikat, passagerarfartygscertifikat och certifikat om godkänd säkerhetsorganisation. Certifikaten ska visa att fartyget vid en besiktning för utfärdande av certifikatet motsvarade föreskrivna krav. För ett svenskt passagerarfartyg gäller enligt 3 kap. 2 § ett krav på passagerarfartygscertifikat där det högsta tillåtna antalet passagerare bestäms. För ett utländskt passagerarfartyg krävs det ett certifikat eller en annan handling som anger det högsta tillåtna antalet passagerare.

Enligt 3 kap. 1 § fartygssäkerhetsförordningen (2003:438) ska dokument om godkänd säkerhetsorganisation och certifikat som utfärdas på grund av föreskrifter i fartygssäkerhetslagen eller föreskrifter meddelade med stöd av den lagen utfärdas på formulär som fastställs av Transportstyrelsen.

Det krävs således någon form av godkännande av Transportstyrelsen för att få bedriva buss-, tåg- och färjetrafik. De krav som ställs på sådana transportföretag bör omfattas av den gällande definitionen i lagen om flygpassageraruppgifter i brottsbekämpningen, under förutsättning att den ändras till att omfatta även andra trafikslag. I bestämmelsen används begreppet giltig operativ licens eller motsvarande, medan det för övriga trafikslag i stället anges att det krävs tillstånd eller certifikat. För att tydliggöra att definitionen omfattar även sådana typer av godkännanden bör det anges i 1 kap. 3 § lagen om passageraruppgifter att transportföretag är ett företag som har giltig operativ licens, tillstånd, certifikat eller motsvarande som ger rätt att mot ersättning utföra transporter av passagerare.

Det framgår vidare i den nuvarande definitionen av lufttrafikföretag att den omfattar företag som i sin normala verksamhet samlar in och behandlar PNR-uppgifter i ett elektroniskt system för hantering av reservationer. För övriga trafikslag genomförs dock resor regelmässigt utan föregående reservation, t.ex. genom köp av biljett genom att ”blippa” ett kontokort vid en biljettspärr eller i samband med påstigning på en buss. I artikel 3.5 i PNR-direktivet anges att PNR-uppgifter är en sammanställning av för resan nödvändiga uppgifter om varje enskild passagerare som gör det möjligt för det lufttrafikföretag som sköter bokningen och andra deltagande lufttrafikföretag att behandla och kontrollera reservationen för varje resa som bokas av en person eller för en persons räkning, oavsett om uppgifterna finns i reservationssystemet, det avgångskontrollsystem som används för att checka in passagerare på flygningar eller likvärdiga system med motsvarande uppgift. I artikel 3.6 definieras reservationssystem som lufttrafikföretagets interna system, där PNR-uppgifter samlas för hantering av reservationer.

Definitionen av PNR-uppgifter i direktivet är således bredare än vad som framgår om insamlingen och behandlingen av PNR-uppgifter i definitionen av lufttrafikföretag i 1 kap. 3 § lagen om passageraruppgifter i brottsbekämpningen. För att även företag som säljer biljetter på andra sätt än det som är gängse inom flygtrafiken bör definitionen

av transportföretag modifieras. Utöver att PNR-uppgifterna behandlas i ett elektroniskt system för hantering av reservationer bör det även anges att uppgifterna kan behandlas i ett avgångssystem för att checka in passagerare, i likhet med bestämmelsen i direktivet. Det bör vidare anges att behandlingen kan ske i ett elektroniskt system för köp av biljetter eller likvärda system med motsvarande uppgifter. På så sätt omfattas även transportföretag som säljer biljetter utan föregående reservation.

16.5 Vilka uppgifter ska överföras?

Förslag

Transportföretagen ska endast överföra PNR-uppgifter till enheten för passagerarinformation som företagen samlar in som en del av sin normala verksamhet. Vilka PNR-uppgifter för respektive trafikslag som ska överföras ska framgå av bilagor till lagen om passageraruppgifter i brottsbekämpningen.

För de företag som agerar på den internationella resemarknaden för tåg-, buss- och färjetrafik finns det stora skillnader i vilka uppgifter som samlas in. När det gäller pendlingstrafiken över Öresundsbron sker många av resorna med periodbiljett som betalas vid ett tillfälle och sedan används under den period som biljetten gäller. För att köpa via en app, t.ex. genom Skånetrafiken eller Hallandstrafiken, krävs det att resenären anger ett mobiltelefonnummer samt betaluppgifter i form av kortuppgifter eller mobiltelefonnummer för att betala med Swish. E-postadress behövs enbart anges om användaren vill skapa ett konto och namn behöver endast anges för att kunna betala mot faktura. Vid köp av ett fysiskt resekort i automat eller hos ombud behöver resenären inte uppge några personuppgifter alls. Däremot förknippas köpet alltid med uppgifter om någon form av betalning, t.ex. kortuppgifter eller ett mobiltelefonnummer kopplat till betalning via Swish. En periodbiljett är inte heller personlig utan kan användas av flera personer, vilket gör det svårt att identifiera vem som har rest med biljetten vid ett visst tillfälle.

Inom sjöfarten är registrering av passagerare reglerad på EU-nivå[4] och genomförd i svensk rätt genom Transportstyrelsens föreskrifter och allmänna råd.[5] Föreskrifterna gäller svenska eller utländska passagerarfartyg som ankommer till eller avgår från svensk hamn, med undantag för örlogsfartyg, trupptransportfartyg och fritidsfartyg. Uppgiftsskyldigheten för fartyg beror på resans längd. För alla resor gäller att före avgång ska samtliga ombordvarande räknas och uppgift om antalet ombordvarande ska lämnas till befälhavaren. Uppgiften ska även lämnas till Sjöfartsverket via, NSW på det sätt som verket anvisar vid det aktuella tillfället. Vid resor som överstiger 20 nautiska mil från avgångshamnen ska efternamn, förnamn eller initialer, kön, ålder, födelseår eller åldersgrupp, nationalitet och uppgifter om behov av särskild vård eller hjälp i nödsituationer som passageraren lämnar av egen vilja registreras. Uppgifterna ska samlas in före avgång och lämnas elektroniskt till Sjöfartsverket via MSW på det sätt som verket anvisar. Uppgifterna får inte lämnas mer än 15 minuter efter avgång, med vissa undantag. När resan säkert har slutförts ska uppgift om detta lämnas elektroniskt till Sjöfartsverket via NSW. I NSW bevaras uppgifterna under 30 dagar. NSW kommer på sikt ersättas av EMSWe, vilket har beskrivits i tidigare avsnitt.

Som synes skiljer sig uppgiftsinsamlingen åt mellan olika trafikslag och olika operatörer. Om skyldigheten att överföra uppgifter endast omfattar uppgifter som transportföretagen redan samlar in av kommersiella skäl kommer uppgifternas kvalitet och kvantitet variera kraftigt beroende på avsändare. Uppgifter om att en periodbiljett har använts för en resa över Öresundsbron ger förhållandevis lite information om en individ jämfört med någon som företagit en gränsöverskridande resa med färja. Trots detta anser vi att det inte är en gångbar lösning att ålägga transportföretagen en skyldighet att samla in vissa specifika passageraruppgifter utan uppgiftsskyldigheten ska endast gälla för uppgifter som företagen samlar in som en del av sin normala verksamhet. Vikten av att undvika ytterligare administrativ belastning väger i detta fall tyngre än brottsbekämpande myndigheters behov av mer omfattande uppgifter. I 2 kap. 1 § lagen om flygpassageraruppp-

[4] Europaparlamentets och rådets direktiv (EU) 2017/2109 av den 15 november 2017 om ändring av rådets direktiv 98/41/EG om registrering av personer som färdas ombord på passagerarfartyg som ankommer till eller avgår från hamnar i gemenskapens medlemsstater och av Europaparlamentets och rådet direktiv 2010/65/EU om rapporteringsformaliteter för fartyg som ankommer till och/eller avgår från hamnar i medlemsstaterna.
[5] Transportstyrelsens föreskrifter om ändring i Transportstyrelsens föreskrifter och allmänna råd (2016:102) om registrering av ombordvarande på passagerarfartyg (TSFS 2023:66).

gifter anges att PNR-uppgifter endast ska överföras i de fall företagen samlar in uppgifterna som en del av sin normala verksamhet och den föreslagna ordningen kräver därför ingen lagstiftningsåtgärd.

Det kan ifrågasättas hur användbara de PNR-uppgifter är som hämtas från obokade resor där ett periodkort eller ett kontokort ”blippas” och det inte sker någon kontroll av vem som reser och den information som en sådan resa innehåller är knapphändig. Även om en enskild resa ofta inte är av intresse för brottsbekämpningen kan den stora mängden information över tid användas för att avslöja mönster. Det uppstår synergieffekter i och med att uppgifter som var för sig inte är användbara i brottsbekämpningen blir intressanta när de ingår i en större mängd data som kan analyseras. Det faktum att uppgifterna för vissa resor kommer att vara knapphändiga innebär också att insamlingen av dem är mindre integritetskränkande än insamlingen av mer omfattande uppgifter som förekommer t.ex. inom flygtrafiken. Eftersom systemen för överföring av PNR-uppgifter till enheten för passagerarinformation är automatiska innebär det inte heller mer administration för transportföretagen att överföra uppgifterna. Vi anser därför att det inte bör göras några undantag från inkludering i PNR-systemet för vissa gränsöverskridande sträckor eller typer av resor.

Vilka passageraruppgifter som ska föras över ska preciseras i lagstiftningen. I PNR-direktivets bilaga I anges de PNR-uppgifter som, om de samlas in av transportföretaget, ska översändas till enheten för passagerarinformation. Uppräkningen består av 19 punkter, varav 18 berör olika typer av uppgifter och en punkt anger att även alla ändringar som har gjorts av PNR-uppgifter ska överföras. Som exempel kan nämnas namn, adress och kontaktuppgifter, betalningsinformation och planerat datum för avresa. Samma uppgifter anges även i bilagan till lagen om flygpassagerarinformation i brottsbekämpningen. Enligt skäl 15 i direktivet har förteckningen i bilaga I till syfte att återspegla de offentliga myndigheternas legitima krav på att kunna förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet och därigenom förbättra den inre säkerheten i unionen, samtidigt som grundläggande rättigheter skyddas, särskilt rätten till skydd av privatlivet och rätten till skydd för personuppgifter.

Uppräkningen av PNR-uppgifter i bilaga I till direktivet bör användas som utgångspunkt för regleringen. Även om flera typer av uppgifter är aktuella för samtliga trafikslag finns det vissa som är spe-

cifika för respektive trafikslag. För tågtrafik kan det t.ex. vara relevant att få tillgång till uppgifter om vilken kupé en viss person är inbokad, vilket inte är tillämpligt för de andra trafikslagen.

Enligt lagen om flygpassageraruppgifter i brottsbekämpningen omfattas inte besättningsmedlemmar av insamlingen av PNR-uppgifter. Inom färjetrafiken är besättningen mycket större och informationen samlas i nuläget redan in inom ramen för NSW och sådan insamling kommer fortsätta genom EMSWe. Det är därför lämpligt att för färjetrafiken även samla in uppgifter om besättningen.

Med tanke på att de intressanta uppgifterna skiljer sig åt mellan trafikslagen förordar vi att det för varje enskilt trafikslag skapas en bilaga till lagen om passageraruppgifter i brottsbekämpningen där det anges en förteckning av vilka uppgifter som ska överföras från transportföretag till enheten för passagerarinformation. Förslag på utformande av dessa förteckningar för tåg-, buss- och färjetrafik återfinns i författningsförslagen. För flygtrafiken ska den nu gällande bilagan till lagen om flygpassageraruppgifter i brottsbekämpningen fortsatt tillämpas. Till följd av detta måste dessutom hänvisningar i den nuvarande lagen om flygpassageraruppgifter i brottsbekämpningen till lagen bilaga ändras så att det i stället anges bilagor.

16.6 Tidpunkt för överföring av PNR-uppgifter

16.6.1 Tåg- och busstrafik

Förslag

Transportföretag som bedriver tåg- och busstrafik ska föra över PNR-uppgifter till enheten för passagerarinformation i samband med att en bokning eller avbokning sker.

Enligt 2 kap. 2 § lagen om flygpassageraruppgifter i brottsbekämpningen ska PNR-uppgifter överföras 24–48 timmar före flygningens avgång, och omedelbart efter det att gatens dörrar har stängts. I praktiken sker den första överföringen 24 timmar före flygningens avgång.

För tåg- och busstrafik är vad som är en avgång inte lika lätt att definiera som det är när det gäller flygtrafik. Ett tåg som avgår från en station i Sverige kan passera flera hållplatser inom landet innan det

korsar gränsen till t.ex. Danmark. Det är möjligt att köpa en biljett efter den ursprungliga avgången och kliva på tåget vid en senare station. Vid den ursprungliga avgången går det alltså inte att ta fram en fullständig lista över vilka passagerare som har köpt en biljett som avser en gränsöverskridande resa och det är inte lämpligt att tiden för överföring bestäms till någon tid innan avgången. Detsamma gäller bestämmelsen om att PNR-uppgifter ska överföras efter att gatens dörrar har stängt, eftersom det inte finns någon motsvarighet för tåg- och busstrafik.

PNR-uppgifter skulle kunna överföras efter att resan har slutförts. Det finns då uppgifter om samtliga som köpt en biljett för en gränsöverskridande resa. Detta omöjliggör dock för brottsbekämpande myndigheter att ingripa om en person av intresse är på väg ut ur landet, vilket innebär att detta inte är någon lämplig lösning.

Den mjukvara som används inom flygtrafiken för att föra över PNR-uppgifter till enheten för passagerarinformation är inte låst till att överföringarna ska ske 24–48 timmar innan avgång och när gaten har stängts. Att så sker beror således på att lagstiftningen ser ut så, och inte på grund av tekniska begränsningar. Det är möjligt att i stället, med samma typ av mjukvara, föra över uppgifter så fort en bokning eller avbokning sker. Det sker i så fall automatiskt och innebär inte någon ytterligare administration eller ytterligare kostnader för transportföretagen. Det har inte heller någon påverkan på bedömningen av intrånget i den personliga integriteten.

För brottsbekämpningen är överföring i realtid att föredra. Det gör det enklare att planera ingripanden och ger mer tid att t.ex. kartlägga kopplingar mellan personer som är inbokade på samma resa. Vi föreslår därför att tåg- och bussföretag kontinuerligt ska föra över PNR-uppgifter i samband med att en bokning eller avbokning sker.

16.6.2 Färjetrafik

Bedömning

Tidpunkten för överföring av PNR-information från färjetrafik ska inte regleras lagen om passageraruppgifter i brottsbekämpningen.

Vår utgångspunkt är att överföring av PNR-information från färjetrafiken kommer kunna ske via EMSWe. Registreringen av passagerare är reglerad på EU-nivå och i svensk rätt genom Transportstyrelsens föreskrifter och allmänna råd. I regleringen är det föreskrivet när uppgifter från passagerarfartyg ska lämnas till Sjöfartsverket. Uppgifterna skickas därefter automatiskt till enheten för passagerarinformation. Med tanke på att tidpunkten för överföring av uppgifter vilar på EU-rättslig grund är det inte aktuellt att i PNR-lagstiftningen föreskriva någon annan tidpunkt för överföring än den redan gällande.

16.6.3 Överföring vid andra tidpunkter

Förslag

Samtliga transportföretag som omfattas av lagstiftningen ska på begäran av enheten för passagerarinformation överföra PNR-uppgifter även vid andra tidpunkter än vad som i övrigt anges i lagen, om enheten bedömer att det i ett enskilt fall är nödvändigt med tillgång till PNR-uppgifter för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller annan allvarlig brottslighet.

I 2 kap. 3 § lagen om flygpassageraruppgifter i brottsbekämpningen framgår att lufttrafikföretag på begäran av enheten för passagerarinformation ska överföra PNR-uppgifter även vid andra tidpunkter än de som anges i 2 §, om det i ett enskilt fall är nödvändigt med tillgång till uppgifterna för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller annan allvarlig brottslighet. Enheten för passagerarinformation som, vanligtvis efter en framställan från en behörig myndighet, ska bedöma om det i ett enskilt fall är nödvändigt med sådan tillgång till uppgifter.

Bestämmelsen bör uppdateras för att återspegla att lagstiftningen omfattar fler trafikslag än flyg. För färjetrafiken är utgångspunkten att PNR-uppgifterna överförs via EMSWe till enheten för passagerarinformation. Det kommer att finnas en viss fördröjning i överföringen och det kan finnas anledning att begära tillgång till uppgifterna innan de har överförts till enheten. En bedömning av om en sådan begäran är nödvändig ska ske i det enskilda fallet. Behovet av att få

tillgång till PNR-uppgifter kan även uppstå innan överföringen till EMSWe har genomförts. Skyldigheten att rapportera till EMSWe ligger förhållandevis nära i tid till ankomst till eller avgång från en svensk hamn men det kan dessförinnan vara berättigat att begära in uppgifterna direkt från ett transportföretag som bedriver passagerartrafik med färja. I lagstiftningen innebär detta inte att någon skillnad görs beroende på om uppgifterna begärs via EMSWe eller direkt från transportföretaget, utan det bör formuleras som en skyldighet för företagen att, på begäran, överföra uppgifter till enheten för passagerarinformation.

När det gäller tåg- och busstrafik ska överföring av uppgifter ske i samband med att en bokning eller avbokning görs. För en stor andel av uppgifterna gäller alltså att enheten för passagerarinformation redan har samma information som finns hos transportföretagen. I vissa situationer kan det emellertid finnas behov av att begära in uppgifter från företagen. Det gäller t.ex. uppgifter från resor inom EU som inte ingår i det urval av sådana resor från vilka PNR-uppgifter bevaras efter den inledande förhandsbedömningen eller uppgifter som har bevarats hos enheten under sex månader och därefter anonymiserats. Med beaktande av att ändamålet med möjligheten att begära in uppgifter i enlighet med den aktuella bestämmelsen är att avvärja en specifik och faktisk fara för terrorism eller annan allvarlig brottslighet bör en sådan möjlighet finnas även avseende tåg- och busstrafik.

16.7 Administration och kostnader för transportföretagen

En skyldighet för transportföretag att översända samtliga passageraruppgifter från gränsöverskridande resor till enheten för passagerarinformation kan komma att innebära en förändrad administrativ börda för transportföretagen. Om detta medför kostnader kan det snedvrida konkurrensen och missgynna de mindre aktörerna som har svårare att hantera större utgifter.

Företagen måste t.ex. implementera tekniska lösningar för att automatiskt kunna skicka passagerarinformation till myndigheten som handhar den centrala databasen. Dessa kostnader ska emellertid kontrasteras mot de kostnader som dagens lagstiftning medför. De begäranden som inkommer till transportföretagen med stöd av t.ex.

25 § polislagen är mer administrativt krävande än en automatisk överföring. Sådana begäranden kan antas kraftigt minska om samtliga passageraruppgifter i stället förs över automatiskt till en central databas där uppgifterna är tillgängliga för behöriga myndigheter. Som exempel kan nämnas att en större aktör inom transportbranschen under 2025 fick in 2 000 begäranden om utlämnande av uppgifter från Polismyndigheten, varav 500 rörde gränsöverskridande resor.

Vid genomförandet av PNR-direktivet bekostades it-infrastrukturen vid enheten för passagerarinformation av allmänna medel, men transportföretagen stod själva för de tekniska lösningar som krävdes för att automatiskt kunna föra över PNR-uppgifter till enheten. I samband med detta utvecklade flera privata leverantörer plattformar som företagen kan använda för överföringen. Det kan t.ex. fungera som ett gränssnitt som samlar in data från lufttrafikföretagen och levererar den i rätt format till enheten. Lufttrafikföretagen betalar för detta vanligtvis en licensavgift som kan vara ett fast pris per månad eller rörlig baserad på antalet genomförda flygningar eller antalet passagerare. Utöver detta tillkommer en initial kostnad för att etablera den tekniska kopplingen mellan lufttrafikföretagets bokningssystem och enheten för passagerarinformation. Det har inte kommit fram annat än att även mindre flygbolag klarade av både den initiala kostnaden och löpande kostnader.

IATA, dvs. flygbolagen globala branschorganisation, har uttalat sig om hur kostnaderna som det medför att en stat kräver passageraruppgifter från lufttrafikföretag.[6] Eftersom säkerheten är ett statligt ansvarsområde är det också staten som har i uppgift att genomföra lämpliga åtgärder och säkerställa att dessa är finansierade. Kostnaderna för it-system och, infrastruktur och löpande kostnader bör fördelas på ett lämpligt sätt mellan allmänna medel och företagen. Mottagande, behandling och analys av passageraruppgifterna bör bekostas av allmänna medel, i likhet med andra åtgärder för att främja gränskontrollen. Enligt IATA har flygbranschen full förståelse för det ansvar som vilar på lufttrafikföretagen och deras möjlighet att ge stöd till myndigheter i brottsbekämpningen.

För att underlätta för transportföretagen och undvika att snedvrida konkurrensen på resemarknaden är ett alternativ att låta utvecklingen av den tekniska infrastrukturen finansieras med offentliga medel. Eftersom syftet med systemet är att bekämpa terrorism och

[6] IATA, *Tackling Passenger Data Charges*, februari 2019.

grov brottslighet kan det argumenteras för att det offentliga, som har det yttersta ansvaret för dessa frågor, bör stå för kostnaden. Om myndigheten som handhar den centrala databasen, dvs. Polismyndigheten genom enheten för passagerarinformation, även ansvarar för framtagande av it-infrastrukturen säkerställs också att systemets design optimeras för att passa enhetens behov. Det kan även innebära fördelar om samtliga transportföretag översänder uppgifter genom en enhetlig och standardiserad teknisk lösning via t.ex. en nationell plattform. Datan som kommer in till den centrala databasen kommer då se likadan ut oavsett vilken operatör som har översänt den.

Även med beaktande av ovanstående anser vi att kostnaden för implementeringen av ett system för insamling av passageraruppgifter bör delas mellan staten och de privata aktörerna. Mottagandet och den fortsatta behandlingen av uppgifterna sker hos enheten för passagerarinformation och eventuella anpassningar av de tekniska lösningar som används för flygtrafiken bör bekostas genom Polismyndighetens anslag. Kostnaderna för att sammanställa och överföra passageraruppgifter till enheten bör dock bäras av respektive företag. De tredjepartslösningar som i stor utsträckning används av lufttrafikföretagen bör vara tillgängliga även för aktörer inom andra trafikslag. En sådan fördelning av kostnaderna ligger också i linje med hur genomförandet av PNR-direktivet finansierades och hur andra regleringar av privata aktörers skyldigheter gentemot det allmänna i brottsbekämpande syfte har finansierats. Utöver detta har transportföretagen, i likhet med vad som har skett i flygbranschen, möjlighet att övervältra kostnaden på passagerare. Såvitt utredningen har kunnat utröna finns det inga beräkningar på hur stora kostnader genomförandet av PNR-direktivet har inneburit per såld flygbiljett. Under arbetet som ledde fram till direktivet förutspådde emellertid kommissionen att det skulle leda till en extrakostnad om 0,10 euro per biljett, dvs. cirka 1 krona, vilket ansågs vara högt räknat.[7] Även med beaktande av osäkerheten i denna prognos bör kostnadsökningen för transportföretagen beräknat per biljett utgöra en marginell del av den totala biljettkostnaden.

Sammantaget anser vi att den lämpligaste lösningen avseende finansieringen är att kostnaderna för insamling och överföring av passa-

[7] Europeiska kommissionen, *Sammanfattning av konsekvensbedömningen. Följedokument till förslag till Europaparlamentets och rådets direktiv om en gemensam strategi för användning av passageraruppgifter (PNR-uppgifter), SEK(2011) 133 slutlig*, 2 februari 2011.

geraruppgifter bärs av transportföretag och att kostnaderna för mottagande och fortsatt behandling finansieras av allmänna medel.

16.8 Inrikes trafik

Bedömning

PNR-lagstiftningen ska inte omfatta inrikestrafik med tåg, buss eller färja.

Av artikel 1.1 a, 2 och 3.3 i PNR-direktivet följer att PNR-systemet för flygtrafik endast omfattar utrikesflygningar. Ett liknande system för andra trafikslag skulle emellertid kunna omfatta även inrikes trafik.

Den fria rörligheten inom Sverige framgår av 2 kap. 8 § regeringsformen där det anges att var och en är gentemot det allmänna skyddad mot frihetsberövande och att den som är svensk medborgare även i övrigt är tillförsäkrad frihet att förflytta sig inom riket och att lämna det. Enligt 2 kap. 20 och 21 §§ får rörelsefriheten begränsas genom lag endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Det framgår vidare att begränsningen ska vara proportionerlig till det ändamål som har föranlett den.

Den grundlagsstadgade inhemska rörlighetsfriheten inom Sverige och eventuella inskränkningar i den skiljer sig från den EU-rättsliga regleringen av fri rörlighet inom unionen och under vilka förutsättningar den får begränsas. Medan gränsöverskridande resor görs mer sällan, utgör inrikesresor en naturlig del av många invånares vardag, arbete och sociala liv. Genom att kontrollera resor inom landet kan myndigheter skapa en mycket detaljerad bild av en individs vanor, relationer och umgängeskrets. Ett sådant ingrepp kan således anses vara av allvarligare grad än insamling av passageraruppgifter från gränsöverskridande resor. Frågan om inrikes resor blir därmed mer komplex än för gränsöverskridande resor.

I våra direktiv anges inte specifikt om det bör övervägas att inkludera inrikestrafik i en trafikslagsneutral lagstiftning. Som exempel på lagstiftning som aktualiseras anges emellertid polislagen och tullbefogenhetslagen, vilka endast berör gränsöverskridande resor. Det nämns vidare att obokade biljetter är vanligt förekommande vid gränspendling och att tillgången till passageraruppgifter från t.ex. färje- och

tågtrafik till och från Sverige är mer begränsad än från flygtrafiken. Slutligen anges att passageraruppgifter från persontransporter till och från Sverige är en viktig del i det brottsbekämpande arbetet. Frågan om inrikes resor diskuteras således inte i utredningsdirektiven.

För tåg-, buss- och färjetrafiken innebär frågan om inrikes resor vissa gränsdragningsproblem. Det är inte praktiskt görbart att samla in uppgifter från kollektivtrafiken utan det behöver ske en avgränsning som t.ex. innebär att endast fjärrtrafik inkluderas. Även med en sådan avgränsning framstår insamling av alla passageraruppgifter som ett synnerligen allvarligt ingrepp i de grundläggande rättigheterna, även med beaktande av att de uppgifter som samlas in i sig är relativt harmlösa. Med tillgång till sådana uppgifter går det att mer kartlägga en persons rörelser i vardagslivet, vilket innebär en viss skillnad i jämförelse med gränsöverskridande resor. Mot bakgrund av detta har vi valt att inte vidare utreda frågan om inrikes resor med tåg, buss och färja kan inkluderas i den trafikslagsneutrala PNR-lagstiftningen. Enligt vår uppfattning finns det dock inga hinder för transportföretag att frivilligt dela passagerarinformation från inrikes resor på samma sätt som inom PNR-lagstiftningen till enheten för passagerarinformation.

16.8.1 Inrikesflyg

Förslag

PNR-lagstiftningen ska även omfatta inrikesflygningar.

Inrikesflyg har en annan karaktär än annan inrikestrafik. Det går inte att på samma sätt kartlägga någons alla förflyttningar inom landet eftersom flyg i större utsträckning används vid enstaka tillfällen, jämfört med andra transportmedel som av många människor används dagligen. Det finns dock en stark samhällelig förväntan att det ska gå att röra sig inom rikets gränser utan att bli föremål för statlig kontroll.

I nuläget sker inhämtning av uppgifter från inrikesflyg genom begäran om uppgifter om en specifik person och inte på ett systematiskt sätt. Genom att i stället hämta in samtliga uppgifter i förväg är det möjligt att följa resvägen för personer av intresse även efter

att de kommit in i Sverige. Ändamålet med insamling av PNR-uppgifter från inrikestrafiken med flyg är att ytterligare öka tillgången till data för brottsbekämpande myndigheter och på så sätt förbättra förutsättningarna för att bekämpa terrorism och annan allvarlig brottslighet. Ett sådant ändamål är, som har konstaterats, godtagbart i ett demokratiskt samhälle. Insamlingen är vidare ägnad att uppnå målet med åtgärden. Den förändrade säkerhetssituation och utvecklingen av den allvarliga brottsligheten talar också för att ytterligare ingrepp i de grundläggande rättigheterna är berättigade. Precis som för gränsöverskridande resor kommer en stor andel av PNR-uppgifterna endast att lagras i databasen vid enheten för passagerarinformation och aldrig granskas av en fysisk person. Uppgifterna kommer vidare att omfattas av samma skydd för personuppgifter och samma rättssäkerhetsgarantier som uppgifter från gränsöverskridande resor. Inrikesflygningar är flygningar inom EU och behandlingen av PNR-uppgifter för sådana flygningar omfattas således av reglerna som föreslås i avsnitt 8.2–3. Mot bakgrund av ovanstående anser vi att värdet av att inkludera inrikesflyg i PNR-systemet väger tyngre än det ingrepp i grundläggande rättigheter som det utgör. PNR-lagstiftningen ska därför justeras för att omfatta även inrikesflygningar.

Den praktiska inkorporeringen av inrikesflyg i PNR-systemet är betydligt enklare än för andra trafikslag. En stor majoritet av inrikesflygen genomförs av två större operatörer som även har utrikesflyg. Det finns ett fåtal mindre aktörer som främst bedriver inrikesflyg, men även dessa trafikerar enstaka rutter utomlands. Såvitt vi har kunnat utröna finns det i dagsläget inget flygbolag som enbart bedriver inrikestrafik i Sverige.

Flygbolagen samlar in i stort sett samma uppgifter om passagerare och har redan den mjukvara som krävs för överföringen och en etablerad kontakt med databasen vid enheten för passagerarinformation. Det som krävs är således endast att de flygningar som avser inrikestrafik läggs till de flygningar som redan ingår i PNR-systemet. Vi föreslår därför att det i 2 kap. 1 § lagen om passageraruppgifter i brottsbekämpningen ska läggas till en bestämmelse med innebörden att skyldigheten för lufttrafikföretag att föra över PNR-uppgifter även omfattar flygningar mellan två flygplatser i Sverige.

17 Speciallagstiftning för brottsbekämpande myndigheter

17.1 Inledning

I avsnitt 14 beskrivs olika lösningar för ett system med central insamling och lagring av passageraruppgifter där behöriga myndigheter har möjlighet att begära tillgång till uppgifterna för att använda i sina respektive verksamheter. Parallellt med ett sådant system finn det speciallagstiftning där brottsbekämpande myndigheter ges befogenhet att begäran in uppgifter direkt från transportföretagen. Sådan lagstiftning finns i dagsläget i form av t.ex. 25 § polislagen och 7 kap. 12 § tullbefogenhetslagen. I detta avsnitt beskriver vi de befintliga möjligheterna för relevanta myndigheter att använda passageraruppgifter i brottsbekämpningen. Vi lägger även fram förslag till ny lagstiftning eller förslag för att förbättra den befintliga lagstiftningen.

En uppenbar nackdel med att – i stället för ett centralt system dit trafikföretag översänder passageraruppgifter vid ett eller, som i PNR-systemet för flygtrafik, två tillfällen – låta brottsbekämpande myndigheter begära tillgång till passageraruppgifter direkt från trafikföretag, är att företagen kommer att ta emot förfrågningar från en rad olika myndigheter. I och med införandet av ett trafikslagsneutralt PNR-system kommer dock sådana förfrågningar att minska.

I detta avsnitt har vi fokuserat på de myndigheter som är behöriga inom PNR-systemet enligt förordningen om flygpassageraruppgifter i brottsbekämpningen. Utöver dessa kan det dessutom diskuteras om ytterligare myndigheter som har ett brottsbekämpande uppdrag bör ges samma möjlighet att begära tillgång till passageraruppgifter. Bland sådana myndigheter kan exempelvis nämnas Skatteverket och Kustbevakningen. Även dessa myndigheter kan anses ha ett behov av passageraruppgifter i sina respektive verksamheter. Vid en kritisk punkt kommer denna lösning att medföra mer administration för trafikföre-

tagen än ett centralt system dit alla passageraruppgifter ska översändas vid vissa givna tidpunkter.

17.2 Tullverket

Förslag

Transportföretag ska vara skyldiga att även lämna uppgifter om passagerares kön som företaget har tillgång till.

Företagens skyldighet att lämna uppgifter om betalningssätt ska ändras till betalningsinformation.

Tullverkets möjligheter att använda uppgifter om varor, passagerare och fordon i brottsbekämpningen förändrades i och med ikraftträdandet av tullbefogenhetslagen i november 2024 samt genom förändringar i tullverkets brottsdatalag. Skyldigheten för transportföretag att på begäran av Tullverket skyndsamt lämna uppgifter utökades från att avse namn, resrutt, bagage och medpassagerare samt sätt för betalning och bokning till att även inkludera födelsedatum, nationalitet, mobiltelefonnummer och e-postadress. Den tidigare lagstiftningen krävde att bokningsuppgifter skulle förstöras så snart det visat sig att de inte hade betydelse för att förebygga, förhindra, upptäcka, utreda eller lagföra brott. Regleringen om omedelbar förstöring försvårade Tullverkets underrättelsearbete påtagligt.[1] Eftersom uppgifterna inte fick bevaras var det inte möjligt att använda dem i syfte att upptäcka historiska samband och mönster, om det inte fanns ett pågående underrättelseuppslag. Det försvårade också arbetet med att ta fram nya riskprofiler och kriterier för riskprofilerna. Lagstiftningen ändrades därför så att Tullverket, enligt 7 kap. 13 § andra stycket tullbefogenhetslagen, får ta del av bokningsuppgifter genom direktåtkomst under högst sex månader från det att transporten har ankommit eller avgått, om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott. Enligt 4 kap. 9 a § tullverkets brottsdatalag ska de uppgifter som med stöd av 7 kap. 13 § tullbefogenhetslagen tillhandahålls på annat sätt än direktåtkomst förstöras senast sex månader efter det att de behandlades första gången.

[1] Prop. 2023/24:132, *Ny tullbefogenhetslag*, s. 373.

Bokningsuppgifterna får numera också behandlas för att göra de analyser som behövs för att uppdatera eller skapa nya kriterier som kan användas vid planering av kontroller eller urval av kontrollobjekt. Utöver detta får bokningsuppgifterna enligt 3 kap. 2 § tullverkets brottsdatalag göras gemensamt tillgängliga, under förutsättning att tillgången till uppgifter begränsas till särskilt angivna tjänstemän som har i uppgift att planera kontroller, välja ut kontrollobjekt och göra analyser som behövs för att uppdatera eller skapa nya kriterier som ska användas vid planering av kontroller eller urval av kontrollobjekt.

Det är för tidigt att utvärdera de förändringar som trädde i kraft i och med den nya tullbefogenhetslagen. I stort framstår lagstiftningen som ändamålsenlig. Det har emellertid framkommit att det finns ett behov att utöka uppgiftsskyldigheten för transportföretag till att även omfatta resenärens kön. Uppgifter om kön kan vara användbart i verksamheten och sådana uppgifter samlas t.ex. in inom ramen för PNR-systemet. Sådana uppgifter kan ytterligare förfina selekteringen när urval för kontroll ska göras. I uppräkningen av uppgifter i 7 kap. 12 § tullbefogenhetslagen bör därför kön läggas till.

I bestämmelsen anges att uppgifter om betalningssätt omfattas av uppgiftsskyldigheten. Begreppet betalningssätt är snävt och föråldrat och det bör i stället formuleras som betalningsinformation. Benämningen betalningssätt fördes in i lagstiftningen 1995 och har inte ändrats sedan dess. Det går nu att få information om t.ex. biljettpris och kortnummer, vilket är av betydelse i brottsbekämpningen. Ordalydelsen i bestämmelsen bör därför ändras till att i stället ange betalningsinformation.

17.3 Polismyndigheten och Säkerhetspolisen

Polismyndighetens och Säkerhetspolisens möjligheter att begära uppgifter om ankommande och avgående transporter från transportföretag som befordrar varor, passagerare eller fordon till eller från Sverige i 25 och 26 §§ polislagen utformades för att efterlikna den reglering som gällde för Tullverket innan ikraftträdandet av tullbefogenhetslagen. I tidigare förarbeten har det bedömts att Polismyndigheten, på motsvarande sätt som Tullverket, har stor nytta av tillgång till uppgifter i transportföretagens bokningsregister och att bestämmelserna

bör utformas på samma sätt som då gällde för Tullverket[2] En naturlig utgångspunkt är därför att beakta om förändringar liknande de som har införts i tullbefogenhetslagen är lämpliga även avseende polislagen. I detta avsnitt behandlas förslag på förändringar av polislagen och anslutande författningar som berör både Polismyndigheten och Säkerhetspolisen. I det därefter följande avsnittet behandlas förslag som enbart berör Polismyndigheten.

17.3.1 Uppgiftsskyldigheten

Förslag

Transportföretag ska vara skyldiga att även lämna uppgifter om passagerares födelsedatum, kön, nationalitet, e-postadress och mobiltelefonnummer som företaget har tillgång till.

Företagens skyldighet att lämna uppgifter om sättet för betalning ska ändras till betalningsinformation.

I 25 § polislagen anges att ett transportföretag endast har skyldighet att lämna de uppgifter som företaget har tillgång till om passagerare som avser namn, resrutt, bagage och medpassagerare samt sättet för betalning och bokning. I tullbefogenhetslagen har dessa uppgifter utökats med födelsedatum, nationalitet, e-postadress och mobiltelefonnummer. Enligt vårt förslag ovan ska det dessutom vara tillåtet att begära uppgifter om kön. Utöver detta ska begreppet betalningssätt, vilket i polislagen motsvaras av sättet för betalning, ersättas av betalningsinformation.

Det kan konstateras att den brottsbekämpande förmågan förbättras ju fler typer av information som tillgängliggörs. De ytterligare uppgifterna kan exempelvis användas för att förhindra att personer med samma namn förväxlas. Ökad tillgång till uppgifter innebär t.ex. en större säkerhet i bedömningar och urval för kontroll om fler uppgifter görs tillgängliga.[3] Uppgifter om e-postadress och mobiltelefonnummer kan även användas för att etablera kopplingar mellan individer som annars inte hade uppdagats eller kopplingar mellan två identiteter som används av en och samma individ.

[2] Prop. 1996/97:175, *Ändringar i polislagen m.m.*, s. 67–68.
[3] Jfr prop. 2023/24:143, *Ny tullbefogenhetslag*, s. 360.

Uppgifterna ger sammantaget en viss bild av en person och dennes planerade eller genomförda resa. För vissa enskilda individer kommer det dessutom gå att kartlägga deras resmönster över tid. Uppgifterna är dock både var för sig och sammantaget relativt harmlösa och inskränkningen av den personliga integriteten som behandlingen av dem innebär får anses vara lindrig. En majoritet av de nu aktuella uppgifterna är sådana som samlas in enligt PNR-direktivet, där det dessutom, i bilaga I till direktivet, anges ytterligare typer av uppgifter som får samlas in. Inom PNR-systemet översänds dessutom samtliga uppgifter som lufttrafikföretagen har tillgång till och som anges i bilaga I till enheten för passagerarinformation. Enligt polislagen ska i stället uppgiftsskyldigheten för transportföretagen gälla när Polismyndigheten eller Säkerhetspolisen begär det. Ett förfarande där myndigheterna framställer en begäran om att uppgifter ska lämnas är betydligt mindre integritetskränkande än ett system där all tillgänglig information om samtliga passagerare samlas in på ett automatiskt och systematiskt vis.

Enligt vår bedömning står det inte i strid med de EU-rättsliga reglerna om respekt för privatlivet och skydd för personuppgifter i artikel 7 och 8 i EU:s rättighetsstadga att möjliggöra för Polismyndigheten och Säkerhetspolisen att, utöver de i nuläget tillåtna uppgifterna, även begära uppgifter om födelsedatum, kön, nationalitet, e-postadress och mobiltelefonnummer.

Under lagstiftningsarbetet med tullbefogenhetslagen förde Polismyndigheten fram att det bör övervägas om Tullverket ska ges möjlighet att i underrättelsesyfte begära alla uppgifter som inte utgör känsliga personuppgifter från transportföretagen.[4] Regeringen ansåg att det var en fråga som kräver ytterligare noggranna överväganden och lämnade inget sådant förslag. Fördelen med att inte definiera vilka uppgifter som får samlas in är att uppgifter som i framtiden kan vara intressanta i underrättelsearbetet får samlas in utan att lagstiftningen behöver ändras. När den nuvarande lagstiftningen genomfördes användes t.ex. inte mobiltelefoner och e-post i samma utsträckning som i dag. För att kunna samla in sådana uppgifter krävs det således att lagstiftningen förändras. Det säger sig självt att liknande situationer kan uppstå även för andra typer av information i framtiden.

Med en så bred reglering av vilka uppgifter som får samlas in är det emellertid svårt att bedöma graden av intrång i den personliga

[4] Prop. 2023/24:132, *Ny tullbefogenhetslag*, s. 359.

integriteten som insamlingen kan innebära. Även om insamling av känsliga uppgifter inte är tillåten kan det på längre sikt vara svårt att förutse vilka typer av uppgifter det kan röra sig om. För att på ett förutsägbart sätt kunna bedöma det intrång i den personliga integriteten som en insamling kan innebära, anser vi därför att skyldigheten för ett transportföretag att, på begäran av Polismyndigheten eller Säkerhetspolisen, lämna uppgifter om passagerare ska begränsas till uppgifter om namn, resrutt, bagage och medpassagerare, sättet för betalning och bokning samt uppgifter om nationalitet, kön, födelsedatum, mobiltelefonnummer och e-postadress.

Vi har i avsnitt 17.2 föreslagit att begreppet betalningssätt i tullbefogenhetslagen ersätts av betalningsinformation till följd av att det är föråldrat samt att det inte omfattar samtliga uppgifter om betalningen som är relevanta i för brottsbekämpningen. Därför bör även 25 § polislagen justeras så att den omfattar betalningsinformation i stället för sättet för betalning.

17.3.2 Vem ska tillhandahålla uppgifterna?

Förslag

Om ett transportföretag har lämnat över uppgiften att hantera uppgifter om transporter till något annat företag har det företaget motsvarande skyldighet att tillhandahålla Polismyndigheten eller Säkerhetspolisen uppgifterna.

Det förekommer att ett annat företag än själva transportföretaget sköter bokningen av transporter. I sådana fall bör skyldigheten att lämna uppgifter även gälla för det företaget. Det kan t.ex. vara en speditör eller något annat företag. Det faktum att ett transportföretag väljer att organisera sin verksamhet på ett visst sätt bör inte hindra Polismyndigheten och Säkerhetspolisen att få den information som normalt sett hade funnits hos transportföretaget. Detta gäller redan i nuvarande reglering, men bör förtydligas i lagtexten i 25 § polislagen.

17.3.3 Föreläggande

Förslag

Polismyndigheten och Säkerhetspolisen ska få förelägga ett transportföretag att fullgöra sina skyldigheter att lämna uppgifter om transporter. Beslutet om föreläggande får förenas med vite och gäller omedelbart.

Ett beslut om föreläggande ska få överklagas till allmän förvaltningsdomstol. Vid överklagande till kammarrätt ska det krävas prövningstillstånd.

Transportföretag har en skyldighet att lämna de uppgifter om transporter som begärs, men Polismyndigheten och Säkerhetspolisen saknar ett effektivt påtryckningsmedel om företaget inte uppfyller sin skyldighet. Om tillgången till information fördröjs kan det innebära att tidskritiska åtgärder inte kan vidtas. I 7 kap. 14 § tullbefogenhetslagen anges att Tullverket får förelägga ett transportföretag att fullgöra sina skyldigheter, att föreläggandet får förenas med vite och att beslutet gäller omedelbart. Det framstår som lämpligt att även Polismyndigheten och Säkerhetspolisen har samma möjlighet. Det ska därför införas en ny paragraf, 26 a §, i polislagen med innebörden att Polismyndigheten och Säkerhetspolisen får förelägga ett transportföretag att fullgöra sina skyldigheter att lämna uppgifter enligt 25 och 26 §§ polislagen, att beslutet får förenas med vite samt att beslutet gäller omedelbart. Ett beslut om föreläggande ska vara överklagbart till allmän förvaltningsdomstol. Vid överklagande till kammarrätt bör det krävas prövningstillstånd.

17.3.4 Överklagande

Förslag

Polismyndighetens och Säkerhetspolisens begäran om uppgifter från transportföretag får inte överklagas.

Enligt 7 kap. 12 § tredje stycket tullbefogenhetslagen får Tullverkets begäran om bokningsuppgifter inte överklagas. I förarbetena angavs bl.a. att det är svårt att förstå varför transportföretagen ska ha rätt att överklaga en begäran från Tullverket om att få tillgång till bokningsuppgifter. Om sådana överklaganden skulle sättas i system finns det risk att syftet med lagstiftningen går förlorat, eftersom Tullverket då inte skulle kunna få uppgifterna i tid för att hinna förbereda kontroller.[5]

Samma argument är giltiga när det gäller Polismyndighetens och Säkerhetspolisens begäranden om uppgifter från transportföretag. Det är av vikt att myndigheternas arbete inte fördröjs, särskilt med beaktande av att många ingripanden är tidskänsliga. Det bör därför anges i 25 § polislagen att en sådan begäran inte får överklagas.

17.3.5 Terminalåtkomst ändras till direktåtkomst

Förslag

Begreppet terminalåtkomst i polislagen och polisens brottsdatalag ska ändras till direktåtkomst.

Enligt 26 § polislagen får transportföretag lämna uppgifter enligt 25 § på så sätt att de görs läsbara för Polismyndigheten eller Säkerhetspolisen genom terminalåtkomst samt att så får ske endast i den omfattning och under den tid som behövs för att kontrollera aktuella transporter. I 2 kap. 14 § polisens brottsdatalag anges att vid terminalåtkomst enligt 26 § polislagen får personuppgifter inte ändras eller bearbetas på annat sätt.

Begreppet terminalåtkomst anses numera vara föråldrat. Det är sällan som terminaler används för att ge tillgång till uppgifter. Begreppet syftar till att möjliggöra en automatiserad tillgång till uppgifter utan att de kan bearbetas eller på annat sätt påverkas. I senare lagstiftning används i stället begreppet direktåtkomst.[6] Det finns ingen legaldefinition av direktåtkomst. Högsta förvaltningsdomstolen har emellertid uttalat att med direktåtkomst menas vanligen att någon har direkt tillgång till någon annans databas eller register

[5] Prop. 2023/24:132, *Ny tullbefogenhetslag*, s. 256.
[6] Se t.ex. prop. 2023/34:132, *Ny tullbefogenhetslag*, s. 375.

och på egen hand kan söka efter information, utan att kunna påverka innehållet i databasen eller registret.[7]

Terminologin i polislagen och polisens brottsdatalag bör uppdateras så att i stället det mer moderna begreppet direktåtkomst används. Detta innebär ingen förändring i sak.

17.4 Polismyndigheten

I detta avsnitt behandlas förslag till förändringar av polislagen och anslutande författningar som berör Polismyndigheten, men inte Säkerhetspolisen.

17.4.1 Tillåten tid för behandling

Förslag

Uppgifter som begärs in från transportföretag med stöd av polislagen ska förstöras sex månader efter att de behandlades första gången, om de inte behövs i ett enskilt fall.

Polismyndigheten får ta del av uppgifter genom direktåtkomst under sex månader efter att transporten ankommit eller avgått.

Den tid som Polismyndigheten får behandla personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott framgår av 4 kap. 1 § polisens brottsdatalag. Med hänvisning till 2 kap. 17 § anges att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Regleringen skiljer sig från tullbefogenhetslagen där det i 7 kap. 13 § anges att Tullverket får ta del av uppgifter genom direktåtkomst innan transporten har inkommit eller avgått. Tullverket får även ta del av sådana uppgifter under högst sex månader därefter om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott. De uppgifter som Tullverket tar del av på annat sätt än direktåtkomst ska enligt 4 kap. 9 a § tullverkets brottsdatalag förstöras senast sex månader efter att de behandlades första gången.

[7] HFD 2017 ref. 67.

I förarbetena[8] till lagstiftningen som rör Polismyndighetens behandling av personuppgifter anges att brottsdatalagens bestämmelse i 2 kap. 17 § om att personuppgifter inte får behandlas under längre tid än nödvändigt med hänsyn till ändamålet med behandlingen ger ett tillräckligt skydd för uppgifterna. Bestämmelsen i brottsdatalagen har sin grund i artikel 6.1 e i dataskyddsdirektivet och är ett uttryck för den grundläggande principen om lagringsminimering vid behandling av personuppgifter.

Gränsen på sex månader som gäller för Tullverkets behandling av bokningsuppgifter motiverades med att den tidigare regleringen om omedelbar förstöring försvårade myndighetens underrättelsearbete påtagligt.[9] Eftersom uppgifterna inte fick bevaras var det inte möjlighet att använda dem i syfte att upptäcka historiska samband och mönster, om det inte fanns ett pågående underrättelseuppslag. Det försvårade även arbetet med att ta fram nya riskprofiler och kriterier för dessa. Regeringen förde vidare fram att det i underrättelseverksamheten är nödvändigt att kunna ta fram uppgifter som speglar systematik avseende resor eller transporter av varor och transportmedel. Det är mycket svårt att göra utan att ha tillgång till uppgifter om transporter över tid. Kravet på omedelbar förstöring medför också att det saknas möjlighet att använda bokningsuppgifterna för att kartlägga kriminella organisationer och deras verksamhet i syfte att få fram nya objekt att kontrollera.

Polismyndigheten har i likhet med Tullverket ett behov av uppgifter för att upptäcka historiska samband och för att kartlägga kriminella organisationer. För att på ett bättre sätt kunna använda uppgifter som begärs in med stöd av 25 § polislagen bör lagringstiden förändras och det framstår som lämpligt att den ligger i linje med vad som gäller för Tullverket. Det ligger även i linje med hur länge PNR-uppgifter från flygtrafik utom EU som huvudregel får lagras enligt PNR-lagstiftningen. Vi bedömer att intresset av en mer effektiv brottsbekämpning vid en avvägning mot skyddet för den personliga integriteten motiverar en lagringstid på sex månader. Det ska därför införas en bestämmelse med sådant innehåll i 4 kap. polisens brottsdatalag. Möjligheten att ta del av uppgifter under sex månader bör även gälla när Polismyndigheten och Säkerhetspolisen tar del av uppgifter genom direktåtkomst. Efter sex månader bör uppgifterna på

[8] Prop. 2017/18:269, *Brottsdatalag – kompletterande lagstiftning*, s. 161–162.
[9] Prop. 2017/18:132, *Ny tullbefogenhetslag*, s. 373–375.

samma sätt som med nuvarande reglering endast få behandlas vidare för nya ändamål om det behövs i ett enskilt fall, t.ex. inom ramen för ett underrättelseärende eller för att utreda och lagföra brott.

17.4.2 Tillåtna ändamål för behandling

Förslag

Uppgifter som begärs in från transportföretag med stöd av polislagen får, utöver det som gäller i dag, även behandlas för att planera kontroller, välja ut kontrollobjekt och göra analyser som behövs för att uppdatera eller skapa nya kriterier som ska användas vid planering av kontroller eller urval av kontrollobjekt.

Möjligheten att behandla personuppgifter är beroende av vilka ändamål med behandlingen som är tillåten. Enligt 25 § andra stycket polislagen krävs det att uppgifterna kan antas ha betydelse för den brottsbekämpande verksamheten. Av 2 kap. 13 § första stycket polisens brottsdatalag framgår det att personuppgifter som tillhandahålls av transportföretag enligt 25 § polislagen får behandlas för att förebygga, förhindra eller upptäcka brottslig verksamhet samt för att utreda eller lagföra brott.

Regleringen för Tullverket återfinns i 2 kap. 10 § tullverkets brottsdatalag och skiljer sig från regleringen för polisen på så sätt att uppgifterna får behandlas för att planera kontroller, välja ut kontrollobjekt och göra analyser som behövs för att uppdatera eller skapa nya kriterier som ska användas vid planering av kontroller eller urval av kontrollobjekt, för att förebygga, förhindra eller upptäcka brottslighet samt för att utreda eller lagföra brott.

Tullverkets reglering motiverades bl.a. med att en av de viktigaste uppgifterna för myndighetens underrättelseverksamhet är att identifiera kriterier som kan motivera att ett visst objekt som ska passera svenska gränsen kontrolleras. Genom att kartlägga olika faktorer, som visat sig vara gemensamma för smugglare, t.ex. resmönster och betalningssätt, kan riskprofiler tas fram.[10]

Polismyndigheten har motsvarande behov av att kunna arbeta med riskprofiler för att selekteringen ska bli mer träffsäker. Med hänvisning

[10] Prop. 2023/24:132, *Ny tullbefogenhetslag*, s. 363.

till att regleringen av Tullverkets behandling av denna typ av uppgifter har ansetts utgöra ett ingrepp i rätten till skydd för privatliv- och familjeliv som är godtagbart samt att den är förenlig med 2 kap. 6 § andra stycket regeringsformen, artikel 7 och 8 i EU:s rättighetsstadga och artikel 8 i Europakonventionen[11] bör detsamma gälla för en liknande reglering av polisens motsvarande behandling. Vi anser därför att det ska införas en bestämmelse i 2 kap. 13 § polisens brottsdatalag med innebörden att personuppgifterna som tillhandahålls av transportföretag enligt 25 § polislagen, utöver det som är tillåtet enligt den nuvarande regleringen, även får behandlas för att planera kontroller, välja ut kontrollobjekt och göra analyser som behövs för att uppdatera eller skapa nya kriterier som ska användas vid planering av kontroller eller urval av kontrollobjekt.

17.4.3 Hur uppgifter ska lämnas

Förslag

Den myndighet som regeringen bestämmer får ge närmare anvisningar om hur bokningsuppgifter ska lämnas.

Det finns ingen enhetlig standard för hur uppgifter ska lämnas från transportföretag till Polismyndigheten eller Säkerhetspolisen enligt 25 § polislagen. Det innebär att transportföretagen kan lämna uppgifter i flera olika filformat och struktur, vilket ökar den manuella hanteringen. För Tullverket infördes rätten att föreskriva om i vilket format uppgifter ska lämnas i och med den nya tullbefogenhetslagen. I förarbetena motiverades det med att avsaknaden av en enhetlig standard försvårade Tullverkets möjlighet att på ett effektivt sätt använda uppgifterna i sin underrättelseverksamhet.[12] Motsvarande behov gäller för uppgifter som begärs in med stöd av polislagen. För att effektivisera hanteringen av informationen bör därför den myndighet som regeringen bestämmer bemyndigas att meddela närmare förskrifter om hur uppgifterna ska lämnas. Det kan göras i form av en verkställighetsföreskrift i enlighet med 8 kap. 7 § regeringsformen. Det ska därför föras in en bestämmelse i 20 § polisförordningen med

[11] Prop. 2023/24:132, *Ny tullbefogenhetslag*, s. 365.
[12] Prop. 2023/24:132, *Ny tullbefogenhetslag*, s. 377.

innebörden att Polismyndigheten får meddela närmare föreskrifter om bestämmelserna om uppgifter från transportföretag i 25 § polislagen. För att underlätta för transportörerna bör det ske samverkan mellan Polismyndigheten och Tullverket för att ta fram standarder och format för hur uppgifterna ska lämnas.

17.5 Försvarsmakten

Förslag

Polismyndigheten ska på begäran från Försvarsmakten lämna uppgifter som har begärts in från transportföretag med stöd av polislagen, om de behövs i försvarsunderrättelseverksamhet eller den militära säkerhetstjänsten.

Enligt 25 § polislagen har Polismyndigheten och Säkerhetspolisen möjlighet att begära uppgifter om ankommande och avgående transporter från transportföretag. Ett sätt att öka Försvarsmaktens tillgång till dessa uppgifter är att ge myndigheten möjlighet att begära ut sådana uppgifter från Polismyndigheten.

Polismyndighetens behandling av de insamlade uppgifterna enligt 25 § polislagen regleras i 2 kap. 13 § polisens brottsdatalag.[13] Där framgår att personuppgifter som tillhandahålls av transportföretag enligt 25 § polislagen får behandlas om det är nödvändigt för att förebygga, förhindra eller upptäcka brottslig verksamhet samt utreda eller lagföra brott. Uppgifterna får endast i ett enskilt fall behandlas för nya ändamål enligt 2 kap. 4 eller 22 §§ brottsdatalagen. För att Försvarsmakten på ett mer systematiskt sätt ska kunna använda uppgifterna i försvarsunderrättelseverksamheten eller den militära säkerhetstjänsten krävs det alltså att denna reglering ändras.

Ett alternativ är att föra in en bestämmelse i 25 § polislagen eller i anslutning till den bestämmelsen som möjliggör för Polismyndigheten att, på begäran, lämna uppgifter till Försvarsmakten. Inom brottsdatalagens tillämpningsområde är emellertid utgångspunkten att myndigheternas personuppgiftsbehandling i så stor utsträckning som

[13] Lag (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område.

möjligt ska regleras i respektive registerförfattning.[14] Bestämmelser om hur Polismyndigheten får behandla personuppgifter från transportföretag bör därför förläggas till polisens brottsdatalag. I 2 kap. 13 § den lagen ska det därför läggas till en bestämmelse med innebörden att Polismyndigheten på begäran av Försvarsmakten ska lämna uppgifter som tillhandahålls av transportföretag enligt 25 § polislagen som behövs i försvarsunderrättelseverksamhet eller den militära säkerhetstjänsten.

Försvarsmakten har till utredningen framfört att myndighetens operativa behov av information täcks av den information som Polismyndigheten begär att få ta del av med stöd av 25 § polislagen. Försvarsmakten förordar därför en ändring i 2 kap. 13 § polisens brottsdatalag.

I 2 kap. 22 § brottsdatalagen anges det att behandling av personuppgifter för ett ändamål utanför lagens tillämpningsområde ska föregås av en bedömning av behandlingens proportionalitet. I andra stycket anges vidare att i den utsträckning skyldigheten att lämna uppgifter följer av lag eller förordning ska någon sådan prövning inte göras. I och med den föreslagna bestämmelsen i 25 § polislagen behöver således en överföring av uppgifter till Försvarsmakten från Polismyndigheten inte föregås av en proportionalitetsbedömning.

När uppgifterna har förts över till Försvarsmakten framgår det av 1 kap. 4 § brottsdatalagen att lagen inte längre gäller. Hos Försvarsmakten regleras personuppgiftsbehandlingen i stället av försvarsdatalagen.[15]

En sådan reglering som beskrivits ovan ger Försvarsmakten ytterligare möjligheter att ta del av uppgifter om transporter. Det har inte framkommit annat än att Försvarsmaktens operativa behov täcks av de uppgifter som inhämtats av Polismyndigheten med stöd av 25 § polislagen. Med hänsyn till detta framstår det inte som rimligt att transportföretagen ska åläggas att samarbeta med ytterligare en myndighet. Utöver detta innebär ett system med direkt kontakt mellan Försvarsmakten och transportföretagen att företag inom privat sektor tar del av de begäranden som Försvarsmakten framställer. Detta ger information om vilka som Försvarsmakten inriktar sin verksamhet mot.

[14] Prop. 2017/18:269, *Brottsdatalagen – kompletterande lagstiftning*, s. 158.
[15] Lag (2021:1171) om behandling av personuppgifter vid Försvarsmakten.

Försvarsmaktens inriktning och metod inom ramen för underrättelseverksamheten är mycket skyddsvärd och omfattas därför av sekretess. Försvarsmaktens behov av information i denna del tillgodoses därför bäst av att möjliggöra ett vidareutnyttjande av den information som Polismyndigheten har inhämtat med stöd av 25 § polislagen. Mot denna bakgrund föreslår vi att det i 2 kap. 13 § polisens brottsdatalag läggs till en bestämmelse med innebörden att personuppgifter som tillhandahålls av transportföretag enligt 25 § polislagen får behandlas för att föra över uppgifterna till Försvarsmakten, om de behövs i försvarsunderrättelseverksamheten eller i den militära säkerhetstjänsten.

I betänkandet En reformerad underrättelseverksamhet[16] lämnas ett antal förslag för en förändrad organisation av underrättelseverksamheten. Bland förslagen kan nämnas att en ny civil underrättelsetjänst ska inrättas. Regeringen har i oktober 2025 beslutat kommittédirektiven Inrättande av en civil utrikes underrättelsetjänst[17] som innebär att en särskild utredare har fått i uppdrag att bl.a. förbereda och genomföra bildandet av en ny myndighet med uppgift att bedriva civil utrikes underrättelsetjänst. Den 12 februari 2026 remitterades promemorian Myndigheten för utrikes underrättelser, där det föreslås att den nya myndigheten ska vara behörig myndighet enligt lagen om flygpassageraruppgifter i brottsbekämpningen. Om förslaget tas vidare kan det bli aktuellt att Polismyndigheten även på begäran av den nya myndigheten, på samma sätt som till Försvarsmakten, ska vara skyldig att lämna ut aktuella uppgifter. Då förslaget om att den nya myndigheten ska vara behörig myndighet befinner sig i ett tidigt stadie lämnar vi dock inget konkret förslag i den frågan.

17.6 Ekobrottsmyndigheten

Förslag

Polismyndigheten och Tullverket ska på begäran från Ekobrottsmyndigheten lämna uppgifter som har begärts in från transportföretag med stöd av polislagen respektive tullbefogenhetslagen, om de behövs i den brottsbekämpande verksamheten.

[16] SOU 2025:78, *En reformerad underrättelseverksamhet.*
[17] Kommittédirektiv 2025:92, *Inrättande av en civil utrikesunderrättelsetjänst*.

Ekobrottsmyndigheten utgör tillsammans med Åklagarmyndigheten det svenska åklagarväsendet. Ekobrottsmyndigheten arbetar mot viss ekonomisk brottslighet som är organiserad och har en gränsöverskridande karaktär. Samtidigt som myndigheten är en åklagarmyndighet har den även polisiär verksamhet.

Under pågående förundersökning begär Ekobrottsmyndigheten regelmässigt uppgifter från trafikföretag med stöd av bestämmelser i rättegångsbalken. I underrättelseskedet sker det emellertid genom att de poliser som är stationerade vid Ekobrottsmyndigheten begär uppgifter med stöd av 25 § polislagen. Ekobrottsmyndighetens civilanställda kan däremot inte begära uppgifter från trafikföretag på samma sätt. Ur myndighetens perspektiv kan detta anses vara en lagstiftningsmässig brist.

För att förbättra Ekobrottsmyndighetens tillgång till passageraruppgifter kan en liknande reglering införas som har föreslagits avseende Försvarsmakten i föregående avsnitt, dvs. att Ekobrottsmyndigheten begär uppgifter från Polismyndigheten. Utöver detta har Ekobrottsmyndigheten även ett behov av att få tillgång till motsvarande uppgifter som Tullverket begära från transportföretag.

För Ekobrottsmyndighetens verksamhet är det angeläget att även civila underrättelsehandläggare och utredare kan begära in uppgifter. Det skulle utgöra en effektivitetsvinst i jämförelse med att det behöver ske genom poliserna vid myndigheten. I och med dagens lagstiftning råder det inte heller några tvivel om att det är tillåtet för Ekobrottsmyndigheten att ta del av de aktuella uppgifterna.

Under utredningen har Ekobrottsmyndigheten fört fram att myndighetens behov av uppgifter bäst tillgodoses genom att kunna ta del av de uppgifter som Polismyndigheten begär med stöd av 25 § polislagen samt de uppgifter som Tullverket begär med stöd av 7 kap. 12 § tullbefogenhetslagen. En sådan reglering är att föredra framför t.ex. en möjlighet för myndigheten att begära uppgifter direkt från transportföretagen.

Vi föreslår därför att 2 kap. 13 § polisens brottsdatalag utvidgas på så sätt Polismyndigheten på begäran ska lämna personuppgifter som tillhandahålls av transportföretag enligt 25 § polislagen till Ekobrottsmyndigheten, om de behövs i den brottsbekämpande verksamheten.

När det gäller Tullverket regleras inte uppgiftsskyldigheter i tullverkets brottsdatalag eller tillhörande förordning, utan i stället i den

nya tullbefogenhetsförordningen (2024:759). I 6 kap. i förordningen regleras befogenheter för att upptäcka brott och i 3 § första stycket anges att information om innehållet i bokningsuppgifter som inhämtats med stöd av 7 kap. 12 § tullbefogenhetslagen får lämnas till andra tulltjänstemän, andra enheter inom tullverket, Polismyndigheten, Kustbevakningen och Skatteverket, om uppgiften behövs i Tullverkets brottsbekämpande verksamhet för att klarlägga om brott eller brottslig verksamhet har förekommit, pågår eller planeras. För att upprätthålla strukturen i Tullverkets reglering bör en bestämmelse om en skyldighet att på begäran lämna de aktuella uppgifterna till Ekobrottsmyndigheten därför föras in i en ny paragraf i 6 kap. tullbefogenhetsförordningen.

I 2 kap. 12 § tullverkets brottsdatalag anges att vid sökning i personuppgifter som lämnats till Tullverket enligt 7 kap. 12 § tullbefogenhetslagen får namn, personnummer, samordningsnummer och andra liknande identitetsbeteckningar användas som sökbegrepp endast om uppgifterna avser en person som är eller har varit misstänkt för brott, är misstänkt för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 3 kap. 2 § första stycket 1, eller övervakas under de förutsättningar som anges i 3 kap. 2 § första stycket 2. Det kan antas att en begäran om uppgifter från Ekobrottsmyndigheten i många fall kommer att göras genom att ange sådana identitetsbeteckningar och sökbegränsningen är i sådana fall tillämplig. Regelmässigt kommer den aktuella personen vara eller ha varit misstänkt för brott, och sökbegränsningen innebär därmed inget hinder. Om personen är misstänkt för att ha utövat eller komma att utöva brottslig verksamhet krävs det emellertid enligt 3 kap. 2 § första stycket 1 att den misstänkta verksamheten innefattar brott för vilket det är föreskrivet fängelse i ett år eller mer eller att den sker systematiskt.

I 3 kap. 2 § tredje stycket anges bl.a. att endast om det behövs i ett enskilt fall får uppgifterna göras tillgängliga för andra än särskilt angivna tjänstemän. Ett enskilt fall kan röra sig om t.ex. en brottsutredning, ett underrättelseärende eller för att genomföra viss en kontroll.[18] För Ekobrottsmyndighetens del bör en begäran falla in under brottsutredning eller underrättelseärende och det är därför möjligt för Tullverket att behandla uppgifterna för att lämna dem till Ekobrottsmyndigheten.

[18] Prop. 2023/24:132, *Ny tullbefogenhetslag*, s. 371–372.

18 Konsekvensutredning

18.1 Inledning

Konsekvenserna i betänkandet analyseras kontinuerligt, särskilt i fråga om konsekvenser för den personliga integriteten och det brottsbekämpande arbetet. I detta kapitel redovisar vi en samlad bedömning av vilka konsekvenser våra förslag förväntas medföra. Konsekvenserna redovisas i enlighet med kommittéförordningen (1998:1474) och förordningen (2024:183) om konsekvensutredningar samt utifrån vad regeringen har angivit i våra direktiv.

I 15 § kommittéförordningen anges att om förslagen i ett betänkande medför kostnadsökningar eller intäktsminskningar för staten, kommuner eller regioner, ska kommittén föreslå en finansiering som i första hand har anknytning till utredningens område och ange skäl för den föreslagna finansieringen. Enligt 16 § anger regeringen närmare i utredningsuppdraget vilka konsekvensbeskrivningar som ska finnas i ett betänkande.

Av 2 § förordningen om konsekvensutredningar framgår att kommittéer, särskilda utredare och förvaltningsmyndigheter ska redovisa en konsekvensutredning när de lämnar förslag till regeringen eller Regeringskansliet om att regeringen ska föreslå eller besluta om nya eller ändrade lagar och förordningar. Kommittéer och särskilda utredare ska även för andra förslag som lämnas i ett betänkande redovisa en konsekvensutredning.

Konsekvensutredningen ska enligt 6 § innehålla redogörelser för det aktuella problemet och vilken förändring som eftersträvas, vilka konsekvenser som kan tänkas uppstå om ingen åtgärd vidtas, de olika alternativ som finns för att uppnå förändringen och de fördelar respektive nackdelar som bedöms finnas med dessa samt det eller de alternativ som bedöms lämpligast och av vilka skäl.

I 7 § anges att konsekvensutredningen ska innehålla en analys av det förslag som lämnas samt att analysen bl.a. ska bestå av en beskrivning och beräkning av förslagets kostnader och intäkter samt, om möjligt, en beräkning av andra relevanta konsekvenser.

Enligt våra direktiv ska vi lägga särskild vikt vid att beskriva förslagens betydelse för möjligheten att förebygga, förhindra, upptäcka, utreda och lagföra brott. Vi ska även redovisa förslagens konsekvenser för den personliga integriteten samt för transportföretag, resenärer och gränsregioner.

Det framgår vidare av kommittédirektiven att vi ska ta ställning till vilka förändringar av den svenska regleringen i fråga om flygpassageraruppgifter i brottsbekämpningen som behöver göras med anledning av EU-domstolens praxis. Lagstiftningen ska i detta avseende endast förändras i den utsträckning det är nödvändigt. Som medlemsstat i EU har Sverige en skyldighet att anpassa svensk rätt efter lagstiftning och praxis på EU-nivå. En medlemsstat som inte följer EU-rätten kan bli föremål för sanktioner, t.ex. böter som döms ut av EU-domstolen, eller överträdelseförfaranden av Europeiska kommissionen. Till följd av detta anser vi det inte är ett gångbart alternativ att inte genomföra de förändringar som EU-rätten kräver. Därför görs det i konsekvensanalysen inte heller någon jämförelse med det s.k. nollalternativet, dvs. att inte genomföra några förändringar.

18.2 Förändringar till följd av PNR-domen

18.2.1 Konsekvenser för brottsbekämpningen

Vår bedömning

Om förslagen i denna del genomförs förväntas de sammantaget medföra påtagligt negativa effekter för möjligheten att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och annan grov brottslighet. Förslagen förväntas även ha en begränsad negativ påverkan på övrig brottsbekämpande verksamhet.

I de situationer där PNR-direktivet tillämpas på samtliga eller en stor andel av flygningarna inom EU har förslagen en mer begränsad negativ påverkan på brottsbekämpningen. Vid ett mindre urval blir effekten större. När det gäller förslagen avseende den generella lagringstiden får det anses sannolikt att det kommer ha

påtagligt negativa konsekvenser för brottsbekämpningen, i synnerhet när det gäller bekämpningen av den mest allvarliga brottsligheten.

Förslagen om att det ska genomföras en förhandskontroll av åklagare eller domstol innan tillgång till PNR-uppgifter medges innebär en tröghet i systemet som är negativ för brottsbekämpningen. Den negativa effekten begränsas emellertid av möjligheten för brottsbekämpande myndigheter att, i vissa brådskande fall, ta del av PNR-uppgifter innan en prövning har kunnat genomföras av åklagare eller domstol.

PNR-systemet har haft en positiv effekt på brottsbekämpningen inom EU. Till övervägande del innebär de uttalanden i PNR-domen som kräver en förändring av svensk rätt en begränsning av möjligheten att använda PNR-uppgifter i brottsbekämpande syfte. Detta gäller särskilt begränsningen av möjligheten att behandla PNR-uppgifter från flygningar inom EU, vilka i nuläget utgör cirka 65 procent av de PNR-uppgifter som behandlas vid enheten för passagerarinformation. I och med de begränsningar som föreslås kommer brottsbekämpande myndigheter att förlora information som till följd av både sin kvantitet och kvalitet är av stort värde för brottsbekämpningen.

Även förslaget som avser en begränsning av lagringstiden för PNR-uppgifter vid enheten för passagerarinformation innebär en förlust av värdefull information. EU-kommissionen konstaterar i sin rapport[1] om översyn av PNR-direktivet att lagringen av PNR-information under fem år för alla passagerare är nödvändig för att uppnå målen avseende säkerhet och skydd för människor genom att beivra terroristbrott och annan grov brottslighet. Kommissionen uttalar vidare att behovet av att lagra uppgifter beror på PNR-systemets karaktär, dvs. att det är ett analytiskt verktyg som syftar till att både identifiera kända hot och att upptäcka okända risker; att PNR-uppgifter används för att identifiera resmönster och för att göra kopplingar mellan kända och okända personer och det ligger i sakens natur att det krävs långsiktig analys för att upptäcka sådana kopplingar. Med tanke på den konstaterade positiva effekten för förhindrande av terroristbrottslig-

[1] Report from the Commission to the European Parliament and the Council On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, (SWD(2020) 128 final, den 24 juli 2020, s. 8.

het och annan allvarlig brottslighet som implementeringen av PNR-direktivet har medfört kommer en konsekvens av föreliggande förslag till ändringar av lagen om flygpassageraruppgifter i brottsbekämpningen vara att terroristbrottslighet och annan allvarlig brottslighet inte kan förhindras, utredas eller lagföras i samma utsträckning som med nuvarande reglering. Detta ökar sannolikheten för terrorattentat.

Sammantaget har förslagen en påtagligt negativ påverkan på brottsbekämpningen i allmänhet. Om förslagen genomförs kommer en stor andel av PNR-uppgifterna som i dagsläget behandlas vid enheten för passagerarinformation att gå förlorade, vilket även innebär att kvaliteten på analysen försämras. Ju mindre data som finns att tillgå, desto mer opålitlig blir analysen.

PNR-uppgifter får endast behandlas för att bekämpa terroristbrottslighet eller annan grov brottslighet. Information som kommer fram vid sådan behandling får dock användas även för att förhindra, utreda eller lagföra andra brott. Förslagen kan därmed ha en negativ effekt på övrig brottsbekämpande verksamhet, även om vi bedömer att sådan påverkan torde vara begränsad.

Förslagen om att alla begäranden om tillgång till PNR-uppgifter ska genomgå en förhandskontroll av åklagare eller domstol innebär att en viss tröghet införs i systemet. Detta gäller särskilt under pågående förundersökning, då allmän domstol ska fatta beslut om tillgång till uppgifterna. Detta kommer endast kunna ske under den tid som domstolen har öppet. De negativa effekterna av detta mildras emellertid genom möjligheten för brottsbekämpande myndigheter att, i vissa brådskande fall, ta del av PNR-uppgifter utan föregående domstolsprövning. I situationer där ändamålet med behandlingen av uppgifterna riskerar att gå förlorad om prövningen avvaktas kan således behandlingen påbörjas i väntan på domstolens avgörande.

18.2.2 Konsekvenser för den nationella säkerheten

Vår bedömning

Förslaget om att ta bort möjligheten för enheten för passagerarinformation att behandla PNR-information när det är nödvändigt att tillhandahålla uppgifter som behövs för verksamhet som rör nationell säkerhet, men som inte omfattas av ändamålen i PNR-direktivet, har negativa konsekvenser för Sveriges nationella säkerhet.

När den svenska regleringen av PNR-systemet genomfördes utökades de tillåtna ändamålen för behandling av PNR-uppgifter till att även omfatta verksamhet som rör nationell säkerhet. Syftet var att kunna använda PNR-uppgifter även för vissa brott som faller utanför PNR-direktivets tillämpningsområde.

I och med att denna möjlighet tas bort minskar myndigheternas möjlighet att bekämpa t.ex. brott enligt 18 och 19 kap. brottsbalken, såsom högmålsbrott och vissa brott mot Sveriges säkerhet. Det kan försvåra identifieringen av okända hot och kartläggningen av utländska underrättelseoperatörer. I förlängningen kan Sveriges försvarsförmåga påverkas.

Hur stor faktisk påverkan detta kommer att ha är svårt att uttala sig om. Det bör emellertid påpekas att det fortfarande kommer att vara möjligt att behandla PNR-uppgifter för att tillhandahålla uppgifter som behövs i verksamhet som rör nationell säkerhet, så länge behandlingen görs för ett ändamål som ryms inom direktivets tillämpningsområde, dvs. terrorism och annan allvarlig brottslighet.

Under utredningens arbete har det övervägts om det bör inrättas ett system liknande PNR-systemet där insamlingen och den vidare behandlingen av passageraruppgifter sker endast i syfte att främja nationell säkerhet. Eftersom utredningens huvudsyfte är att förbättra tillgången till passageraruppgifter i brottsbekämpningen samt att ett sådant system kräver djupgående analyser och noggranna överväganden anser vi att det inte ryms inom ramen för denna utredning att föreslå ett sådant system.

18.2.3 Konsekvenser för enskilda

Vår bedömning

Förslagen som avser flygningar inom EU samt lagringstid innebär att färre PNR-uppgifter vid varje enskild tidpunkt kommer att behandlas vid enheten för passagerarinformation samt att vissa PNR-uppgifter lagras under betydligt kortare tid. Detta medför ett ökat skydd för enskildas personliga integritet.

Förslagen som berör förhandskontroll vid begäran om tillgång till PNR-uppgifter samt beslut om och rättslig prövning av utvidgad tillämpning av PNR-direktivet innebär garanter för att PNR-systemet tillämpas på ett rättssäkert sätt. Även detta medför ett ökat skydd för den personliga integriteten.

Som nämnts ovan avseende konsekvenserna för brottsbekämpningen innebär PNR-domen till övervägande del att behandlingen av PNR-uppgifter begränsas. PNR-uppgifter som härrör från ej utvalda flygningar inom EU kommer efter den inledande förhandsbedömningen, då slagningar görs mot relevanta databaser, omedelbart att anonymiseras under förutsättning att slagningarna inte har gett någon träff. Detta medför att en överväldigande majoritet av PNR-uppgifterna från ej utvalda flygningar inom EU kommer att lagras vid enheten för passagerarinformation under en mycket kort tid samt att uppgifterna inte kommer granskas av någon som arbetar vid enheten eller av någon behörig myndighet. I jämförelse med nuvarande reglering som innebär att samtliga PNR-uppgifter för flygningar inom EU lagras under sex månader, och därefter behörighetsbegränsas och lagras i fem år, innebär förslaget en förstärkning av skyddet för personuppgifter och den personliga integriteten. Under nuvarande reglering lagras PNR-uppgifter kontinuerligt för personer som reser inom EU med intervaller om högst fem år. I och med förslaget kommer uppgifterna lagras under begränsade tidsperioder i samband med att en person flyger inom EU. Efter anonymisering kan uppgifterna inte heller bli föremål för en begäran om tillgång till PNR-uppgifter från en behörig myndighet. Hur stor påverkan detta har beror på hur stort urvalet av flygningar inom EU är. I en situation där terrorhotet motiverar att PNR-uppgifter samlas in från samtliga flygningar inom EU

innebär förslagen en mer marginell förbättring ur ett integritetsperspektiv.

I och med den minskade tillgången till PNR-uppgifter kommer analysen av de befintliga uppgifterna att försämras. En fördel med PNR-systemet ur ett brottsbekämpande perspektiv är tillgången till en stor mängd data. Mängden data innebär att det både är lättare att identifiera intressanta personer och att avskriva personer som inte är intressanta. Detta kommer att försvåras med betydligt mindre data att tillgå.

För en mycket stor majoritet av de PNR-uppgifter som finns hos enheten för passagerarinformation innebär dagens system att den enda behandling som uppgifterna utsätts för är att uppgifterna översänds och sedan lagras i en databas. Det är en liten minoritet av uppgifterna som behandlas på något annat sätt än lagring under den tid som de finns hos enheten. Av de olika former av personuppgiftsbehandling som kan ske av PNR-uppgifter vid enheten för passagerarinformation är själva lagringen den minst integritetskränkande. Även om det utan tvekan förhåller sig så att förslagen stärker skyddet för den personliga integriteten är detta perspektiv viktigt att belysa.

Säkerhetspolisen utses till prövningsinstans för beslut om att tillämpa PNR-direktivet på samtliga flygningar inom EU. Sådana beslut ska underställas och prövas av Försvarsunderrättelsedomstolen. När förutsättningar för ett sådant beslut saknas har enheten för passagerarinformation, efter inhämtning av synpunkter från de behöriga myndigheterna, möjlighet att besluta om ett urval av flygningar inom EU. När det gäller förhandskontroll vid begäran om tillgång till PNR-uppgifter ska dessa utföras av åklagare eller av allmän domstol. Genom dessa förslag säkerställs att prövningarna sker på ett rättssäkert och gediget sätt. Detta utgör ytterligare en skyddsmekanism för enskildas personliga integritet.

Sammantaget innebär förslagen ett förhöjt skydd för personuppgifter och enskildas personliga integritet i jämförelse med dagens reglering.

18.2.4 Konsekvenser för lufttrafikföretagen

Vår bedömning

Förslagen innebär inte någon förändring av lufttrafikföretagens verksamhet och kommer inte att innebära någon ytterligare belastning arbets- eller kostnadsmässigt.

Förslagen innebär att lufttrafikföretagen fortsätter översända PNR-uppgifter till enheten för passagerarinformation i samma utsträckning som under nuvarande reglering. Förslagen innebär inte heller några andra förändringar som påverkar lufttrafikföretagen.

18.2.5 Konsekvenser för Åklagarmyndigheten, Ekobrottsmyndigheten och domstolarna

Vår bedömning

Försvarsunderrättelsedomstolen ska pröva beslut om att tillämpa PNR-direktivet på samtliga flyg inom EU. Kostnaderna för detta får antas rymmas inom befintliga budgetramar.

Allmän domstol ska pröva begäranden om tillgång till PNR-uppgifter under pågående förundersökning och åklagare motsvarande prövning i andra fall. Detta bedöms leda till kostnadsökningar som inte ryms inom befintliga ekonomiska ramar utan finansieringen bör ligga inom det allmänna reformutrymmet.

I enlighet med våra förslag ska Försvarsunderrättelsedomstolen utses till prövningsinstans avseende beslut om att tillämpa PNR-direktivet på samtliga flyg inom EU. Den aktuella typen av beslut ska regelbundet omprövas och ha en giltighetstid om högst ett år. Det mest sannolika utfallet enligt vår bedömning är att det kommer underställas ett beslut om året till Försvarsunderrättelsedomstolen, med undantag för enstaka fall där nytt beslut fattas innan det föregående har löpt ut. Det finns även scenarier där inget beslut fattas under en längre tid. Även om varje enskilt mål är komplicerat innebär detta att kostnadsökningen för Försvarsunderrättelsedomstolen är begränsad.

Allmän domstol och åklagare åläggs att pröva begäranden om tillgång till PNR-uppgifter i efterhand under pågående förundersökning respektive i andra fall. I dagsläget rör det sig om knappt cirka 7 000 ärenden om året, varav ungefär hälften avser pågående förundersökning och hälften andra fall. Varje ärende kan omfatta flera personer och det har förekommit ärenden som avser flera hundra personer. I snitt omfattar ett ärende två personer. Ungefär 500 ärenden om året avser behörighetsbegränsade PNR-uppgifter, vilka har prövats av åklagare respektive Polismyndigheten. För övriga ärenden har en prövning genomförts av enheten för passagerarinformation.

Antalet prövningar kommer att påverkas av det faktum att färre PNR-uppgifter vid varje given tidpunkt kommer att lagras vid enheten för passagerarinformation till följd av den betydligt kortare generella lagringstiden om sex månader. Ytterligare en osäkerhetsfaktor är om behöriga myndigheter kommer att förändra antalet beställningar för att kompensera för de föreslagna förändringarna i regelverket.

Även om det är vanskligt att dra några säkra slutsatser om antalet ärenden bedömer vi att den faktor som har störst inverkan är de kortare generella lagringstiden och att det totala antalet prövningar till följd av detta kommer att sjunka. Andra förslag i betänkandet, framför allt de som rör en trafikslagsneutral PNR-lagstiftning, kan leda till fler ärenden, eftersom det innebär en ökning av antalet uppgifter som är möjliga att begära tillgång till. Oaktat osäkerheten i hur de olika förslagen kommer att påverka antalet ärenden kan det dock konstateras att det kommer att krävas ett betydande antal prövningar varje år. För domstolarna är det en ny typ av ärenden som inte har hanterats tidigare och som dessutom ska handläggas skyndsamt. I ett lagförslag om polisens användning av AI för ansiktsigenkänning har den där aktuella tillståndsgivningen jämförts med styckkostnaden för domstolsärenden inklusive ärenden om utsökning.[2] I likhet med vårt förslag ska sådana tillståndsärenden avgöras genom skriftligt förfarande och utan ett offentligt ombud. Kostnaden för en sådan prövning har beräknats till 5 317 kronor för år 2023.

Vid ett oförändrat antal ärenden kommer domstolarna behöva genomföra prövningar av cirka 3 500 ärenden avseende cirka 7 000 personer om året. En kostnad om 5 300 kronor per prövning, dvs. per varje person vars PNR-uppgifter prövas, skulle innebära en kostnadsökning för domstolarna med cirka 37 miljoner kronor årligen, under

[2] Prop. 2025/26:150, *Polisens användning av AI för ansiktsigenkänning i realtid*, s. 122.

förutsättning att antalet prövningar inte förändras. Enligt vår bedömning kommer antalet prövningar troligen vara oförändrat eller öka något, med beaktande både av förslagen som följer av PNR-domen och förslagen som avser en trafikslagsneutral PNR-lagstiftning. Sveriges domstolar hade 2025 en sammanlagd budget på cirka 8,2 miljarder kronor. Kostnadsökningen vid oförändrat antal prövningar skulle därmed utgöra knappt en halv procent av budgeten. Detta bör med hänsyn till situationen hos de allmänna domstolarna inte finansieras genom befintligt anslag utan det bör ligga inom det allmänna reformutrymmet.

Åklagare kommer enligt förslagen pröva begäran om tillgång till PNR-uppgifter i efterhand i andra fall, till skillnad från dagens lagstiftning som innebär att åklagaren prövar begäran under pågående förundersökning. En annan väsentlig skillnad är att en prövning ska genomföras även vid en begäran under de första sex månaderna efter att PNR-uppgifter kommer in till enheten för passagerarinformation. De cirka 250 ärendena som avser tillgång till PNR-uppgifter under pågående förundersökning kommer således att ersättas av ett antal tusen ärenden som rör andra fall. Ett oförändrat antal begäranden skulle innebära cirka 3 500 ärenden avseende 7 000 personer om året. Den stora majoriteten av ärendena kommer att hanteras av åklagare anställda vid Åklagarmyndigheten, och en mindre andel av åklagare vid Ekobrottsmyndigheten. För Åklagarmyndigheten utgör detta en kraftig ökning av antalet ärenden, som dessutom är av annan beskaffenhet än de som åklagare hittills har genomfört. Enligt förslaget ska åklagare göra förhandskontroller som ska genomföras innan en historisk sökning skickas från enheten för passagerarinformation till andra länder. Det är ett ansvar åklagare inte har i dagsläget. Det rör sig om cirka 100 ärenden i månaden, dvs. ungefär 1 200 årligen. Om det land som skickar förfrågan om att ta del av PNR-information i efterhand inte har genomfört en prövning av en oberoende myndighet eller domstol av denna förfrågan ankommer det på åklagare att göra en sådan förhandskontroll. Det inkommer cirka 25 sådana begäranden i månaden och det är svårt att i nuläget bedöma hur många av övriga länder som inte har en oberoende myndighet som fattar beslut när denna lagstiftning träder i kraft, men vår uppskattning är att det kommer att röra sig om cirka 15 sådana begäranden i månaden. Sammantaget tillkommer det således cirka 115 förhandskontroller i månaden, vilket blir 1 400 om året. Tillsammans med tidigare angivna uppskattningen

om 3 500 ärenden om året handlar det alltså om cirka 4 900 prövningar om året, eller 13 prövningar per dygn.

Det finns inga beräknade kostnader för den prövning som hittills har genomförts av åklagare. Det finns däremot beräkningar avseende kostnaden per brottsmisstanke och brottsgrupp från 2024.[3] Den genomsnittliga kostnaden för att handlägga en brottsmisstanke var 6 237 kronor under 2024. För olika brottstyper är kostnaden som lägst 2 258 kronor för ett trafikbrott och som högst 19 061 kronor för miljö- och arbetsmiljöbrott. De olika kostnaderna beror bl.a. på tidsutdräkten och ärendets komplexitet.

En begäran om tillgång till PNR-uppgifter leder inte till några ytterligare åtgärder utöver beslutet som ska fattas. I och med detta ligger det nära till hands att anta att kostnaden för ett sådan prövning ligger närmare brottstyper som kostar minst per brottsmisstanke. Vid en kostnad om 2 500 kronor per ärende och 4 900 begäranden beräknas kostnaderna uppgå till cirka 12,3 miljoner kronor. Även om Åklagarmyndigheten i dagsläget har vissa kostnader för de prövningar som genomförs i förundersökningsskedet innebär detta sammantaget en påtaglig kostnadsökning. För 2024 hade myndigheten disponibla medel om cirka 2,7 miljarder kronor[4], och vid oförändrat antal ärenden innebär det en kostnadsökning om cirka 0,5 procent. Detta bör inte rymmas inom befintligt anslag utan bör finansieras genom det allmänna reformutrymmet.

Förslagen innebär ett flertal begränsningar av behandlingen av PNR-uppgifter. Dessa begränsningar för med sig negativa konsekvenser för brottsbekämpningen. Som ett resultat av detta kan det antas att färre brottsutredningar kommer att leda till åtal, samt att vissa brottsutredningar aldrig kommer att inledas till följd av den brist på information som förslagen leder till. Detta leder till ett något minskat antal brottmål vid allmän domstol, men detta får anses ha försumbar påverkan på domstolarnas och Åklagarmyndighetens verksamhet.

[3] Åklagarmyndighetens årsredovisning 2024, s. 28.
[4] Åklagarmyndighetens årsredovisning 2024, s. 84.

18.2.6 Övriga konsekvenser

Vår bedömning

Förslagen antas inte ha någon påverkan på statens finanser utöver vad som redan nämnts eller på det privata näringslivet.

Förslagen minskar möjligheten för enheten för passagerarinformation i en annan medlemsstat, en behörig myndighet i en annan medlemsstat samt Europol att ta del av PNR-uppgifter från den svenska enheten för passagerarinformation. Detta har negativa konsekvenser för EU:s gemensamma möjlighet att bekämpa terroristbrott och annan allvarlig brottslighet.

Utöver de ekonomiska konsekvenser som berörts i tidigare avsnitt i detta kapitel bör förslagen inte medföra någon ytterligare påverkan på statens finanser eller på det privata näringslivet.

PNR-uppgifterna hos den svenska enheten för passagerarinformation används inte bara av svenska brottsbekämpande myndigheter. Det finns även andra behöriga mottagare i form av enheten för passagerarinformation i en annan medlemsstat, en behörig myndighet i en annan medlemsstat samt Europol. Det sker regelmässigt utlämnande av PNR-uppgifter från enheten för passagerarinformation till dessa behöriga mottagare. Begränsningarna som föreslås avseende PNR-systemets tillämpning i Sverige har därmed negativa konsekvenser för EU:s gemensamma möjlighet att bekämpa terroristbrott och annan allvarlig brottslighet.

18.3 Trafikslagsneutral PNR-lagstiftning och utökade befogenheter för brottsbekämpande myndigheter

18.3.1 Konsekvenser för brottsbekämpningen

Bedömning

Förslagen om en trafikslagsneutral PNR-lagstiftning förväntas få positiva konsekvenser för arbetet med att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och annan allvarlig brottslighet, samt indirekta positiva konsekvenser för bekämpande av brottslighet i allmänhet.

Förslagen som avser speciallagstiftning för brottsbekämpande myndigheter förväntas ha positiva effekter för brottsbekämpningen i allmänhet.

Förslagen innebär att PNR-lagstiftningen görs trafikslagsneutral, dvs. även tåg-, buss- och färjetrafik ska ingå i enheten för passagerarinformations insamling av passageraruppgifter. Syftet är att ge brottsbekämpande myndigheter en mer heltäckande och ändamålsenlig tillgång till passageraruppgifter. PNR-systemet för flygtrafik har varit framgångsrikt och utgör ett viktigt verktyg för att bekämpa de aktuella brottstyperna och uppgifter från andra trafikslag bedöms bidra ytterligare till detta arbete. Förslagen innebär vidare att det finns utökade möjligheter att utbyta PNR-information med andra medlemsstater, vilket bidrar positivt både till brottsbekämpningen i Sverige och globalt.

Behandlingen av PNR-uppgifter får ske i syfte att bekämpa terroristbrott och annan allvarlig brottslighet, men om det kommer fram uppgifter om ett annat brott i samband med en brottsbekämpande åtgärd får informationen användas för att förhindra, utreda eller lagföra brottet. Mer omfattande tillgång till PNR-uppgifter bör därför indirekt medföra positiva effekter för brottsbekämpningen i allmänhet.

Förslagen som avser brottsbekämpande myndigheters möjligheter att med stöd av speciallagstiftning begära uppgifter från transportföretag innebär att förbättrad tillgång till sådana uppgifter. Syftet med inhämtningen är generell brottsbekämpning och inte avgränsad till bekämpande av brott av en viss allvarsgrad. Även dessa förslag förväntas påverka brottsbekämpningen positivt.

18.3.2 Konsekvenser för enskilda

Bedömning

Förslagen innebär ett allvarligt ingrepp i de grundläggande rättigheterna till rätt till respekt för privatlivet och skydd för personuppgifter. Ingreppet görs dock för att uppnå ett allmänt samhällsintresse och bedöms vara proportionerligt.

Förslagen förväntas ha en försumbar påverkan på biljettpriser.

Förslaget om en trafikslagsneutral PNR-lagstiftning innebär att PNR-uppgifter avseende ett stort antal personer kommer att överföras och behandlas vid enheten för passagerarinformation och av behöriga myndigheter. Sådan behandling sker redan i dagsläget, om än inte i samma omfattning. Samtliga PNR-uppgifter som översänds till enheten för passagerarinformation kommer att genomgå en automatisk förhandsbedömning där det genomförs en jämförelse mot relevanta register eller andra uppgiftssamlingar. Det är enbart PNR-uppgifter som vid den automatiska behandlingen ger en träff som kommer att behandlas manuellt av personalen vid enheten. En mycket stor andel av PNR-uppgifterna som översänds kommer aldrig granskas av en fysisk person.

PNR-lagstiftningen innehåller strikta krav på hur PNR-uppgifter får behandlas. Det får ske för begränsade ändamål och känsliga uppgifter får inte behandlas alls. Lagringstiden har också begränsats i enlighet med EU-domstolens uttalanden. Innan PNR-uppgifter överförs till en behörig mottagare eller ett tredjeland ska det ske en prövning av en åklagare eller domstol, vilket utgör en rättssäkerhetsgaranti för enskilda. Förslagen ger ett tillfredsställande skydd för enskildas personliga integritet vid behandlingen av deras PNR-uppgifter. Sammantaget bedömer vi att ingreppet är proportionerligt med hänsyn till det allmänna samhällsintresset att bekämpa terrorism och annan allvarlig brottslighet.

Förslagen riskerar att skapa mer administration för transportföretag, vilket kan leda till högre kostnader. Även om dessa kostnader kan vältras över på resenärer bedömer vi att påverkan på biljettpriserna kommer att vara försumbar.

18.3.3 Konsekvenser för transportföretagen

Bedömning

Förslagen kommer att belasta företag inom transportsektorn på olika sätt. För tåg- och busstrafiken innebär införlivandet i PNR-systemet både initiala och löpande kostnader för att uppfylla skyldigheten att överföra uppgifter till enheten för passagerarinformation.

För färjetrafiken innebär förslagen inte några ytterligare rapporteringsskyldigheter än de redan befintliga. Antalet förfrågningar

med stöd av polislagen och tullbefogenhetslagen kan antas minska, vilket innebär att arbetsbördan avseende sådana förfrågningar också kommer att minska.

För lufttrafikföretag som trafikerar sträckor inom Sverige innebär det att PNR-uppgifter från dessa flygningar ska överföras till enheten för passagerarinformation. Det bör inte medföra någon märkbar ytterligare arbetsbelastning eller kostnadsökning.

Tåg- och busstrafiken

Tåg- och bussföretag åläggs en skyldighet att föra över PNR-uppgifter till enheten för passagerarinformation. Initialt kan detta medföra kostnader för utveckling eller införskaffande av den mjukvara som krävs för att föra över uppgifterna samt för att etablera den tekniska kopplingen till enheten för passagerarinformation. Licenskostnaden för mjukvaran kan variera beroende på antalet genomförda resor eller antalet passagerare, vilket innebär att kostnaderna för mindre operatörer också kan bli lägre. När systemet väl är igång bör kostnaderna, utöver licensen, inte vara särskilt höga.

I och med införandet av ett trafikslagsneutralt PNR-system kommer behovet för brottsbekämpande myndigheter att begära uppgifter med stöd av polislagen och tullbefogenhetslagen att minska. Hanteringen av sådana begäranden sker manuellt och är resurskrävande. Detta kan till viss mån kompensera för en eventuell kostnadsökning.

Det är svårt att förutse exakt hur förslagen kommer att påverka transportföretagen, särskilt med beaktande av de olika förutsättningar som finns mellan olika aktörer och branscher. Eventuella kostnadsökningar kan dock vara möjliga att övervältra på konsumenterna, dvs. alla som köper resor. Som nämnts i avsnitt 16.6 förutsågs PNR-direktivet innebära att kostnaden per biljett skulle öka med ungefär 1 krona. Prognosen har inte bekräftats och andra förutsättningar gäller för tåg- och busstrafik, men det är sannolikt att eventuella kostnadsökningar inte är större än att de går att övervältra på konsumenterna utan att det påverkar efterfrågan nämnvärt. Sammantaget bedömer vi att våra förslag kommer att medföra vissa kostnader för tåg- och bussföretagen, men att de sannolikt kan bäras av konsumenterna, samt att de till viss del kommer att kompenseras av att hanteringen av begäranden med stöd av polislagen och tullbefogenhetslagen kommer att minska.

Färjetrafiken

Färjetrafiken åläggs samma uppgiftsskyldighet som andra transportföretag. Utgångspunkten är dock att företagen inte kommer att föra över uppgifterna direkt till enheten för passagerarinformation. Uppgifterna skickas i stället till EMSWe, som administreras av Sjöfartsverket, varifrån de därefter översänds till enheten. PNR-regleringen innebär inte att ytterligare uppgifter ska rapporteras än vad som redan gäller för gränsöverskridande passagerartrafik inom sjöfart. Även tidpunkten för överföring följer av andra regelverk än PNR-lagstiftningen. För färjetrafiken innebär förslagen avseende en trafikslagsneutral PNR-lagstiftning således ingen förändring i någon del av verksamheten i den här delen. Däremot kommer myndigheternas behov av att hämta in information från färjetrafiken med stöd av polislagen och tullbefogenhetslagen att minska, vilket leder till mindre hantering av sådana förfrågningar för transportföretagen.

Inrikesflyg

Det finns i nuläget inga flygbolag som enbart trafikerar sträckor inom Sverige utan samtliga bolag har åtminstone ett fåtal gränsöverskridande flygningar. Inrikesflyg bedrivs således av samma bolag som även bedriver utrikesflyg och som till följd av detta är anslutna till PNR-systemet. Alla aktörer har alltså tillgång till de tekniska lösningar som krävs för att föra över uppgifter och har redan etablerad kontakt med enheten för passagerarinformation. Tidsåtgången för att lägga till ytterligare flygningar för vilka uppgifter ska föras över bedöms inte leda till några märkbara kostnader för flygbolagen.

18.3.4 Konsekvenser för Åklagarmyndigheten, Ekobrottsmyndigheten och domstolarna

Bedömning

Förslagen kan medföra ökad arbetsbelastning och ökade kostnader för Åklagarmyndigheten, Ekobrottsmyndigheten och domstolarna.

Konsekvenserna för Åklagarmyndigheten och domstolarna till följd av förändringar som sker i ljuset av PNR-domen har beskrivits i avsnitt 18.2.5. De PNR-uppgifter som härrör från andra trafikslag än flyg ska genomgå samma prövning vid en begäran om att ta del av uppgifterna, dvs. en prövning av allmän domstol under pågående förundersökning och av åklagare i andra fall.

Beräkningarna i avsnitt 18.2.5 har gjorts med beaktande av att förslagen i den här delen innebär att fler uppgifter kommer att lagras vid enheten för passagerarinformation, vilket kan leda till att fler begäranden kommer att behöva prövas. Som vi har angett i det nämnda avsnittet är beräkningarna relevanta, även med beaktande av förslagen som rör en trafikslagsneutral PNR-lagstiftning.

18.3.5 Konsekvenser för Polismyndigheten

Enheten för passagerarinformation

Bedömning

Förslagen innebär en ökad arbetsbörda och kostnad för enheten för passagerarinformation inom Polismyndigheten. Kostnadsökningen uppskattas till cirka 4,5 miljoner kronor.

Inkluderingen av fler trafikslag i PNR-lagstiftningen innebär att kontakt måste etableras mellan fler transportföretag och enheten för passagerarinformation, vilket kan vara resurskrävande. Detta är dock redan i dag en del av enhetens uppgifter och förslagen bör inte innebära någon märkbar förändring avseende arbetsbörda och kostnader.

Förslagen som avser en trafikslagsneutral PNR-lagstiftning innebär att enheten kommer att hantera minst 200 procent fler passagerare varje dygn. En ökning från cirka 50 000 i dagens PNR-system till åtminstone 150 000 om dagen, vilket innebär att fler träffar behöver hanteras och skickas till behöriga myndigheter under dygnets alla timmar. Förhandskontroller vid varje begäran om tillgång till PNR-information i efterhand kommer att leda till ökad administration. Sannolikt kommer även antalet beställningar till enheten att öka. Vår bedömning är att den vanligaste konsekvensen kommer vara att

beställningen blir bredare, dvs. omfattar en bevakning, analys eller sökning i fler transportslag, snarare än att de blir fler.

Hantering av en bredare bevakning tar mer tid och att kunna hantera den stora ökningen av passagerare med bibehållen servicenivå kommer att öka kostnaderna. Hanteringen är dock till stor del automatiserad och därför bör det inte leda till några större kostnadsökningar. Sammantaget bedömer vi att kostnaderna för att driva enheten för passagerarinformation med bibehållen servicenivå utifrån de nya förutsättningarna ökar med runt 15 procent, vilket motsvarar 4,5 miljoner kronor baserat på enhetens budget på 30 miljoner kronor för 2026.

Polismyndighetens it-verksamhet

Bedömning

Förslagen innebär en ökning Polismyndighetens it-uppdrag vilket medför en uppskattad kostnadsökning om cirka 68–100 miljoner kronor.

Inkluderingen av fler trafikslag i PNR-lagstiftningen innebär att PNR-databasen behöver utvecklas och fler trafikslag läggas till. Polismyndighetens it-avdelnings preliminära bedömning är att kostnaden för ett driftsatt trafikslagsneutralt PNR-system vid ett införande den 1 januari 2028 är mellan 68 och 100 miljoner kronor. Eftersom enheten för passageraruppgifter är inordnad under Polismyndigheten innebär det att myndigheten tar hela utvecklingskostnaden för ett trafikslagsneutralt PNR-system. Kostnaden innefattar även förslagen om utökade befogenheter enligt polislagen och är beräknad utifrån ett it-system som innebär att transportörer endast behöver rapportera in information vid ett tillfälle, dvs. oavsett om det sker inom ramen för det trafikslagsneutrala PNR-systemet eller med 25 § polislagen som grund. Inräknat i kostnaden är även den nödvändiga anpassningen till de nya API-förordningarna avseende brottsbekämpning och gränskontroll.

Polismyndighetens anslag för 2025 var 48 miljarder kronor, och kostnaden för utvecklingen av it-miljön utgör därmed 0,15 procent av Polismyndighetens budget. Tillsammans med de ökade kostnaderna för enheten för passagerarinformation utgör de totala kostnadsökning-

arna för Polismyndigheten visserligen en liten andel av den totala budgeten. Det rör sig dock om betydande summor och vår bedömning är att kostnaderna inte ryms inom befintligt anslag utan bör bekostas genom det allmänna reformutrymmet.

18.3.6 Övriga konsekvenser

Bedömning

Förslagen bedöms inte få några konsekvenser i övrigt.

Förslagen får inte några konsekvenser för kommuner eller regioner eller för den kommunala självstyrelsen. Förslagen medför inte heller några andra konsekvenser som inte har kommenterats på andra ställen i detta kapitel.

19 Ikraftträdande

Förslag

Författningsförslagen ska träda i kraft den 1 januari 2028.

Det är angeläget att förslagen träder i kraft så snart som möjligt, dels för att justera svensk rätt så att den är förenlig med EU-domstolens praxis, dels för att vidta åtgärder mot terrorism och annan allvarlig brottslighet. Förslaget om en trafikslagsneutral PNR-lagstiftning innebär förändringar i verksamheten för aktörer inom den gränsöverskridande tåg- och busstrafiken. För dessa aktörer krävs det att den tekniska infrastrukturen är på plats för att lagstiftningen ska kunna tillämpas. Det bör därför ges viss tid för förberedelser. För färjetrafiken är utgångspunkten att passageraruppgifter förs över till enheten för passagerarinformation via EMSWe. Systemet planeras att tas i bruk i Sverige under det andra halvåret 2027 och det är detta vi har utgått ifrån i bedömningen av när den föreslagna lagstiftningen bör träda i kraft. För det fall att driftstarten försenas ytterligare bör uppgiftsskyldigheten för färjetrafiken inte inträda förrän systemet har tagits i bruk.

Förändringarna som avser Åklagarmyndigheten, domstolsväsendet samt de behöriga myndigheterna kräver i sammanhanget inte lika mycket förberedelser som de som avser transportföretagen. Med beaktande av detta samt sedvanlig tid för remissbehandling och beredning inom Regeringskansliet föreslås förslagen träda i kraft den 1 januari 2028. Detta ger transportföretagen tillräckligt med tid för att genomföra nödvändiga anpassningar och förbereda sig för tillämpningen av den nya regleringen.

20 Författningskommentar

20.1 Förslaget till lag om ändring av lagen (2018:1181) om flygpassageraruppgifter i brottsbekämpningen

Lag (2018:1180) om passageraruppgifter i brottsbekämpningen

1 kap.

Lagens innehåll

1 §

Denna lag *innehåller bestämmelser om transportföretags överföring av PNR-uppgifter till enheten för passagerarinformation och om behandling av PNR-uppgifter i verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet.* Med PNR-uppgifter avses i lagen uppgifter om varje enskild passagerare som har lämnats vid bokning av en *transport, köp av biljett* och vid incheckning.

Lagen genomför också Europaparlamentets och rådets direktiv (EU) 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet, här benämnt PNR-direktivet.

Med terroristbrottslighet avses i lagen brott enligt artiklarna 3–12 och 14 i Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF.

Med annan allvarlig brottslighet avses i lagen de brott som anges i bilaga II till PNR-direktivet och för vilka det i Sverige eller andra medlemsstater är föreskrivet fängelse i tre år eller mer.

Paragrafen uppdateras så att den omfattar transportföretag och inte enbart lufttrafikföretag.

Andra uttryck i lagen

3 §

Transportföretag	Ett företag som har giltig operativ licens, *tillstånd*, *certifikat* eller motsvarande som ger rätt att mot ersättning utföra *transporter* av passagerare med *flygplan*, *tåg, buss eller färja*, och som i sin normala verksamhet samlar in och behandlar PNR-uppgifter i ett elektroniskt system för hantering av reservationer, *avgångskontrollsystem för att checka in passagerare*, *elektroniskt system för köp av biljetter eller likvärdiga system med motsvarande uppgifter.*
Medlemsstat	En stat som är medlem i Europeiska unionen och har antagit PNR-direktivet. *När det gäller transporter med tåg, buss eller färja avses samtliga stater som är medlemmar i Europeiska unionen.*
Passagerare	Alla personer, förutom besättningsmedlemmar, som transporteras eller ska transporteras med ett flygplan, *tåg, buss eller färja.*
Transport utanför EU	*Transport som utförs av ett transportföretag, med avgång från ett tredjeland och planerad ankomst på en medlemsstats territorium eller transport från en medlemsstats territorium med planerad ankomst i ett tredjeland, i båda fallen inklusive eventuella mellanlandningar eller stopp på territorier i medlemsstater eller tredjeländer.*
Transport inom EU	*Transport som utförs av ett transportföretag, med avgång från en medlemsstats territorium och planerad ankomst på en eller flera andra medlemsstaters territorium, utan eventuella mellanlandningar eller stopp på tredjeländers territorier samt transport som utförs av ett lufttrafikföretag mellan två inrikes flygplatser i Sverige.*

I paragrafen definieras vissa uttryck i lagen. Paragrafen justeras så att lufttrafikföretag ersätts av transportföretag, att passagerare omfattar även resande med tåg, buss eller färja samt att definitionen av transportföretag även omfattar företag som samlar in och behandlar PNR-uppgifter i ett elektroniskt system för biljettköp, utöver tidigare angivna hantering av reservationer. Paragrafen kompletteras vidare med definitioner av begreppen transport utanför EU och transport inom EU. Definitionerna motsvarar det som anges för flygresor i artikel 3.2–3 i PNR-direktivet, med tillägget att resor inom EU även inkluderar inrikes flygtrafik.

Enhet för passagerarinformation

4 §

Det ska vid Polismyndigheten finnas en enhet för passagerarinformation. Enheten ska ansvara för att

1. samla in PNR-uppgifter från *transportföretag,* bevara och i övrigt behandla uppgifterna, och
2. överföra PNR-information till behöriga mottagare och tredjeländer.

Paragrafen uppdateras så att den omfattar transportföretag och inte enbart lufttrafikföretag.

Tillåten behandling av PNR-information

5 §

PNR-information får endast behandlas i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet, om inte annat anges i 5 kap. 3 §.

Paragrafen, som behandlas i avsnitt 8.7, anger de tillåtna syftena för att behandla PNR-information. Hänvisningen till 1 kap. 6 § i lagen tas bort till följd av att andra stycket i den paragrafen, som hänvisningen syftar till, upphävs.

6 §

Lagens bestämmelser om behandling av personuppgifter gäller inte för behöriga myndigheter i verksamhet som rör nationell säkerhet.

Paragrafen anger att lagens bestämmelser om behandling av personuppgifter inte ska gälla för behöriga myndigheter i verksamhet som rör nationell säkerhet. Bestämmelsen innebär att behöriga myndigheter i sådan verksamhet ska tillämpa bestämmelser i respektive registerförfattning i stället för bestämmelser om behandling av personuppgifter i denna lag.

Det tidigare andra stycket upphävs för att svensk rätt ska överensstämma med den uttömmande uppräkningen i artikel 1.2 i PNR-direktivet av tillåtna syften med behandling av PNR-uppgifter som samlas in i enlighet med direktivet. Övervägandena finns i avsnitt 8.9.

2 kap. *Transportföretagens* skyldigheter

Överföring av PNR-uppgifter till enheten för passagerarinformation

1 §

Transportföretag ska till enheten för passagerarinformation inför varje *transport inom eller utanför EU* överföra sådana PNR-uppgifter som anges i *bilagorna* till lagen. PNR-uppgifterna ska endast överföras i de fall *transportföretagen* samlar in uppgifterna som en del av sin normala verksamhet.

Skyldigheten för transportföretag som bedriver färjetrafik att överföra PNR-uppgifter enligt första stycket omfattar även de uppgifter om besättningen som anges i punkt 17 i bilaga 4.

Om *transportens* linjebeteckning delas med ett eller flera andra *transportföretag*, ska det *transportföretag* som utför *transporten* överföra PNR-uppgifter om samtliga passagerare.

Paragrafens *första* och *fjärde stycke* uppdateras så att den omfattar transportföretag och inte enbart lufttrafikföretag och ordalydelsen flygningen ersätts av transporten.

Paragrafens *andra stycke*, som är nytt, innebär att lufttrafikföretag har en skyldighet att överföra PNR-uppgifter till enheten för passagerarinformation även inför varje flygresa mellan två flygplatser belägna inom Sveriges gränser. Övervägandena finns i avsnitt 7.1.

Paragrafens *tredje stycke*, som också är nytt, anger en skyldighet för transportföretag som bedriver färjetrafik att även överföra de upp-

gifter om besättningen som anges i punkt 17 i bilaga 4, vilka är namn, telefonnummer, e-postadress, födelsedatum, identitetshandling och identitetshandlingens nummer. Övervägandena finns i avsnitt 16.4.

2 §

PNR-uppgifterna *för en flygning* ska överföras
1. 24–48 timmar före flygningens avgång, och
2. omedelbart efter det att gatens dörrar har stängts.

Den andra överföringen får begränsas till uppdateringar och kompletteringar av de uppgifter som överfördes vid det första tillfället.

PNR-uppgifter för övriga transportföretag, med undantag för sådana som bedriver färjetrafik, ska överföras i samband med att en bokning eller avbokning av en transport sker.

Paragrafens *första stycke* gäller när PNR-uppgifter från en flygning ska överföras till enheten för passagerarinformation. PNR-uppgifter från tåg- och busstrafik ska i stället överföras så snart en bokning eller avbokning sker. Övervägandena finns i avsnitt 16.6.1.

Registrering av passagerare inom färjetrafiken är reglerad på EU-nivå och i svensk rätt genom Transportstyrelsens föreskrifter och allmänna råd. I regleringen är det föreskrivet när uppgifter från passagerarfartyg ska lämnas till Sjöfartsverket. Uppgifterna skickas därefter till enheten för passagerarinformation. Till följd av detta regleras inte tidpunkten för överföring av PNR-uppgifter för färjetrafik i lagen. Övervägandena finns i avsnitt 16.6.2.

3 §

Transportföretag ska på begäran av enheten för passagerarinformation överföra PNR-uppgifter även vid andra tidpunkter än de som anges i 2 §, om enheten bedömer att det i ett enskilt fall är nödvändigt med tillgång till PNR-uppgifter för att avvärja en specifik och faktisk fara med anknytning till terroristbrottslighet eller annan allvarlig brottslighet.

Paragrafen uppdateras så att den omfattar transportföretag och inte enbart lufttrafikföretag. Bestämmelsen gäller samtliga transportföretag, dvs. även sådana som bedriver passagerartrafik med färja, även om sådana företag inte nämns i 2 §. Övervägandena finns i avsnitt 16.6.3.

4 §

Transportföretag ska överföra PNR-uppgifterna elektroniskt. Enheten för passagerarinformation får inte medges direktåtkomst till PNR-uppgifter som behandlas vid *transportföretagen*.

Paragrafen uppdateras så att den omfattar transportföretag och inte enbart lufttrafikföretag.

5 §

Transportföretag som är skyldiga att överföra PNR-uppgifter får anlita ett personuppgiftsbiträde för att utföra överföringen.

Paragrafen uppdateras så att den omfattar transportföretag och inte enbart lufttrafikföretag.

Information till passagerare

6 §

Transportföretag ska informera passagerare om överföringen av PNR-uppgifter till enheten för passagerarinformation och om skälen till överföringen.

Paragrafen uppdateras så att den omfattar transportföretag och inte enbart lufttrafikföretag.

Rätt att meddela föreskrifter

7 §

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om *transportföretagens* överföring av PNR-uppgifter till enheten för passagerarinformation.

Paragrafen uppdateras så att den omfattar transportföretag och inte enbart lufttrafikföretag.

3 kap.

PNR-databas

1 §

PNR-uppgifter som har överförts från ett *transportföretag* ska bevaras i en databas vid enheten för passagerarinformation.

Paragrafen uppdateras så att den omfattar transportföretag och inte enbart lufttrafikföretag.

Tillåtna ändamål för behandling av PNR-uppgifter

4 §

Enheten för passagerarinformation får endast behandla PNR-uppgifter som har överförts från ett *transportföretag* för att

1. göra en förhandsbedömning av passagerare före deras beräknade ankomst till eller avresa från Sverige i syfte att välja ut personer som behöver utredas ytterligare av behöriga myndigheter eller Europol, på grund av att dessa personer kan vara inblandade i terroristbrottslighet eller annan allvarlig brottslighet,
2. fullgöra sina uppgifter att överföra PNR-information till behöriga mottagare eller tredjeländer, eller
3. göra analyser för att uppdatera eller skapa nya kriterier som ska användas vid förhandsbedömningar.

Paragrafen anger de tillåtna ändamålen för behandling av PNR-uppgifter. Hänvisningen till 1 kap. 6 § i lagen tas bort till följd av att det andra stycket i den paragrafen, som hänvisningen avser, upphävs. Övervägandena finns i avsnitt 8.9. Paragrafen uppdateras även så att den omfattar transportföretag och inte enbart lufttrafikföretag.

5 §

Vid en förhandsbedömning får PNR-uppgifter

1. jämföras med register eller andra uppgiftssamlingar *över personer eller föremål som är eftersökta eller finns uppförda på en spärrlista samt med register eller andra uppgiftssamlingar* som är relevanta för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet, och

2. behandlas enligt på förhand utformade och fastställda kriterier som är riktade, proportionella och avgränsade och som inte grundas på sådana känsliga personuppgifter som avses i 1 kap. 7 §.

Med relevanta register och uppgiftssamlingar enligt första stycket 1 avses register och uppgiftssamlingar som förvaltas av de behöriga myndigheterna eller, när det gäller EU-databaser och internationella databaser, används av de behöriga myndigheterna för de syften som anges i första stycket 1.

Jämförelse enligt första stycket 1 får endast ske om registret eller uppgiftssamlingen används i samband med bekämpningen av terroristbrottslighet eller annan allvarlig brottslighet som har ett åtminstone indirekt objektivt samband med transport av passagerare.

Paragrafen har justerats för att tydliggöra vad som krävs för att ett visst register eller en viss uppgiftssamling, vilket i PNR-direktivet benämns som databas, ska få användas vid en förhandsbedömning av PNR-uppgifter. Övervägandena finns i avsnitt 8.6. Det krävs inte att det framgår eller går att utläsa av det uttryckliga syftet med ett register eller annan uppgiftssamling är att bekämpa terroristbrott eller annan allvarlig brottslighet. Det krav som PNR-domen ställer upp är att registret eller uppgiftssamlingen ska användas i sådan verksamhet. Förtydligandet av detta bör inte medföra några större förändringar eftersom regleringen sedan tidigare krävt att register och andra uppgiftssamlingar ska vara relevanta för att bekämpa sådan brottslighet.

Tid som PNR-uppgifter ska bevaras

9 §

PNR-uppgifter som behandlas vid enheten för passagerarinformation ska bevaras i *sin fullständiga form i sex månader* från det att de kommit in från ett *transportföretag.* Därefter ska de *anonymiseras. Samtliga PNR- uppgifter som behandlas vid enheten för passagerarinformation ska förstöras senast fem år från det att de kommit in från ett transportföretag.*

PNR-uppgifter för transporter där det förekommer personer vars resor har ett direkt eller indirekt samband med en risk för terroristbrottslighet eller annan grov brottslighet ska behörighetsbegränsas i enlighet med 3 kap. 11 § i stället för anonymiseras sex månader efter att de kommit in från ett transportföretag.

Paragrafen behandlas i avsnitt 8.6 och genomför delvis artikel 12.1 och 12.4 i PNR-direktivet. I direktivet föreskrivs att PNR-uppgifter som mottagits från lufttrafikföretagen ska lagras i databasen för PNR-uppgifter vid enheten för passagerarinformation i fem år. I PNR-

domen anges emellertid att PNR-direktivet och EU-stadgan utgör hinder för en nationell lagstiftning som föreskriver en generell lagringstid på fem år för PNR-uppgifter, om lagringstiden tillämpas utan åtskillnad på alla flygpassagerare. PNR-uppgifter får däremot bevaras i upp till fem år om det föreligger en risk för terroristbrott eller annan grov brottslighet som har ett direkt eller indirekt samband med en passagerares flygresa.

Under de första sex månaderna går det, om det är absolut nödvändigt, att lagra PNR-uppgifter avseende samtliga flygpassagerare som omfattas av PNR-systemet. För den efterföljande perioden får emellertid sådan urskillningslös lagring inte ske. Huvudregeln ska således vara att anonymisering av uppgifterna sker efter sex månader. Med anonymisering avses en process som gör det nära nog omöjligt att identifiera en enskild person utifrån uppgifterna. Det ska inte heller gå att återupprätta kopplingen mellan de anonymiserade uppgifterna och individen. För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel, som t.ex. utgallring, som, antingen av den personuppgiftsansvarige eller av en annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att fastställa om hjälpmedel med rimlig sannolikhet kan komma att användas för att identifiera den fysiska personen bör man beakta samtliga objektiva faktorer, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten som den tekniska utvecklingen. När uppgifterna har anonymiserats utgör de inte längre personuppgifter.

Vissa uppgifter ska behörighetsbegränsas i stället för att anonymiseras. Detta gäller PNR-uppgifter från flygningar där det förekommer personer vars flygresor har ett direkt eller indirekt samband med en risk för terroristbrott eller annan grov brottslighet. Sådana indikationer kan komma fram under förhandsbedömningen enligt 3 kap. 4 § 1, genom andra eventuella kontroller som utförts under den inledande sexmånadersperioden eller någon annan omständighet. Exempel på omständigheter som kan utgöra ett sådant samband är att det vid förhandsbedömningen kommer fram att en specifik person med kopplingar till ett terrornätverk finns med på en viss flygning eller att en person uppfyller kriterierna i en regelbaserad sökning. Om ett sådant samband har konstaterats avseende en person bör det innebära att det finns ett, åtminstone indirekt, samband även för övriga passagerare på samma flygning. PNR-uppgifterna för samtliga resenärer på en

sådan flygning får således undantas från anonymisering efter sex månader.

Samtliga uppgifter ska förstöras senast fem år från det att de kommit in från ett lufttrafikföretag.

Paragrafen uppdateras även så att den omfattar transportföretag och inte enbart lufttrafikföretag.

10 §

PNR-uppgifter som inte anges i *bilagorna* till lagen eller som utgör sådana känsliga personuppgifter som avses i 1 kap. 7 § ska omedelbart förstöras om de kommer in till enheten för passagerarinformation.

Paragrafen ändras så att den hänvisar till bilagorna till lagen i stället för bilagan.

Behörighetsbegränsning av PNR-uppgifter

11 §

Följande PNR-uppgifter ska, *om de inte ska anonymiseras enligt 3 kap. 9 §*, behörighetsbegränsas sex månader efter att de har kommit in från ett *transportföretag* om de kan användas för att identifiera en person:

1. namn på passagerare,
2. antal passagerare som reser tillsammans,
3. adress och kontaktuppgifter,
4. alla former av betalningsinformation, inklusive faktureringsadress,
5. uppgifter om bonusprogram,
6. allmänna anmärkningar, och
7. uppgifter om *alla ändringar som har gjorts av de PNR-uppgifter som anges i bilagorna* till lagen.

Paragrafen kompletteras med ett undantag från behörighetsbegränsning för de uppgifter som i stället ska anonymiseras enligt 3 kap. 9 §.

Punkt 7 ändras så att hänvisning görs till samtliga bilagor till lagen.

3 a kap. Behandling av PNR-uppgifter för transporter inom EU

1 §

Detta kapitel gäller för enheten för passagerarinformations behandling av PNR-uppgifter för transporter inom EU.

Om inte annat anges i detta kapitel, ska alla bestämmelser i lagen gälla för transporter inom EU som om de vore transporter utanför EU och för PNR-uppgifter för transporter inom EU som om det vore PNR-uppgifter för transporter utanför EU.

Paragrafen anger att tillämpningsområdet för kapitlet är transporter inom EU. Bestämmelserna i kapitlet behandlas i avsnitt 8.2 och 8.3. Definitioner av transporter utanför respektive inom EU finns i 1 kap. 3 §. Alla bestämmelser i lagen i övrigt gäller även avseende transporter inom EU, såvida inte annat anges i detta kapitel.

2 §

PNR-uppgifter för transporter inom EU ska anonymiseras efter att förhandsbedömningen enligt 3 kap. 4 § 1 har genomförts. PNR-uppgifter för transporter där det förekommer personer som efter förhandsbedömningen behöver utredas ytterligare av behöriga myndigheter eller Europol får fortsatt behandlas för de ändamål som anges i 3 kap. 4 § 2 och 3.

Paragrafen anger att huvudregeln är att PNR-uppgifter för transporter inom EU ska anonymiseras efter att förhandsbedömningen har genomförts. Syftet med förhandsbedömningen är att välja ut personer som behöver utredas ytterligare av behöriga myndigheter eller Europol, på grund av att personerna kan vara inblandade i terroristbrottslighet eller annan allvarlig brottslighet. För att ytterligare utredning ska kunna genomföras ska PNR-uppgifter från dessa resor fortsatt få behandlas av enheten för passagerarinformation.

I avsnitt 8.7 behandlas anonymiseringen. Genom anonymiseringen upphör uppgifterna att vara personuppgifter och bevarandet av uppgifterna står därmed inte i strid med uttalandena i PNR-domen som avser flygningar inom EU. Övervägandena finns i avsnitt 8.2.

3 §

Om det föreligger ett verkligt och aktuellt eller förutsebart terroristhot mot Sverige får beslut fattas om att enheten för passagerarinformation får behandla PNR-uppgifter i sin fullständiga form för samtliga resor inom EU även efter förhandsbedömningen enligt 3 kap. 4 § 1.

Paragrafen anger förutsättningarna för att besluta om utvidgad tillämpning av PNR-systemet till att omfatta samtliga resor inom EU. Övervägandena finns i avsnitt 8.2. Om en medlemsstat bedömer att det föreligger tillräckligt konkreta omständigheter som visar att medlemsstaten ska anses stå inför ett verkligt och aktuellt eller förutsebart terrorhot, går det inte utöver vad som är strikt nödvändigt att tillämpa PNR-direktivet på samtliga resor inom EU från eller till medlemsstaten under en viss tid. Att det finns ett sådant hot är i sig ägnat att upprätta ett samband mellan överföring och behandling av de berörda uppgifterna och kampen mot terrorism. Omständigheter som kan vara av betydelse vid bedömningen av terrorhotet är t.ex. om det inträffar ett terrordåd eller terrorhotsnivån mot Sverige är förhöjd.

4 §

Om det inte föreligger något terroristhot mot Sverige i enlighet med 3 § får ett urval av resor tillämpas för vilka PNR-uppgifter för samtliga passagerare får bevaras i sin fullständiga form även efter förhandsbedömningen enligt 3 kap. 4 § 1.

Urvalet av resor ska begränsas till vad som är absolut nödvändigt för att uppnå syftet med behandlingen av PNR-uppgifterna.

När en medlemsstat beslutar att tillämpa PNR-direktivet på utvalda resor inom EU ska den välja de resor för vilka det finns uppgifter som kan motivera en sådan tillämpning. I bedömningen får utöver terrorhotet även beaktas risken för annan allvarlig brottslighet. Medlemsstaten får när som helst besluta att ändra urvalet av resor inom EU och ska säkerställa att tillämpningen alltid är begränsad till vad som är absolut nödvändigt. Övervägandena finns i avsnitt 8.2.

5 §

Beslut enligt 3 § ska fattas av Säkerhetspolisen. Inför beslutet kan Säkerhetspolisen vid behov inhämta synpunkter från Försvarsmakten och andra myndigheter. Beslutet upphör att gälla ett år efter den dag då det fattades.

Säkerhetspolisens beslut gäller omedelbart och ska expedieras till enheten för passagerarinformation.

Paragrafen behandlas i avsnitt 8.2.1. Det är Säkerhetspolisen som fattar beslut om utvidgad tillämpning av PNR-systemet i enlighet med 3 §. Säkerhetspolisen kan vid behov inhämta synpunkter från Försvarsmakten inför beslutet. Säkerhetspolisen får också, i den mån det är lämpligt och nödvändigt, inhämta information från andra myndigheter som kan ha relevant information om omständigheter som är av betydelse för bedömningen av terrorhotet mot Sverige.

Paragrafen reglerar även beslutets längsta giltighetstid om ett år. Om Säkerhetspolisen gör bedömningen att ett tillräckligt allvarligt terrorhot kvarstår efter ett år, får myndigheten fatta ett nytt beslut.

I *andra stycket* anges att beslutet gäller omedelbart. För att enheten för passagerarinformation omedelbart ska kunna förändra tillämpningen av PNR-systemet ska beslutet expedieras till enheten.

6 §

Beslut om urval av transporter enligt 4 § ska fattas av enheten för passagerarinformation. Inför beslutet ska enheten inhämta synpunkter från de behöriga myndigheterna. Urvalet av resor ska regelbundet ses över.

Om det inte föreligger ett tillräckligt allvarligt terrorhot mot Sverige att behandla PNR-uppgifter från samtliga resor inom EU får ett beslut om urval av flygningar fattas. Paragrafen fastställer att det är enheten för passagerarinformation som ska fatta beslutet om urval av resor. Medlemsstaten ska regelbundet göra en översyn av tillämpningen med hänsyn till utvecklingen de villkor som motiverat urvalet, för att säkerställa att tillämpningen av systemet på dessa resor alltid är begränsad till vad som är strikt nödvändigt. Inför beslutet ska synpunkter inhämtas från de behöriga myndigheterna. Övervägandena finns i avsnitt 8.2.1.

7 §

Beslut enligt 3 § ska underställas Försvarsunderrättelsedomstolen utan onödigt dröjsmål och senast inom en vecka från den dag då beslutet fattades.

Paragrafen behandlas i avsnitt 8.3. Ett beslut om sådan tillämpning som avses i 3 § måste kunna bli föremål för effektiv kontroll antingen av en domstol eller av en oberoende förvaltningsmyndighet, vars avgörande har bindande verkan. Syftet med prövningen är att kontrollera om det föreligger ett sådant terrorhot och att de villkor och garantier som måste ställas upp är uppfyllda. Försvarsunderrättelsedomstolen är exklusivt forum för prövning av Säkerhetspolisens beslut.

8 §

När ett beslut har underställts Försvarsunderrättelsedomstolen ska domstolen hålla sammanträde. Till sammanträdet ska Säkerhetspolisen kallas.

Paragrafen innebär att mål avseende underställda beslut ska avgöras efter sammanträde dit Säkerhetspolisen kallas. Övervägandena finns i avsnitt 8.3.2.

9 §

Försvarsunderrättelsedomstolens beslut enligt denna lag får inte överklagas.

Paragrafen innebär att överklagandeförbud avseende Försvarsunderrättelsedomstolens beslut enligt denna lag.

4 kap.

Överföring av PNR-information på begäran

11 §

PNR-information får endast överföras till behöriga mottagare eller ett tredjeland om det rimligen kan antas vara nödvändigt för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet.

Om en förundersökning *enligt rättegångsbalken* pågår ska en begäran från en behörig myndighet om att få tillgång till *PNR-information* beslutas av *allmän domstol.*

I de fall som inte omfattas av andra stycket *ska ett sådant beslut fattas av åklagare.*

Paragrafen reglerar förutsättningarna för överföring av PNR-information till behöriga myndigheter eller tredjeländer. Den genomför artikel 12.3 i PNR-direktivet. Övervägandena finns i avsnitt 8.5. Paragrafen uppdateras för att ligga i linje med PNR-domens uttalanden om att prövningen ska genomföras av en domstol eller en oberoende förvaltningsmyndighet samt att den ska genomföras oavsett om PNR-informationen är behörighetsbegränsad eller inte.

Rubriken och första, andra och fjärde stycket ändras så att PNR-information, och inte bara PNR-uppgifter, omfattas. Rubriken ändras även för att särskilja överföring som görs på begäran från överföring som görs efter förhandsbedömningen.

Enligt andra stycket ska prövningen genomföras av allmän domstol om en förundersökning pågår. För att förtydliga att detta inte gäller förundersökningar som bedrivs i andra medlemsstater anges att det gäller förundersökningar enligt rättegångsbalken.

Enligt *tredje stycket* ska beslut i övriga fall, dvs. när det inte pågår någon förundersökning enligt rättegångsbalken, fattas av åklagare. Det innebär att begäranden från behöriga mottagare i en annan medlemsstat, ett tredjeland eller Europol hanteras av åklagare enligt detta stycke.

12 §

Om en begäran om tillgång till PNR-information från en behörig mottagare i en annan medlemsstat har föregåtts av en prövning av om tillgång till informationen ska medges av en domstol eller oberoende förvaltningsmyndighet, ska beslut enligt 11 § tredje stycket inte fattas.

Det första stycket gäller även en begäran från ett tredjeland som har slutit avtal med EU om överföring och behandling av passageraruppgifter.

I paragrafen, som är ny, regleras situationen där en rättslig prövning redan har genomförts i landet från vilken begäran framställts. I sådana situationer ska inte ytterligare en prövning göras av en svensk åklagare. Regleringen omfattar medlemsstater i EU och andra stater som har slutit avtal med EU om överföring och behandling av passageraruppp-

gifter, och således inte övriga tredjeländer. Övervägandena finns i avsnitt 8.5.7.

13 §

Om den efterfrågade PNR-informationen inte finns hos enheten för passagerarinformation ska det inte fattas något beslut enligt 11 § andra eller tredje stycket.

I paragrafen anges att om den efterfrågade PNR-informationen inte finns hos enheten för passagerarinformation ska det inte fattas något beslut enligt 11 § andra eller tredje stycket. Av detta följer att enheten måste konstatera att informationen finns hos enheten innan begäran underställs rätt prövningsinstans.

Prövningen i domstol

14 §

En begäran om tillgång till PNR-information under en pågående förundersökning enligt rättegångsbalken prövas av den domstol som anges i 19 kap. rättegångsbalken.

En begäran enligt första stycket från Försvarsmakten eller Säkerhetspolisen prövas av Stockholms tingsrätt.

Paragrafen reglerar vilken domstol som är behörig att pröva en begäran om tillgång till PNR-information under pågående förundersökning. Övervägandena finns i avsnitt 8.5.5.

Bestämmelsen motsvarar den ordning som gäller vid en ansökan om hemliga tvångsmedel i en förundersökning enligt rättegångsbalken. En begäran om tillgång till PNR-information prövas enligt reglerna i rättegångsbalken om laga domstol i brottmål. Som huvudregel är rätten i den ort där brottet begicks behörig. Om det är lämpligt får prövningen i stället föras där den misstänkte har hemvist eller mera varaktigt uppehåller sig. I vissa brådskande fall får frågan även prövas av domstol på annan ort.

I andra paragrafen anges att när det gäller en begäran om tillgång till PNR-uppgifter som framställs av Försvarsmakten eller Säkerhetspolisen är Stockholms tingsrätt exklusivt forum.

15 §

Förfarandet i domstol är skriftligt. På förfarandet tillämpas reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande i sådana frågor. Det som föreskrivs om offentliga ombud i 27 kap. 28 § rättegångsbalken ska dock inte tillämpas.

I paragrafen regleras formen för domstolens handläggning av en begäran om tillgång till PNR-information under pågående förundersökning. Övervägandena finns i avsnitt 8.5.4.

Domstolen handläggning av begäran om tillgång ska vara skriftlig. Ärendet avgörs således utan sammanträde. Paragrafen anger vidare att rättegångsbalkens regler om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor är tillämpliga på förfarandet. Det gäller t.ex. regler om rättens sammansättning och om överklagande. Av paragrafen framgår emellertid att bestämmelsen om offentligt ombud i 27 kap. 28 § rättegångsbalken inte ska tillämpas.

Skyndsam handläggning

16 §

En begäran om tillgång till PNR-information ska handläggas skyndsamt.

Paragrafen reglerar inom vilken tid en begäran om tillgång till PNR-information ska hanteras. Övervägandena finns i avsnitt 8.5.4.

I paragrafen anges att en begäran om tillgång till PNR-information ska handläggas skyndsamt. Hur snabbt en begäran ska hanteras får avgöras i det enskilda fallet utifrån de förutsättningar som gäller. Kravet på skyndsamhet gäller för både åklagarens prövning i underrättelseskedet och domstolens prövning under pågående förundersökning, liksom i överrätt om domstolens avgörande överklagas.

Tillfällig tillgång till PNR-information utan tillstånd

17 §

Om det är fara i dröjsmål, får enheten för passagerarinformation medge tillgång till PNR-information efter en vederbörligen motiverad begäran från en behörig mottagare utan att tillstånd har meddelats av åklagare eller domstol.

Det första stycket gäller även för en begäran från ett tredjeland som har slutit avtal med EU om överföring och behandling av passageraruppgifter.

Paragrafen innebär att behöriga mottagare, i vissa brådskande situationer, kan medges tillgång till PNR-information utan tillstånd. Övervägandena finns i avsnitt 8.4.1 och 8.5.4.

Enligt paragrafen får enheten för passagerarinformation medge tillgång till PNR-information utan tillstånd från åklagare eller domstol om det är fara i dröjsmål. Sådan behandling av PNR-information ska begränsas till situationer där ändamålet med användningen av uppgifterna riskerar att gå förlorad om den behöriga myndigheten avvaktar den rättsliga prövningen. Ju mer angeläget det är att lokalisera en viss individ eller av annat skäl få tillgång till uppgifterna, desto större bör utrymmet vara att får tillgång till PNR-information utan tillstånd. Den behöriga mottagaren ska i sin begäran motivera varför den har en sådan brådskande karaktär.

I det *andra stycket* anges att samma reglering gäller avseende en begäran från ett tredjeland som har slutit avtal med EU om överföring och behandling av passageraruppgifter. Av regleringen följer att en begäran från ett tredjeland som inte har slutit ett sådant avtal med EU alltid ska föregås av en rättslig prövning i Sverige, även i brådskande fall.

18 §

Om tillgång till PNR-information har medgetts utan tillstånd ska begäran om tillgång underställas rätt prövningsinstans utan onödigt dröjsmål och senast inom 24 timmar från det att tillgången medgavs.

Om tillgången har medgetts utan tillstånd och det inte längre finns skäl för behandling av uppgifterna ska behandlingen hos den behöriga myndigheten omedelbart upphöra.

Paragrafen reglerar förfarandet när en behörig myndighet medges tillgång till PNR-information utan föregående prövning av åklagare eller domstol. Övervägandena finns i avsnitt 8.4.1.

Paragrafen innebär att om tillgång till PNR-information har medgetts utan tillstånd, ska begäran om tillgång underställas prövningsinstansen utan onödigt dröjsmål och senast 24 timmar från det att tillgången medgavs.

19 §

Om en begäran om tillgång till PNR-information avslås ska behandling som har påbörjats av en behörig myndighet utan att tillstånd har meddelats av åklagare eller domstol omedelbart upphöra.

Paragrafen reglerar följderna av att tillgång till PNR-information har medgetts utan tillstånd när det inte har funnits förutsättningar för det. Övervägandena finns i avsnitt 8.4.1.

Paragrafen anger att om en begäran om tillgång till PNR- information avslås när behandling redan har påbörjats av en behörig myndighet, ska behandlingen omedelbart upphöra. Om behandlingen hinner avslutas innan den rättsliga prövningen bör det ändå ankomma på enheten för passagerarinformation att underställa begäran till rätt prövningsinstans.

6 kap.

Överträdelser av transportföretag

1 §

En sanktionsavgift ska tas ut av ett *transportföretag* som inte har överfört PNR-uppgifter enligt bestämmelserna i denna lag eller föreskrifter som har meddelats i anslutning till lagen.

Paragrafen uppdateras så att den omfattar transportföretag och inte enbart lufttrafikföretag.

2 §

Sanktionsavgiften ska för varje *transport* som har utförts utan att *transportföretaget* har fullgjort sin överföringsskyldighet bestämmas till lägst 20 000 kronor och högst 100 000 kronor. När sanktionsavgiftens storlek fastställs ska särskild hänsyn tas till antal passagerare på *transporten* och om *transportföretaget* tidigare har begått en överträdelse.

Sanktionsavgiften får sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

Paragrafen uppdateras så att den omfattar transportföretag och inte enbart lufttrafikföretag. Begreppet flygning ersätts av transport.

3 §

Polismyndigheten beslutar om sanktionsavgift för *transportföretag*.
Sanktionsavgiften tillfaller staten.

Paragrafen uppdateras så att den omfattar transportföretag och inte enbart lufttrafikföretag.

20.2 Förslaget till lag om ändring i polislagen (1984:387)

Uppgifter från transportföretag

25 §

Ett transportföretag som befordrar varor, passagerare eller fordon till eller från Sverige ska på begäran av Polismyndigheten eller Säkerhetspolisen skyndsamt lämna de aktuella uppgifter om ankommande och avgående transporter, som företaget har tillgång till. *Det som sägs om transportföretag gäller även andra företag som yrkesmässigt får tillgång till transportföretagets uppgifter om transporter.* Transportföretaget har endast skyldighet att lämna *följande* uppgifter om passagerare.

– namn,
– *födelsedatum*,
– *kön*,
– *nationalitet*,
– resrutt,
– bagage,
– medpassagerare,
– *betalningsinformation* och sättet för bokning,
– *mobiltelefonnummer, och*
– *e-postadress.*

Polismyndigheten får begära uppgifter enligt första stycket endast om uppgifterna kan antas ha betydelse för den brottsbekämpande verksamheten.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om hur transportföretag ska lämna uppgifter.

En begäran om uppgifter om en transport får inte överklagas.

Paragrafen reglerar Polismyndighetens och Säkerhetspolisens rätt att begära att ett transportföretag lämnar uppgifter om ankommande och avgående transporter. Övervägandena finns i avsnitt 17.3.

Uppräkningen i *första stycket* av de uppgifter om passagerare som transportföretagen har skyldighet att lämna är uttömmande och har

utökats med födelsedatum, kön, nationalitet, mobiltelefonnummer och e-postadress. Begreppet sättet för betalning har ersatts av betalningsinformation. I övrigt är uppräkningen oförändrad. Skyldigheten att lämna uppgifter gäller utöver transportföretag även andra företag som yrkesmässigt får tillgång till transportföretagets uppgifter om transporter.

Det *tredje stycket* är en upplysningsbestämmelse om att regeringen eller den myndighet som regeringen bestämmer, med stöd av 8 kap. För att underlätta för transportföretagen bör det ske samverkan mellan Polismyndigheten och Tullverket för att ta fram standarder och format för hur uppgifterna ska lämnas. Övervägandena finns i avsnitt 17.3.8.

I det *fjärde stycket* anges att en begäran om uppgifter från ett transportföretag inte får överklagas. Övervägandena finns i avsnitt 17.3.9.

26 §

Transportföretag får lämna uppgifter enligt 25 § på så sätt att de görs läsbara för Polismyndigheten eller Säkerhetspolisen genom *direktåtkomst*.

Polismyndigheten och Säkerhetspolisen får ta del av uppgifter genom *direktåtkomst innan transporten har ankommit eller avgått och under högst sex månader därefter, om det* behövs för att kontrollera aktuella transporter.

Paragrafens *första stycke* uppdateras så begreppet terminalåtkomst ersätts av direktåtkomst. Det innebär ingen förändring i sak. Övervägandena finns i avsnitt 20.3.10.

I det *andra stycket* anges att ett transportföretag i stället för att lämna uppgifter om en enskild transport får ge Polismyndigheten och Säkerhetspolisen tillgång till uppgifter genom direktåtkomst. Uppgifterna får finnas tillgängliga under ytterligare sex månader efter det att transporten har ankommit eller avgått. Sådan tillgång till historiska uppgifter om transporter ger myndigheterna möjlighet att bl.a. analysera resmönster. Övervägandena finns i avsnitt 17.3.6.

26 a §

Polismyndigheten och Säkerhetspolisen får förelägga ett transportföretag att fullgöra sina skyldigheter enligt 25 och 26 §§.

Beslutet om föreläggande får förenas med vite. Beslutet gäller omedelbart.

Paragrafen reglerar vilka medel Polismyndigheten och Säkerhetspolisen har om ett transportföretag inte lämnar de uppgifter som har begärts av respektive myndighet. Övervägandena finns i avsnitt 20.3.3.

Enligt *första stycket* för Polismyndigheten och Säkerhetspolisen utfärda ett föreläggande mot ett transportföretag som inte fullgör sina skyldigheter att lämna uppgifter enligt 25 och 26 §§.

I *andra stycket* anges att ett sådant föreläggande får förenas med vite och att det gäller omedelbart, dvs. oberoende av om föreläggandet överklagas.

26 b §

Ett beslut om föreläggande enligt 26 a § får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen anger att beslut av Polismyndigheten eller Säkerhetspolisen om föreläggande för ett transportföretag att fullgöra sina skyldigheter enligt 25 och 26 §§ får överklagas till allmän förvaltningsdomstol. Vid överklagande till kammarrätt ska det krävas prövningstillstånd. Övervägandena finns i avsnitt 17.3.3.

20.3 Förslaget till lag om ändring i lagen (2009:966) om Försvarsunderrättelsedomstol

Försvarsunderrättelsedomstolens uppgifter

1 §

Försvarsunderrättelsedomstolen ska pröva frågor om tillstånd till signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Försvarsunderrättelsedomstolen ska även

1. pröva frågor om tillstånd till framtagning enligt lagen (2026:000) om säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar,

2. pröva beslut som ska överklagas dit enligt lagen (2026:000) om Säkerhetspolisens behandling av personuppgifter, *och*

3. pröva underställda beslut enligt lagen (2018:1180) om passageraruppgifter i brottsbekämpningen.

I paragrafen anges Försvarsunderrättelsedomstolens uppgifter. I *andra stycket* läggs en bestämmelse till med innebörden att domstolen ska pröva underställda beslut enligt lagen om passageraruppgifter i brottsbekämpningen.

5 §

Ett integritetsskyddsombud ska bevaka enskildas integritetsintresse i mål vid domstolen *om tillstånd till signalspaning*. Ombudet har rätt att ta del av det som förekommer i målet och att yttra sig.

I paragrafen anges att ett integritetsskyddsombud ska bevaka enskildas integritetsintresse i mål vid domstolen. Paragrafen justeras så att den endast omfattar mål om tillstånd till signalspaning. Mål som rör underställda beslut enligt lagen (2018:1180) om passageraruppgifter i brottsbekämpningen omfattas således inte av bestämmelsen. Övervägandena finns i avsnitt 8.3.2.

14 a §

Domstolen får besluta att ett underställt beslut enligt lagen (2018:1180) om passageraruppgifter i brottsbekämpningen tills vidare inte ska gälla.

Ett beslut om utvidgad tillämpning av PNR-systemet enligt lagen om passageraruppgifter i brottsbekämpningen gäller omedelbart. I denna paragraf införs därför en möjlighet för Försvarsunderrättelsedomstolen att besluta att ett sådant beslut tills vidare inte ska gälla. Övervägandena finns i avsnitt 8.3.

16 §

Att Försvarsunderrättelsedomstolens beslut i frågor som rör signalspaning inte får överklagas framgår av 13 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. *Att domstolens beslut som rör underställda beslut i enlighet med lagen (2018:1180) om passageraruppgifter i brottsbekämpningen inte får överklagas framgår av 3 a kap. 9 § samma lag.* Inte heller domstolens beslut i övrigt enligt denna lag får överklagas.

Paragrafen innehåller hänvisningar till överklagandeförbuden i 13 § lagen om signalspaning i försvarsunderrättelseverksamhet och 3 a kap. 8 § lagen om passageraruppgifter i brottsbekämpningen. Andra beslut får inte heller överklagas. De beslut som omfattas av detta är t.ex. beslut om avvisning av en ansökan och om ersättning till integritetsskyddsombud.

20.4 Förslaget till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område

1 kap.

3 §

Särskilda bestämmelser om behandling av personuppgifter finns

1. i lagen (2017:496) om internationellt polisiärt samarbete och i föreskrifter som regeringen har meddelat i anslutning till den lagen,
2. i lagen (2018:1180) om *passageraruppgifter* i brottsbekämpningen och i föreskrifter som regeringen har meddelat i anslutning till den lagen,
3. i lagen (2022:613) om finansiell information i brottsbekämpningen och i föreskrifter som regeringen har meddelat i anslutning till den lagen, och
4. i lagen (2023:474) om polisiära befogenheter i gränsnära områden.

Om det i dessa författningar finns avvikande bestämmelser, ska de tillämpas i stället för bestämmelserna i denna lag.

Paragrafen uppdateras så att hänvisningen i punkt 2 avser lagen om passageraruppgifter i brottsbekämpningen.

2 kap.

13 §

Personuppgifter som tillhandahålls av transportföretag enligt 25 § polislagen (1984:387) får behandlas för att utföra en uppgift som anges i 1 § 1 och 2.

Polismyndigheten ska på begäran lämna sådana personuppgifter som avses i första stycket till

– Försvarsmakten, om de behövs i försvarsunderrättelseverksamheten eller den militära underrättelsetjänsten, och

– Ekobrottsmyndigheten, om de behövs i den brottsbekämpande verksamheten.

Personuppgifter som avses i första stycket får även behandlas förföljande ändamål för at utföra en uppgift som anges i 1 § 1 eller 2:

– planera kontroller,

– välja ut kontrollobjekt, och

– göra analyser som behövs för att uppdatera eller skapa nya kriterier som ska användas vid planering av kontroller eller urval av kontrollobjekt.

Personuppgifter som avses i första stycket får endast i ett enskilt fall behandlas för nya ändamål enligt 2 kap. 4 eller § brottsdatalagen (2018:1177).

Paragrafen reglerar den tillåtna behandlingen av personuppgifter som tillhandahålls av transportföretag enligt 25 § polislagen. Övervägandena finns i avsnitt 17.4–5.

I det *andra stycket* anges en skyldighet för Polismyndigheten att på begäran lämna personuppgifter som har tillhandahållits av transportföretag till Försvarsmakten, om de behövs i försvarsunderrättelseverksamheten, och till Ekobrottsmyndigheten, om de behövs i den brottsbekämpande verksamheten. Detta innebär att bestämmelsen är sekretessbrytande i enlighet med 10 kap. 28 § offentlighets- och sekretesslagen (2009:400).

14 §

Vid *direktåtkomst* enligt 26 § polislagen (1984:387) får personuppgifterna inte ändras eller bearbetas på annat sätt.

Paragrafen uppdateras så begreppet terminalåtkomst ersätts av direktåtkomst. Det innebär ingen förändring i sak. Övervägandena finns i avsnitt 17.3.10.

4 kap.

11 b §

Personuppgifter som med stöd av 25 § polislagen (1984:387) tillhandahålls på annat sätt än genom direktåtkomst, ska förstöras sex månader efter det att de behandlades första gången.

Paragrafen, som är ny, anger hur länge vissa uppgifter från transportföretag får bevaras. Övervägandena finns i avsnitt 17.3.6.

Utgångspunkten för all behandling av personuppgifter är att de inte får behandlas längre än vad som är nödvändigt i det enskilda fallet. För vissa kategorier av uppgifter anges det dock en yttersta gräns för hur länge de får behandlas. Uppgifter som tillhandahålls av transportföretag på annat sätt än genom direktåtkomst ska förstöras sex månader efter det att de behandlades första gången.

Kravet på förstöring gäller inte om uppgifterna behandlas för ett nytt ändamål i ett enskilt fall, t.ex. om de används i en brottsutredning eller har tagits in i ett underrättelseärende. Då ska i stället de bestämmelser som gäller för längsta tid för behandling av sådana uppgifter tillämpas.

20.5 Förslaget till lag om ändring i lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område

1 kap.

2 §

Särskilda bestämmelser om behandling av personuppgifter finns

1. i lagen (2017:496) om internationellt polisiärt samarbete och i föreskrifter som regeringen har meddelat i anslutning till den lagen,
2. i lagen (2018:1180) om *passageraruppgifter* i brottsbekämpningen och i föreskrifter som regeringen har meddelat i anslutning till den lagen,
3. i lagen (2022:613) om finansiell information i brottsbekämpningen och i föreskrifter som regeringen har meddelat i anslutning till den lagen,
4. i lagen (2023:474) om polisiära befogenheter i gränsnära områden, och
5. i tullbefogenhetslagen (2024:710).

Om det i dessa författningar finns avvikande bestämmelser, ska de tillämpas i stället för bestämmelserna i denna lag.

Paragrafen uppdateras så att hänvisningen i punkt 2 avser lagen om passageraruppgifter i brottsbekämpningen.

20.6 Förslaget till lag om ändring i tullbefogenhetslagen (2024:710)

7 kap.

12 §

Om uppgifterna kan antas ha betydelse för Tullverkets brottsbekämpande verksamhet, får Tullverket begära att ett transportföretag, som befordrar varor, passagerare eller fordon till eller från Sverige, lämnar uppgifter om ankommande eller avgående transporter som företaget har tillgång till (bokningsuppgifter). Det som sägs om transportföretag gäller även andra företag som yrkesmässigt får tillgång till transportföretagets bokningsuppgifter.
I fråga om passagerare omfattas endast uppgifter om

– namn,
– födelsedatum,
– *kön,*
– nationalitet,
– resrutt,
– bagage,
– medpassagerare,
– mobiltelefonnummer,
– e-postadress,
– *betalningsinformation,*
– bokningssätt.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om hur bokningsuppgifter ska lämnas.

Tullverkets begäran om bokningsuppgifter får inte överklagas.

I *första stycket* regleras Tullverkets rätt att begära att ett transportföretag som befordrar varor, passagerare eller fordon till eller från Sverige lämnar uppgifter om ankommande eller avgående transporter som företaget har tillgång till.

Uppräkningen av vilka uppgifter som ska lämnas avseende passagerare är uttömmande. Kön har lagts till i uppräkningen och betalningssätt har ändrats till betalningsinformation. I övrigt är uppräkningen oförändrad. Övervägandena finns i avsnitt 17.2.

Särskilt yttrande

Särskilt yttrande av experterna Cecilia Danielsson, Mattias Fogelgren, Malin Lundberg, Anna Saarikoski, Fredrik Sjöberg och Eric Åmell

Inledning

PNR-uppgifter är ett viktigt verktyg i samhällets arbete för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet och annan allvarlig brottslighet, både i Sverige och övriga europeiska länder som deltar i PNR-samarbetet. Att PNR-uppgifterna får lagras över tid i PNR-databasen är centralt i detta sammanhang. Det beror på att PNR-lagstiftningen avser komplex brottslighet där både kartläggning och utredning oundvikligen tar lång tid. Behovet av historiska PNR-uppgifter som är äldre än sex månader har visat sig vara väsentligt för att framgångsrikt kunna bekämpa den brottslighet som PNR-lagstiftningen avser. Att PNR-uppgifter lagras på ett generellt och odifferentierat sätt över tid i PNR-databasen är också fundamentalt för att kunna utföra kvalificerade och träffsäkra analyser med hjälp av på förhand fastställda kriterier (s.k. profiler). Dessa analyser bidrar till att tidigare okända misstänkta brottslingar kan upptäckas.

Utredarens föreliggande förslag i frågan om lagringstid innebär en huvudregel om att PNR-uppgifter som behandlas vid enheten för passagerarinformation endast ska bevaras i sin fullständiga form i sex månader från det att de har kommit in från ett lufttrafikföretag. Därefter ska uppgifterna anonymiseras. Undantag från denna huvudregel kan göras om det finns någon omständighet som visar att det föreligger en risk för terroristbrott eller grov brottslighet som har ett direkt eller indirekt samband med en passagerares flygresor. I sådana

fall får PNR-uppgifterna bevaras i sin fullständiga form i upp till fem år från det att de har inkommit från ett lufttrafikföretag.

Med utredningens förslag kommer PNR-databasen, vilken med stöd av befintlig lagstiftning uppgår till cirka 130 miljoner passageraruppgifter, att reduceras avsevärt. Uppskattningar från Polismyndigheten gör gällande att uppgifterna i databasen kan komma att minska med upp till 90 procent.

Vi förstår utredarens tolkning av EU-domstolens avgörande i denna del. Samtidigt menar vi att det finns utrymme för att på olika sätt tolka och tillämpa EU-domstolens avgörande på ett mer tillåtande sätt än vad utredaren gör. Vår uppfattning är således att det är möjligt att ha en generell och odifferentierad lagring av PNR-uppgifter under en avsevärt längre tid än i utredarens förslag. PNR-uppgifterna ska dock, på samma sätt som gäller i dag, behörighetsbegränsas efter sex månader.

Vi vill i sammanhanget framhålla att utredningens övergripande mål enligt kommittédirektiven är att öka tillgången till passageraruppgifter i brottsbekämpningen.[1] I uppdraget har bl.a. ingått att analysera och ta ställning till vilka förändringar av svensk rätt som behöver göras med anledning av EU-domstolens praxis och lämna förslag på *nödvändiga författningsändringar* [egen kursivering]. De författningsändringar som föreslås ska samtidigt *säkerställa att brottsbekämpande myndigheter har en så god tillgång till passageraruppgifter som möjligt* [egen kursivering].

Vi anser att de långtgående negativa konsekvenserna som utredarens förslag medför för den brottsbekämpande verksamheten och förmågan att beivra den allvarliga brottslighet som PNR-direktivet tar sikte på, borde ha värderats högre, särskilt som vi befinner oss i ett läge där det svenska och europeiska säkerhetsläget allvarligt har försämrats efter EU-domstolens avgörande.

Med dessa ingångsvärden och det utrymme som vi ser i fråga om tolkning och tillämpning av vad som utgör en längsta tillåten tid för en generell och odifferentierad lagring av PNR-uppgifter tycker vi att utredarens förslag går längre än vad som är nödvändigt. Med hänsyn till förslagets långtgående negativa följder för den brottsbekämpande verksamheten förordar vi den tolkningsmodell som formuleras nedan.

[1] Dir. 2025:36. *Ökad tillgång till passageraruppgifter i brottsbekämpningen*, s. 1.

Alternativ tolkning och tillämpning

Vi menar att det finns två sätt att tolka och tillämpa EU-domstolens avgörande på ett sätt som möjliggör en mer långtgående generell och odifferentierad lagring av PNR-uppgifter än sex månader. För det första menar vi att innehållet i domen ger en sådan möjlighet. För det andra menar vi att en sådan lagring kan ske genom en dynamisk tolkning av unionsrätten och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR)[2].

EU-domstolens avgörande och annan unionsrättslig praxis

Inledningsvis vill vi framhålla att EU-domstolen slutsatser alltid måste tolkas i ljuset av de tolkningsfrågor som har ställts till domstolen i det aktuella målet.[3] Det som den belgiska författningsdomstolen hade efterfrågat besked om var ifall

> … artikel 12 i PNR-direktivet utgör hinder för en sådan nationell lagstiftning som den angripna lagen, i vilken det föreskrivs en allmän lagringstid på fem år för uppgifterna, varvid det inte görs någon åtskillnad beroende på om det vid förhandsbedömningen framkommit att de berörda passagerarna kan utgöra en risk för den allmänna säkerheten eller ej?[4]

Det EU-domstolen, utifrån den ställda tolkningsfrågan, faktiskt beslutar[5] är att artikel 12.1 i PNR-direktivet jämförd med artiklarna 7, 8 och 52.1 i EU:s rättighetsstadga ska tolkas som att den utgör ett hinder för en nationell lagstiftning som föreskriver en generell lagringstid på fem år för PNR-uppgifter, tillämplig utan åtskillnad på alla flygpassagerare, inklusive på passagerare för vilka varken den förhandsbedömning som avses i artikel 6.2 a i detta direktiv, eller eventuella kontroller som utförts under den sexmånadersperiod som avses i artikel 12.2 i direktivet eller någon annan omständighet har utvisat att det föreligger objektiva omständigheter som visar att det föreligger en risk för terroristbrott eller grov brottslighet med ett åtminstone indirekt objektivt samband med lufttransport av passagerare.

[2] I 2 kap. 19 § regeringsformen framgår att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av EKMR.
[3] Jfr prop. 2018/19:86 s. 29.
[4] Punkten 62 i mål C-817/19 (Ligue des droits humains).
[5] Punkterna 262 och 299 i mål C-817/19 (Ligue des droits humains).

Det ska understrykas att EU-domstolen inte underkänner PNR-direktivet utan i stället tolkar hur detta ska tillämpas för att vara förenligt med grundläggande fri- och rättigheter. EU-domstolen framhåller också särskilt[6] att det som framgår i skäl 25 till PNR-direktivet ska utgöra utgångspunkt när direktivet ska tolkas utifrån grundläggande fri- och rättigheter, dvs. att lagringstiden för PNR-uppgifter bör vara tillräckligt lång och stå i proportion till ändamålen, nämligen att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet.

EU-domstolen är inte heller kategorisk och definitiv i skälen som den lägger till grund för sin bedömning. EU-domstolen uttalar härvid bl.a. följande.[7]

> I förevarande fall *tycks*[8] [egen kursivering] den lagstiftning som är aktuell i det nationella målet föreskriva en allmän lagringstid för PNR-uppgifter på fem år, och denna är tillämplig utan åtskillnad på alla passagerare, inklusive på passagerare för vilka varken den förhandsbedömning som avses i artikel 6.2 a i PNR-direktivet, eller eventuella kontroller som utförts under den inledande sexmånadersperioden *eller någon annan omständighet har utvisat att det föreligger objektiva omständigheter*[9] *som visar att det föreligger en risk för terroristbrott eller grov brottslighet* [egen kursivering]. Den lagstiftningen *torde* i så fall strida mot artikel 12.1 i direktivet jämförd med artiklarna 7, 8 och 52.1 i stadgan, *såvida den inte kan tolkas på ett sätt som är förenligt med dessa bestämmelser, vilket det ankommer på den hänskjutande domstolen att avgöra*. [Egna kursiveringar.]

EU-domstolens bedömning synes således vila på en viss osäkerhet kring den belgiska lagstiftningens faktiska innehåll och effekt. Vidare öppnar EU-domstolen genom sina uttalanden upp för att det kan finnas andra omständigheter än de som har framkommit inom ramen för en förhandsbedömning eller eventuella kontroller under den inledande sexmånadersperioden och som på objektiva grunder kan utvisa att det föreligger en risk för terroristbrott eller annan grov brottslighet som motiverar en längre generell och odifferentierad lagringstid.

EU-domstolen avslutar också med att påminna om att det är medlemsstatens domstol som ansvarar för att avgöra om den nationella

[6] Punkten 250 i mål C-817/19 (Ligue des droits humains).
[7] Punkten 261 i mål C-817/19 (Ligue des droits humains).
[8] ”the legislation at issue in the main proceedings appears to prescribe” i den engelska språkversionen av domen.
[9] Här ska noteras särskilt att EU-domstolen inte talar om objektiva omständigheter i ett enskilt fall (in specific cases), jfr punkt 259.

rätten kan tolkas på ett sätt som är förenligt med EU-domstolens uttalanden.

Allt detta ligger i linje med vår bedömning att det som EU-domstolen har prövat är införlivandet av ett unionsrättsligt direktiv, vilket är bindande för varje medlemsstat avseende det resultat som ska uppnås, men att det överlåts åt de nationella myndigheterna att bestämma form och tillvägagångssätt för genomförandet.[10] EU-domstolens uttalanden kring tolkningen av ett direktiv måste alltså, som vi pekade på inledningsvis, alltid läsas och tolkas i förhållande till den nationella lagstiftning som varit föremål för prövning, men också omsättas i en nationell kontext.

Sammanfattningsvis menar vi att det som EU-domstolen har prövat och uttalat sig i förhållande till är en generell och odifferentierad lagringstid om fem år som inte motiverats på någon annan grund än att PNR-direktivet föreskriver detta, vilket domstolen bedömer utgör ett oproportionerligt intrång i rätten till privatliv och den personliga integriteten. Även om EU-domstolens således synes ha som utgångspunkt att en generell och odifferentierad lagring efter den initiala sexmånadersperioden utgör ett oproportionerligt intrång i förhållande till grundläggande fri- och rättigheter lämnar domstolen ändå en öppning för att det kan finnas objektiva omständigheter som kan motivera en längre lagringstid.

Vad som kan utgöra en sådan annan omständighet som utvisar att det föreligger objektiva omständigheter som visar att det föreligger en risk för terrorbrott eller grov brottslighet, som enligt EU-domstolen kan motivera en längre generell och odifferentierad lagring av PNR-uppgifter, är inte närmare klarlagt.[11]

Några generella hållpunkter går dock att härleda ur EU-domstolens praxis.

Som EU-domstolen återkommit till upprepade gånger skiljer sig hotet om terroristbrott till sin art, sitt speciella allvar och den specifika karaktären på de omständigheter som hotet består i, från den allmänna och permanenta risken för grova brott. Kampen mot terroristbrott anses således kunna motivera ett större intrång i den personliga integ-

[10] Artikel 288 fördraget om Europeiska unionens funktionssätt (FEUF).
[11] Se t.ex. Europeiska rådet, EU-ordförandeskapet, *Improving compliance with the judgment in case C-817/19 – ideas for Discussion*, daterat den 9 september 2022, s. 9 ff. samt *Implementing the c-817/19 Decision: A common approach in the fight against terrorist offences and serious crime*, daterat den 16 april 2024, s. 3 ff.

riteten, bl.a. genom insamling av PNR-uppgifter från samtliga intra-EU flygningar.[12]

EU-domstolen har som alternativ till en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter från elektronisk kommunikation, pekat på att avgränsningar utifrån ett geografiskt kriterium kan göra att lagringen uppfyller krav på nödvändighet och proportionalitet. EU-domstolen har därvid pekat på att en sådan avgränsning får ske när behöriga nationella myndigheter på grundval av objektiva och icke-diskriminerande faktorer bedömer att det i ett eller flera geografiska områden finns en förhöjd risk för förberedelse eller genomförande av grov brottslighet. Dessa områden kan enligt EU-domstolen bl.a. utgöras av platser som utmärks av att det där begås ett stort antal grova brott, platser vilka är särskilt utsatta med avseende på grov brottslighet, såsom platser och infrastruktur som regelbundet besöks eller nyttjas av ett stort antal personer, eller strategiskt viktiga platser, såsom flygplatser, järnvägsstationer eller motorvägsbetalstationer.[13] Vi menar att det faktum att PNR-uppgifter bara samlas in från flygningar som ankommer till eller avgår från Sverige, dvs. flygplatser med internationell passagerartrafik, innebär att insamlingen och lagringen i sig är geografisk avgränsad till strategiskt viktig infrastruktur som är särskilt utsatt för såväl terroristbrott som annan grov brottslighet. Detta behöver beaktas särskilt när en bedömning av nödvändigheten och proportionaliteten av en generell och odifferentierad lagring av PNR-uppgifter görs.

Vår uppfattning är att hotbilden mot Sverige är en sådan objektiv omständighet som kan motivera en generell och odifferentierad lagring av PNR-uppgifter i mer än sex månader. Vi vill därvid framhålla följande.

I PNR-direktivet framgår uttryckligen att varje medlemsstat bör ansvara för att bedöma potentiella hot från terroristbrott och grov brottslighet.[14]

Den rådande hotbilden mot Sverige är komplex och hoten går in i varandra och förstärks. I detta ingår bl.a. att terrorhotet mot Sverige blir allt mer komplext och brett med olika aktörer som har avsikt att

[12] Se punkterna 170 och 171 i mål C-817/19 (Ligue des droits humains) och där angiven praxis. Se även Psychogiopoulou, *Fundamental rights in CJEU data retention case law: A refined regime in response to Member States' concerns, or compensating for the lack of legislative intervention in the digital age?* i Jiptec (2/2024), s. 194-208.
[13] Jfr punkt 150 i de förenade målen C-511/18, C-512/18 och C-520/18 (La Quadrature du Net) och punkt 111 i förenade målen C203-15 och C-691/15 (Tele2).
[14] Se skäl 19 i PNR-direktivet.

agera i och mot Sverige.[15] I Sverige har vi dessutom en organiserad brottslighet som är systemhotande[16] där vi de senaste åren har sett ett ökat samarbete mellan organiserad brottslighet och främmande makt,[17] vilket suddar ut gränserna mellan terrorism och annan allvarlig brottslighet. Den kriminella ekonomin är samhällsskadlig då den hotar välfärdssystemet och förtroendet för demokratin. Även hybridkrigföringen från länder som Ryssland, Kina och Iran är ett växande problem.[18]

Därtill har vi även problem med ett ökat extraterritoriellt auktoritärt styre (i form av illegitim säkerhetshotande diasporapåverkan)[19] och ser ett ökat sabotagehot med angrepp på samhällsviktiga strukturer kopplat till Sveriges inträde i Nato och det svenska militära stödet till Ukraina.

Sammantaget utgör denna breda, komplexa och mångfacetterade hotbild sådana konkreta objektiva omständigheter som vi menar gör att Sverige står inför en verklig, aktuell och förutsägbar risk för att utsättas för terrorbrott och annan allvarlig brottslighet som påvisar och motiverar behovet en generell och odifferentierad lagringstid i mer än sex månader.

Det är slutligen viktigt att understryka att ingen annan medlemsstat, såvitt vi känner till, ännu har lagt fram några författningsförslag eller genomfört författningsändringar i frågan om lagringstid med samma långtgående negativa konsekvenser för brottsbekämpningen som de utredaren nu föreslår. Tvärtom är signalerna vi får i våra underhandskontakter med företrädare i andra medlemsstater att de resonerar på ett liknande sätt som det vi nu fört fram. Vi menar därför att det är viktigt att bedriva en fortsatt omvärldsbevakning i samband med beredningen av utredarens förslag för att få ytterligare underlag i strävan att både säkerställa att svensk rätt är förenlig med unionsrätten och att inte beskära de brottsbekämpande myndigheternas möjligheter att fullgöra sina uppdrag mer än absolut nödvändigt i en utmanande tid.

---

[15] Se SOU 2025:114, s. 179 ff.
[16] Regeringens skrivelse (2023/24:67) *Motståndskraft och handlingskraft – en nationell strategi mot organiserad brottslighet*, s. 1.
[17] Se t.ex. *Säkerhetspolisens lägesbild 2024–2025*, s. 6 och 27, *MUST:s årsöversikt 2024*, s. 11, Totalförsvarets forskningsinstitut, *Organiserad brottslighet och hybrida hot – Nya hot mot den svenska samhällsmodellen*, november 2025 (FOI-R--5808--SE) samt SOU 2025:114 s. 143.
[18] *MUST:s årsöversikt 2024*, s. 6, 19 f. och 23.
[19] Se t.ex. *Säkerhetspolisens lägesbild 2024–2025,* s. 26–29, Totalförsvarets forskningsinstitut, *Diaspora och påverkan från främmande makt – En översikt över fem staters extraterritoriella auktoritära styre*, mars 2023 (FOI-R--5436--SE) och SOU 2025:114, s. 183.

Dynamisk tolkning av unionsrätten och EKMR

Även om vår uppfattning inte delas om att EU-domstolens avgörande lämnar utrymme för en generell och odifferentierad lagringstid av PNR-uppgifter som överstiger sex månader, är vår uppfattning att en sådan ordning är möjlig att införa i nationell rätt genom en dynamisk tolkning av unionsrätten och EKMR.

I sitt avgörande har EU-domstolen tolkat hur PNR-direktivet ska tillämpas för att vara förenligt med grundläggande fri- och rättigheter i EU:s rättighetsstadga[20] vid en given tidpunkt. Såväl rättighetsstadgan som EKMR, på vilken rättighetsstadgan vilar i nu aktuella delar,[21] ska dock tolkas dynamiskt.[22]

En dynamisk tolkning innebär att bestämmelser om de grundläggande fri- och rättigheter som inte är absoluta, hela tiden måste tolkas och tillämpas utifrån nutida samhälleliga förhållanden, värderingar och utveckling, så att det rättsliga innehållet kan anpassas och förändras över tid utan att behöva skrivas om.

I detta sammanhang ska understrykas att sådana grundläggande fri- och rättigheter så som rätten till privatlivet och skyddet för den personliga integriteten, alltid måste värderas och vägas mot vad som uppnås genom de rättighetsbegränsande åtgärderna, som många gånger vidtas i det uttryckliga syftet att skydda andra grundläggande fri- och rättigheter, t.ex. rätten till liv och andra aspekter av rätten till privatliv. Staten har enligt EU:s rättighetsstadga och EKMR en skyldighet att skydda enskildas privatliv och personliga integritet mot intrång som begås av andra enskilda och, om intrång görs, se till att brotten utreds. En förutsättning för att staten ska kunna leva upp till kraven på att upprätthålla rättstryggheten för enskilda är att staten har en välfungerande och effektiv brottsbekämpning. Att ha en välfungerande brottsbekämpning innebär t.ex. att myndigheterna ska ha tillgång till effektiva utredningsverktyg – även i den elektroniska miljön.[23]

---

[20] Europeiska unionens stadga om de grundläggande rättigheterna (2012/C 326/02).
[21] Se artikel 52.3 EU:s rättighetsstadga och e-Justice, Del III – Stadgans tillämpningsområde, tolkning och effekter, avsnitt 5 (https://e-justice.europa.eu/topics/your-rights/fundamental-rights/fundamental-rights-european-union/charter-tutorial/part-iii-scope-application-interpretation-and-effects-charter_sv). Se även punkterna 120–128 i EU-domstolens avgörande i de förenade målen C-511/18, C-512/18 och C-520/18 (La Quadrature du Net).
[22] Se t.ex. SOU 2025:2, *Några frågor om grundläggande fri- och rättigheter*, s. 367 och Sicilianos, *Interpretation of the European Convention on Human Rights: Remarks on the Court's Approach* (1680a05732).
[23] Prop. 2018/19:86, *Datalagring vid brottsbekämpning – anpassningar till EU-rätten*, s. 27.

Som framgått i föregående avsnitt är hotbilden mot Sverige både bred och komplex. I tiden efter EU-domstolens avgörande har en rad omständigheter i vår omvärld gjort att både det svenska och det europeiska säkerhetsläget allvarligt har försämrats på ett sätt som inte gick att förutse. Detta bl.a. till följd av Sverige inträde i Nato, Rysslands fortsatta krig i Ukraina, konfliktutvecklingen i Mellanöstern och USA:s nya nationella säkerhetsstrategi.

Ovanstående omständigheter menar vi utgör sådana tillkommande omständigheter som medför att det vid en prövning av nödvändighet och proportionalitet utifrån grundläggande fri- och rättigheter med hänsyn till rådande förhållanden går att rättfärdiga en mer långtgående generell och odifferentierad lagring av PNR-uppgifter än sex månader.

Kommittédirektiv 2025:36

Ökad tillgång till passageraruppgifter i brottsbekämpningen

Beslut vid regeringssammanträde den 10 april 2025

Sammanfattning

För att framgångsrikt bekämpa terroristbrott och annan allvarlig brottslighet behöver de brottsbekämpande myndigheterna ha tillgång till ändamålsenliga och effektiva verktyg. Ett sådant verktyg kan vara passageraruppgifter. En särskild utredare ska se över reglerna om passageraruppgifter i brottsbekämpningen i syfte att anpassa regleringen av flygpassageraruppgifter till EU-rätten samt analysera förutsättningarna och överväga förbättrade möjligheter att inhämta passageraruppgifter från andra trafikslag. De författningsändringar som föreslås ska säkerställa att brottsbekämpande myndigheter har en så god tillgång till passageraruppgifter som möjligt samtidigt som förslagens konsekvenser för transportbranschen beaktas och skyddet för enskildas personliga integritet säkerställs.

Utredaren ska bl.a.

- analysera och ta ställning till vilka förändringar av den svenska regleringen i fråga om flygpassageraruppgifter i brottsbekämpningen som behöver göras med anledning av EU-domstolens praxis,
- analysera och ta ställning till om den svenska regleringen i fråga om flygpassageraruppgifter i brottsbekämpningen bör göras neutral vad gäller trafikslag och samtidigt se över nuvarande möjligheter att inhämta tillgängliga passageraruppgifter från andra transportföretag, och

- lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

Uppdraget ska redovisas senast den 14 april 2026.

Uppdraget att se över reglerna om flygpassageraruppgifter i brottsbekämpningen

PNR-direktivet

PNR är en förkortning av det engelska begreppet Passenger Name Record och avser uppgifter som passagerare kan lämna vid bokning av flygresor och incheckning. Det kan t.ex. vara uppgifter om namn, resedatum, resväg, bagageinformation och betalningssätt. Frågor om PNR-uppgifter i brottsbekämpningen regleras i det s.k. PNR-direktivet (Europaparlamentets och rådets direktiv 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar [PNR-uppgifter] för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet). Syftet med PNR-direktivet är att bekämpa terrorism och annan grov brottslighet.

Enligt PNR-direktivet ska lufttrafikföretag överföra vissa uppgifter om passagerare som reser med flyg till eller från EU. Lufttrafikföretagen behöver bara föra över uppgifter om sina passagerare som de samlar in för sina egna kommersiella syften. Uppgifterna ska överföras till den berörda medlemsstatens enhet för passagerarinformation, som i sin tur ska göra en bedömning av passagerare före deras beräknade ankomst till eller avresa från medlemsstaten. Syftet är att identifiera personer som kan vara inblandade i terroristbrott eller annan grov brottslighet och därför behöver utredas ytterligare av behöriga myndigheter. Efter denna förhandsbedömning lagras uppgifterna, så att de behöriga myndigheterna i den berörda medlemsstaten eller myndigheterna i en annan medlemsstat vid behov ska kunna göra en senare bedömning. Medlemsstaterna får besluta att tillämpa direktivet även på flygningar inom EU.

Det svenska genomförandet av PNR-direktivet

PNR-direktivet har genomförts i svensk rätt framför allt genom lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen. Lagen ska tillgodose behovet av tillgång till PNR-uppgifter i viss brottsbekämpande verksamhet och samtidigt skydda människor mot att deras personliga integritet kränks när uppgifterna behandlas. Enligt lagen ska det vid Polismyndigheten finnas en enhet för passagerarinformation som ska samla in PNR-uppgifter från lufttrafikföretag, bevara och i övrigt behandla uppgifterna samt överföra PNR-information till behöriga mottagare (1 kap. 4 §). Inför varje flygning som ankommer till eller avgår från Sverige, dvs. även flygningar inom EU, ska lufttrafikföretag överföra vissa PNR-uppgifter till enheten (2 kap. 1 §). Enheten ska sedan göra en förhandsbedömning av passagerare i syfte att välja ut personer som behöver utredas ytterligare av behöriga myndigheter eller Europol, på grund av att de kan vara inblandade i terroristbrottslighet eller annan allvarlig brottslighet (3 kap. 4 § 1). Vid en sådan bedömning får uppgifterna bl.a. jämföras med register eller andra uppgiftssamlingar som är relevanta för att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet (3 kap. 5 § 1). Enheten för passagerarinformation ska bevara PNR-uppgifter i fem år från det att de kommit in från ett lufttrafikföretag (3 kap. 9 §). Det ska finnas ett dataskyddsombud som den enskilde ska ha rätt att kontakta i alla frågor som rör behandling av hans eller hennes PNR-uppgifter (3 kap. 12 och 13 §§). Enligt förordningen (2018:1181) om flygpassageraruppgifter i brottsbekämpningen är de behöriga myndigheterna Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Tullverket och Försvarsmakten.

EU-domstolens dom om PNR-direktivet

Den 21 juni 2022 meddelade EU-domstolen dom i mål C-817/19, som rör PNR-direktivet. Belgisk författningsdomstol hade innan dess begärt ett förhandsavgörande och hade då ställt ett antal tolkningsfrågor, bl.a. i fråga om giltighet och tolkning av direktivet.

Vad gäller PNR-direktivets giltighet konstaterar domstolen inledningsvis att direktivet innebär betydande ingrepp i de rättigheter som garanteras i Europeiska unionens stadga om de grundläggande

rättigheterna (EU-stadgan). Domstolen pekar bl.a. på att direktivet syftar till att införa ett system för övervakning som är kontinuerligt, systematiskt och inte riktat, och som innefattar automatisk utvärdering av personuppgifter för samtliga personer som använder sig av lufttransporttjänster. Domstolen framhåller att medlemsstaternas möjlighet att motivera ett sådant ingrepp ska bedömas med hänsyn till hur allvarligt ingreppet är. Det ska också kontrolleras att betydelsen av det mål av allmänt samhällsintresse som eftersträvas med begränsningen står i proportion till hur allvarligt ingreppet är. Domstolen bedömer att den överföring, behandling och lagring av PNR-uppgifter som föreskrivs i direktivet kan anses vara begränsad till vad som är strikt nödvändigt för att bekämpa terroristbrott och annan grov brottslighet. Det förutsätter dock att de befogenheter som föreskrivs i direktivet tolkas restriktivt.

Domstolens övergripande slutsats är alltså att direktivet är giltigt med hänsyn till att det ska tolkas restriktivt och på ett sätt som är förenligt med EU-stadgan. Domen innehåller ett flertal klargöranden kring hur denna tolkning ska göras.

Ett av domens mest betydelsefulla klargöranden gäller möjligheten att tillämpa direktivet på flygningar inom EU. Domstolen konstaterar att en utvidgad tillämpning av direktivet som omfattar alla flygningar inom EU måste kunna bli föremål för effektiv kontroll av en domstol eller av en oberoende förvaltningsmyndighet. Endast när en medlemsstat bedömer att det finns tillräckligt konkreta omständigheter i form av ett verkligt och aktuellt eller förutsebart terrorhot får medlemsstaten föreskriva att direktivet ska tillämpas på alla flygningar inom EU från eller till den berörda medlemsstaten under en viss tidsperiod. Denna tidsperiod ska enligt domstolen begränsas till vad som är strikt nödvändigt, men den kan förlängas. Vidare konstaterar domstolen att om det inte finns något sådant terroristhot får tillämpningen av direktivet inte utsträckas till alla flygningar inom EU utan måste begränsas till vissa flyglinjer, resmönster eller flygplatser där det enligt medlemsstatens bedömning finns indikationer som kan motivera en sådan tillämpning. Det ska också regelbundet omprövas om det fortfarande är strikt nödvändigt att tillämpa direktivet på de flygningar inom EU som har valts ut.

Domen behandlar även frågor om vilken information som får samlas in, vilka brott som direktivet kan tillämpas på och vilka databaser som får användas för jämförelser vid förhandsbedömningar.

Vidare finns klargöranden om hur kontrollerna ska utföras efter att man har fått en träff och om hur förhandsbedömningarna ska gå till. Domstolen gör också uttalanden om information till berörda enskilda och om eventuella överklaganden från enskilda.

I domen behandlas också bl.a. frågan om lagringstid för PNR-uppgifter. Enligt domstolen går den generella lagringen av sådana uppgifter under en inledande sexmånadersperiod inte principiellt utöver vad som är strikt nödvändigt. Efter denna period krävs dock objektiva omständigheter som visar att det finns en risk för terroristbrott eller annan grov brottslighet som har ett åtminstone indirekt objektivt samband med dessa passagerares flygresor. Domstolen bedömer också att PNR-direktivet utgör hinder för en nationell lagstiftning som föreskriver en generell lagringstid på fem år tillämplig på alla flygpassagerare utan åtskillnad.

Den svenska regleringen behöver ses över

EU-domstolens dom innehåller alltså ett flertal uttalanden om hur PNR-direktivet ska tolkas och medför att den svenska regleringen som genomför direktivet behöver ses över.

De brottsbekämpande myndigheterna behöver ha tillgång till ändamålsenliga och effektiva verktyg för att kunna förebygga, förhindra och upptäcka brottslig verksamhet och utreda och lagföra brott. Då terroristbrott och annan grov brottslighet ofta innefattar gränsöverskridande moment är tillgången till PNR-uppgifter från flygtrafik ett viktigt verktyg i brottsbekämpningen.

Det kan noteras att Polismyndigheten i en hemställan till Justitiedepartementet (Ju2024/02188) betonat vikten av PNR-uppgifter för att identifiera och agera mot kriminella aktörer som kartläggs eller eftersöks av myndigheten. Uppgifterna används även för att hindra att efterlysta individer lämnar landet och för att gripa misstänkta när de anländer hit samt för att barn som riskerar att bli offer för t.ex. bortgifte eller könsstympning ska kunna upptäckas och omhändertas innan de förs bort.

Den svenska regleringen som genomför PNR-direktivet har varit verkningsfull. Likafullt innebär EU-domstolens avgörande att anpassningar av den svenska regleringen kan behöva göras. Författningsändringar kan exempelvis komma att krävas utifrån vad domstolen

uttalat om förutsättningarna för insamling av flygpassageraruppgifter på flygningar inom EU, samt hur ett beslut om sådan insamling ska omprövas alternativt kunna kontrolleras av domstol eller oberoende förvaltningsmyndighet. Det kan även krävas författningsändringar i fråga om exempelvis lagringstid. Utredningsarbetet bör inriktas mot att upprätthålla de brottsbekämpande myndigheternas tillgång till ändamålsenliga och effektiva verktyg, samtidigt som skyddet för enskildas personliga integritet säkerställs. Av det nämnda följer att regleringen bör förändras endast i den utsträckning det är nödvändigt.

Utredaren ska därför

- analysera hur den svenska regleringen förhåller sig till EU-domstolens dom när det gäller flygpassageraruppgifter i brottsbekämpningen
- föreslå förändringar av regelverket som innebär att brottsbekämpande myndigheters tillgång till flygpassageraruppgifter upprätthålls i möjligaste mån samtidigt som skyddet för enskildas personliga integritet säkerställs
- lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

Uppdraget att överväga en trafikslagsneutral lagstiftning

Inhämtning av passageraruppgifter från andra transportföretag än lufttrafikföretag

PNR-direktivet påverkar inte medlemsstaternas möjligheter att tillhandahålla system för insamling och behandling av PNR-uppgifter från andra transportföretag än lufttrafikföretag, förutsatt att sådan nationell rätt är förenlig med unionsrätten (se skäl 33). När PNR-direktivet genomfördes valde Sverige att behålla sådan befintlig lagstiftning, med den ändringen att lufttrafikföretag som omfattas av PNR-direktivet undantogs från den (se prop. 2017/18:234 s. 45 f.).

Möjligheten att i brottsbekämpande syfte begära in tillgängliga passageraruppgifter från andra transportföretag regleras för Polismyndigheten i 25 och 26 §§ polislagen (1984:387) och för Tullverket i 7 kap. 12 och 13 §§ tullbefogenhetslagen (2024:710). Av 25 § polis-

lagen följer att ett transportföretag som befordrar bl.a. passagerare till eller från Sverige är skyldigt att på begäran av Polismyndigheten skyndsamt lämna de aktuella uppgifter om ankommande och avgående transporter som företaget har tillgång till. Skyldigheten att lämna uppgifter om passagerare omfattar namn, resrutt, bagage och medpassagerare samt sättet för betalning och bokning. I 26 § anges att transportföretag får lämna uppgifter enligt 25 § på så sätt att de görs läsbara genom terminalåtkomst. Transportföretagen har dock ingen skyldighet att samla in och lämna uppgifter till Polismyndigheten som de inte har. Exempelvis är obokade biljetter vanligt förekommande vid gränspendling över Öresund och vid lokal busstrafik mellan Haparanda och Torneå, varför tillgången till passageraruppgifter, som t.ex. namn, från sådan trafik kan antas vara relativt begränsad. Regleringen för Tullverket överensstämmer i stort med den för Polismyndigheten, men har bl.a. moderniserats språkligt i samband med att tullbefogenhetslagen infördes. I samband med det har även transportföretags skyldigheter att lämna uppgifter till Tullverket utökats till att omfatta även passagerares födelsedatum, nationalitet, e-postadress och mobiltelefonnummer, i den mån transportföretag har sådan information.

En PNR-lagstiftning som omfattar fler trafikslag bör övervägas

Möjligheten för Polismyndigheten och Tullverket att i den brottsbekämpande verksamheten få del av passageraruppgifter även från andra transportföretag än lufttrafikföretag utgör ett viktigt komplement till PNR-lagstiftningen. Samtidigt går det inte att bortse från att regleringen i polislagen och tullbefogenhetslagen medför att myndigheterna får en mer begränsad tillgång till passageraruppgifter från t.ex. färje- och tågtrafik till och från Sverige än från flygtrafik. Polismyndigheten och Tullverket behöver nämligen begära in passageraruppgifter från aktuellt transportföretag, vilket skiljer sig från PNR-regleringen där lufttrafikföretagen under givna förutsättningar på ett systematiskt och närmast automatiserat sätt för överaktuella uppgifter till enheten för passagerarinformation. I förhållande till PNR-lagstiftningen rör det sig även om en mer begränsad typ av uppgifter som myndigheterna kan begära in, särskilt vad gäller Polismyndigheten. I båda fallen gäller dock att transportörerna endast

behöver föra över uppgifter som de redan väljer att samla in av kommersiella skäl.

Polismyndigheten har i sin hemställan till Justitiedepartementet pekat på att skillnaden mellan de två regelverken leder till svårigheter i det brottsbekämpande arbetet. Bland annat kan kriminella anpassa resor för att försvåra upptäckt, t.ex. genom att helt eller delvis resa till eller från Sverige med andra färdmedel än flyg.

I kampen mot den organiserade brottsligheten är det avgörande att de brottsbekämpande myndigheterna har rätt förutsättningar att bedriva ett effektivt brottsbekämpande arbete. Passageraruppgifter från persontransporter till och från Sverige är en viktig del i det arbetet. Det finns därför skäl att se över hur Polismyndighetens och Tullverkets tillgång till passageraruppgifter från färje-, buss- och järnvägstrafik kan förbättras.

Ett alternativ är att låta den svenska PNR-regleringen omfatta även andra trafikslag än lufttrafik. Att på detta sätt utgå från det etablerade PNR-systemet för lufttrafikföretag och bygga vidare på det med fler trafikslag kan antas ha flera fördelar. Ett sammanhållet system för inhämtande av passageraruppgifter från samtliga transportföretag skulle t.ex. kunna leda till effektivitets- och säkerhetsvinster vid hanteringen av sådana uppgifter.

Som redogörs för ovan har även Säkerhetspolisen, Ekobrottsmyndigheten och Försvarsmakten möjlighet att enligt nuvarande PNR-regelverk begära uppgifter från enheten för passageraruppgifter. Uppdraget att överväga om PNR-regelverket ska göras trafikslagsneutralt bör omfatta motsvarande möjligheter för nämnda myndigheter.

En PNR-lagstiftning som omfattar fler trafikslag aktualiserar frågor om hur ett sådant regelverk ska förhålla sig till nuvarande regler för Polismyndigheten och Tullverket när det gäller möjligheten att inhämta passageraruppgifter från andra transportföretag. Utredaren ska därför i sitt övervägande om en trafikslagsneutral PNR-lagstiftning särskilt beakta frågan om förhållandet till befintlig lagstiftning. Det ska i sammanhanget särskilt framhållas att transportföretags uppgiftsskyldighet enligt polislagen och tullbefogenhetslagen inte enbart omfattar uppgifter om passagerare utan även t.ex. varor. Det kan vidare även vid en trafikslagsneutral PNR-lagstiftning finnas behov av en reglering för Polismyndigheten och Tullverket som säkerställer att myndigheterna kan inhämta passageraruppgifter i de fall

PNR-regleringen inte är tillämplig, t.ex. för att brottet inte omfattas av PNR-direktivets förteckning över brott som anses utgöra allvarlig brottslighet. Ett sådant behov kan också finnas om utredaren bedömer att endast vissa ytterligare trafikslag ska omfattas av PNR-regelverket, men att andra trafikslag även framöver ska falla utanför.

Vid översynen av aktuella bestämmelser i polislagen ska utredaren särskilt beakta att dessa även reglerar Säkerhetspolisens möjligheter att inhämta passageraruppgifter från transportföretag, inklusive uppgifter från lufttrafikföretag i verksamhet som rör nationell säkerhet. Det är viktigt att eventuella förslag om såväl PNR-regleringen som aktuella bestämmelser i polislagen säkerställer Säkerhetspolisens tillgång till passageraruppgifter i verksamheter som rör nationell säkerhet.

I Sverige förekommer gränsöverskridande arbetspendling med tåg, buss och till viss del även med färja. Ett krav på att transportörer inom dessa trafikslag på ett mer systematiskt sätt ska tillgängliggöra passageraruppgifter de har tillgång till kan innebära en ökad administration och kostnader, bl.a. för investeringar i it-system. Utredaren ska därför analysera och jämföra skillnader i förutsättningarna att överföra passageraruppgifter mellan olika trafikslag och typer av resor. Fördelar med att ställa nya typer av krav på transportföretag inom fler trafikslag bör vägas mot nackdelar i form av minskad lönsamhet i berörda företag som i förlängningen kan innebära försämrad tillgänglighet på kommunikationer till och från Sverige.

Om det skulle finnas skäl mot en trafikslagsneutral PNR-lagstiftning kan det i stället finnas anledning att se över 25 och 26 §§ polislagen och 7 kap. 12 och 13 §§ tullbefogenhetslagen. Särskilt kan det finnas skäl att se över de bestämmelser som gäller för Polismyndigheten, vars reglering i stort är oförändrad sedan bestämmelserna infördes 1998. Detta gäller oavsett utredarens överväganden i frågan om trafikslagsneutralitet. Vid en sådan översyn ska utredaren även se över de bestämmelser som reglerar Polismyndighetens och Tullverkets hantering av de uppgifter som inhämtats med stöd av polislagen och tullbefogenhetslagen (se exempelvis 2 kap. 13 och 14 §§ lagen [2018:1693] om polisens behandling av personuppgifter inom brottsdatalagens område och 2 kap. 10–12 §§ lagen [2018:1694] om Tullverkets behandling av personuppgifter inom brottsdatalagens område). Det innefattar att överväga utökade möjligheter att dela passageraruppgifter till andra myndigheter, t.ex. Försvarsmakten.

En analys av frågan om huruvida PNR-regleringen ska göras trafikslagsneutral och om det finns skäl att ändra aktuella bestämmelser i polislagen och tullbefogenhetslagen kräver också överväganden i frågan om enskildas integritet. Även frågor om personuppgiftshantering, som t.ex. lagringstid, behöver analyseras. I den mån utredaren finner det lämpligt kan det i nämnda frågor finnas anledning att göra jämförelser med andra EU-länder som har trafikslagsneutrala PNR-system, såsom Belgien.

Utredaren ska därför

- •analysera och ta ställning till för- och nackdelar med en trafikslagsneutral PNR-reglering
- •bedöma på vilket sätt en trafikslagsneutral PNR-reglering skulle krävaförändringar av de bestämmelser som i dagsläget gör det möjligt för Polismyndigheten och Tullverket att inhämta passageraruppgifter från andra transportföretag än lufttrafikföretag
- analysera risken för minskad lönsamhet i berörda transportföretag och ökade priser för berörda resenärer
- analysera om det finns behov av en revidering av befintliga regler i polislagen och tullbefogenhetslagen, särskilt för det fall ett trafikslagsneutralt PNR-system framstår som mindre lämpligt
- särskilt överväga hur eventuella förslag när det gäller PNR-regleringen och polislagen och annan berörd lagstiftning påverkar Säkerhetspolisens tillgång till passageraruppgifter i verksamhet som rör nationell säkerhet
- lämna förslag på de författningsändringar och andra åtgärder som bedöms lämpliga.

Övriga frågor

De förslag som utredaren lämnar kan aktualisera frågor om t.ex. sekretess och det övriga dataskyddsregelverket. Utredaren ska lämna nödvändiga förslag även i de delarna. Om utredaren bedömer att det är ändamålsenligt och ryms inom tiden för uppdraget får utredaren ta upp och lämna förslag också i andra frågor som aktualiseras med anledning av uppdraget.

Konsekvensbeskrivningar

Utredaren ska redovisa en konsekvensbeskrivning för de förslag som lämnas i enlighet med kommittéförordningen (1998:1474) och förordningen (2024:183) om konsekvensutredningar. Utredaren ska lägga särskild vikt vid att beskriva förslagens betydelse för möjligheten att förebygga, förhindra, upptäcka, utreda och lagföra brott. Utredaren ska även redovisa förslagens konsekvenser för den personliga integriteten. Utredaren ska vidare bedöma förslagens konsekvenser för transportföretag, resenärer och gränsregioner. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras.

Kontakter och redovisning av uppdraget

Under uppdraget ska utredaren inhämta synpunkter och upplysningar från Polismyndigheten, Säkerhetspolisen, Tullverket, Ekobrottsmyndigheten, Försvarsmakten, Transportstyrelsen, Integritetsskyddsmyndigheten,

Domstolsverket och Åklagarmyndigheten, samt andra statliga myndigheter som kan vara berörda av aktuella frågor. Utredaren ska även inhämta synpunkter och upplysningar från transportföretag, branschorganisationer och andra aktörer som kan beröras av förslagen.

Utredaren ska hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet, utredningsväsendet och EU. Utredaren ska särskilt följa det arbete som pågår i EU när det gäller regleringen av API-uppgifter och EU-kommissionens studier om insamling av passageraruppgifter från sjö- och landtransport.

Uppdraget ska redovisas senast den 14 april 2026.

(Justitiedepartementet)

Statens offentliga utredningar 2026

Kronologisk förteckning

1. Skatteincitament för forskning och utveckling – ett nytt incitament baserat på utgifter för FoU-personal. Fi.
2. 710 miljoner skäl till reformer. Ju.
3. Genomförande av plattformsdirektivet. A.
4. Rektor i fokus – förutsättningar för ett pedagogiskt ledarskap. U.
5. Utvidgad avdragsrätt för sponsring m.m. Fi.
6. En nationell digital infrastruktur i hälso- och sjukvården. Styrning med tydliga roller och ansvar för aktörerna. S.
7. Förstärkt uppföljning och utvärdering av folkhälsopolitiken.
   Del I: Effektivare folkhälsoinsatser genom hälsoekonomiska analyser.
   Del II: Utvärdering av alkoholpolitikens styrmedel. S.
8. Rättssäker samhällsvård för barn och unga. S.
9. Registrering av EES-medborgare. Ju.
10. Ökade möjligheter till tillgångsinriktad brottsbekämpning. Del 1 och 2. Ju.
11. Om överföring av Första AP-fondens verksamhet och tillgångar till Tredje och Fjärde AP-fonderna. Fi.
12. Om överföring av Sjätte AP-fondens verksamhet och tillgångar till Andra AP-fonden. Fi.
13. Straffansvar för deltagande i och samröre med kriminella sammanslutningar. Ju.
14. Ädelmetallutredningen – en moderniserad reglering av handel med ädelmetallarbeten. KN.
15. Marken, vattnet, tankarna. Konsekvenser för samer av svensk politik. Volym 1 och 2. Ku.
16. Försvarsexportinitiativ. För gemensam säkerhet. Fö.
17. Öresundsförbindelser 2050 – behov av kapacitet, redundans och svensktdanskt samarbete. LI.
18. Odlingstorv och klimatet. Fi.
19. Stärkt tillsyn och uppföljning – förslag för att motverka oegentlig läkemedelsförskrivning. S.
20. Belägg för broms? Åtgärder för starkare incitament till lägre kommunalskattesatser. Fi.
21. Återkallelse av svenskt medborgarskap. Ju.
22. Stärkt läkemedelsförsörjning i samverkan. Nationella åtgärder för fördelning, omfördelning och inköp vid brist. S.
23. Tolkavgift och förbud mot barntolkning. A.
24. Mervärdesskatt vid uthyrning och överlåtelse av fastighet. Fi.
25. Ett smittskydd för framtiden. S.
26. Digitala verktyg inom bolagsrätten. Genomförande av EU:s direktiv om ytterligare digitalisering inom bolagsrätten. Ju.
27. Lättnader i kraven på hållbarhetsrapportering. Ju.
28. Tillgång till passageraruppgifter i brottsbekämpningen. Ju.

Statens offentliga utredningar 2026

Systematisk förteckning

Arbetsmarknadsdepartementet

Genomförande av plattformsdirektivet. [3]

Tolkavgift och förbud mot barntolkning. [23]

Finansdepartementet

Skatteincitament för forskning och utveckling – ett nytt incitament baserat på utgifter för FoU-personal. [1]

Utvidgad avdragsrätt för sponsring m.m. [5]

Om överföring av Första AP-fondens verksamhet och tillgångar till Tredje och Fjärde AP-fonderna. [11]

Om överföring av Sjätte AP-fondens verksamhet och tillgångar till Andra AP-fonden. [12]

Odlingstorv och klimatet. [18]

Belägg för broms? Åtgärder för starkare incitament till lägre kommunalskattesatser. [20]

Mervärdesskatt vid uthyrning och överlåtelse av fastighet. [24]

Försvarsdepartementet

Försvarsexportinitiativ. För gemensam säkerhet. [16]

Justitiedepartementet

710 miljoner skäl till reformer. [2]

Registrering av EES-medborgare. [9]

Ökade möjligheter till tillgångsinriktad brottsbekämpning. Del 1 och 2. [10]

Straffansvar för deltagande i och samröre med kriminella sammanslutningar. [13]

Återkallelse av svenskt medborgarskap. [21]

Digitala verktyg inom bolagsrätten. Genomförande av EU:s direktiv om ytterligare digitalisering inom bolagsrätten. [26]

Lättnader i kraven på hållbarhetsrapportering. [27]

Tillgång till passageraruppgifter i brottsbekämpningen. [28]

Klimat- och näringslivsdepartementet

Ädelmetallutredningen – en moderniserad reglering av handel med ädelmetallarbeten. [14]

Kulturdepartementet

Marken, vattnet, tankarna. Konsekvenser för samer av svensk politik. Volym 1 och 2. [15]

Landsbygds- och infrastrukturdepartementet

Öresundsförbindelser 2050 – behov av kapacitet, redundans och svenskt-danskt samarbete. [17]

Socialdepartementet

En nationell digital infrastruktur i hälso- och sjukvården. Styrning med tydliga roller och ansvar för aktörerna. [6]

Förstärkt uppföljning och utvärdering av folkhälsopolitiken. Del I: Effektivare folkhälsoinsatser genom hälsoekonomiska analyser. Del II: Utvärdering av alkoholpolitikens styrmedel. [7]

Rättssäker samhällsvård för barn och unga. [8]

Stärkt tillsyn och uppföljning – förslag för att motverka oegentlig läkemedelsförskrivning. [19]

Stärkt läkemedelsförsörjning i samverkan. Nationella åtgärder för fördelning, omfördelning och inköp vid brist. [22]

Ett smittskydd för framtiden. [25]

Utbildningsdepartementet

Rektor i fokus – förutsättningar för ett pedagogiskt ledarskap. [4]