

Behandling av känsliga personuppgifter i testverksamhet

Enligt utlänningsdatalagen (2016:27) är det normalt förbjudet att behandla känsliga personuppgifter i testverksamhet. I promemorian föreslås att sådana personuppgifter ska få behandlas i testverksamhet om uppgifterna är absolut nödvändiga för syftet med behandlingen. Förslaget innebär att Migrationsverket, Polismyndigheten och utlandsmyndigheterna kan få behandla känsliga personuppgifter för att t.ex. kontrollera att befintliga it-system fungerar på ett effektivt och rättssäkert sätt eller pröva och utveckla ny teknik för att kunna delta i det internationella samarbetet.

Lagändringen föreslås träda i kraft den 1 januari 2021.

Innehållsförteckning

| | | |
|---|---|----|
| 1 | Förslag till lag om ändring i utlänningsdatalagen (2016:27) | 3 |
| 2 | Ärendet..... | 4 |
| 3 | Nuvarande regler..... | 5 |
| 4 | Känsliga personuppgifter ska få användas i testverksamhet | 9 |
| 5 | Ikraftträdande- och övergångsbestämmelser..... | 11 |
| 6 | Konsekvenser..... | 11 |
| 7 | Författningskommentar | 12 |

1 Förslag till lag om ändring i utlänningsdatalagen (2016:27)

Härigenom föreskrivs att 14 § utlänningsdatalagen (2016:27) ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

14 §¹

Personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning (känsliga personuppgifter) får endast behandlas

1. för de ändamål som anges i 11 § 1–4 och 6 samt 13 § om uppgifterna är absolut nödvändiga för syftet med behandlingen, eller

2. i löpande text för det ändamål som anges i 12 § 2, om uppgifterna är absolut nödvändiga för att fullgöra arbetsuppgifter i sådan verksamhet som anges i 2 §.

Första stycket hindrar inte att känsliga personuppgifter behandlas med stöd av 15 §.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela

- ytterligare föreskrifter om inskränkningar av möjligheten att behandla känsliga personuppgifter, och
- föreskrifter om gallring.

Denna lag träder i kraft den 1 januari 2021.

¹ Senaste lydelse 2018:1611.

2 Ärendet

Polismyndigheten behandlar personuppgifter i samband med gränskontroll och inre utlänningskontroll. Om kontrollverksamheten har ett brottsbekämpande syfte omfattas personuppgiftsbehandlingen av brottsdatalogens (2018:1177) tillämpningsområde. Om syftet är att kontrollera en inresandes identitet och huruvida personen uppfyller de formella och materiella kraven för inresa och vistelse i Sverige omfattas personuppgiftsbehandlingen av 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, här benämnd dataskyddsförordningen). Vid behandling av personuppgifter i bl.a. Polismyndighetens verksamhet som rör utlänningsars inresa och vistelse i Sverige kompletteras dataskyddsförordningen av utlänningsdatalogen (2016:27). Om en och samma personuppgiftsbehandling har mer än ett syfte kan regelverken vara parallellt tillämpliga.

Flera EU-rättsakter som rör utlänningsars inresa, utresa och vistelse i medlemsstaternas territorium innehåller bestämmelser som möjliggör eller kräver behandling av känsliga personuppgifter. Enligt kommande EU-lagstiftning ska bl.a. ansiktsgenkänning kunna användas vid gränskontroller i hela Schengenområdet. För att kunna genomföra detta måste tekniska system först utvecklas och testas. Ansiktsbilder som bearbetas i ett ansiktsgenkänningsprogram utgör känsliga personuppgifter. Enligt utlänningsdatalogen är det förbjudet att behandla känsliga personuppgifter i testverksamhet. Det innebär att det inte finns rättsligt stöd för berörda myndigheter att skapa och utveckla de tekniska system som är nödvändiga för att kunna utföra kontrollerna. Datainspektionen bedömde i december 2019, inom ramen för ett förhandssamråd om en planerad pilotstudie med ansiktsgenkänning vid Skavsta flygplats, att det finns ett uppenbart behov för Polismyndigheten att kunna behandla känsliga personuppgifter i testverksamhet men att det saknas lagstöd för det i utlänningsdatalogen.

I annan lagstiftning, t.ex. brottsdatalogen och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalogens område finns en möjlighet att behandla känsliga personuppgifter om det är absolut nödvändigt för ändamålet med behandlingen. Det finns alltså inget förbud mot att behandla känsliga personuppgifter i testverksamhet som sker för brottsbekämpande syften. I denna promemoria behandlas frågan om känsliga personuppgifter bör få användas i testverksamhet i sådan behandling som sker med stöd av utlänningsdatalogen.

3 Nuvarande regler

Grundläggande reglering om skydd av den personliga integriteten

Enligt 2 kap. 6 § andra stycket regeringsformen är var och en – utöver vad som anges i första stycket i paragrafen – skyddad gentemot det allmänna mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Inskränkningar i detta skydd får endast göras genom lag och bara för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle (2 kap. 20 och 21 §§ regeringsformen). För andra än svenska medborgare får skyddet dock begränsas genom lag utan de särskilda krav som följer av 2 kap. 21 § regeringsformen (2 kap. 25 § första stycket 3 regeringsformen).

Grundlagsskyddet omfattar enbart betydande intrång i den personliga integriteten. I förarbetena till bestämmelsen framhålls att det är naturligt att det läggs stor vikt vid uppgifternas karaktär vid bedömningen av hur ingripande intrånget kan anses vara i samband med insamling, lagring och bearbetning eller utlämnande av uppgifter om enskildas personliga förhållanden. Ju känsligare uppgifterna är, desto mer ingripande anses det allmännas hantering av uppgifterna normalt vara. Även hantering av ett fåtal uppgifter kan med andra ord innebära ett betydande intrång i den personliga integriteten om uppgifterna är av mycket känslig karaktär. Vid bedömningen av intrångets karaktär är det också naturligt att stor vikt läggs vid ändamålet med behandlingen. En hantering som syftar till att utreda brott kan enligt förarbetena normalt anses vara mer känslig än t.ex. en hantering som uteslutande sker för att ge en myndighet underlag för förbättringar av kvaliteten i handläggningen. Mängden uppgifter kan också vara en betydelsefull faktor i sammanhanget (prop. 2009/10:80 s. 183).

Den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna gäller som svensk lag (SFS 1994:1219). Enligt artikel 8 har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Inskränkningar i dessa rättigheter får endast göras med stöd av lag och för vissa i artikeln uppräknade ändamål, bl.a. hänsyn till den allmänna säkerheten och förebyggande av oordning och brott. Artikel 8 skyddar bl.a. mot felaktig behandling av personuppgifter (se Segerstedt-Wiberg m.fl. mot Sverige, Ansökan 62332/00, dom den 6 juni 2006). Även Europeiska unionens stadga om de grundläggande rättigheterna innehåller bestämmelser om behandling av personuppgifter.

Dataskyddsförordningens bestämmelser om känsliga personuppgifter

För att behandling av personuppgifter ska vara laglig måste minst ett av de villkor som anges i artikel 6.1 a–f i dataskyddsförordningen vara uppfyllt. Dessa villkor utgör den rättsliga grunden för uppgiftsbehandlingen. Av särskilt intresse för myndigheters verksamhet är artikel 6.1 c som gäller när behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige och artikel 6.1 e som gäller när behandlingen är nödvändig för att utföra en uppgift av allmänt intresse

eller som ett led i den personuppgiftsansvariges myndighetsutövning. De rättsliga grunderna i artikel 6.1 c och e ska vara fastställda i enlighet med unionsrätten eller den nationella rätten för att kunna läggas till grund för personuppgiftsbehandling (artikel 6.3 första stycket). Vidare ska syftet med behandlingen fastställas i den rättsliga grunden eller, i fråga om behandling enligt artikel 6.1 e, vara nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.3 andra stycket).

Dataskyddsförordningen innehåller ett principiellt förbud mot att behandla vissa särskilda kategorier av personuppgifter (artikel 9.1). Förbudet omfattar uppgifter 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 person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. I svensk rätt betecknas särskilda kategorier av personuppgifter som känsliga personuppgifter (se t.ex. 14 § första stycket utlänningsdatalagen).

Förbudet i dataskyddsförordningen mot behandling av känsliga personuppgifter kompletteras av ett antal undantag som gör det möjligt att behandla sådana personuppgifter i vissa fall. Ett sådant undantag är om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska 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 (artikel 9.2 g).

Utlänningsdatalagen kompletterar dataskyddsförordningen

Utlänningsdatalagen är en registerförfattning som kompletterar dataskyddsförordningen (4 a §). Lagen innehåller bestämmelser om Migrationsverkets, Polismyndighetens och utlandsmyndigheternas behandling av personuppgifter i sin verksamhet enligt utlännings- och medborgarskapslagstiftningen. Syftet med lagen är att ge myndigheterna möjlighet att behandla personuppgifter på ett ändamålsenligt sätt och att skydda människor mot att deras personliga integritet kränks vid sådan behandling (1 §). Lagen gäller bl.a. behandling av personuppgifter i myndigheternas verksamhet som rör utlänningars inresa och vistelse i Sverige och utresa eller avlägsnande från Sverige (2 § 1 och 2 samt 3 §). Utlänningsdatalagen gäller dock inte all personuppgiftsbehandling som myndigheterna utför inom migrationsrättsområdet. Enligt 5 och 6 §§ är t.ex. vissa EU-rättsakter undantagna från lagens tillämpningsområde; såsom Europaparlamentets och rådets förordning (EG) nr 810/2009 av den 13 juli 2009 om införande av en gemenskapskodex om viseringar (viseringskodex), Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande

myndigheter begär jämförelser med Eurodacuppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (omarbetning) (här benämnd Eurodacförordningen) och – bortsett från rätt till ersättning – Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen).

I 11 och 12 §§ utlänningsdatalagen anges för vilka primära ändamål som myndigheterna får behandla personuppgifter. Personuppgifter får behandlas bl.a. om det behövs för att kontrollera en utlänning i samband med inresa och utresa samt för kontroll under vistelsen i Sverige (11 § 2). Personuppgifter får även behandlas om det behövs för att utföra testverksamhet (11 § 5). I förarbetena till utlänningsdatalagen uttalade regeringen att myndigheter som bedriver verksamhet enligt utlännings- och medborgarskapslagstiftningen ofta har ett behov av att kunna använda personuppgifter i testverksamhet. Testverksamheten kan t.ex. handla om att kontrollera att befintliga it-system fungerar på ett effektivt och rättssäkert sätt eller att pröva ny teknik i syfte att kunna delta i det internationella samarbetet (prop. 2015/16:65 s. 64 och 117).

I propositionen Anpassning av utlänningsdatalagen till EU:s dataskyddsförordning bedömde regeringen att den behandling av personuppgifter som får utföras enligt utlänningsdatalagen är tillåten enligt artikel 6.1 och 6.3 i dataskyddsförordningen (prop. 2017/18:254 s. 14 f.).

Utlänningsdatalagens bestämmelser om känsliga personuppgifter

Känsliga personuppgifter förekommer i stor utsträckning i den verksamhet som bedrivs på utlännings- och medborgarskapsområdet. Behandling av känsliga personuppgifter regleras i bl.a. 14 § utlänningsdatalagen. Av paragrafen framgår bl.a. att känsliga personuppgifter får behandlas för samtliga primära ändamål i 11 § utom testverksamhet (14 § första stycket 1). Känsliga personuppgifter får dock endast behandlas om det är absolut nödvändigt för syftet med behandlingen.

När det gäller testverksamhet föreslog 2014 års Utlänningsdatautredning att känsliga personuppgifter skulle få behandlas i testverksamhet (SOU 2015:73 s. 294 f.). Under remitteringen av betänkandet ansåg dock Datainspektionen att det saknades underlag för att bedöma Migrationsverkets behov av att kunna behandla känsliga personuppgifter i sådan verksamhet. Regeringen instämde i Datainspektionens uppfattning att det inte fanns tillräckliga skäl att tillåta behandling av känsliga personuppgifter för testverksamhet (prop. 2015/16:65 s. 78 f.).

Bestämmelserna om känsliga personuppgifter i 14 § hindrar inte att sådana personuppgifter behandlas med stöd av 15 § (14 § andra stycket). Enligt den paragrafen får Migrationsverket föra separata register över fingeravtryck och fotografier som tas med stöd av 9 kap. 8 § utlänningslagen (2005:716). Den sistnämnda paragrafen reglerar möjligheten att ta fotografi och fingeravtryck bl.a. om en utlänning inte kan styrka sin identitet när han eller hon kommer till Sverige. Uppgifter

om fingeravtryck eller fotografier i registren får användas i testverksamhet (15 § andra stycket 3 utlänningsdatalagen).

I propositionen Anpassning av utlänningsdatalagen till EU:s dataskyddsförordning bedömde regeringen att den behandling av känsliga personuppgifter som möjliggörs genom utlänningsdatalagen uppfyller de krav som ställs i artikel 9.2 g i dataskyddsförordningen för att få behandla känsliga personuppgifter (prop. 2017/18:254 s. 30 f.).

EU-rättsliga krav på kontroll av biometriska uppgifter

Flera EU-rättsakter som rör utlänningars inresa, utresa och vistelse i medlemsstaternas territorium innehåller bestämmelser som möjliggör eller kräver behandling av biometriska uppgifter, t.ex. Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016 om en unionskodex om gränspassage för personer (kodex om Schengengränserna) (kodifiering, här benämnd gränskodexen).

Biometriska uppgifter definieras som personuppgifter som erhållits genom en särskild teknisk behandling som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter (artikel 4.14 i dataskyddsförordningen). I skäl 51 i dataskyddsförordningen anges bl.a. att behandling av foton inte systematiskt bör anses utgöra behandling av känsliga personuppgifter. Regeringen har bedömt att fotografier och filmer som inte bearbetas tekniskt i syfte att åstadkomma identifiering faller utanför definitionen av biometriska uppgifter. Om de däremot bearbetas i exempelvis ett ansiktigenkänningsprogram så att det går att identifiera personer på bilden eller filmen omfattas de av definitionen (prop. 2017/18:232 s. 86 och prop. 2017/18:254 s. 33 f.). I utlänningslagen används genomgående begreppen fotografier och fotografering även för ansiktsbilder. Syftet är att skapa enhetlighet inom utlänningslagen (prop. 2010/11:123 s. 13).

I slutet av 2017 trädde en ny EU-förordning i kraft om inrättande av ett in- och utresesystem för tredjelandsmedborgare som passerar unionens yttre gränser; 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 (här benämnd EES-förordningen). Samtidigt trädde ändringar i gränskodexen i kraft; Europaparlamentets och rådets förordning (EU) 2017/2225 av den 30 november 2017 om ändring av förordning (EU) 2016/399 vad gäller användningen av in- och utresesystemet.

När förordningarna börjar tillämpas kommer biometriska uppgifter att behöva tas upp i flera situationer (se t.ex. artikel 23 och artikel 26 i EES-förordningen). Biometriska uppgifter ska bl.a. ingå i tredjelandsmedborgarnas personakter i in- och utresesystemet och gränsmyndigheterna kommer att använda sig av bl.a. ansiktigenkänning för att kontrollera tredjelandsmedborgares identitet i samband med

gränskontroller. Det finns även regler om självbetjäningssystem som tredjelandsmedborgarna bl.a. kan använda för att förhandsregistrera biometriska uppgifter och genomföra vissa in- och utresekontroller som kräver att de lämnar biometriska uppgifter. Det finns också regler som innebär att biometriska uppgifter kan användas inom medlemsstaternas territorium för kontroll av utlänningars identitet. Bestämmelserna i förordningarna beräknas börja tillämpas under 2022.

Bestämmelser om biometriska kontroller finns även i tre nya EU-förordningar om Schengens informationssystem (SIS); Europaparlamentets och rådets förordning (EU) 2018/1860 av den 28 november 2018 om användning av Schengens informationssystem för återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna, Europaparlamentets och rådets förordning (EU) 2018/1861 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området in- och utresekontroller, om ändring av konventionen om tillämpning av Schengenavtalet och om ändring och upphävande av förordning (EG) nr 1987/2006, och Europaparlamentets och rådets förordning (EU) 2018/1862 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området polissamarbete och straffrättsligt samarbete, om ändring och upphävande av rådets beslut 2007/533/RIF och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1986/2006 och kommissionens beslut 2010/261/EU.

SIS är ett system som Schengenländerna använder för att utbyta information med varandra inom ramen för polissamarbete, straffrättsligt samarbete och migrationskontroll. Enligt SIS-förordningarna ska fotografier, ansiktsbilder och fingeravtrycksuppgifter i vissa fall kunna användas för identifiering (se t.ex. artikel 33 i förordning [EU] 2018/1861).

4 Känsliga personuppgifter ska få användas i testverksamhet

Förslag: Känsliga personuppgifter ska få behandlas i testverksamhet enligt utlänningsdatalagen om uppgifterna är absolut nödvändiga för syftet med behandlingen.

Skälen för förslaget

Det är nödvändigt att kunna behandla känsliga personuppgifter i testverksamhet

Som nämnts kräver vissa EU-rättsakter som rör utlänningars inresa, utresa och vistelse i medlemsstaterna att känsliga personuppgifter kan behandlas. Det är viktigt att säkerställa att den programvara och teknik som ska användas för olika kontroller, t.ex. biometriska kontroller, är tillförlitlig innan den tas i skarp drift. Utlänningsdatalagens nuvarande utformning

innebär att Polismyndigheten, Migrationsverket och utlandsmyndigheterna har rättsligt stöd för att behandla känsliga personuppgifter om uppgifterna är absolut nödvändiga för att kontrollera en utlänning i samband med inresa och utresa eller under vistelsen i Sverige. Det är däremot förbjudet att behandla sådana uppgifter för att utföra den testverksamhet som är nödvändig för att kunna skapa och utveckla de tekniska system som ska användas vid kontrollerna. Motsvarande begränsning saknas i t.ex. lagen om polisens behandling av personuppgifter inom brottsdatalogens område, liksom när personuppgifter behandlas med stöd av vissa EU-rättsakter på migrationsområdet t.ex. Eurodac-förordningen.

Förbudet att behandla känsliga personuppgifter i testverksamhet innebär alltså ett hinder för berörda myndigheter att skapa och utveckla nya tekniska system som är nödvändiga för att kunna utföra kontroller som de är ålagda att utföra. Även befintliga it-system kan behöva kontrolleras genom tester så att de fungerar på ett effektivt och rättssäkert sätt. När det gäller ansiktsigenkänning behöver programvaran exempelvis kunna tränas och valideras på verkliga förhållanden gällande förmågan att jämföra nytagna ansiktsbilder med befintliga ansiktsbilder i chip och på bild i olika länders resehandlingar. Uppgifterna som används vid test och validering behöver återspegla verkliga förhållanden, t.ex. avseende glasögon, smink, frisyrier och huvudbonader. Testverksamheten är alltså en nödvändig förutsättning för att ett sådant system ska kunna användas i skarpt läge på ett rättssäkert och icke-diskriminerande sätt. Det är till och med så att det kan diskuteras om det ens är tekniskt möjligt att ta tekniska system i drift utan en föregående testperiod.

Behandling av känsliga personuppgifter i testverksamhet bör tillåtas

För att genomföra test och validering och nå tillförlitliga och rättssäkra resultat kan en relativt stor mängd känsliga personuppgifter behöva behandlas, särskilt när det gäller ansiktsigenkänning. Detta innebär ett integritetsintrång. Att ta ett system i drift utan testperiod skulle dock medföra onödiga och oproportionerliga ingrepp i enskildas personliga integritet eftersom systemet sannolikt skulle innehålla fel och brister. En sådan behandling av känsliga personuppgifter riskerar att strida mot artikel 9.2 g i dataskyddsförordningen eftersom behandlingen knappast skulle anses uppfylla kraven på proportionalitet och lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen. Möjligheten att testa ny teknik bidrar alltså till att det kan införas träffsäkra, rättssäkra och effektiva system, där risken för olägenheter i form av felbedömningar till den enskildes nackdel minimeras samtidigt som en hög säkerhetsnivå kan upprätthållas. Det intrång i enskildas personliga integritet som kan uppkomma när ett system är i skarp drift blir alltså mindre om systemet först kan testas.

Utlänningsdatalogen bör alltså ändras så att känsliga personuppgifter får behandlas i testverksamhet. I likhet med vad som gäller för de övriga ändamål som anges i 14 § utlänningsdatalogen bör bestämmelsen omfatta samtliga kategorier av känsliga personuppgifter. Av integritetsskyddsskäl bör det, i likhet med övriga bestämmelser om behandling av känsliga personuppgifter, krävas att uppgifterna är absolut nödvändiga för syftet

med behandlingen. Härigenom tydliggörs att behandlingen av känsliga personuppgifter ska ske med försiktighet. Utlänningsdatalagen innehåller även andra bestämmelser som är ägnade att värna den enskildes personliga integritet, t.ex. behörighetsregler och regler om förbud mot att söka på bl.a. känsliga personuppgifter i databaser. I propositionen Anpassning av utlänningsdatalagen till EU:s dataskyddsförordning bedömde regeringen att den nuvarande regleringen uppfyllde dataskyddsförordningens krav på lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen och att utlänningsdatalagens bestämmelser om känsliga personuppgifter var förenliga med dataskyddsförordningen (prop. 2017/18:254 s. 33). Samma bedömning görs här. Den personuppgiftsbehandling som möjliggörs genom förslaget uppfyller alltså de krav som ställs i artikel 9.2 g i dataskyddsförordningen. Förslaget ligger också i linje med annan lagstiftning, t.ex. lagen om polisens behandling av personuppgifter inom brottsdatalagens område.

De krav som dataskyddsförordningen uppställer på bl.a. öppenhet, uppgiftsminimering, riktighet, proportionalitet och säkerhet måste naturligtvis uppfyllas även vid testverksamhet. En myndighet som önskar behandla känsliga personuppgifter med stöd av den föreslagna bestämmelsen är i vissa fall också skyldig att samråda med Datainspektionen före behandling (artikel 36.1 i dataskyddsförordningen).

5 Ikraftträdande- och övergångsbestämmelser

Förslag: Lagändringen ska träda i kraft den 1 januari 2021.

Bedömning: Det behövs inte några övergångsbestämmelser.

Skälen för förslaget och bedömningen: Lagändringen bör träda i kraft så snart som möjligt, vilket bedöms vara den 1 januari 2021.

Det finns inte något behov av övergångsbestämmelser.

6 Konsekvenser

Bedömning: Förslaget innebär inte ökade kostnader.

Skälen för bedömningen: Genom förslaget undanröjs förbudet för Polismyndigheten, Migrationsverket och utlandsmyndigheterna att behandla känsliga personuppgifter i testverksamhet. Det innebär att myndigheterna, om det är absolut nödvändigt, kan få behandla sådana personuppgifter för att t.ex. kontrollera att befintliga it-system fungerar på ett effektivt och rättssäkert sätt och pröva och utveckla ny teknik. Om förslaget inte genomförs blir möjligheterna till kontroll och utveckling av tekniska system begränsad. Sverige skulle t.ex. inte kunna införa de tekniska system som krävs enligt det europeiska samarbetet.

Förslaget innebär i sig inga ökade kostnader, vare sig för det allmänna eller för enskilda. Förslaget bedöms inte heller ha någon påverkan på jämställdheten mellan kvinnor och män eller få några sociala eller miljömässiga konsekvenser.

När det gäller den personliga integriteten innebär förslaget att känsliga personuppgifter får användas i fler situationer än i dag. Konsekvenserna beskrivs i avsnitt 4.

7 Författningskommentar

Förslaget till lag om ändring i utlänningsdatalagen (2016:27)

14 §

Personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning (känsliga personuppgifter) får endast behandlas

1. för de ändamål som anges i 11 och 13 §§ om uppgifterna är absolut nödvändiga för syftet med behandlingen, eller

2. i löpande text för de ändamål som anges i 12 § 2, om uppgifterna är absolut nödvändiga för att fullgöra arbetsuppgifter i sådan verksamhet som anges i 2 §.

Första stycket hindrar inte att känsliga personuppgifter behandlas med stöd av 15 §.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela

1. ytterligare föreskrifter om inskränkningar av möjligheten att behandla känsliga personuppgifter, och

2. föreskrifter om gallring.

Paragrafen reglerar behandling av känsliga personuppgifter. Övervägandena finns i avsnitt 4.

Ändringen i *första stycket 1* innebär att känsliga personuppgifter får behandlas i testverksamhet om uppgifterna är absolut nödvändiga för syftet med behandlingen. Genom ändringen får myndigheterna möjlighet att använda känsliga personuppgifter t.ex. för att kontrollera att befintliga tekniska system fungerar eller för att pröva och utveckla nya tekniska system. Att behandlingen av de känsliga personuppgifterna ska vara absolut nödvändig innebär att behandlingen bör ske med försiktighet och aldrig slentrianmässigt. Det innebär däremot inte att känsliga personuppgifter endast får behandlas i undantagsfall. Genom kravet på absolut nödvändighet markeras dock att behandling ska ske med restriktivitet och att behovet av att behandla sådana uppgifter ska prövas noga i det enskilda fallet. En sådan prövning ska inte bara göras när uppgiften samlas in eller behandlas för första gången utan även vid senare behandling av redan insamlade uppgifter (jfr prop. 2015/16:65 s. 81 och 121).