Innehåll

1 Promemorians huvudsakliga innehåll

Promemorian innehåller förslag till en lag om behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas samt hyres- och arrendenämndernas rättskipande och rättsvårdande verksamhet, en domstolsdatalag.

Det övergripande syftet med lagen är att ge domstolarna och nämnderna möjlighet att behandla personuppgifter på ett effektivt och ändamålsenligt sätt i sin rättskipande och rättsvårdande verksamhet och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

Målsättningen är att skapa en teknikneutral och flexibel lag som innehåller de bestämmelser som är av central betydelse för integritetsskyddet medan kompletterande bestämmelser meddelas genom förordning eller föreskrifter. Personuppgifter ska få behandlas om det behövs för handläggning av mål och ärenden eller författningsenligt uppgiftslämnande. Det ställs vidare upp begränsningar för särskilt integritetskänsliga behandlingar. Personuppgiftsbehandlingen i domstolarna och nämnderna ska präglas av öppenhet gentemot den registrerade.

Domstolsdatalagen föreslås ersätta de nuvarande förordningarna om registerföring m.m. vid domstolarna och nämnderna. Lagen ska gälla i stället för personuppgiftslagen (1998:204) men innehålla hänvisningar till de bestämmelser i den lagen som ska vara tillämpliga i domstolarnas och nämndernas verksamhet.

Lagförslagen föreslås träda i kraft den 1 april 2014.

2 Författningsförslag

Förslag till domstolsdatalag

Härigenom föreskrivs följande.

Lagens tillämpningsområde

1 § Denna lag gäller vid behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas samt hyres- och arrendenämndernas rättskipande och rättsvårdande verksamhet.

Lagen gäller om behandlingen är helt eller delvis automatiserad eller om personuppgifter ingår i eller är avsedda att ingå i en strukturerad samling av uppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Lagens syfte

2 § Syftet med denna lag är att ge de allmänna domstolarna, de allmänna förvaltningsdomstolarna samt hyres- och arrendenämnderna möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin rättskipande och rättsvårdande verksamhet och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

Förhållandet till personuppgiftslagen m.m.

3 § Om inte annat anges i 4 § gäller denna lag i stället för personuppgiftslagen (1998:204).

4 § När personuppgifter behandlas enligt denna lag eller enligt föreskrifter som har meddelats i anslutning till lagen, gäller följande bestämmelser i personuppgiftslagen (1998:204):

1. 3 § om definitioner,
2. 8 § om förhållandet till offentlighetsprincipen,
3. 9 § om grundläggande krav på behandling av personuppgifter,
4. 23 och 25–27 §§ om information till den registrerade,
5. 28 § om rättelse,
6. 30 och 31 §§ samt 32 § första stycket om säkerheten vid behandling,
7. 33–35 §§ om överföring av personuppgifter till tredje land,
8. 38, 40 och 41 §§ om personuppgiftsombud m.m.,
9. 43 och 44 §§, 45 § första stycket och 47 § om tillsynsmyndighetens befogenheter,
10. 48 § om skadestånd, samt
11. 51 § första stycket och 53 § om överklagande.

Förbud enligt 44 eller 45 § personuppgiftslagen får inte förenas med vite.

5 § Om det i lagen (2013:000) om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen eller i föreskrifter som regeringen har meddelat i anslutning till den lagen finns avvikande bestämmelser, ska de tillämpas i stället för bestämmelserna i denna lag.

Tillåtna ändamål

6 § Personuppgifter får behandlas om det behövs för handläggning av mål och ärenden.

7 § Personuppgifter som behandlas enligt 6 § får även behandlas om det behövs för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning.

Tillgången till personuppgifter

8 § Tillgången till personuppgifter ska begränsas till vad varje anställd behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om tillgången till personuppgifter.

Personuppgiftsansvar

9 § En allmän domstol, allmän förvaltningsdomstol eller hyres- och arrendenämnd är personuppgiftsansvarig för den behandling av personuppgifter som den domstolen eller nämnden utför.

Personuppgiftsombud

10 § Den personuppgiftsansvarige ska utse ett eller flera personuppgiftsombud.

Den personuppgiftsansvarige ska enligt personuppgiftslagen (1998:204) anmäla till tillsynsmyndigheten när ett personuppgiftsombud utses eller entledigas.

Förteckning över personuppgiftsbehandlingar

11 § Den personuppgiftsansvarige ska föra en förteckning över de behandlingar som utförs med stöd av denna lag.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om vilka uppgifter en sådan förteckning ska innehålla.

Upplysningar till allmänheten

12 § Den personuppgiftsansvarige ska till var och en som begär det skyndsamt och på lämpligt sätt lämna upplysningar om de behandlingar som utförs med stöd av denna lag. Upplysningarna ska omfatta de uppgifter som en förteckning enligt 11 § ska innehålla. Den personuppgiftsansvarige är dock inte skyldig att lämna ut sekretessbelagda uppgifter eller uppgifter om vilka säkerhetsåtgärder som har vidtagits.

Känsliga personuppgifter

13 § Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.

Sökning

14 § Uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening liksom uppgifter som rör hälsa eller sexualliv får användas som sökbegrepp endast vid sökning som avser uppgifter hos allmän förvaltningsdomstol. Detsamma gäller uppgifter som avslöjar nationell anknytning.

En sökning enligt första stycket får ske endast om det är absolut nödvändigt för handläggning av mål och ärenden.

15 § Uppgifter som avslöjar brott eller misstanke om brott får användas som sökbegrepp endast vid sökning som avser uppgifter hos allmän domstol.

En sökning enligt första stycket får ske endast om det är absolut nödvändigt för handläggning av mål och ärenden.

16 § Bestämmelserna i 14 och 15 §§ gäller inte vid sökning i en viss handling eller i ett visst mål eller ärende.

17 § Regeringen meddelar ytterligare föreskrifter om begränsning av möjligheterna att söka.

Utlämnande på medium för automatiserad behandling

18 § Personuppgifter får lämnas ut till en myndighet på medium för automatiserad behandling.

Personuppgifter i ett mål eller ärende får även lämnas ut till en part och till en parts ombud, biträde eller försvarare på medium för automatiserad behandling.

I övrigt får enstaka personuppgifter lämnas ut på medium för automatiserad behandling.

19 § Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att uppgifter får lämnas ut på medium för automatiserad behandling även i andra fall än som avses i 18 §.

Direktåtkomst

20 § Direktåtkomst till personuppgifter får medges en allmän domstol, en allmän förvaltningsdomstol eller en hyres- och arrendenämnd.

En part och en parts ombud, biträde eller försvarare får medges direktåtkomst till personuppgifter i sitt mål eller ärende.

21 § Regeringen eller den myndighet som regeringen bestämmer meddelar ytterligare föreskrifter om begränsning av direktåtkomsten enligt 20 § samt om behörighet och säkerhet vid sådan åtkomst.

Bevarande i arkiv m.m.

22 § Regeringen eller den myndighet som regeringen bestämmer meddelar ytterligare föreskrifter om bevarande av personuppgifter som hänför sig till ett mål eller ärende som har avgjorts genom dom eller beslut som har vunnit laga kraft.

Överklagande

23 § En hovrätts, tingsrätts eller förvaltningsrätts beslut om upplysningar enligt 12 §, information enligt 26 § personuppgiftslagen (1998:204) samt om rättelse och underrättelse till tredje man enligt 28 § samma lag får överklagas till kammarrätten. En kammarrätts beslut i sådana frågor får överklagas till Högsta förvaltningsdomstolen. Högsta domstolens och Högsta förvaltningsdomstolens beslut i sådana frågor får inte överklagas.

En hyres- och arrendenämnds beslut i sådana frågor som avses i första stycket får överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 1 april 2014.

3 Ärendet

Dåvarande regeringen beslutade i oktober 2000 att tillkalla en särskild utredare med uppdrag att granska regleringen och användningen av personregister och annan behandling av personuppgifter i verksamhet vid de allmänna domstolarna, de allmänna förvaltningsdomstolarna samt hyres- och arrendenämnderna. Utredaren skulle föreslå de författningsförändringar som behövdes för den framtida behandlingen av personuppgifter i dessa verksamheter.

Utredningen, som antog namnet Domstolsdatautredningen, överlämnade i mars 2001 delbetänkandet Domstolars register och personuppgiftslagen (SOU 2001:32). Den delen av uppdraget begränsade sig till sådana rättsliga åtgärder som var nödvändiga att genomföra före den 30 september 2001 då datalagen (1973:289) helt upphörde att gälla. Utredningen föreslog att automatiserad behandling av personuppgifter i domstolarna och nämnderna tills vidare skulle regleras i förordning.

På grundval av utredningens förslag utfärdade regeringen fyra nya och inbördes likartat uppbyggda förordningar om registerföring m.m. med hjälp av automatiserad behandling; en för de allmänna domstolarna, en för länsrätterna (numera förvaltningsrätterna), en för Regeringsrätten (numera Högsta förvaltningsdomstolen) och kammarrätterna samt en för hyres- och arrendenämnderna. Förordningarna trädde i kraft den 1 oktober 2001.

Domstolsdatautredningen överlämnade i januari 2002 slutbetänkandet Informationshantering och behandling av uppgifter vid domstolar, En rättslig översyn (SOU 2001:100). I betänkandet föreslog utredningen tre särskilda lagar som skulle reglera

behandlingen av personuppgifter i verksamheten vid de allmänna domstolarna, de allmänna förvaltningsdomstolarna respektive vid hyres- och arrendenämnderna. Betänkandet har remissbehandlats. En sammanställning av remissyttrandena finns tillgänglig i Justitiedepartementet (dnr Ju2002/586/DOM). Utredningens förslag redovisas närmare i *bilaga 1*.

Under den fortsatta beredningen av slutbetänkandet har det framkommit att förslagen behöver ändras och kompletteras i sådan utsträckning att det inte längre bedöms möjligt att lägga betänkandet till grund för lagstiftning. De sätt på vilka personuppgifter behandlas i domstolarnas och nämndernas verksamhet och kraven på den reglering som styr behandlingen har nämligen i flera avseenden förändrats sedan utredningen avslutade sitt arbete för drygt tio år sedan. Under senare år har vidare en motsvarande översyn gjorts inom flera myndighetsområden, t.ex. polisen, Åklagarmyndigheten och Kustbevakningen, vilket en ny reglering för domstolarna och nämnderna måste ta hänsyn till. Ett nytt underlag behöver alltså tas fram och i denna promemoria görs därför en förnyad översyn av personuppgiftsregleringen för domstolarna och nämnderna.

4 Övergripande rättslig reglering

4.1 Regeringsformen

Grundläggande bestämmelser till skydd för den personliga integriteten finns i regeringsformen. I målsättningsstadgandet i 1 kap. 2 § första stycket slås det fast att den offentliga makten ska utövas med respekt bl.a. för den enskilda människans frihet och i fjärde stycket anges bl.a. att det allmänna ska värna den enskildes privatliv och familjeliv. Av 2 kap. 6 § andra stycket följer vidare sedan den 1 januari 2011 att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Begränsningar av denna fri- och rättighet får dock under vissa förutsättningar göras i lag (2 kap. 20 och 21 §§). I en övergångsbestämmelse anges att äldre föreskrifter som innebär betydande intrång i den personliga integriteten behåller sin giltighet, dock längst t.o.m. den 31 december 2015.

4.2 Internationella konventioner

4.2.1 Europakonventionen och FN-konventionen om medborgerliga och politiska rättigheter

År 1948 antog Förenta nationerna (FN) den allmänna förklaringen om de mänskliga rättigheterna. De rättigheter som räknas upp i förklaringen har därefter vidareutvecklats bl.a. i den euro-

piska konventionen om skydd för de mänskliga rättigheterna och grundläggande friheterna (Europakonventionen) från år 1950 och FN:s konvention om medborgerliga och politiska rättigheter från år 1966.

Enligt artikel 8 i Europakonventionen har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. En offentlig myndighet får inte inskränka åtnjutandet av denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

När det gäller laglighetskriteriet krävs bl.a. att den nationella författningen uppfyller vissa minimikrav i fråga om kvalitet och tydlighet. Reglerna ska vara tillräckligt tydliga för att tillämpningen ska vara förutsebar och den ska vara allmänt tillgänglig. Kravet att ett ingripande ska vara nödvändigt i ett demokratiskt samhälle innebär att det ska föreligga ett ”angeläget samhälleligt behov” av åtgärden i fråga. I det ligger bl.a. en begränsning som innebär att åtgärden inte får gå längre än vad som är nödvändigt med beaktande av proportionalitetsprincipen, dvs. den ska stå i rimlig relation till det intresse åtgärden är avsedd att tillgodose. Vid denna avvägning har staterna ett visst handlingsutrymme att inom rimliga gränser avgöra vilka åtgärder som kan anses nödvändiga för att tillgodose det eftersträvade ändamålet.

I artikel 13 i Europakonventionen föreskrivs att var och en, vars i konventionen angivna fri- och rättigheter kränkts, ska ha tillgång till ett effektivt rättsmedel inför en nationell myndighet. Detta gäller även om kränkningen förövats av någon under utövning av offentlig myndighet. Innebörden av artikeln är att den enskilde ska ha tillgång till en nationell instans för att kunna få saken prövad och kunna få rättelse. Prövningen kan utföras av domstol, men även prövning av en stats regering eller av en förvaltningsmyndighet kan vara tillräcklig.

Europakonventionen gäller som lag i Sverige. Av regeringsformen följer att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden enligt konventionen (2 kap. 19 §).

Även i FN:s konvention om medborgerliga och politiska rättigheter finns en bestämmelse till skydd mot godtyckligt eller olagligt ingripande i någons privat- och familjeliv (artikel 17).

4.2.2 Dataskyddskonventionen

Reglering om automatiserad behandling av personuppgifter finns i bl.a. Europarådets konvention från 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter (Dataskyddskonventionen) och dess tilläggsprotokoll. Konventionen trädde i kraft den 1 oktober 1985 och Sverige har, i likhet med övriga medlemsstater i EU, anslutit sig till den. Under år 2010 har Europarådet inlett en översyn av konventionen.

Dataskyddskonventionens syfte är att säkerställa den enskildes rätt till personlig integritet i samband med automatiserad behandling av personuppgifter. Konventionens innehåll kan ses som en precisering av skyddet för den personliga integriteten som följer av artikel 8 i Europakonventionen.

Dataskyddskonventionen innehåller principer för dataskydd som de konventionsanslutna staterna måste iaktta i sin nationella lagstiftning. Personuppgifter som är föremål för automatiserad behandling ska samlas in och behandlas på ett korrekt sätt för särskilt angivna ändamål. Vidare måste uppgifterna vara relevanta för ändamålen med behandlingen och får inte senare användas på ett sätt som är oförenligt med dessa. Uppgifterna måste också vara riktiga och aktuella och de får inte bevaras längre än vad som är nödvändigt för ändamålen.

Vissa kategorier av personuppgifter får, enligt konventionen, behandlas endast om den nationella lagstiftningen ger ett ändamålsenligt skydd. Till sådana personuppgifter hör uppgifter som avslöjar ras, politisk tillhörighet, religiös tro eller övertygelse i övrigt, sexualliv samt uppgifter om brott.

För att skydda personuppgifter mot bl.a. oavsiktlig eller otillåten förstörelse föreskriver konventionen att lämpliga skyddsåtgärder ska vidtas. Vidare föreskrivs att den registrerade bl.a. ska ha möjlighet till insyn i register och till att få uppgifter rättade. Under vissa förutsättningar får undantag göras från bestämmelserna i konventionen bl.a. i fråga om uppgifternas beskaffenhet och rätten till insyn. Sådana inskränkningar förutsätter stöd i den nationella lagstiftningen och att inskränkningen är nödvändig i ett demokratiskt samhälle för vissa angivna ändamål, t.ex. statens ekonomiska intressen och brottsbekämpning, samt för att skydda enskildas fri- och rättigheter.

4.3 EU-rättslig reglering

4.3.1 Stadgan om de grundläggande rättigheterna

Lissabonfördraget innebär att Europeiska unionens stadga om de grundläggande rättigheterna, tillkännagiven av parlamentet, rådet och kommissionen den 7 december 2000 och anpassad den 12 december 2007, är rättsligt bindande. En referens till stadgan har införts i artikel 6.1 i det ändrade EU-fördraget. I stadgan bekräftas de rättigheter som har sin grund i medlemsstaternas gemensamma författningstraditioner och internationella förpliktelser, Europakonventionen, unionens och Europarådets sociala stadgor samt rättspraxis vid Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna. Stadgans syfte är att kodifiera de grundläggande fri- och rättigheter som EU redan erkänner.

I stadgans artikel 7 föreskrivs att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sin korrespondens. Vidare föreskrivs i artikel 8 att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Personuppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få till-

gång till insamlade uppgifter som rör honom eller henne och att få dem rättade. En oberoende myndighet ska kontrollera att reglerna efterlevs. När det gäller de garanterade rättigheternas räckvidd följer av artikel 52 i stadgan att varje begränsning i utövningen av de rättigheter och friheter som erkänns i stadgan ska vara föreskriven i lag och vara förenlig med proportionalitetsprincipen och det väsentliga innehållet i fri- och rättigheterna. I den mån rättigheterna i stadgan motsvarar rättigheter som skyddas av Europakonventionen ska de ha samma innebörd och räckvidd som enligt konventionen. Stadgans artiklar får inte tolkas som att de inskränker eller inkräktar på rättigheter enligt andra konventioner eller överenskommelser om fri- och rättigheter.

4.3.2 Dataskyddsdirektivet

Den 24 oktober 1995 antogs Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter[1] (dataskyddsdirektivet). Direktivets principer om skydd för enskilda personers fri- och rättigheter är en precisering och förstärkning av Dataskyddskonventionen.

Dataskyddsdirektivet syftar till att garantera en hög och i alla medlemsstater likvärdig skyddsnivå när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter och att främja ett fritt flöde av personuppgifter mellan medlemsstaterna i EU. Medlemsstaterna får inom den ram som anges i direktivet närmare precisera villkoren för när behandling av personuppgifter får förekomma. Sådana preciseringar får dock inte hindra det fria flödet av personuppgifter inom unionen. Direktivet gäller inte för sådan behandling av

[1] EGT L 281, 23.11.1995, s. 31–50, Celex 31995L0046.

personuppgifter som rör allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område.

Dataskyddsdirektivet är endast tillämpligt på behandling av uppgifter om fysiska personer och berör således inte skyddet för juridiska personer. Direktivet omfattar inte bara automatiserad behandling, utan också manuell behandling av personuppgifter som ingår eller kommer att ingå i ett register. Direktivet omfattar inte behandling av personuppgifter för privat bruk.

Enligt dataskyddsdirektivet måste all behandling av personuppgifter vara laglig och korrekt. Uppgifterna måste vara riktiga och aktuella samt adekvata, relevanta och nödvändiga med hänsyn till de ändamål för vilka de behandlas. Ändamålen ska vara uttryckligt angivna vid tiden för insamling av uppgifterna. De ändamål för vilka uppgifterna senare behandlas får inte vara oförenliga med de ursprungliga ändamålen.

Personuppgifter får enligt direktivet behandlas bara i vissa fall. Här kan nämnas att uppgifter får behandlas i första hand efter att den registrerade otvetydigt har lämnat sitt samtycke, men också om det är nödvändigt för att fullgöra en rättslig förpliktelse som åligger den registeransvarige eller för att utföra en arbetsuppgift som antingen är av allmänt intresse eller utgör ett led i myndighetsutövning. Personuppgifter får även behandlas om intresset av att den registeransvarige får behandla uppgifterna överväger den registrerades intresse av att de inte behandlas.

Vissa särskilda i direktivet angivna kategorier av uppgifter får inte behandlas. Det gäller uppgifter som avslöjar den enskildes ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse eller medlemskap i fackförening samt uppgifter som rör hälsa och sexualliv. I direktivet görs undantag från detta förbud i vissa särskilt angivna situationer, bl.a. om det finns ett uttryckligt samtycke av den registrerade. Medlemsstaterna får vidare under förutsättning att lämpliga skyddsåtgärder införs och av hänsyn till ett viktigt allmänt intresse besluta om undantag från förbudet.

Dataskyddsdirektivet innehåller vidare regler om bl.a. information till den registrerade och om rätt för denne att få sådana

personuppgifter som inte har behandlats i enlighet med direktivet rättade, utplånade eller blockerade. Direktivet innehåller även regler om säkerhet vid behandlingen och överföring av personuppgifter till tredje land.

EU-kommissionen presenterade den 25 januari 2012 ett förslag till en genomgripande reform av EU:s regler om skydd för personuppgifter. Förslaget innebär bl.a. att dataskyddsdirektivet ska ersättas av en ny allmän dataskyddsförordning (KOM(2012) 11). Det huvudsakliga syftet med förslaget är att ytterligare harmonisera och effektivisera skyddet av personuppgifter i syfte att förbättra den inre marknadens funktion och öka enskildas kontroll över sina personuppgifter. Förordningsförslaget är dock till stor del baserad på den reglering som redan gäller enligt dataskyddsdirektivet.

4.3.3 Dataskyddsrambeslutet

Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd för personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet) reglerar dataskyddet inom angivna områden. Rambeslutet är föranlett av ett antal EU-instrument rörande utvidgat polisiärt och rättsligt samarbete avseende gränsöverskridande informationsutbyte.

Dataskyddsrambeslutet förpliktar medlemsstaterna att behandla uppgifter som utbyts mellan staterna inom ramen för det polisiära och rättsliga samarbetet på ett sådant sätt att skyddet för enskildas integritet värnas. Det innehåller bestämmelser som avser att förstärka skyddet vid behandling av personuppgifter som överförs. Rambeslutet innehåller bl.a. bestämmelser om allmänna utgångspunkter för behandlingen av personuppgifter och känsliga personuppgifter, rättelse, radering och gallring av personuppgifter, information till den registrerade samt skadestånd och sanktioner. Till stora delar motsvarar innehållet dataskyddsdirektivet. Vidare finns bl.a. särskilda bestämmelser

som begränsar möjligheterna att behandla personuppgifter som mottagits från en annan stat.

Rambeslutet uppfylls redan till stora delar av befintliga dataskyddsregler i svensk rätt. Den 15 mars 2011 överlämnade Utredningen om informationsutbyte vid brottsbekämpning m.m. delbetänkandet Dataskydd vid europeiskt polisiärt och straffrättsligt samarbete (SOU 2011:20) med förslag om hur de återstående delarna av rambeslutet ska genomföras. Regeringen har den 21 februari 2013 beslutat en proposition med förslag som utgår från betänkandet (prop. 2012/13:73).

Som en del av det förslag till genomgripande reform av EU:s regler om skydd för personuppgifter som EU-kommissionen presenterade den 25 januari 2012 (se avsnitt 4.3.2) har kommissionen föreslagit att rambeslutet ska ersättas av ett särskilt dataskyddsdirektiv för de brottsbekämpande myndigheterna (KOM(2012) 10).

4.4 Personuppgiftslagen

Personuppgiftslagen (1998:204) har till syfte att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Genom lagen, som trädde i kraft den 24 oktober 1998, genomfördes dataskyddsdirektivet i svensk rätt. Personuppgiftslagen kompletteras av personuppgiftsförordningen (1998:1191, PUF).

Personuppgiftslagen syftar till att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter (1 §). Lagen är teknikneutral och tillämpas på helt eller delvis automatiserad behandling av personuppgifter och på manuell behandling av personuppgifter, om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier (5 §).

Personuppgifter i personuppgiftslagens mening är all slags information som direkt eller indirekt kan hänföras till en fysisk

person som är i livet. Uppgifter om juridiska personer och avlidna omfattas således inte. Begreppet behandling av personuppgifter omfattar i stort sett allt man kan göra med sådana uppgifter, exempelvis att samla in, bearbeta, lagra, sammanställa och förstöra (3 §).

I personuppgiftslagen anges vissa grundläggande krav för all behandling av personuppgifter. Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål och de får inte behandlas för något ändamål som är oförenligt med det ändamål för vilket de samlades in (den s.k. finalitetsprincipen). De personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålet med behandlingen, och fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till behandlingen. Vidare ska de personuppgifter som behandlas vara riktiga och, om nödvändigt, aktuella och alla rimliga åtgärder ska vidtas för att rätta, blockera eller utplåna sådana uppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen. Personuppgifter får som regel inte heller bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen (9 §).

I lagen finns en uppräkning av under vilka förutsättningar behandling av personuppgifter är tillåten. Personuppgifter får alltid behandlas om den registrerade har gett sitt samtycke. I vissa fall får personuppgifter behandlas även utan samtycke. En förutsättning i dessa fall är att behandlingen är nödvändig för ändamålen. Till exempel får behandling utföras om det är nödvändigt för att kunna fullgöra en rättslig skyldighet, för att skydda vitala intressen för den registrerade eller för att kunna utföra en arbetsuppgift i samband med myndighetsutövning. Vidare får personuppgifter behandlas om en avvägning ger vid handen att den personuppgiftsansvariges berättigade intresse av behandling väger tyngre än den registrerades intresse av skydd (10 §).

Personuppgiftslagen innehåller ett förbud att behandla känsliga personuppgifter. Med känsliga uppgifter avses ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk över-

tygelse, medlemskap i en fackförening eller uppgifter som rör hälsa eller sexualliv (13 §). Förbudet är dock inte undantagslöst. Om den registrerade har gett sitt uttryckliga samtycke till behandlingen eller på ett tydligt sätt offentliggjort de känsliga uppgifterna får de behandlas. Vidare görs undantag för behandling som är nödvändig bl.a. för att den registrerades eller annans vitala intressen ska kunna skyddas eller rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras. Undantag görs också för behandlingen av känsliga personuppgifter för t.ex. hälso- och sjukvårdsändamål samt forskning och statistik. Regeringen, eller den myndighet regeringen bestämmer får också föreskriva ytterligare undantag från förbudet, om det behövs med hänsyn till ett viktigt allmänt intresse (14–20 §§).

Personuppgiftslagen ställer också upp begränsningar i möjligheterna att behandla personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden samt personnummer eller samordningsnummer (21 och 22 §§).

Personuppgiftslagen innehåller flera bestämmelser som syftar till att genom information trygga den enskildes rätt att kontrollera om behandling av personuppgifter om honom eller henne pågår (23–27 §§). Personuppgifter som är felaktiga eller ofullständiga eller som annars inte har behandlats i enlighet med personuppgiftslagen, ska på begäran av den registrerade rättas, utplånas eller blockeras av den personuppgiftsansvarige (28 §). Lagen innehåller vidare bestämmelser om säkerheten vid behandling av personuppgifter (30–32 §§).

Enligt personuppgiftslagen är det förbjudet att till tredje land föra över personuppgifter om landet inte har en adekvat nivå för skyddet av personuppgifterna. Förbudet gäller inte stater som anslutit sig till dataskyddskonventionen. I vissa fall får dock överföring av personuppgifter till tredje land ske även om det aktuella landet inte har en sådan adekvat skyddsnivå som avses i personuppgiftslagen, t.ex. om den registrerade har lämnat sitt samtycke eller för att rättsliga anspråk ska kunna fastställas (33–35 §).

Personuppgiftslagen innehåller också bestämmelser om bl.a. tillsyn, skadestånd, straff och överklagande (43–49 och 51–53 §§). Datainspektionen är tillsynsmyndighet.

Personuppgiftslagen innehåller sedan januari 2007 en särskild regel om behandling av personuppgifter i ostrukturerat material som gör undantag från ett flertal av lagens bestämmelser (5 a §). Sådan behandling får dock inte innebära att den registrerades personliga integritet kränks.

Personuppgiftslagen innehåller generella regler och är tillämplig endast om det inte i någon annan lag eller i en förordning har meddelats avvikande bestämmelser (2 §). Sedan ett antal år tillbaka har det införts en stor mängd s.k. registerförfattningar med bestämmelser om behandling av personuppgifter. Syftet med registerförfattningarna är att anpassa regleringen till de särskilda behov som myndigheterna har i sina respektive verksamheter samt att göra avvägningar mellan behovet av effektivitet i berörd verksamhet och behovet av skydd för den enskildes integritet.

5 Nuvarande reglering av personuppgiftsbehandlingen i domstolarna och nämnderna

5.1 Inledning

Sveriges Domstolar är uppbyggt huvudsakligen kring två parallella domstolsorganisationer; de allmänna domstolarna (tingsrätt, hovrätt och Högsta domstolen) och de allmänna förvaltningsdomstolarna (förvaltningsrätt, kammarrätt och Högsta förvaltningsdomstolen). I Sveriges Domstolar ingår även hyres- och arrendenämnderna, Domstolsverket och Rättshjälpsmyndigheten och Domarnämnden.

Behandlingen av personuppgifter i domstolarnas och nämndernas verksamhet reglerades tidigare för de allmänna domstolarnas och länsrätternas del i förordning och för Regeringsrättens, kammarrätternas samt hyres- och arrendenämndernas del i tillstånd meddelade av Datainspektionen. Den behandling som där reglerades avsåg olika personregister som hade inrättats för domstolarnas och nämndernas verksamhet. Det förekom även behandling av personuppgifter som endast utfördes med stöd av den då gällande datalagen (1973:289). Även den lagen omfattade enbart behandling av personuppgifter i personregister, varför behandling av personuppgifter i löpande text, t.ex. i domar och beslut, var oreglerad.

5.2 Vera-förordningarna

Tillämpningsområde

Sedan den 1 oktober 2001 regleras all automatiserad behandling av personuppgifter – i register eller på annat sätt – i den rättskipande och rättsvårdande verksamheten vid domstolarna och nämnderna i fyra förordningar, de s.k. Vera-förordningarna:

- förordningen (2001:639) om registerföring m.m. vid allmänna domstolar med hjälp av automatiserad behandling,
- förordningen (2001:640) om registerföring m.m. vid förvaltningsrätt med hjälp av automatiserad behandling,
- förordningen (2001:641) om registerföring m.m. vid Högsta förvaltningsdomstolen och kammarrätterna med hjälp av automatiserad behandling, och
- förordningen (2001:642) om registerföring m.m. vid hyres- och arrendenämnder med hjälp av automatiserad behandling.

Förordningarna är sinsemellan likartat uppbyggda och överensstämmer i flera avseenden helt med varandra.

Samtliga fyra förordningar gäller utöver personuppgiftslagen vid automatiserad behandling i den rättskipande och rättsvårdande verksamheten. Manuella register eller den administrativa verksamheten omfattas således inte av regleringarna. Att förordningarna gäller utöver personuppgiftslagen innebär att bestämmelserna i den lagen ska tillämpas i de fall någon särskild reglering inte finns i förordningarna.

Personuppgiftsansvarig för den behandling som omfattas av förordningarna är respektive domstol eller nämnd samt Domstolsverket. När en viss behandling utförs av en domstol eller nämnd ansvarar denna för den behandlingen. Det gäller det mesta av den dagliga hanteringen av personuppgifter i domstolen och nämnden, t.ex. registrering av uppgifter i systemen och utlämnande av uppgifter från ett register. Domstolsverket är

personuppgiftsansvarig för främst frågor om systemens uppbyggnad, t.ex. säkerhetsfrågor.

Verksamhetsregister

I förordningarna anges att domstolarna och nämnderna får föra automatiserade register över mål och ärenden som handläggs vid respektive myndighet. Ett sådant verksamhetsregister får användas för handläggning av mål och ärenden, för planering, uppföljning och utvärdering av verksamheten samt för framställning av statistik. För de allmänna domstolarna finns ett ytterligare ändamål, nämligen att fullgöra författningsenlig underrättelseskyldighet. Vidare får Högsta förvaltningsdomstolen och kammarrätterna använda sina verksamhetsregister för återsökning av vägledande avgöranden.

Ett verksamhetsregister får endast innehålla de uppgifter som anges i en detaljerad uppräkning i en bilaga till respektive förordning. Det rör sig om uppgifter om bl.a. mål eller ärenden, om parter och andra aktörer, om personer som ska höras eller yttra sig, om förhandling, om handläggningen i övrigt och om rättegångskostnader.

Vid angivande av vad saken gäller (ärendemening) får känsliga personuppgifter och uppgifter om lagöverträdelser m.m. behandlas endast om det är nödvändigt för att saken ska kunna återges på ett ändamålsenligt sätt. I övrigt får sådana uppgifter behandlas endast om uppgifterna har lämnats i ett mål eller ärende eller om de behövs för handläggningen av målet eller ärendet.

Enligt förordningen för Högsta förvaltningsdomstolen och kammarrätterna får dessa domstolar ha full tillgång till varandras register. Tillgång till dessa register kan också medges Domstolsverket, förvaltningsrätterna och Riksdagens ombudsmän. Dessutom får Skatteverket och länsstyrelserna ha tillgång till nämnda register för återsökning av vägledande avgöranden. För övriga domstolar och för nämnderna finns inga regler om direktåtkomst.

Förordningarna innehåller vidare bestämmelser om sökbegränsningar i registren. För samtliga domstolar och nämnder gäller att de inte får använda känsliga personuppgifter eller uppgift om nationalitet som sökbegrepp. Inte heller får uppgifter om saken och andra liknande uppgifter om ett mål eller ärende användas som sökbegrepp tillsammans med uppgifter om parter eller andra aktörer i ett mål eller ärende. De allmänna domstolarna får vidare inte använda uppgifter om brottspåföljd, frihetsberövande eller tvångsmedel som sökbegrepp medan de allmänna förvaltningsdomstolarna är förbjudna att använda uppgifter om utfärdandeland för körkort som sökbegrepp. För de myndigheter som har direktåtkomst till Högsta förvaltningsdomstolen eller kammarrätternas register gäller dessutom att de inte får använda uppgifter om parter eller andra aktörer i ett mål som sökbegrepp.

I förordningarna för de allmänna domstolarna respektive för förvaltningsrätterna finns särskilda bestämmelser om gallring. För de allmänna domstolarnas del gäller att uppgifter i tvistemål och ärenden ska gallras senast nio år efter avgörandeåret, medan uppgifter i ett brottmål ska gallras efter fem år. I förvaltningsrätt ska personuppgifter i vissa angivna måltyper, bl.a. skattemål, gallras senast nio år efter avgörandeåret medan övriga mål ska gallras senast efter fem år. För Högsta förvaltningsdomstolens, kammarrätternas och nämndernas del hänvisas i förordningarna avseende dessa till de gallringsföreskrifter från Riksarkivet som gäller för domstolarna eller nämnderna.

Rättsfallsregister

Enligt förordningarna får domstolarna och nämnderna vid sidan av sina mål- och ärenderegister föra automatiserade rättsfallsregister för återsökning av vägledande avgöranden, rättsutredningar och liknande rättslig information. Ett sådant register får endast innehålla de uppgifter som anges i en detaljerad bilaga till förordningarna, bl.a. uppgifter om beteckning på handling, mål-

eller ärendenummer, avgörandedatum, sökord, författningshänvisning och problembeskrivning (sammanfattning). Personuppgiftslagens regler om gallring tillämpas på registren.

Annan automatiserad behandling av personuppgifter

Förordningarna innehåller också bestämmelser om att domstolarna och nämnderna vid sidan av eller i anslutning till registren får behandla personuppgifter automatiserat i löpande text (t.ex. ordbehandling och e-post), ljudupptagningar och ljud- och bildupptagningar. Den begränsning för sådan behandling som föreskrivs i förordningarna gäller känsliga personuppgifter och uppgifter om lagöverträdelser m.m. Sådana uppgifter får behandlas endast om uppgifterna har lämnats i eller behövs för handläggningen av ett mål eller ärende.

För personuppgifter som behandlas vid sidan av eller i anslutning till registren gäller personuppgiftslagens bestämmelser om bevarande och gallring, om inte något annat är särskilt föreskrivet, vilket innebär att de inte får bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Särskilda föreskrifter finns för ljudupptagningar och ljud- och bildupptagningar. Sådana upptagningar ska gallras senast sex veckor efter det att målet eller ärendet har avgjorts genom dom eller beslut som har vunnit laga kraft (se t.ex. 20 § förordningen [1996:271] om mål och ärenden i allmän domstol).

Rättigheter för enskilda

Förordningarna för domstolarna och nämnderna innehåller i huvudsak bestämmelser som reglerar hur uppgifter får behandlas och riktar sig i första hand till de personuppgiftsansvariga domstolarna och nämnderna. Förordningarna innehåller dock även vissa bestämmelser som rör enskildas rättigheter i form av rättelse och skadestånd.

En personuppgiftsansvarig är enligt personuppgiftslagen skyldig att på begäran av en registrerad rätta, blockera eller utplåna uppgifter som inte har behandlats i enlighet med lagen (28 §). I förordningarna anges att den bestämmelsen gäller även i de fall då personuppgifter har behandlats i strid med de från personuppgiftslagen avvikande bestämmelserna i förordningarna. På motsvarande sätt som i fråga om rättelse, anges i förordningarna att personuppgiftslagens bestämmelser om enskildas rätt till skadestånd (48 §) gäller även när personuppgifter behandlats i strid med förordningarna.

Överklagande

Vissa beslut av personuppgiftsansvariga domstolar och nämnder kan överklagas av en enskild. Det gäller beslut om att inte meddela rättelse eller att inte lämna information till enskild.

Beslut av en tingsrätt, en hovrätt eller en förvaltningsrätt överklagas till kammarrätt och ett beslut av kammarrätt överklagas till Högsta förvaltningsdomstolen. Beslut av Högsta domstolen eller Högsta förvaltningsdomstolen får inte överklagas. Beslut av hyres- och arrendenämnder och Domstolsverket överklagas i den för myndigheters förvaltningsbeslut vanliga ordningen, nämligen till förvaltningsrätt med krav på prövningstillstånd vid överklagande till kammarrätten.

6 En lag om domstolarnas behandling av personuppgifter

6.1 Behovet av en ny reglering

Bedömning: För att främja en effektiv och rättssäker verksamhet och samtidigt ge ett starkt skydd för den personliga integriteten behöver regleringen av personuppgiftsbehandlingen i domstolarna samt hyres- och arrendenämnderna moderniseras.

Skälen för bedömningen

En effektiv och rättssäker verksamhet

Enligt nuvarande ordning regleras den automatiserade personuppgiftsbehandlingen vid de allmänna domstolarna, de allmänna förvaltningsdomstolarna samt hyres- och arrendenämnderna till stor del av de s.k. Vera-förordningarna, vilka gäller utöver personuppgiftslagen. Förordningarna tillkom år 2001 som en provisorisk lösning för att tillgodose det behov av regler som uppstod då datalagen (1973:289) upphörde att gälla.

Förordningarna tar i huvudsak sikte på den behandling som sker i myndigheternas automatiserade register och innehåller detaljerade och uttömmande uppräkningar av vilka uppgifter som får behandlas i registren. Sedan den nuvarande regleringen infördes har dator- och informationsteknologin utvecklats och fortsätter att utvecklas i betydande omfattning. Detta har

medfört att allt mer avancerade automatiserade behandlingar kan utföras och att den digitala tekniken får nya användningsområden. Denna utveckling är en del av regeringens strävan att effektivisera samtliga myndigheters arbete och ytterligare stärka rättssäkerheten och kvaliteten i deras verksamhet.

Sedan flera år är modern informationsteknik en naturlig del i domstolarnas arbete och det har bl.a. bidragit till en ökad elektronisk ärendehantering. I princip all framställning av skriftlig information hos domstolarna sker numera på elektronisk väg (t.ex. stämningar, föreläggande, kallelser, domar). Domstolarna tar dessutom i allt större uträckning emot och lagrar information i elektronisk form. På samma sätt som redan skett vid vissa myndigheter, kommer domstolarna förr eller senare att lämna den pappersbaserade hanteringen bakom sig och övergå till elektroniska akter.

En viktig del i en väl fungerande och effektiv domstolsprocess är att informationsförsörjningen mellan Sveriges Domstolar och övriga myndigheter fungerar på ett bra sätt. Regeringen har t.ex. sedan en tid tillbaka en uttalad målsättning att skapa en helt elektronisk och strukturerad informationsförsörjning för rättsväsendets myndigheter genom arbete inom ramen för Rådet för rättsväsendets informationsförsörjning (RIF). Arbetet leds av Justitiedepartementet och samordnas på myndighetsnivå av rådet. Detta består av elva myndigheter, däribland Domstolsverket.[1] Arbetet syftar till att information ska överföras elektroniskt mellan rättsväsendets myndigheter. Avsikten är att skapa ett elektroniskt flöde av information såväl framåt i rättskedjan som bakåt. Arbetet fokuseras inledningsvis på brottmålsprocessen. Under år 2012 inleddes genomförandet av den första etappen som innebär att bl.a. stämningsansökningar och förundersökningsprotokoll ska kunna mottas och lagras

[1] Övriga myndigheter är Rikspolisstyrelsen, Åklagarmyndigheten, Kriminalvården, Brottsförebyggande rådet, Brottsoffermyndigheten, Tullverket, Skatteverket, Ekobrottsmyndigheten, Kustbevakningen och Rättsmedicinalverket.

elektroniskt vid domstolarna samt att domstolarna ska expediera domar elektroniskt till andra myndigheter.

Den pågående utvecklingen skapar alltså goda möjligheter att ytterligare effektivisera domstolarnas samt hyres- och arrendenämndernas verksamheter, att stärka rättssäkerheten samt att förbättra kommunikationen med andra myndigheter. Att återanvända uppgifter som redan finns registrerade hos andra myndigheter är arbetsbesparande och främjar effektiviteten. Genom att samma uppgifter inte behöver registreras flera gånger minskar också risken för inmatningsfel, vilket bidrar till rättssäkerheten. Informationsutbytet har också betydelse för t.ex. statistikframtagning och uppföljningsarbete inom rättsväsendet. Den elektroniska hanteringen medför även vinster för miljön.

En strävan måste vara att de fördelar som tekniken erbjuder kan tas till vara i så stor utsträckning som möjligt och att regleringen om personuppgiftsbehandlingen möjliggör detta. Eftersom den nuvarande regleringen innehåller brister i detta avseende finns det mot den angivna bakgrunden behov av att modernisera regelverket.

Skydd för den personliga integriteten

Samtidigt som utvecklingen mot mer elektronisk hantering kan förbättra effektiviteten och rättssäkerheten kan den även medföra ökade risker för otillbörliga intrång i den personliga integriteten. Ett viktigt syfte med personuppgiftsreglering i allmänhet är att skydda den personliga integriteten. Begreppet personlig integritet är inte definierat vare sig i lag eller i annan författning men det har uppmärksammats i flera statliga utredningar och har varit föremål för analys även i flera andra sammanhang[2].

[2] Se Stig Strömholm, SvJT 1971 s. 695 samt Individens skyddade personlighetssfär, Om våra rättigheter, antologi utgiven av Rättsfonden, 1980. Se även SOU 1984:54 s. 42, SOU 1992:84 s. 187, SOU 2007:22 s. 52 f. och SOU 2010:4 s. 97 f.

Den grundläggande bestämmelsen till skydd för den personliga integriteten återfinns sedan den 1 januari 2011 i 2 kap. 6 § regeringsformen (RF). Av förarbetena till den bestämmelsen framgår att utgångspunkten för grundlagsregleringen har varit att kränkningen av den personliga integriteten kan sägas utgöra ett intrång i en fredad sfär som bör kunna avvisas (prop. 2009/10:80 s. 175). Bestämmelsen innebär att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Enligt förarbetena till bestämmelsen är uppgifter i t.ex. databaser med information som är knuten till en myndighets ärendehantering i många fall tillgängliga för myndigheterna på ett sådant sätt att lagringen och behandlingen av uppgifterna kan sägas innebära att enskilda kartläggs även om det huvudsakliga ändamålet med behandlingen är ett helt annat. Av förarbetena framgår vidare att bestämmelsen är avsedd att omfatta 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 (a. prop. s. 180 och 250).

Integritetsskyddskommittén gjorde redan år 2007 bedömningen att behandlingen av personuppgifter i domstolarnas rättskipande och rättsvårdande verksamhet är av sådan karaktär och omfattning att de grundläggande principerna för behandlingen bör slås fast i lag (SOU 2007:22 s. 151). Det kan konstateras att ett stort antal uppgifter som rör enskildas personliga förhållanden behandlas i domstolarna och nämnderna och att mängden uppgifter kommer att öka. I flera mål- och ärendetyper, t.ex. brottmål, migrationsmål och socialförsäkringsmål, behandlas dessutom regelmässigt känsliga personuppgifter. En stor del av den personuppgiftsbehandling som behöver ske i domstolarna och nämnderna får därför anses ha sådan karaktär och omfattning att den omfattas av regeringsformens bestämmelse om integritetsskydd.

Detta skydd mot integritetsintrång kan begränsas i lag under förutsättning att begränsningen sker för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle (2 kap. 20 § 2 och 21 § RF). Det är av grundläggande betydelse i ett demokratiskt samhälle att det finns ett effektivt och väl fungerande domstolsväsende. Mål och ärenden måste kunna handläggas på ett rättssäkert sätt och den som vänder sig till domstol ska kunna få ett avgörande inom rimlig tid. Modern teknik är i detta avseende ett viktigt verktyg för domstolarna och nämnderna. Ett av skälen för att se över den nuvarande regleringen är att skapa lagliga förutsättningar för att använda sådan teknik på ett ändamålsenligt sätt. Det måste mot denna bakgrund stå klart att de begränsningar av grundlagsskyddet mot integritetsintrång som kan bli aktuella att överväga för domstolarnas personuppgiftsbehandling typiskt sett får anses nödvändiga för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle.

Mot den angivna bakgrunden finns det skäl att förändra regelverket i syfte att åstadkomma ett starkt och hållbart skydd för den personliga integriteten i den tekniskt allt mer dynamiska och komplexa verkligheten. I de följande avsnitten kommer det att redovisas närmare vilka behov som finns av att kunna behandla personuppgifter på olika sätt i domstolarna samt hyres- och arrendenämnderna samt hur dessa behov lämpligen bör vägas mot intresset av integritetsskydd.

6.2 En ny reglering i lag

Förslag: Nuvarande registerförordningar för domstolarna samt hyres- och arrendenämnderna ska ersättas med en ny flexibel och teknikneutral reglering. Ramarna och de grundläggande principerna för personuppgiftsbehandlingen ska anges i lag medan kompletterande bestämmelser meddelas genom förordning eller myndighetsföreskrifter.

Skälen för förslaget

Behov av särskild författningsreglering

Personuppgiftslagen är den lag som allmänt sett har till syfte att uppfylla regeringsformens krav och övriga överordnade principer och bestämmelser i fråga om integritetsskydd vid automatiserad behandling av personuppgifter. Personuppgiftsbehandlingen i de allmänna domstolarna, de allmänna förvaltningsdomstolarna samt hyres- och arrendenämnderna regleras såvitt gäller dessa myndigheters rättskipande och rättsvårdande verksamhet dels genom personuppgiftslagen, dels genom de fyra Vera-förordningarna, vilka gäller utöver personuppgiftslagen.

Personuppgiftslagen är utformad för att kunna fungera i vitt skilda sammanhang, för alla skiftande former av personuppgiftsbehandling som kan förekomma hos enskilda, personer, företag, föreningar eller myndigheter. Reglerna har således inte tillkommit med någon särskild hänsyn till sådan personuppgiftsbehandling som behöver ske i verksamheter och sammanhang av mer särpräglad natur. I det lagstiftningsärende som föregick personuppgiftslagen uttalade regeringen att lagen i princip bara bör innehålla generella regler och att behovet av undantag och särregler för mer speciella områden får tillgodoses genom andra författningar (prop. 1997/98:44 s. 40 f.).

Det är vanligt att den personuppgiftsbehandling som utförs vid en viss myndighet regleras av en så kallad registerförfattning, som innehåller bestämmelser som i större eller mindre utsträck-

ning avviker från personuppgiftslagen. Sådan särreglering kan tillgripas bl.a. då det finns ett behov av att möjliggöra avsteg från personuppgiftslagens krav på samtycke, att åstadkomma ett förstärkt integritetsskydd eller att i andra avseenden anpassa regelverket till de särskilda förhållanden som råder inom den aktuella myndighetens verksamhet. Sådana behov gör sig gällande även i fråga om domstolarnas och nämndernas verksamhet. Det bör därför även i fortsättningen gälla särskilda regler för den personuppgiftsbehandling som sker i domstolarnas och nämndernas verksamhet.

En ny reglering i lag

Personuppgiftsbehandlingen i domstolarna samt hyres- och arrendenämnderna regleras för närvarande huvudsakligen i förordning. Den 1 januari 2011 infördes en bestämmelse i regeringsformen om förstärkt skydd mot intrång i den personliga integriteten (2 kap. 6 § RF). Som redovisas i avsnitt 6.1 görs bedömningen att en stor del av den personuppgiftsbehandling som behöver ske i domstolarna och nämnderna innebär ett sådant intrång i enskildas personliga integritet som avses i regeringsformen. Behandlingar som innebär begränsningar i detta integritetsskydd kan endast tillåtas genom bestämmelser i lag (2 kap. 20 § första stycket 2 RF).

Det innebär att ramarna för domstolarnas och nämndernas personuppgiftsbehandling måste slås fast i lag, liksom att de bestämmelser som är av central betydelse för integritetsskyddet bör ges lagform. Det är också lämpligt att reglera för integritetsskyddet viktiga frågor såsom direktåtkomst och sökbegränsningar i lag. Härigenom åstadkoms ett förstärkt integritetsskydd i förhållande till vad som gäller för närvarande. Det är å andra sidan lämpligt att inte tynga lagen med den detaljreglering som i vissa fall är nödvändig. Lagregleringen avseende domstolarnas och nämndernas personuppgiftsbehandling bör därför kompletteras med bestämmelser som meddelas genom förordning. De

föreskrifter regeringen meddelar får förstås inte innebära ett betydande intrång i den personliga integriteten (2 kap. 6 § andra stycket RF). Det kan slutligen i vissa fall vara lämpligt att regeringen delegerar rätten att meddela verkställighetsföreskrifter.

En flexibel och teknikneutral reglering

De nuvarande Vera-förordningarna utgår i stor utsträckning från att personuppgifter lagras och struktureras i särskilda register och i förordningarna anges exakt vilka uppgifter som får behandlas i registren. Regleringen är alltså inte teknikneutral utan förutsätter att vissa tekniska lösningar används.

Med hänsyn till den utveckling som nu sker är det inte möjligt att förutse hur de tekniska lösningarna och den elektroniska kommunikationen kommer att se ut framöver inom domstolarna eller vid hyres- och arrendenämnderna. Inte desto mindre måste ambitionen vara att den reglering som föreslås ska kunna fungera inte bara under de närmaste åren utan under lång tid. Lagstiftningen bör alltså inte vara beroende av att vissa tekniska lösningar används, utan ska tillåta användningen av ny teknik. Det krävs därför att regleringen under skiftande förhållanden effektivt kan styra användandet av ny teknik i verksamheten utan att den i onödan försvårar önskvärda effektiviseringar inom och mellan myndigheter, tillgänglighet för allmänheten och rättssäkerhetsvinster. Likaså bör den vara flexibel så till vida att den i möjligaste mån ska vara oberoende av nya faktiska, organisatoriska eller rättsliga förutsättningar som påverkar domstolarnas och nämndernas verksamhet. Sammanfattningsvis bör det skapas ett rättsligt utrymme för att välja olika tekniska lösningar, arbetssätt och kommunikationsvägar inom verksamheterna.

Att lagstiftningen är teknikneutral och flexibel är vidare särskilt viktigt ur ett integritetsskyddsperspektiv. Om regleringen i alltför hög grad byggs upp kring att informationshanteringen organiseras på ett visst sätt och med vissa tekniska

lösningar, finns det en risk att bestämmelserna i praktiken förlorar sin förmåga att skydda mot integritetskränkande personuppgiftsbehandling då verksamheterna utvecklas och nya tekniska lösningar tas i bruk. Regleringen bör därför utformas så att den under skiftande förutsättningar kan säkerställa ett effektivt och långsiktigt hållbart skydd för den personliga integriteten.

Att användningen av datorstöd redan nu är normen för all skriftlig informationshantering, bör återspegla sig i hur lagen utformas. Till skillnad från nuvarande registerförordning bör lagen ta sin utgångspunkt i att personuppgiftsbehandling är tillåten inom vissa ramar. De överväganden som görs i denna promemoria bör därför i första hand ta sikte på vilka former av behandling som bör begränsas eller inte tillåtas alls – snarare än uttryckligen peka ut vilka behandlingar som ska tillåtas. Därutöver finns det naturligtvis anledning att överväga bestämmelser rörande allmänt integritetsfrämjande åtgärder, såsom bestämmelser om information till allmänheten, personuppgiftsombud och möjligheter t.ex. till rättelse eller blockering av uppgifter

7 Lagens tillämpningsområde

7.1 En gemensam lag för domstolar och nämnder

Förslag: Personuppgiftsbehandlingen i de allmänna domstolarna, de allmänna förvaltningsdomstolarna samt hyres- och arrendenämnderna ska regleras i en gemensam lag benämnd domstolsdatalag.

Skälen för förslaget: Enligt nuvarande ordning regleras den automatiserade personuppgiftsbehandlingen vid domstolarna och nämnderna till stor del av de fyra Vera-förordningarna (se avsnitt 5). Förordningarna är till stora delar identiska. I domstolsdatautredningens delbetänkande som låg till grund för dessa förordningar motiverades uppdelningen med att förordningarna endast var avsedda att utgöra en tillfällig lösning och att det inte fanns någon anledning att ändra tillämpningsområdet i fråga om vilka myndigheter varje förordning ska omfatta i förhållande till vad som dittills hade gällt (SOU 2001:32 s. 100).

Domstolsdatautredningen föreslog sedermera i sitt slutbetänkande att behandlingen i de aktuella domstolarna och nämnderna skulle regleras genom tre lagar: en för de allmänna domstolarna, en för de allmänna förvaltningsdomstolarna och en för hyres- och arrendenämnderna (SOU 2001:100 s. 96 f.). Som skäl för uppdelningen angav utredningen att man inte kunde se några egentliga vinster med att ha en gemensam lag för dessa tre grupper av myndigheter. Utredningen fann tvärtom att flera skäl talade emot en gemensam lag, framför allt med hänsyn till att

processreglerna och behovet av tillgång till uppgifter skiljde sig åt mellan domstolsslagen.

Sedan utredningen presenterade sitt förslag har det hänt mycket i fråga om vilken teknik som står till förfogande för domstolarna och nämnderna och hur den elektroniska mål- och ärendehanteringen har utvecklats. Den lagreglering som nu föreslås ska vara flexibel och teknikneutral och framför allt innehålla de grundläggande principerna för personuppgiftsbehandlingen. Avsikten är att reglerna ska kunna fungera väl oavsett vilken materiell rätt som tillämpas samt att ändringar i de processuella regelverken som regel inte ska behöva föranleda några ändringar i personuppgiftsregleringen.

Som utredningen framhållit har visserligen en domstol eller nämnd i första hand behov av att utbyta information med myndigheter av samma slag. Med den utveckling som nu pågår i fråga om e-förvaltning och andra projekt för att underlätta den elektroniska kommunikationen måste det emellertid antas att det kan bli aktuellt med direktåtkomst mellan domstolsslagen. Utformningen av denna reglering underlättas om samma lag är tillämplig för både de som medges direktåtkomst och de som öppnar upp sina datorsystem för denna åtkomst, eftersom man då kan utgå från att samma skyddsnivå gäller vid alla de domstolarna och nämnderna. Som redovisas i följande avsnitt bedöms det i stort sett saknas behov av lagregler som skiljer sig åt mellan de olika domstolarna och nämnderna.

En praktisk fördel med att samla regleringen i en enda lag är att praxisbildningen främjas. Behovet av vägledande avgöranden bedöms också bli större när allt fler uppgifter behandlas automatiserat och därmed omfattas av personuppgiftsregleringen. En annan fördel med en gemensam lag är att den blir mindre känslig för eventuella framtida organisatoriska förändringar inom Sveriges Domstolar.

Mot den angivna bakgrunden finns det i fråga om de allmänna domstolarna och de allmänna förvaltningsdomstolarna goda skäl för att samla de lagbestämmelser som nu ska föreslås i en gemensam lag. Fråga är då om regleringen även bör omfatta

hyres- och arrendenämnderna, som visserligen har rättskipande och rättsvårdande uppgifter och ingår i Sveriges Domstolar, men som inte är domstolar. Nämnderna använder sig i likhet med de allmänna domstolarna och de allmänna förvaltningsdomstolarna av verksamhetsstödet Vera. Såväl författningstekniskt som materiellt är den förordning som enligt för närvarande reglerar personuppgiftsbehandlingen vid nämnderna till största delen identisk med motsvarande förordningar som gäller för domstolarna. Sedan år 2006 är många hyres- och arrendenämnders administration samordnad med en tingsrätt på samma ort. Utredningen om hyres- och arrendetvister har i sitt betänkande (SOU 2012:82) föreslagit att hyres- och arrendenämnderna ska ersättas av särskilda hyres- och arrendedomstolar som ska inrättas inom vissa tingsrätter. Mot den angivna bakgrunden framstår det som ändamålsenligt att den lag som nu ska föreslås även får omfatta hyres- och arrendenämnderna. I flera fall är de överväganden som görs i denna promemoria giltiga även i fråga om hyres- och arrendenämnderna. Om inget annat särskilt anges avser de fortsatta övervägandena även hyres- och arrendenämnderna.

Övriga myndigheter inom Sveriges Domstolar, dvs. Domstolsverket, Rättshjälpsmyndigheten och Domarnämnden, bedriver inte rättskipande eller rättsvårdande verksamhet och bör därför inte omfattas av den nya lagen (se avsnitt 7.2). Arbetsdomstolen, Försvarsunderrättelsedomstolen, Marknadsdomstolen och Patentbesvärsrätten är specialdomstolar utanför Sveriges Domstolar och bör av den anledningen inte omfattas av den nya lagen.

Vad gäller namnet på den nya lagen ligger det nära till hands att i linje med flera på senare år tillkomna lagar på personuppgiftsområdet, t.ex. patientdatalagen (2008:355), polisdatalagen (2010:361) och kustbevakningsdatalagen (2012:145), benämna den nya lagen domstolsdatalag. Namnet skulle möjligen kunna anses något missvisande, eftersom lagen även ska omfatta hyres- och arrendenämnderna, vilka inte är domstolar. Fördelarna med detta namn överväger dock, med hänsyn dels till intresset av

konsekvens i förhållande till andra lagar på personuppgiftsområdet, dels till intresset av att åstadkomma ett så kort men ändå informativt namn som möjligt.

7.2 Rättskipande och rättsvårdande verksamhet

Förslag: Domstolsdatalagen ska tillämpas vid behandling av personuppgifter i domstolarnas rättskipande och rättsvårdande verksamhet.

Skälen för förslaget: I Vera-förordningarna anges inledningsvis att dessas tillämpningsområde är domstolarnas ”rättskipande och rättsvårdande verksamhet” samt att de gäller utöver personuppgiftslagen. Begränsningen till rättskipande och rättsvårdande verksamhet innebär att den personuppgiftsbehandling som utförs i domstolarnas administrativa verksamhet inte omfattas utan i stället styrs av personuppgiftslagen.

Fråga är då vilket tillämpningsområde domstolsdatalagen bör ha. Skälen som ligger till grund för att i denna promemoria föreslå en särreglering i förhållande till personuppgiftslagen hänför sig i allt väsentligt till domstolarnas rättskipande och rättsvårdande verksamhet, dvs. deras kärnverksamhet. Skälen har sin grund i de särskilda förhållanden som råder inom den rättskipande och rättsvårdande verksamheten, nämligen att stora mängder personuppgifter behandlas, att dessa uppgifter ofta är känsliga, att verksamheten i hög grad styrs av andra regelverk (t.ex. rättegångsbalken och förvaltningsprocesslagen) samt att enskildas möjligheter till insyn är särskilt goda.

I den administrativa verksamheten råder inte sådana särskilda förhållanden. Personuppgiftsbehandlingarna i denna verksamhet gäller vanligtvis handläggningen av personalärenden, lokalförsörjning och liknande och skiljer sig inte i något väsentligt hänseende från personuppgiftsbehandlingarna som sker i motsvarande verksamhet hos andra myndigheter eller hos privata

företag. Det rör sig om behandling av personuppgifter i samband med hantering av löner, reseräkningar, sjukfrånvaro m.m. Det kan konstateras att registerförfattningarna som gäller för exempelvis polisen och för Åklagarmyndigheten inte omfattar personuppgiftsbehandlingen i dessa myndigheters administrativa verksamhet (1 kap. 2 § polisdatalagen och 1 § förordning [2006:937] om behandling av personuppgifter inom åklagarväsendet).

Det är rimligt att en särreglering av personuppgiftsbehandlingen i förhållande till personuppgiftslagen sker endast när det är motiverat. Sedan ikraftträdandet av Vera-förordningarna, vilka alltså inte omfattar den administrativa verksamheten, har det inte framkommit något tydligt behov av en sådan särreglering för den administrativa verksamheten i domstolarna.

Det kan naturligtvis finnas personuppgifter som förekommer i såväl den administrativa som den dömande verksamheten. Domstolsdatautredningen diskuterade i detta sammanhang bl.a. uppgifter om nämndemän, tolkar och advokater, vilka i vissa fall t.o.m. kan behandlas i särskilda register. Utredningen utgick ifrån att sådana uppgifter och register skulle omfattas av den administrativa verksamheten (SOU 2001:100 s. 93 f.). Det avgörande bör dock vara i vilken verksamhet uppgifterna samlas in eller på annat sätt behandlas. När uppgifter om nämndemän eller tolkar behandlas i den rättskipande och rättsvårdande verksamheten, t.ex. vid kallelse till förhandling eller när uppgifter om dem tas in i domar och beslut bör domstolsdatalagens bestämmelser tillämpas medan annan personuppgiftsbehandling, t.ex. vid handläggningen av ersättning till nämndemän, kan ske i domstolarnas administrativa verksamhet. Att det härigenom uppstår vissa gränsdragningsfrågor är ofrånkomligt och bör inte behöva medföra några egentliga problem.

Mot den angivna bakgrunden framstår det som lämpligt att även inom domstolarna fortsätta att låta personuppgiftsbehandlingen i den administrativa verksamheten endast omfattas av de allmänna reglerna i personuppgiftslagen. Tillämpningsområdet för den lagreglering som nu föreslås bör därför vara den rättskipande och rättsvårdande verksamheten.

7.3 Automatiserade behandlingar och manuella register

Förslag: Domstolsdatalagen ska vara tillämplig i fråga om behandling av personuppgifter som är helt eller delvis automatiserad eller sker i manuella register.

Skälen för förslaget: Personuppgiftslagen omfattar all behandling av personuppgifter som är helt eller delvis automatiserad. Vidare omfattas även viss manuell behandling av personuppgifter om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier (5 § PUL). Personuppgiftslagens tillämpningsområde överensstämmer med dataskyddsdirektivets (artikel 2 c och 3).

Det finns inte något utrymme för att i domstolarnas rättskipande och rättsvårdande verksamhet ha ett mer begränsat tillämpningsområde. Det bedöms inte heller ändamålsenligt att låta den manuella behandlingen regleras av personuppgiftslagen medan övrig behandling sker enligt domstolsdatalagen. Inom ramen för den rättskipande och rättsvårdande verksamheten bör därför all personuppgiftsbehandling ske enligt samma regelverk. Härigenom blir domstolsdatalagen teknikoberoende. Domstolsdatalagen bör alltså, i likhet med vad som gäller för polisdatalagen och flertalet andra registerförfattningar, ha samma tillämpningsområde som personuppgiftslagen och således omfatta helt eller delvis automatiserad behandling av personuppgifter och behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

7.4 Uppgifter om avlidna och juridiska personer

Bedömning: Domstolsdatalagen bör inte omfatta behandling av uppgifter om avlidna eller om juridiska personer.

Skälen för bedömningen

Inledning

Bestämmelserna i såväl personuppgiftslagen som Vera-förordningarna gäller behandling av personuppgifter, men inte behandling av andra uppgifter. Med begreppet personuppgifter avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet (3 § PUL). Denna definition föreslås gälla även vid tillämpningen av domstolsdatalagen (se avsnitt 8.5). Definitionen innebär att bestämmelserna i domstolsdatalagen som utgångspunkt inte är tillämpliga i fråga om uppgifter som avser avlidna eller juridiska personer.

Domstolsdatautredningen föreslog i sitt slutbetänkande att vissa bestämmelser i de av utredningen föreslagna domstolsdatalagarna skulle vara tillämpliga även vid behandling av uppgifter om avlidna och juridiska personer (SOU 2001:100 s. 103 f.). Flertalet remissinstanser tillstyrkte förslaget eller invände inte mot det. Mot den bakgrunden finns det anledning att överväga om uppgifter om juridiska personer och avlidna bör omfattas av domstolsdatalagens tillämpningsområde.

Juridiska personer

I domstolarnas rättskipande och rättsvårdande verksamhet behandlas i flera fall uppgifter om juridiska personer. Företag kan uppträda som parter i många olika typer av mål i såväl allmän förvaltningsdomstol som i allmän domstol, t.ex. mål om fordran, skadestånd, firmaregistrering och upphandling samt ärenden om konkurs. Varken dataskyddsdirektivets, personuppgiftslagens

eller Vera-förordningarnas tillämpningsområde omfattar sådana uppgifter. Däremot har i vissa registerförfattningar, t.ex. polisdatalagen, de grundläggande bestämmelserna om personuppgiftsbehandlingen gjorts tillämpliga även på juridiska personer.

Ett av de huvudsakliga syftena med den lagstiftning som nu föreslås är att skydda den personliga integriteten. Som anges i avsnitt 6.1 finns det inte någon fastslagen definition av personlig integritet men det står klart att begreppet är nära knutet till skyddet för privatlivet. Det framstår därför som tveksamt om begreppet personlig integritet verkligen har någon relevans för juridiska personer.

Begreppet personuppgift är ett vitt begrepp och omfattar all slags information som direkt eller indirekt kan hänföras till en fysisk person. Behandling av uppgifter som i och för sig är hänförliga till juridiska personer kan därför i vissa fall anses vara personuppgiftsbehandling och innebära en risk för fysiska personers personliga integritet. Till exempel bör en uppgift om firmatecknare anses utgöra en personuppgift. Samma sak gäller en uppgift om en enskild firma, eftersom firman direkt kan knytas till en bestämd fysisk person. I företag med endast ett fåtal ägare som är fysiska personer kan ägarna vara så nära förknippade med företaget att behandling av uppgifter om företaget kan anses avse även ägarna. Det kan således finnas ett indirekt skyddsbehov för vissa juridiska personer, som dock har sin grund i intresset av integritetsskydd för fysiska personer. Detta skyddsbehov torde därför i allt väsentligt vara tillgodosett genom de regler som nu föreslås till skydd för de fysiska personernas personliga integritet.

Mot den angivna bakgrunden bedöms det inte finns tillräckliga skäl att avvika från vad som gäller enligt personuppgiftslagen och utvidga domstolsdatalagens tillämpningsområde till att omfatta uppgifter som avser juridiska personer.

Detta ställningstagande innebär inte att domstolarna måste behandla uppgifter om juridiska personer annorlunda än personuppgifter. Att uppgifter om juridiska personer inte omfattas av domstolsdatalagen och därmed inte tillerkänns mer specifika

rättigheter, såsom t.ex. rätt att få personuppgifter som behandlas i strid med lagen rättade, blockerade eller utplånade, utesluter inte heller att en skyldighet för den personuppgiftsansvarige att företa sådana åtgärder ändå kan finnas på annan grund. Högsta förvaltningsdomstolen har slagit fast att det förhållandet att lagen (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet saknade bestämmelser om rättelse av felaktiga uppgifter såvitt avsåg juridiska personer inte rimligen kunde innebära att en juridisk person skulle kunna vägras att få en sådan uppgift rättad (RÅ 2004 ref. 104).

Avlidna personer

I domstolarnas rättskipande och rättsvårdande verksamhet behandlas ibland uppgifter om avlidna. Det gäller t.ex. vid handläggning av ett brottmål som avser åtal för mord eller ett tvistemål om klander av testamente. I t.ex. ärenden om dödförklaring är just frågan om en person ska anses avliden det som rätten ska pröva. Det kan undantagsvis även inträffa att en part eller annan avlider under handläggningen av ett mål eller ärende.

Enligt dataskyddsdirektivet avses med personuppgift varje upplysning som avser en fysisk person som är identifierad eller som kan identifieras (artikel 2 a). Av de uttalanden som tagits till rådets protokoll i samband med den gemensamma ståndpunkten beträffande direktivet framgår att medlemsstaterna kan bestämma om uppgifter om avlidna personer ska omfattas av den nationella lagstiftningen (se SOU 1997:39 s. 113). Datalagskommittén gjorde bedömningen att möjligheten att begränsa tillämpningen av personuppgiftslagen till att avse bara uppgifter om person som är livet borde utnyttjas (a. SOU s. 337). I propositionen med förslag till personuppgiftslagen gjordes ingen annan bedömning (prop. 1997/98:44 s. 116). Polisdatalagen har exkluderat avlidna personer med hänvisning till intresset av enhetlig terminologi i förhållande till personuppgiftslagen (prop. 2009/10:85 s. 82). Motsvarande gäller för flertalet andra register-

författningar. Bland annat patientdatalagen omfattar dock i tillämpliga delar även behandling av uppgifter som avser avlidna, vilket i förarbetena motiverades med att uppgifter om avlida patienter kan vara integritetskänsliga (prop. 2007/08:126 s. 52).

Det framstår i och för sig inte som främmande att även för avlidna tala i termer av personlig integritet (jfr t.ex. 5 kap. 4 § brottsbalken). Som Datalagskommittén framförde som skäl mot att inkludera avlidna kan alla personuppgiftsbestämmelser dock inte utan vidare tillämpas på avlidna. Det finns vidare ett stort värde i att synen på vilka uppgifter som ska omfattas av domstolsdatalagens skyddsregler ansluter sig personuppgiftslagens. Mot den angivna bakgrunden bedöms det inte finnas tillräckligt starka skäl att låta reglerna i domstolsdatalagen omfatta behandling av uppgifter om avlidna. På samma sätt som gäller för juridiska personer innebär dock detta ställningstagande inte att domstolarna vid handläggning av mål och ärenden måste behandla uppgifter om avlidna annorlunda än personuppgifter.

8 Lagens syfte och struktur

8.1 Lagens syfte

Förslag: Syftet med domstolsdatalagen ska vara att ge domstolarna möjlighet att behandla personuppgifter på ett ändamålsenligt sätt samt att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

Skälen för förslaget: Samhällets rättmätiga krav på en rättssäker och effektiv dömande verksamhet förutsätter bl.a. att domstolarna ges möjlighet att behandla personuppgifter på ett ändamålsenligt sätt, vilket bl.a. förutsätter ett rationellt datorstöd för behandling av personuppgifter. Samtidigt kan hanteringen av personuppgifter innebära en risk för intrång i den personliga integriteten. Skyddet av den enskildes personliga integritet måste värnas. Det är viktigt att hitta en väl avvägd balans mellan å ena sidan skyddet för den personliga integriteten och å andra sidan kravet på att på ett effektivt och rättssäkert sätt kunna handlägga och avgöra mål och ärenden i domstolarna.

Begränsningarna av skyddet mot integritetsintrång får inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som föranlett dem (2 kap. 21 § RF). Detta stadgande ger uttryck för en proportionalitetsprincip liknande den som gäller enligt Europakonventionen. Den närmare utformningen av en reglering om personuppgiftsbehandling bör således återspegla en avvägning mellan å ena sidan intresset av en effektiv och rättssäker verksamhet och å andra sidan intresset av att skydda

den personliga integriteten. Vissa faktorer är särskilt viktiga att ta hänsyn till när det gäller att bedöma integritetskänsligheten vid automatiserad behandling av personuppgifter. Det gäller arten av personuppgifter som samlas in, för vilka ändamål detta görs, hur och av vem uppgifterna används, hur sökning får ske, hur uppgifterna sparas samt mängden av uppgifter som samlas på ett och samma ställe eller som på något annat sätt är tillgängliga för bearbetningar och sammanställningar. Särskild omsorg måste ägnas åt att personuppgiftsregleringen effektivt kan förhindra kränkningar av den personliga integriteten.

Mot den angivna bakgrunden kan syftet med domstolsdatalagen sägas vara tvådelat: att möjliggöra en ändamålsenlig personuppgiftsbehandling i domstolarna samt att skydda mot integritetsintrång. I likhet med bl.a. polisdatalagen bör detta dubbla syfte komma till tydligt uttryck i lagen.

8.2 Lagens förhållande till personuppgiftslagen

Förslag: Domstolsdatalagen ska inom sitt tillämpningsområde gälla i stället för personuppgiftslagen. Det ska särskilt i lagen anges vilka bestämmelser i personuppgiftslagen som ska tillämpas.

Skälen för förslaget: De registerförordningar som enligt nuvarande ordning är tillämpliga i domstolarnas rättskipande och rättsvårdande verksamhet (Vera-förordningarna) utgör ingen självständig reglering i förhållande till personuppgiftslagen. Förordningarna gäller i stället utöver den lagen.

Personuppgiftslagen är subsidiär i förhållande till annan lag eller förordning. Lagen ska således inte tillämpas i den utsträckning det i sådan annan författning finns bestämmelser som avviker från personuppgiftslagen (2 § PUL). Vid den översyn som nu sker är det därför möjligt att utgå från personuppgiftslagen och i domstolsdatalagen föreslå sådana avvikande

eller kompletterande bestämmelser som bedöms vara nödvändiga. Detta skulle alltså vara samma lagstiftningsmetod som använts i fråga om Vera-förordningarna. Ett annat alternativ är att föreslå en mer självständig reglering som ersätter personuppgiftslagen inom domstolsdatalagens tillämpningsområde.

Det första alternativet innebär att domstolsdatalagen kommer att gälla utöver personuppgiftslagen. Om en fråga är oreglerad i domstolsdatalagen kommer bestämmelserna i personuppgiftslagen därmed att vara tillämpliga. Detta kan ske genom att i domstolsdatalagen överhuvudtaget inte nämna personuppgiftslagen, vilket innebär att den lagens bestämmelser utan vidare kommer att vara tillämpliga i den mån domstolsdatalagen inte innehåller någon avvikande bestämmelse. En närliggande och tydligare lösning är att i domstolsdatalagen ange att den gäller utöver personuppgiftslagen. En sådan lösning har bl.a. den fördelen att ändringar som görs i den generella lagstiftningen får direkt genomslag även på det särreglerade området. Nackdelen med detta alternativ är att tillämparen kan ha svårt att få överblick över vilka bestämmelser i personuppgiftslagen som är tillämpliga. Metoden har dock använts i flera särskilda registerförfattningar, däribland patientdatalagen (2008:355) och studiestödsdatalagen (2009:287).

Det andra alternativet innebär den fördelen att den leder till en tydlig reglering i fråga om vilka bestämmelser som faktiskt är tillämpliga i en viss situation. Det är detta alternativ som använts i bl.a. lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet, polisdatalagen (2010:361) och kustbevakningsdatalagen (2012:145). Utvecklingen går mot ökat samarbete inom rättsväsendet, bl.a. såvitt gäller informationshanteringen i rättskedjan. Det ligger med hänsyn till detta ett särskilt värde i att så långt som möjligt använda samma lagstiftningsteknik för all behandling av personuppgifter inom rättsväsendets myndigheter, oavsett vilken myndighet det gäller.

Ytterligare ett skäl för att välja detta alternativ är att man genom en självständig reglering i större utsträckning kan ta hänsyn till de särskilda rättsliga och faktiska förhållanden under

vilka domstolarna bedriver sin verksamhet. Med en sådan lösning är det lättare att på ett efter verksamheterna avpassat sätt balansera intresset av integritetsskydd mot intresset av rättssäkerhets- och effektivitetsvinster.

Sammanfattningsvis talar övervägande skäl för att föreslå en självständig reglering som ersätter personuppgiftslagen inom det aktuella tillämpningsområdet. Detta kan åstadkommas på två sätt. Antingen genom en fullständig reglering som innebär att de bestämmelser som föreslås vara oförändrade i förhållande till personuppgiftslagen likväl upprepas i registerförfattningen, eller att det i registerförfattningen införs uttryckliga hänvisningar till de bestämmelser i personuppgiftslagen som ska vara tillämpliga.

Exempel på den första typen av författningar är lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Metoden kan medföra praktiska fördelar för tillämparen då alla bestämmelser som är relevanta finns samlade i en särskild författning. En sådan reglering har dock den nackdelen att identiska bestämmelser upprepas i olika författningar. Detta kan göra det svårare att tillämpa den praxis och de relevanta förarbetsuttalanden som finns, eftersom dessa i de flesta fall torde avse personuppgiftslagen men i praktiken ha relevans även för registerförfattningarna. Dessa nackdelar undviks om man i stället väljer den andra typen av reglering, vilken alltså innebär en registerförfattning med uttryckliga hänvisningar till personuppgiftslagen. Denna lagstiftningsmodell har använts i polisdatalagen och kustbevakningsdatalagen.

En tydlig fördel med en sådan lösning i jämförelse med att låta regleringen gälla utöver personuppgiftslagen är att tillämparen inte lämnas utan vägledning när det gäller vilka bestämmelser i personuppgiftslagen som är tillämpliga. En sådan lösning ansluter samtidigt tydligare till tanken att personuppgiftslagens regler bör gälla om det inte finns skäl att i den specifika verksamheten meddela avvikande eller preciserade bestämmelser och att den särskilda registerförfattningen alltså bör begränsas till att avse frågor som är specifika för den verksamheten.

Alternativet att hänvisa till relevanta bestämmelser i personuppgiftslagen har tidigare fått kritik av Lagrådet som bl.a. ansett att lagstiftningstekniken är riskfylld, med hänsyn såväl till svårigheten att överblicka om dataskyddsdirektivet blir till fullo genomfört i registerförfattningarna som till möjligheten att vid kommande lagändringar hänvisningarna till personuppgiftslagen blir felaktiga eller ofullständiga (se prop. 2000/01:33 s. 345). Inte desto mindre har denna lösning sedermera använts i de särskilda registerförfattningarna för tullen, polisen och kustbevakningen och Lagrådet har då inte haft några invändningar mot lagstiftningstekniken.

Intresset av att så långt som möjligt använda samma lagstiftningsteknik för all behandling av personuppgifter inom rättsväsendet och flera andra myndigheter innebär att det nu saknas skäl att föreslå någon annan typ av lösning för domstolarnas del än vad som gäller för bl.a. polisen. Domstolsdatalagen bör alltså gälla i stället för personuppgiftslagen och i de fall bestämmelser i personuppgiftslagen ska tillämpas bör domstolsdatalagen innehålla tydliga hänvisningar till dessa bestämmelser.

Hänvisningar bör i allmänhet göras till bestämmelser i personuppgiftslagen vilkas innehåll är så grundläggande och allmängiltiga att det inte finns något behov av att anpassa deras innehåll till de särskilda förhållanden under vilka domstolarna bedriver sin rättskipande och rättsvårdande verksamhet. Det kan också vara bestämmelser vilkas innehåll är sådant att det är särskilt angeläget att regleringen är enhetlig i förhållande till personuppgiftslagen. I vilka fall hänvisningar till personuppgiftslagen föreslås ske redovisas under respektive sakavsnitt.

8.3 Lagens förhållande till offentlighetsprincipen

Förslag: Det ska genom en hänvisning till 8 § första stycket PUL tydliggöras att domstolsdatalagen inte ska tillämpas i den utsträckning det skulle inskränka skyldigheten att lämna ut personuppgifter enligt 2 kap. TF.

Skälen för förslaget: Bestämmelsen i 8 § första stycket PUL innebär att personuppgiftslagen inte ska tillämpas i den utsträckning det skulle inskränka en myndighets skyldighet att lämna ut personuppgifter enligt 2 kap. TF (om allmänna handlingars offentlighet). Bestämmelsen i 8 § PUL har tillkommit för att tydliggöra det som i och för sig ändå gäller, nämligen att bestämmelser i grundlag alltid har företräde framför bestämmelser i vanlig lag (prop. 1997/98:44 s. 46). Av tydlighetsskäl bör det komma till uttryck att detta även gäller i fråga om domstolsdatalagen genom en uttrycklig hänvisning till 8 § PUL.

Offentlighetsprincipen innebär ingen rätt för enskilda att ta del av allmänna handlingar i elektroniskt format. I vilken utsträckning domstolsdatalagen ska tillåta domstolarna att lämna ut handlingar elektroniskt behandlas i avsnitt 14.

I avsnitt 15.2 behandlas frågan om domstolsdatalagen även bör hänvisa till 8 § andra stycket PUL, enligt vilken myndigheter ges möjlighet att bevara allmänna handlingar.

8.4 Lagens förhållande till viss annan lagstiftning

Förslag: Det ska i domstolsdatalagen särskilt anges att bestämmelser i den föreslagna lagen om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen i förekommande fall har företräde framför bestämmelserna i domstolsdatalagen.

Skälen för förslaget: Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd för personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet) reglerar dataskyddet inom angivna områden (se avsnitt 4.3.3).

Som en återstående del i genomförandet av rambeslutet har regeringen den 21 februari 2013 i propositionen Dataskydd vid europeiskt polissamarbete och straffrättsligt samarbete (prop. 2012/13:73) föreslagits en ny lag om skydd för personuppgifter vid sådant samarbete. Lagen ska gälla för behandling av personuppgifter i verksamhet som har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller verkställa straffrättsliga påföljder om uppgifterna inom ramen för polissamarbete eller straffrättslig samarbete utbyts mellan en svensk myndighet och en annan EU-medlemsstat, ett EU-organ, Island, Norge, Schweiz eller Liechtenstein. Även utbyte med ett EU-informationssystem omfattas av lagen.

I den föreslagna lagen regleras bl.a. för vilka ändamål uppgifterna får behandlas och vad som gäller för den fortsatta behandlingen. Lagen anger vidare i vilka situationer personuppgifter får överföras till enskilda, till tredje land och till internationella organ. Svenska myndigheter åläggs att följa villkor om användningen som ställts upp av den som överfört uppgifterna eller gjort dem tillgängliga.

I propositionen föreslås att det i registerförfattningar, bl.a. polisdatalagen, ska införas en hänvisning till den nya lagen. Av hänvisningen ska det framgå att om det i den nya lagen eller i

föreskrifter som regeringen har meddelat i anslutning till den lagen finns bestämmelser som avviker från registerförfattningens bestämmelser ska de förstnämnda bestämmelserna tillämpas. I propositionen uttalas vidare att motsvarande hänvisningar bör införas i bl.a. de registerförfattningar som gäller för domstolarna och i åklagarnas verksamheter och som för närvarande har formen av förordning (se avsnitt 6.16 i propositionen).

Enligt förslagen i denna promemoria kommer domstolsdatalagen att ersätta de registerförfattningar som gäller i domstolarnas verksamhet. Den nya lagen föreslås innehålla bestämmelser som delvis kommer att avvika från domstolsdatalagens bestämmelser. Mot den angivna bakgrunden bör det därför i domstolsdatalagen tas in en hänvisning till den föreslagna lagen om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen. Hänvisningen bör, i enlighet med vad som föreslås gälla för polisdatalagen, innehålla ett klargörande om att avvikande bestämmelser i den föreslagna lagen eller i föreskrifter som regeringen har meddelat i anslutning till den lagen i förekommande fall har företräde framför domstolsdatalagens bestämmelser.

8.5 Begrepp och definitioner

Förslag: Domstolsdatalagen ska hänvisa till de definitioner av begrepp som finns i 3 § PUL.

Skälen för förslaget: I personuppgiftslagen definieras vissa begrepp som är centrala vid behandling av personuppgifter, bl.a. behandling, personuppgifter, personuppgiftsansvarig, den registrerade och tredje man (3 §). Dessa begrepp är avsedda att ha samma innebörd som motsvarande uttryck har i dataskyddsdirektivet (artikel 2).

Begreppet personuppgifter definieras som ”[a]ll slags information som direkt eller indirekt kan hänföras till en fysisk

person som är i livet". Personuppgifter kan utgöras av namn, personnummer, målnummer, registreringsnummer för fordon, fastighetsbeteckningar etc. Begreppet personuppgift omfattar såväl objektiva upplysningar som subjektiva bedömningar och åsikter. Även bild- och ljudupptagningar kan utgöra personuppgifter.

Med behandling avses "[v]arje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring". Detta innebär att det t.ex. är fråga om behandling av personuppgifter även när sådana skrivs ut på papper.

Definitionerna i personuppgiftslagen gäller för den personuppgiftsbehandling som för närvarande sker med stöd av Veraförordningarna. Det finns inte skäl att göra någon ändring i detta hänseende. Det är viktigt att terminologin i domstolsdatalagen överensstämmer med personuppgiftslagens och att de begrepp som används i de båda författningarna har samma innebörd, även om de materiella bestämmelserna naturligtvis kan skilja sig åt. En hänvisning till 3 § PUL bör därför tas in i domstolsdatalagen.

8.6 Gemensamt tillgängliga uppgifter

Bedömning: Bestämmelserna i domstolsdatalagen bör vara tillämpliga oavsett om behandlingen sker hos en enskild anställd eller i ett register eller en databas där uppgifter är tillgängliga för många i verksamheten. Begreppet gemensamt tillgängliga uppgifter bör inte användas i domstolsdatalagen.

Skälen för bedömningen: Risken för otillbörliga intrång i den personliga integriteten är generellt större när personuppgifter

används av flera anställda gemensamt än när personuppgifter behandlas av en anställd vid den egna datorn utan att någon annan har åtkomst till uppgifterna. Traditionellt har det varit vanligt att i författningar om personuppgiftsbehandling använda begreppen register och databas för att definiera uppgifter som har gjorts tillgängliga för en större krets inom en myndighet. Till respektive register har sedan knutits regler om åtkomst, sökmöjligheter m.m.

Registerbegreppet har i olika sammanhang kritiserats, bl.a. därför att det har en teknisk anknytning och därför att moderna datasystem normalt inte byggs som traditionella register. Även begreppet databas riskerar att leda tanken till ett visst, i tekniskt avseende avgränsat, informationssystem. Detta är inte ett helt relevant sätt att se på samlingar av uppgifter i elektronisk form. Som anförs i avsnitt 6.2 bör domstolsdatalagen vara teknikneutral och flexibel. Regleringen bör därför inte bygga på att behandlingen av personuppgifter sker i olika register eller databaser. Motsvarande bedömning har gjorts i fråga om polisdatalagen (prop. 2009/10:85 s. 124 f.).

Beträffande polisdatalagen ansågs det dock alltjämt finnas ett behov av att inom polisens verksamhet införa mer begränsande regler i fråga om behandling av uppgifter som flera personer har tillgång till. Ett annat sätt att se på detta är att det för uppgifter som endast är tillgängliga för en eller ett fåtal personer inte borde gälla lika restriktiva regler. För att åstadkomma en distinktion i polisdatalagens reglering introducerades begreppet *gemensamt tillgängliga uppgifter*, med vilket avses uppgifter som fler än ett fåtal personer har faktisk möjlighet och rättslig behörighet att ta del av. De mer restriktiva regler som enligt polisdatalagen gäller för gemensamt tillgängliga uppgifter är av två olika slag. Det finns dels bestämmelser om vilka personuppgifter som överhuvudtaget får göras gemensamt tillgängliga, dels integritetsskyddande bestämmelser som enbart är tillämpliga i fråga om gemensamt tillgängliga uppgifter, bl.a. om sökning, direktåtkomst och bevarande (a. prop. s. 124 f.).

Även om domstolarna sammantaget hanterar över 500 olika mål- och ärendetyper inom de flesta av samhällets olika områden är det i grunden fråga om en och samma verksamhet som bedrivs, nämligen att handlägga mål och ärenden. Denna verksamhet regleras på ett relativt heltäckande sätt genom processrättsliga regelverk och principer. Domstolsdatalagens tillämpningsområde föreslås vara begränsat just till denna verksamhet, dvs. domstolarnas rättskipande och rättsvårdande verksamhet (avsnitt 7.2) och behandling ska få ske endast för vissa särskilt angivna ändamål, i första hand om det behövs för handläggning av mål och ärenden (avsnitt 10.2).

Det är svårt att se hur en ytterligare avgränsning skulle kunna göras vad gäller frågan om vilka uppgifter som får vara gemensamt tillgängliga. Visserligen innehåller polisdatalagen någorlunda brett formulerade regler i detta avseende, t.ex. att uppgifter ”som förekommer i ett ärende om utredning eller beivrande av brott” får göras gemensamt tillgängliga (3 kap. 2 § 3). Polisens verksamhet är dock mycket mer divergerad än domstolarnas, varför en avgränsning där fyller ett tydligare syfte.

I domstolsdatalagen föreslås en skyldighet för domstolarna att för varje anställd begränsa tillgången till personuppgifter till vad han eller hon behöver för att kunna fullgöra sina arbetsuppgifter (avsnitt 11.2). Det innebär att det kommer att finnas ett uttryckligt skydd mot att personuppgifter sprids inom domstolen i större utsträckning än vad som är motiverat med hänsyn till de krav som verksamheten ställer. Ur integritetssynvinkel bedöms det därför inte finnas något behov av en bestämmelse om vilka uppgifter som får göras gemensamt tillgängliga i domstolarnas verksamhet.

Även om det således inte bedöms nödvändigt att föreslå några ytterligare begränsningar av spridning av personuppgifter, skulle polisdatalagens distinktion avseende gemensamt och icke gemensamt tillgängliga uppgifter kunna användas i domstolsdatalagen för att undanta behandlingar som utförs av endast en eller ett fåtal anställda från exempelvis bestämmelserna om sökning, om direktåtkomst och om bevarande.

Personuppgiftsbehandlingen i domstolarnas verksamhet bör präglas av ett starkt integritetsskydd. Med hänsyn till de typer av personuppgifter som förekommer i denna verksamhet och de alltmer avancerade möjligheterna att behandla dessa bedöms även behandling av personuppgifter som endast ett fåtal har tillgång till, kunna innefatta vissa integritetsrisker. Dessa risker måste vägas mot det tänkta behov som kan finnas av att kunna behandla personuppgifter utan hinder av de begränsningar som föreslås gälla i domstolsdatalagen. Vid en sådan avvägning framstår inte behovet av att mera fritt kunna t.ex. söka eller på annat sätt behandla personuppgifter som så framträdande att det är motiverat att föreskriva undantag från den skyddsreglering som ska gälla i övrigt. Det är därför rimligt att en högre nivå av integritetsskydd gäller även i de situationer då endast ett fåtal anställda har tillgång till de personuppgifter som behandlas.

Av samma skäl finns det inte anledning att i domstolsdatalagen hänvisa till 5 a § PUL som innebär att behandling av personuppgifter i ostrukturerat material såsom löpande text får utföras i princip fritt så länge som det inte innebär en kränkning av den registrerades personliga integritet.

Sammantaget görs bedömningen att domstolsdatalagen bör vara generellt tillämplig på all behandling av personuppgifter i domstolarnas rättskipande och rättsvårdande verksamhet, oavsett om behandlingen sker hos en enskild anställd eller i ett register eller en databas där uppgifter är tillgängliga för många i verksamheten. Det innebär att lagens bestämmelser ska tillämpas på all behandling av uppgifter, oavsett om det gäller e-posthantering, ordbehandling eller förandet av gemensamma mål- och ärendehanteringssystem.

8.7 Samtycke

Bedömning: Behandling av personuppgifter som är tillåten enligt domstolsdatalagen bör få utföras även om den registrerade motsätter sig det.

Skälen för bedömningen: I artikel 7 i dataskyddsdirektivet anges att medlemsstaterna ska föreskriva att personuppgifter endast får behandlas i vissa fall. Exempel på sådana fall är om den registrerade otvetydigt har lämnat sitt samtycke eller om behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den registeransvarige för att utföra en arbetsuppgift av allmänt intresse eller som ett led i myndighetsutövning som utförs av den registeransvarige. I 10 § PUL finns en bestämmelse med i huvudsak samma innehåll. Dataskyddsrambeslutet innehåller däremot ingen motsvarande reglering.

Enligt vad som föreslås i avsnitt 10.2 kommer det enligt domstolsdatalagen att vara tillåtet för domstolarna att behandla personuppgifter om det behövs för handläggning av mål och ärenden eller för uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Domstolsdatalagen föreslås vidare endast vara tillämplig i domstolarnas rättskipande och rättsvårdande verksamhet (avsnitt 7.2). De behandlingar som ryms inom dessa ramar får anses vara nödvändiga för att domstolarna ska kunna fullgöra sina rättsliga förpliktelser eller kunna utföra sina arbetsuppgifter av allmänt intresse. Behandlingarna får vidare anses vara nödvändiga som ett led i myndighetsutövningen. Det finns således rättsliga förutsättningar att i domstolsdatalagen tillåta att behandlingar sker utan den registrerades samtycke.

Det finns inte heller i övrigt skäl att uppställa ett krav på samtycke i domstolsdatalagen. Domstolarnas handläggning av mål och ärenden styrs i hög grad av processuella regler. Det är sällan domstolen som styr över att en viss personuppgift behöver behandlas, utan behovet uppstår typiskt sett när en part ger in en

handling som innehåller en personuppgift till domstolen. Ett av huvudsyftena med domstolsdatalagen är just att ge domstolarna möjlighet att behandla sådana personuppgifter på ett ändamålsenligt sätt. Det bör alltså redan av dessa skäl inte komma i fråga att låta behandlingen vara beroende av den registrerades samtycke. Det skulle vidare inte vara motiverat med hänsyn till de kostnader och olägenheter som skulle uppstå om domstolarna exempelvis skulle behöva inhämta samtycke från de registrerade (t.ex. parter, vittnen, advokater osv.) innan deras personuppgifter kan behandlas i domstolarnas datorsystem.

Mot den angivna bakgrunden bör domstolarna tillåtas behandla personuppgifter utan den registrerades samtycke så länge behandlingen sker enligt domstolsdatalagens tillämpningsområde och inom de ramar som uppställs genom de ändamålsbestämmelser som föreslås i avsnitt 10.2.

Fråga är om detta ställningstagande bör komma till uttryck i domstolsdatalagen. Av dataskyddsdirektivet framgår att medlemsstaterna i fråga om behandlingar som är ett led i myndighetsutövning ska tillförsäkra den registrerade rätten att motsätta sig behandling av uppgifter som rör honom eller henne, utom när den nationella lagstiftningen föreskriver något annat (artikel 14). I några registerförfattningar har samtyckets betydelse reglerats (se t.ex. 2 kap. 2 § patientdatalagen och 5 § studiestödsdatalagen). Dessa lagar gäller utöver personuppgiftslagen och genom att reglera samtyckesfrågan förtydligas att personuppgiftslagens bestämmelse om samtycke inte gäller inom dessa lagars tillämpningsområde. Den aktuella bestämmelsen i dataskyddsdirektivet har emellertid inte generellt ansetts innebära att registerförfattningar ska innehålla en uttrycklig bestämmelse om samtycke. I exempelvis polisdatalagen och kustbevakningsdatalagen saknas uttryckliga bestämmelser om att behandling får ske utan samtycke. Det kan noteras att dessa lagar – i likhet med domstolsdatalagen men till skillnad från patientdatalagen och studiestödslagen – ersätter personuppgiftslagen inom sina respektive tillämpningsområden.

Mot den angivna bakgrunden bedöms det inte nödvändigt att i domstolsdatalagen uttryckligen ange att domstolarna får behandla personuppgifter i enlighet med lagen oavsett den registrerades samtycke.

9 Personuppgiftsansvarig och personuppgiftsbiträden

9.1 Personuppgiftsansvarig

Förslag: En domstol ska vara personuppgiftsansvarig för behandling som den utför.

Skälen för förslaget: Personuppgiftslagen innehåller ett stort antal hanteringsregler som innebär olika skyldigheter för den som är ansvarig för den personuppgiftsbehandling som sker i en verksamhet. Personuppgiftslagen definierar en personuppgiftsansvarig som den vilken ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter (3 § PUL). Den personuppgiftsansvarige har ett långtgående ansvar för att all behandling av personuppgifter sker i överensstämmelse med tillämpliga personuppgiftsbestämmelser. Den personuppgiftsansvarige har bl.a. ansvaret för att registrerade uppgifter är korrekta och att de inte behandlas på ett sätt som strider mot tillämpliga bestämmelser. I personuppgiftsansvarets konstruktion ligger dessutom att även underlåtenhet att vidta föreskrivna åtgärder omfattas, t.ex. underlåtenhet att genomföra den behandling som krävs för att lämna ett registerutdrag.

Det är bara den personuppgiftsansvarige som kan göras skadeståndsansvarig för behandlingar som sker i strid med bestämmelserna i personuppgiftslagen, även om andra personer deltagit i en behandling. De personer som arbetar under den

personuppgiftsansvariges ledning får bara behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige (30 § PUL).

I registerförfattningar finns det ofta bestämmelser genom vilken det tydligt pekas ut vem som är personuppgiftsansvarig för den behandling av uppgifter som regleras i respektive författning. Ett sådant utpekande gör det lättare för enskilda att förstå vem som är personuppgiftsansvarig. Den som t.ex. vill begära rättelse kan då direkt veta vart han eller hon ska vända sig. Eftersom det inte bedöms finnas några egentliga nackdelar med att särskilt ange vem som är personuppgiftsansvarig, bör en bestämmelse om detta tas in i domstolsdatalagen.

Enligt Vera-förordningarna gäller att varje domstol är personuppgiftsansvarig för den behandling som den domstolen utför samt att Domstolsverket är ansvarig för den behandling som verket utför. Denna reglering innebär alltså en fördelning av personuppgiftsansvaret mellan domstolarna och Domstolsverket. Till grund för bestämmelserna ligger det förslag som Domstolsdatautredningen lämnade i sitt delbetänkande. Enligt utredningen innebar denna fördelning att Domstolsverket i första hand har ett ansvar för sådana fel som kan uppstå till följd av funktioner i den fasta programvaran i det datorsystem som verket ansvarar för. Som skäl för uppdelningen av personuppgiftsansvaret anförde utredningen (SOU 2001:32 s. 104 f.) bl.a. följande:

> Med hänsyn till det samarbete som finns mellan Domstolsverket och domstolarna i fråga om datorsystem, inte minst under den närmaste framtiden då det under ledning av verket pågår arbete med framtagande av nya datorsystem för domstolarna, är det dock sannolikt att det kan komma att uppstå situationer då det snarare är Domstolsverket än den aktuella domstolen som har reell möjlighet att ansvara för hur uppgifter behandlas. Som exempel kan nämnas att den personuppgiftsansvarige enligt 31 § personuppgiftslagen ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter som behandlas. Detta ansvar kommer i normalfallet inte att kunna läggas på enskilda domstolar och nämnder när de

utnyttjat helhetslösningar för datorsystem som har utvecklats och tillhandahålls genom Domstolsverkets försorg.

Flera remissinstanser var kritiska till utredningens förslag om fördelning av personuppgiftsansvaret. Kritiken gick i huvudsak ut på att gränsdragningen för personuppgiftsansvaret mellan Domstolsverket och domstolarna kunde bli komplicerad vilket gjorde det svårare för enskilda att hävda sin rätt. I sitt slutbetänkande tog Domstolsdatautredningen till sig av remisskritiken som hade lämnats med anledning av delbetänkandet. Utredningen framhöll att Domstolsverket i sin ordinarie verksamhet enligt de författningar som utredningen föreslog inte skulle ha någon tillgång till personuppgifter i domstolarnas datorsystem. Domstolsverket kunde därför närmast betraktas som ett rent serviceorgan som tillhandahåller de tekniska systemen (SOU 2001:100 s. 113 f.). Utredningen föreslog därför att Domstolsverket inte skulle utpekas som personuppgiftsansvarig i de lagar som enligt utredningens förslag skulle reglera personuppgiftsbehandlingen vid domstolarna. Flertalet remissinstanser tillstyrkte eller hade inte något att erinra mot detta förslag.

Vad gäller frågan vem som ska vara personuppgiftsansvarig enligt domstolsdatalagen bör inledningsvis framhållas att Domstolsverket över huvud taget inte omfattas av domstolsdatalagens tillämpningsområde, vilket har sin grund i att verket inte bedriver rättsvårdande eller rättskipande verksamhet (se avsnitt 7.1). Om Domstolsverket skulle utpekas som personuppgiftsansvarig enligt domstolsdatalagen skulle det i så fall vara ett ansvar som närmast tog sikte på den behandling som sker i domstolarnas rättskipande och rättsvårdande verksamhet. Eftersom varje domstol är en egen myndighet som formellt sett använder sig av ett eget datorsystem i sin verksamhet är det på ett principiellt plan varje enskild domstol som i det enskilda fallet ytterst har att bestämma vilka personuppgifter som ska registreras i respektive verksamhetsstöd och hur personuppgifter i övrigt ska behandlas.

I personuppgiftsansvaret ligger bl.a. ett ansvar för att bestämma ändamålen och medlen för personuppgiftsbehandlingen, en skyldighet att kontrollera och ansvara för de behandlingar som utförs samt att vidta åtgärder som rättelse och blockering. Att låta Domstolsverket vara personuppgiftsansvarig i förhållande till den behandling som sker i domstolarnas rättskipande och rättsvårdande verksamhet (dvs. den behandling som omfattas av domstolsdatalagen) skulle vara svårt att förena med domstolarnas självständiga ställning. Domstolsverket har varken i författning eller på annat sätt en självständig roll i den rättskipande och rättsvårdande verksamheten. Mot den angivna bakgrunden bör det i domstolsdatalagen anges att det är varje enskild domstol som är personuppgiftsansvarig för den personuppgiftsbehandling som sker i den rättskipande och rättsvårdande verksamheten.

Domstolsverket utvecklar och tillhandahåller de verksamhetsstöd (Vera) som domstolarna för närvarande använder. RIF-samarbetet innebär ökade krav på domstolarna att skicka information elektroniskt till andra myndigheter och samarbetet förutsätter att denna informationsförmedling sker i bestämda kanaler, enligt överenskomna standarder och att informationen filtreras så att rätt uppgifter hamnar hos rätt myndighet. För domstolarnas del har Domstolsverket en nyckelroll för att få de tekniska systemen att fungera på ett sätt så att domstolarna kan fullgöra sin roll i RIF-samarbetet. Även om Domstolsverket på grund av sin roll som systemutvecklare har ett stort inflytande över hur datorsystemen utformas, är verkets roll på ett principiellt plan att bistå domstolarna med ett datorsystem som tillgodoser deras behov av att kunna behandla personuppgifter. Denna distinktion ändras inte av det faktum att domstolarnas handlingsutrymme i realiteten kan vara begränsat, bl.a. med hänsyn till de krav på uppgiftslämnande som åvilar domstolarna i enlighet med författning, på grund av de krav som följer av RIF-samarbetet eller av andra skäl.

När Domstolsverket behandlar personuppgifter i sin egen verksamhet sker det med stöd av personuppgiftslagen. I den mån

Domstolsverket i sin roll som tekniskt serviceorgan åt domstolarna behandlar personuppgifter i domstolarnas rättskipande och rättsvårdande verksamhet får det anses ske för domstolarnas räkning. Domstolsverket är då personuppgiftsbiträde åt domstolarna (se avsnitt 9.2). När Domstolsverket i den egenskapen utför personuppgiftsbehandlingar på domstolarnas uppdrag sker behandlingen med stöd av domstolsdatalagen och inte med stöd av personuppgiftslagen.

9.2 Personuppgiftsbiträde

Förslag: Domstolsdatalagen ska hänvisa till föreskrifterna i 3, 30 och 31 §§ PUL som gäller personuppgiftsbiträden.

Skälen för förslaget: För att på olika sätt bistå en personuppgiftsansvarig finns det enligt personuppgiftslagen möjligheter för denne att anlita ett personuppgiftsbiträde. Ett personuppgiftsbiträde definieras som någon som behandlar personuppgifter för den personuppgiftsansvariges räkning (3 § PUL). Det torde följa av denna definition att personuppgiftsbiträdet kan utföra behandlingarna med stöd av den registerförfattning som gäller för den personuppgiftsansvarige, trots att personuppgiftsbiträdet annars inte skulle ha omfattats av dessa regler. Personuppgiftsbiträdet är vanligen ett externt organ som anlitas för att utföra uppgifter för den personuppgiftsansvariges räkning, vilka innebär att personuppgifter behandlas.

Det framgår av 30 § andra stycket PUL att det ska finnas ett skriftligt avtal om den personuppgiftsbehandling som personuppgiftsbiträdet utför för den personuppgiftsansvariges räkning. I 31 § andra stycket PUL anges vidare att den personuppgiftsansvarige ska förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att biträdet verkligen vidtar åtgärderna. Det är dock den personuppgiftsansvarige som har ansvaret gentemot den registrerade

avseende behandlingen även när ett personuppgiftsbiträde har anlitats (prop. 1997/98:44 s. 92).

Den omständigheten att Domstolsverket utvecklar och tillhandahåller den tekniska infrastrukturen i form av verksamhetsstödet Vera som domstolarna använder behöver inte i sig innebära att Domstolsverket behandlar personuppgifter. Domstolsverket bör dock ha möjlighet att utföra personuppgiftsbehandlingar i domstolarnas rättskipande och rättsvårdande verksamhet för att bistå dem, bland annat med att leva upp till de krav som följer av RIF-samarbetet. En domstol bör också ha möjlighet att anlita andra än Domstolsverket, t.ex. tekniska konsulter, för att utföra behandlingar å domstolens vägnar. Av dessa skäl bör domstolsdatalagen hänvisa till bestämmelserna i 3, 30 och 31 §§ PUL så att det finns ett rättsligt stöd för Domstolsverket och för andra utomstående att utföra personuppgiftsbehandlingar med stöd av domstolsdatalagen för en eller flera domstolars räkning. Bestämmelserna innebär att domstolarna ska teckna ett skriftligt avtal med den som agerar personuppgiftsbiträde om den personuppgiftsbehandling som personuppgiftsbiträdet utför för domstolarnas räkning.

10 En rättslig ram

10.1 Grundläggande krav på domstolarnas personuppgiftsbehandling

Förslag: Domstolsdatalagen ska hänvisa till 9 § PUL om grundläggande krav avseende personuppgiftsbehandling.

Dessa krav innebär bl.a. att de behandlingar som utförs måste vara lagliga, att behandlingarna sker på ett korrekt sätt och i enlighet med god sed samt att uppgifterna som behandlas ska vara nödvändiga, adekvata, relevanta och riktiga.

Vidare ska personuppgifter endast få samlas in för särskilda och uttryckligt angivna ändamål. Insamlade personuppgifter ska inte få vidarebehandlas för ett ändamål som är oförenligt med det för vilket uppgifterna samlades in.

Skälen för förslaget: I personuppgiftslagen slås fast grundläggande krav på all behandling av personuppgifter. Syftet är att behandlingar som på ett otillbörligt sätt kränker den personliga integriteten inte ska få förekomma. Kraven riktar sig mot den personuppgiftsansvarige, som ska se till att personuppgifter endast behandlas om det är lagligt och att personuppgifter alltid ska behandlas på ett korrekt sätt och i enlighet med god sed (9 § första stycket a och b PUL). Den personuppgiftsansvarige ska vidare se till att de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen, att fler personuppgifter än som är nödvändigt inte behandlas, att de personuppgifter som behandlas är riktiga och om nödvändigt

aktuella, samt att alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen (9 § första stycket e–h PUL). Motsvararande krav återfinns i dataskyddsdirektivet (artikel 6).

Dessa bestämmelser ska redan enligt nuvarande ordning tillämpas i domstolarnas verksamhet. De flesta av kraven som uppställs är allmängiltiga och av grundläggande betydelse ur integritetssäkerhetssynpunkt, vilket talar för att de bör gälla i domstolarnas verksamhet. Dessutom har bestämmelserna sin grund i de tvingande krav som följer av dataskyddsdirektivet. Det bör av dessa skäl tas in en hänvisning till bestämmelserna i domstolsdatalagen. I avsnitt 17.1 berörs frågan vad skyldigheten att rätta, blockera och utplåna kan innebära i domstolarnas verksamhet.

En annan grundläggande förutsättning för personuppgiftsbehandling enligt personuppgiftslagen är att personuppgifter får samlas in endast för särskilda och uttryckligt angivna ändamål (9 § första stycket c PUL). Enligt gällande rätt är bestämmelsen även tillämplig i domstolarnas rättskipande och rättsvårdande verksamhet. Bestämmelsen har tillkommit för att tillgodose de krav som följer av dataskyddsdirektivet (artikel 6.1 b). Den innebär bl.a. att uppgifter inte får samlas in utan att det finns en tydlig anledning till att insamlandet sker.

Dessa krav på personuppgiftsbehandlingen riktar sig mot den personuppgiftsansvarige. Att kraven ska gälla även i domstolarnas dömande verksamhet är självklart. Den insamling av personuppgifter som domstolarna normalt företar under handläggning av mål och ärenden får också anses leva upp till de aktuella kraven, eftersom insamlandet av uppgifter för domstolarnas del styrs av andra bestämmelser, såsom rättegångsbalken, förvaltningsprocesslagen samt andra handläggnings- och förfaranderegler. Av dessa regelverk framgår i huvudsak i vilka fall och under vilka förutsättningar uppgifter ska tillföras verksamheten vid handläggning av mål och ärenden. På så sätt tydliggörs det för vilka ändamål som personuppgifter samlas in. När en dom-

stol samlar in uppgifter är det i det enskilda fallet dessutom oftast uppenbart för vilket ändamål uppgifterna samlas in. Av ett föreläggande om att komma in med uppgifter framgår det exempelvis varför domstolen efterfrågar uppgifterna. För att det inte ska råda någon tvekan om att kraven i direktivet avseende insamlande av personuppgifter uppfylls bör det i domstolsdatalagen tas in en hänvisning till bestämmelsen i personuppgiftslagen.

En annan grundläggande förutsättning enligt personuppgiftslagen är att personuppgifter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (9 § första stycket d PUL). Detta brukar kallas *finalitetsprincipen*. Även denna bestämmelse har tillkommit för att tillgodose de krav som följer av dataskyddsdirektivet (artikel 6.1 b). Den innebär att det uppställs en begränsning i fråga om vidarebehandling av uppgifter som redan finns insamlade i verksamheten. Finalitetsprincipen är enligt gällande rätt tillämplig vid personuppgiftsbehandlingen i domstolarna. Det saknas skäl för att inte låta finalitetsprincipen gälla även fortsättningsvis inom domstolarna. Detta bör i likhet med polisdatalagen och kustbevakningsdatalagen komma till uttryck genom en hänvisning till den aktuella bestämmelsen i personuppgiftslagen.

I 9 § andra stycket PUL anges att behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål generellt inte ska anses strida mot finalitetsprincipen. Detta förtydligande av finalitetsprincipens innebörd bör domstolsdatalagen också hänvisa till.

10.2 Verksamhetsspecifika ändamålsbestämmelser

Förslag: Personuppgifter i domstolarnas rättskipande och rättsvårdande verksamhet ska få behandlas om det behövs för handläggning av mål och ärenden.

Personuppgifter som behandlas på denna grund ska även få vidarebehandlas om det behövs för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning.

Skälen för förslaget

Inledning

Genom att domstolsdatalagen föreslås hänvisa till 9 § första stycket c och d PUL kommer en generell ram att gälla för hur personuppgifter får samlas in respektive vidarebehandlas. Fråga är om det i domstolsdatalagen dessutom bör föreskrivas en snävare och verksamhetsanpassad ram för den personuppgiftsbehandling som sker med stöd av lagen. Sådana bestämmelser finns ofta i registerförfattningar i form av så kallade ändamålsbestämmelser. Genom verksamhetsspecifika ändamålsbestämmelser slås det fast vilka ändamål som domstolarna ska kunna behandla personuppgifter för. Det innebär för det första att domstolen eller de anställda inte själva kan besluta fritt om vilka ändamål som personuppgifter behandlas för i verksamheten. För det andra blir det genom sådana verksamhetsspecifika ändamålsbestämmelser tydligt vilka åtgärder som är tillåtna respektive otillåtna. För att åstadkomma ett starkt integritetsskydd bör det införas sådana ändamålsbestämmelser även i domstolsdatalagen.

Primära och sekundära ändamål

Det är vanligt att i registerförfattningar dela upp ändamålen i primära och sekundära. Bestämmelserna om *primära ändamål*

utformas för att tillgodose behoven av att behandla personuppgifter i de berörda myndigheternas egen verksamhet. Registerförfattningarna brukar innehålla ändamålsbestämmelser som innebär att uppgifter inte får samlas in för annat än primära ändamål. Begreppet insamling får anses avse inte bara situationer då uppgifter lämnas till en myndighet på begäran av myndigheten, utan även andra tillvägagångssätt genom vilka myndigheten får del av personuppgifter för sådan behandling som omfattas av författningen (jfr Öman och Lindblom Personuppgiftslagen, en kommentar, 4 uppl., s. 374). Bestämmelser om primära ändamål medger dock både behandling som består av insamling och av vidarebehandling, t.ex. genom bearbetning, lagring, utlämnande, arkivering osv.

Bestämmelser om *sekundära ändamål* kompletterar bestämmelserna om primära ändamål och tillgodoser i första hand andra än verksamhetens egna behov. Dessa bestämmelser medger inte insamling, utan tillåter endast att uppgifter som redan behandlas i verksamheten får behandlas för nya ändamål. Genom att lagtekniskt skilja på behandlingar för primära och sekundära ändamål blir det möjligt att ge ändamålsbestämmelserna en mer specifik innebörd utan att bestämmelserna för den skull behöver bli för detaljerade eller oflexibla. Bestämmelserna i domstolsdatalagen bör utformas utifrån denna distinktion.

Handläggning av mål och ärenden

Som föreslås i avsnitt 7.2 ska domstolsdatalagen gälla för den rättskipande och rättsvårdande verksamheten, vilket får sägas utgöra domstolarnas kärnverksamhet. Domstolarna behöver samla in och vidarebehandla personuppgifter i de fall då handläggningen av mål och ärenden kräver det. I jämförelse med exempelvis polisen styrs domstolarnas berättigade behov av att samla in personuppgifter i hög grad av andra regelverk än personuppgiftsregleringen, nämligen av processlagarna och tillhörande regler och principer. Vilka uppgifter som domstolarna

ska samla in i mål och ärenden och hur de fortsatt ska hanteras inom ramen för handläggning av mål och ärenden är frågor som av principiella skäl inte bör styras av personuppgiftsregleringen utan av processrätten. Detta gör att det varken är möjligt eller lämpligt att i domstolsdatalagen i detalj ange för vilka ändamål personuppgifter ska få samlas in och vidarebehandlas.

Den verksamhet som ska regleras – domstolarnas rättskipande och rättsvårdande verksamhet – är i flera avseenden föränderlig. Domstolarnas yttre och inre organisation samt arbetssätt kommer även fortsättningsvis att utvecklas i olika hänseenden och nya måltyper tillföras verksamheten allt eftersom. Redan nu handlägger domstolarna över 500 olika mål- och ärendetyper av skilda slag. Utvecklingen inom dator- och informationsteknologin fortgår också i snabb takt. Allt detta påverkar på vilka sätt personuppgifter kommer att behandlas inom domstolarna och vid deras kommunikation med varandra, med andra myndigheter och med allmänheten. Den reglering som nu föreslås bör vara utformad på ett sådant sätt att den ger domstolarna möjlighet att utnyttja de fördelar som tekniken erbjuder samt att den inte hindrar domstolarna från att utveckla sina arbetssätt och sin organisation. Regleringen bör dels avgränsa sådan behandling som ska vara tillåten, dels förhindra sådan behandling som inte är motiverad av verksamhetsbehov.

Mot den angivna bakgrunden bör det i domstolsdatalagen anges att domstolarna får behandla (dvs. samla in eller vidarebehandla) personuppgifter om det behövs för handläggning av mål och ärenden. Det saknas skäl att tillåta insamlande av personuppgifter för några andra ändamål och den nu föreslagna bestämmelsen innebär således en uttömmande reglering av de primära ändamål för vilka personuppgifter får behandlas i domstolarnas rättskipande och rättsvårdande verksamhet. Ändamålsregleringen innebär att den styrning av domstolarnas verksamhet som följer av processrätten får genomslag även i personuppgiftshänseende. Genom ändamålsbestämmelsen förhindras obefogade personuppgiftsbehandlingar.

Planering, uppföljning och utvärdering

Domstolarna har som de flesta myndigheter ett behov av att vidarebehandla insamlade uppgifter för *planering, uppföljning och utvärdering*. Det kan t.ex. röra sig om framställning av statistik med hjälp av uppgifter från målhanteringssystemet. I lagrådsremissen Behandling av uppgifter i Tullverkets brottsbekämpande verksamhet år 2005 föreslog regeringen en uttrycklig bestämmelse om att uppgifter som behandlas för något av de enligt lagförslaget tillåtna primära ändamålen även skulle få behandlas för att planera, följa upp och utvärdera verksamheten. Lagrådet framhöll emellertid vid sin granskning av lagförslaget att planering, uppföljning och utvärdering är en integrerad del av själva verksamheten. Enligt Lagrådet var det självklart att uppgifter som får användas i verksamheten också får användas för planering m.m. och att lagen inte borde innehålla någon uttrycklig ändamålsbestämmelse avseende denna typ av åtgärder. Regeringen delade Lagrådets bedömning i denna del (se prop. 2004/05:164 s. 66 f. och 162 samt prop. 2009/10:85 s. 116).

Samma synsätt kan anläggas på den personuppgiftsbehandling som behöver ske vid en domstol för planering, uppföljning och utvärdering av domstolens egen verksamhet, t.ex. för framställning av statistik över verksamheten. Med hänsyn härtill behöver det i domstolsdatalagen inte införas någon särskild bestämmelse om behandling som behövs för planering, uppföljning och utvärdering av den rättskipande och rättsvårdande verksamheten.

Uppgiftslämnande

Domstolarna behöver i många olika sammanhang tillhandahålla information till myndigheter, till andra utomstående eller internt inom domstolen. En allt större del av domstolarnas uppgiftshantering datoriseras och genom RIF-samarbetet utvecklas informationsflödena mellan rättskedjans olika myndigheter. När

personuppgifter ska lämnas behöver därför domstolarna i allt större utsträckning ta fram dessa uppgifter från sina datorsystem, vare sig uppgifterna ska lämnas ut i fysisk form eller elektroniskt. I båda fallen innebär framtagandet automatiserad behandling av personuppgifter. Det som beskrivs är sekundära ändamål, eftersom behandlingarna endast avser redan insamlade uppgifter.

De utlämnanden som behöver ske i anslutning till handläggningen av mål och ärenden, t.ex. kommunicering med parterna, kallelser osv. täcks av den ovan föreslagna ändamålsbestämmelsen som gäller handläggning av mål och ärenden. Därutöver finns det en rad situationer då domstolen behöver kunna behandla personuppgifter automatiserat för att lämna uppgifter till andra, och för vilka det behövs en regel som uttryckligen tillåter behandling för sådana ändamål.

För det första är domstolarna enligt bestämmelser i olika författningar skyldiga att lämna uppgifter till utpekade myndigheter, t.ex. uppgifter om brottmålsdomar till Rikspolisstyrelsen eller om domar i upphandlingsmål till Konkurrensverket. Genom de reformer som följer av RIF-samarbetet kommer en del av denna hantering att bli helt automatiserad.

För det andra är domstolarna enligt lag eller förordning skyldiga att på begäran lämna ut uppgifter. Domstolarna är t.ex. enligt offentlighetsprincipen skyldiga att lämna ut allmänna handlingar, vilket kommer till uttryck i 2 kap. TF. Vidare följer av 6 kap. 5 § OSL en skyldighet att på begäran av en annan myndighet lämna uppgifter som domstolen förfogar över under förutsättning att uppgifterna inte är sekretessbelagda och att det inte skulle hindra arbetets behöriga gång.[1]

För det tredje bör de situationer beaktas i vilka det inte finns någon skyldighet att lämna uppgifter men där det ändå kan anses påbjudet eller önskvärt att en domstol lämnar uppgifter till andra

[1] Vad gäller utlämnande till myndigheter finns det generella sekretessbrytande bestämmelser i 10 kap. 27 och 28 §§ OSL, samt, såvitt gäller utlämnande till riksdagen eller regeringen, i 10 kap. 15 § samma lag.

domstolar, myndigheter eller andra utomstående. Det kan t.ex. vara fråga om en åtgärd som vidtas för att fullgöra service-skyldigheten gentemot enskilda enligt 4 § förvaltningslagen eller skyldigheten att hjälpa andra myndigheter enligt 6 § samma lag.

För det fjärde kan en domstol behöva lämna personuppgifter internt, exempelvis till den administrativa verksamheten som omfattas av personuppgiftslagen. Det kan exempelvis röra sig om rapportering av nämndemäns eller särskilda ledamöters tjänstgöring i syfte att administrationen ska kunna betala ut ersättning.

Gemensamt för samtliga fall av uppgiftslämnande som beskrivs ovan är att de sker med stöd av bestämmelser som påbjuder eller tillåter utlämnande. Regeringen har i ett tidigare lagstiftningsärende (prop. 2007/08:126 s. 60) anfört följande rörande huvudsakligen likalydande bestämmelser:

> När sådana bestämmelser har införts, får det förutsättas att det har gjorts en avvägning mellan intresset av att uppgiften lämnas ut och intresset av att skydda enskilda personers integritet, vid vilken man funnit att uppgiften ska eller får lämnas ut. Det saknas därför anledning att i en integritetsskyddslagstiftning, som den föreslagna patientdatalagen, förhindra att personuppgifter som finns i hälso- och sjukvården lämnas ut i dessa fall bara därför att dessa numera hanteras med modern informationsteknik i stället för som tidigare på papper.

Det framstår som naturligt att göra samma bedömning i fråga om personuppgiftsbehandlingen i domstolarnas rättskipande och rättsvårdande verksamhet. Utvecklingen går mot att allt fler uppgifter lagras elektroniskt och att elektroniskt utlämnande tillåts i större utsträckning. Exempelvis har E-offentlighets-kommittén i sitt slutbetänkande föreslagit att myndigheter ska lämna ut elektroniskt lagrade handlingar i elektronisk form om det inte är olämpligt (SOU 2010:4). Beträffande utlämnande mellan myndigheter som är tillåtet enligt offentlighets- och sekretesslagen har regeringen tagit ställning för att det inte bör införas ändamålsbestämmelser som begränsar utlämnande av

allmänna handlingar i större utsträckning än vad som följer av finalitetsprincipen (dir. 2011:86).

Mot den angivna bakgrunden bör en utgångspunkt vara att personuppgifter ska kunna behandlas för uppgiftslämnande i alla de ovan beskrivna fallen. Förebilder för en sådan reglering finns exempelvis i polisdatalagen och patientdatalagen. Polisdatalagen innehåller en förhållandevis detaljerad reglering rörande vidarebehandling för uppgiftslämnande (2 kap. 8 §), men regleringen är inte uttömmande. Personuppgifter får nämligen i ett enskilt fall behandlas för att tillhandahålla information för ytterligare ändamål under förutsättning att detta är förenligt med finalitetsprincipen. I patientdatalagen anges mer generellt att personuppgifter som behandlas för ett primärt ändamål också får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning (2 kap. 5 §).

Som redovisas ovan styrs domstolarnas uppgiftsutlämnande av flera andra regelverk med mer eller mindre detaljerade bestämmelser om utlämnande. För att undvika dubbelreglering är det därför lämpligast att i domstolsdatalagen, i likhet med patientdatalagen, införa en generellt formulerad ändamålsbestämmelse avseende uppgiftslämnande. Det bör således föreslås en ändamålsbestämmelse med innebörden att uppgifter som behandlas för ett primärt ändamål, också får behandlas för uppgiftslämnande som sker i enlighet med gällande lagar och förordningar. Finalitetsprincipen (9 § första stycket d PUL) gäller dock som en yttersta begränsning beträffande vilka nya ändamål domstolarna får behandla personuppgifter för.

Övervägandena i detta avsnitt avser frågan i vilken utsträckning personuppgifter bör få behandlas för att uppgiftslämnande ska kunna ske, oavsett om behandlingen leder till att personuppgifter skrivs ut på ett papper som lämnas ut i fysisk form eller om uppgiftslämnandet fullföljs genom utlämnande i elektroniskt format, exempelvis genom ett e-postmeddelande. I vilken utsträckning utlämnande i elektroniskt format bör vara tillåtet övervägs särskilt i avsnitt 14.

Sökning efter domar och beslut m.m.

Frågan är om det finns behov av att vidarebehandla uppgifter för ytterligare ändamål. Som redovisas i avsnitt 13.1 behöver domstolarna söka efter tidigare avgöranden för att kunna bedriva verksamheten så effektivt och så rättssäkert som möjligt. Domstolarna behöver också kunna söka efter avgöranden för att gå allmänheten och andra myndigheter till mötes. Att kunna identifiera och ta fram avgöranden är viktigt för offentligheten och insynen i domstolarnas verksamhet. Domstolsdatalagen föreslog att återsökning av vägledande avgöranden i lag skulle anges som ett särskilt ändamål (SOU 2001:100 s. 111 f.).

Det övervägs i avsnitt 13 under vilka förutsättning och i vilken utsträckning som olika typer av sökningar bör tillåtas. Någon särskild ändamålsbestämmelse som tar sikte på sökning bedöms dock inte behövas i domstolsdatalagen, eftersom de befogade sökningar som behöver ske kan utföras med stöd av de föreslagna ändamålsbestämmelserna som tillåter behandlingar som behövs för handläggning av mål och ärenden samt för uppgiftslämnande som sker i överensstämmelse med lag eller förordning.

11 Säkerhet och intern åtkomst

11.1 Säkerheten vid behandling

Förslag: Domstolsdatalagen ska hänvisa till föreskrifterna i 30 och 31 §§ PUL som gäller säkerheten vid personuppgiftsbehandling.

Skälen för förslaget: I takt med att domstolarna utvecklar nya it-lösningar måste domstolarna tillsammans med Domstolsverket också utveckla rutinerna för dataskydd och säkerheten vid behandlingen. Om allmänheten ska ha förtroende för den informationsbehandling som sker inom domstolarna krävs det nämligen inte bara en modern lagstiftning. Domstolarna måste också aktivt verka för att den tillämpas på avsett sätt. Detta gäller både vid byggandet av nya datorsystem, vid förvaltningen av befintliga system och vid den dagliga användningen av datorsystemen. Domstolarna bör följa upp att lagstiftningen tillämpas med respekt för enskildas integritet. Det måste också finnas en god säkerhet mot externa försök att komma åt eller påverka informationen. En viktig och allt vanligare del av personuppgiftsbehandlingen utgörs av elektronisk kommunikation, t.ex. e-posthantering, där särskilda säkerhetsåtgärder behöver vidtas när känsliga personuppgifter överförs (se Datainspektionens beslut 2006-12-06, dnr 1082-2006).

Ju mer omfattande ett informationssystem är och ju känsligare uppgifter det innehåller, desto viktigare är det att det finns olika behörighetsnivåer för skilda kategorier av uppgifter

och användare. Domstolsdatalagen kommer att ställa större krav än tidigare på att domstolarna genom tekniska åtgärder och på andra sätt begränsar tillgången för varje anställd till sådan information som han eller hon behöver för att fullgöra sina arbetsuppgifter (se avsnitt 11.2).

Tekniska åtgärder är emellertid bara en del av säkerheten. En annan viktig säkerhetsaspekt är domstolens instruktioner till sina anställda rörande hanteringen av personuppgifter samt de anställdas medvetenhet om frågor som rör dataskydd och informationssäkerhet. Domstolarna måste tillsammans med Domstolsverket försäkra sig om att personalen får tillräcklig utbildning rörande dessa frågor.

I 30 och 31 §§ PUL finns regler om hur den personuppgiftsansvarige ska organisera arbetet med behandling av personuppgifter för att garantera säkerheten. Den personuppgiftsansvarige ska bl.a. ge instruktioner till personalen om hur personuppgifter får behandlas. Vidare ska den personuppgiftsansvarige genom tekniska och organisatoriska åtgärder se till att personuppgifter skyddas och att det åstadkoms en säkerhetsnivå som är lämplig med hänsyn till tillgänglig teknik, kostnader, särskilda risker och uppgifternas känslighet.

Bestämmelserna i 30 och 31 §§ PUL ger uttryck för viktiga och allmängiltiga datorsäkerhetsprinciper, vilka bör gälla i domstolarnas rättskipande och rättsvårdande verksamhet. Det bör därför tas in en hänvisning till dessa bestämmelser i domstolsdatalagen. I avsnitt 16.3 föreslås vidare att domstolsdatalagen ska hänvisa till 32 § PUL, vilket innebär att Datainspektionen i enskilda fall ska kunna besluta om vilka säkerhetsåtgärder som domstolarna ska vidta enligt 31 § PUL. I andra lagstiftningsärenden har regeringen konstaterat att närmare riktlinjer för informationssäkerhetsarbetet inte bör ges i lag utan vid behov bör ges på lägre föreskriftsnivå (prop. 2007/08:126 s. 149 och prop. 2009/10:85 s. 271). Det bör mot den bakgrunden inte införas några särskilda bestämmelser om informationssäkerhet i domstolsdatalagen, utöver personuppgiftslagens regler om säkerheten vid behandlingen.

11.2 Tillgång till personuppgifter

Förslag: Tillgången till personuppgifter i domstolarna ska begränsas till vad varje anställd behöver för att fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om tillgången till personuppgifter.

Skälen för förslaget: Vem som har rätt att använda elektroniskt lagrade uppgifter och hur de sprids är omständigheter som påverkar risken för intrång i den personliga integriteten. Riskerna för integritetsintrång när allmänheten får tillgång till sådana uppgifter övervägs särskilt i avsnitten om sökning och om elektroniskt utlämnande (avsnitt 13 och 14). Otillbörliga intrång i den personliga integriteten kan även orsakas av att någon som är anställd vid en domstol bereder sig tillgång till elektroniskt lagrad information. Det bör därför säkerställas att tillgången till personuppgifter i så stor utsträckning som möjligt begränsas till vad var och en behöver för att fullgöra sitt arbete.

I 9 § första stycket a PUL anges att den personuppgiftsansvarige ska se till att personuppgifter behandlas bara om det är lagligt. Det föreskrivs vidare i 31 § samma lag att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna, och hur pass känsliga de behandlade personuppgifterna är. Det föreslås i avsnitt 10.1 och 11.1 att domstolsdatalagen ska hänvisa till dessa bestämmelser.

Efter ett påpekande från Datainspektionen valde regeringen att i polisdatalagen, utöver de redovisade bestämmelserna i personuppgiftslagen, föreslå en uttrycklig bestämmelse om att

tillgången till personuppgifter alltid ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter. För att åstadkomma ett allsidigt och starkt integritetsskydd i domstolarna bör en motsvarande regel tas in i domstolsdatalagen.

Innebörden av hänvisningen till 9 och 31 §§ PUL är bl.a. att domstolarna bör använda de tekniska möjligheter som finns för att hjälpa de anställda att efterleva kraven och begränsningarna som domstolsdatalagen uppställer. Modern teknik gör det enklare att på ett mer sofistikerat sätt begränsa tillgången till uppgifter som behandlas automatiserat så att var och en kan få tillgång just till de uppgifter de behöver. Tillgången till domsutkast bör exempelvis begränsas till de personer vid domstolen som deltar i handläggningen av det aktuella målet. Det bör vidare finnas möjligheter att kunna spärra användningen av sådana sökbegrepp som inte är tillåtna att använda.

I många fall är frågan om en viss åtgärd får vidtas eller inte något som måste bedömas av användaren i det enskilda fallet. Även i dessa situationer finns det dock tekniska lösningar som kan bidra till att säkerställa lagstiftningens genomslag i praktiken. Datorsystemen kan konstrueras på ett sådant sätt att användaren varnas när han eller hon försöker använda ett sökbegrepp eller vidta någon annan åtgärd som kan vara förbjuden. Om användaren väljer att ändå utföra åtgärden kan det vara lämpligt att låta datorsystemet göra en loggning.

Det är inte lämpligt att i lag ange detaljerade riktlinjer för hur tillgången till personuppgifter bör avgränsas. I stället bör det vara domstolarnas uppgift att med stöd av Domstolsverket, utifrån respektive myndighets organisation och struktur, säkerställa att åtkomsten till personuppgifter begränsas i enlighet med bestämmelsen. Regeringen eller den myndighet som regeringen bestämmer bör också ha möjlighet att meddela närmare föreskrifter om tillgången till personuppgifter (jfr prop. 2009/10:85 s. 95).

12 Känsliga personuppgifter och personnummer

12.1 Känsliga personuppgifter

Förslag: Uppgifter om en person ska inte få behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv (känsliga personuppgifter).

Skälen för förslaget

Nuvarande reglering

Känsliga personuppgifter är uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i en fackförening samt uppgifter som rör hälsa eller sexualliv (13 § PUL). Som utgångspunkt är det enligt såväl dataskyddsdirektivet och personuppgiftslagen som dataskyddsrambeslutet förbjudet att behandla känsliga personuppgifter. Från förbudet att behandla sådana personuppgifter görs undantag för vissa situationer, t.ex. då den enskilde har samtyckt till behandlingen eller om behandlingen är nödvändig på grund av vissa särskilt angivna skäl (se t.ex. 14–20 §§ PUL).

I domstolarna gäller Vera-förordningarna utöver personuppgiftslagen. I dessa förordningar anges att känsliga personupp-

gifter får behandlas automatiserat i löpande text om uppgifterna har lämnats i ett mål eller ärende eller om de behövs för handläggningen av målet eller ärendet. Vidare anges i förordningarna att känsliga personuppgifter får behandlas vid angivande av saken i ett mål eller ärende (ärendemening). Vera-förordningarna innebär således ingen generell begränsning avseende behandling av känsliga personuppgifter.

Rättsliga förutsättningar

Det framgår av dataskyddsdirektivet att ett tillåtet skäl att behandla känsliga personuppgifter är om det bedöms nödvändigt för att kunna fastslå, göra gällande eller försvara rättsliga anspråk (artikel 8.2 e). Motsvarande framgår av personuppgiftslagen (16 c §). Själva behandlingen behöver inte gå ut på att fastställa, göra gällande eller försvara sådana anspråk. Det är tillräckligt att behandlingen är nödvändig för att någon, t.ex. den personuppgiftsansvarige, ska kunna göra detta. Detta skäl för behandling av känsliga personuppgifter återspeglar tydligt den kärnverksamhet som bedrivs i domstolarna och som, vad gäller personuppgiftsbehandlingen, kommer till uttryck i de föreslagna ändamålsbestämmelserna. Utgångspunkten enligt både direktivet och personuppgiftslagen kan således sägas vara att känsliga personuppgifter får behandlas i domstolarnas rättskipande och rättsvårdande verksamhet.

Av dataskyddsrambeslutet följer att Sverige är skyldig att förhindra behandling av känsliga personuppgifter som inte är absolut nödvändig (artikel 6). I rambeslutet finns, till skillnad från dataskyddsdirektivet, inte någon specifikation av situationer i vilka känsliga personuppgifter får behandlas. Rambeslutet lämnar i stället ett utrymme för medlemsstaterna att tolka kravet på absolut nödvändighet. Det får förutsättas att detta generellt formulerade krav inte är avsett att förhindra de nationella domstolarna att utföra behandlingar som behövs för att t.ex. fastslå rättsliga anspråk, i likhet med vad som gäller enligt

dataskyddsdirektivet. Rambeslutet bör med andra ord inte anses medföra någon skyldighet för medlemsstaterna att begränsa domstolarnas möjligheter att behandla känsliga personuppgifter i den utsträckning sådan behandling behöver ske för att de ska kunna fullgöra sina rättskipande och rättsvårdande uppgifter.

Det finns således rättsliga förutsättningar att behandla känsliga personuppgifter i domstolarnas rättskipande och rättsvårdande verksamhet.

Känsliga personuppgifter bör få behandlas i domstolarna

I domstolarna sker en utveckling mot att allt fler uppgifter behandlas automatiserat. Utvecklingen kan för domstolarnas del bl.a. förväntas leda till ökad effektivitet och rättssäkerhet i handläggningen och till förbättrad tillgänglighet för parter och allmänheten.

Känsliga personuppgifter förekommer i många måltyper och i olika sorters handlingar. Det stora flertalet sådana uppgifter som behandlas i domstol härrör från vad parterna anfört i inlagor och vid domstolsförhandlingar, vilket innebär att det ligger utanför domstolarnas kontroll om en viss uppgift förekommer i verksamheten eller inte. För domstolarnas egen del är det i huvudsak fråga om att använda redan inkomna känsliga personuppgifter vid framställning av olika dokument som är nödvändiga för handläggning och avgörande av mål och ärenden. I fråga om formulerande av domskäl har domstolarna i och för sig en möjlighet att påverka i vilken utsträckning känsliga personuppgifter återges eller tillförs texten. Det är dock av principiella skäl inte lämpligt att genom bestämmelser i domstolsdatalagen inskränka domarnas frihet att formulera domskäl i syfte att undvika att känsliga personuppgifter behandlas (jfr även 8 § PUF som anger att myndigheter får behandla känsliga personuppgifter i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av ärendet).

Det finns strängt taget inga skillnader mellan i vilken utsträckning domstolarna behöver behandla känsliga personuppgifter och andra personuppgifter. För att domstolarna ska kunna sköta sin informationshantering elektroniskt måste de också kunna behandla känsliga personuppgifter för att på ett ändamålsenligt sätt vidta de åtgärder som behövs för att handlägga mål och ärenden.

Att domstolarna tillåts behandla känsliga personuppgifter som ett led i handläggningen av mål och ärenden, t.ex. genom elektronisk lagring av partsinlagor, domsskrivning, expediering av domar osv., bedöms typiskt sett inte medföra särskilt stora risker ur integritetshänseende. Domstolarnas hantering av känsliga personuppgifter är i hög grad styrd av de processuella regelverken, vilket innebär att det finns en yttre ram för vad domstolen överhuvudtaget får göra.

Mot den angivna bakgrunden får behovet av att kunna behandla känsliga personuppgifter och de effektivitetsvinster som elektronisk hantering medför anses väga tyngre än den risk för integritetsintrång som en sådan behandling kan innebära. Behandlingen av känsliga personuppgifter bör därför på ett generellt plan endast begränsas genom den rättsliga ram som föreslås i avsnitt 10, vilken bl.a. består av verksamhetsspecifika ändamålsbestämmelser. Detta är i linje med vad som gäller enligt polisdatalagen inom den del av polisens verksamhet där förutsättningarna mest liknar de som gäller i domstolarna, nämligen polisens handläggning av anmälningar (2 kap. 9 § 2 och 10 § andra stycket andra meningen polisdatalagen), och med vad som gäller enligt patientdatalagen[1].

[1] Se prop. 2007/08:126 s. 63 där regeringen gjort bedömningen att behandlingen av känsliga personuppgifter bör styras av de allmänna ändamålsbestämmelserna, eftersom det skulle innebära tillämpningsproblem och försvåra ett rationellt utnyttjande av it inom verksamheten om det i lag närmare måste specificeras vilka känsliga personuppgifter som får behandlas.

Känsliga personuppgifter som enda grund för behandlingen

För att minimera riskerna för att känsliga personuppgifter trots allt missbrukas är det lämpligast att föreslå bestämmelser som direkt tar sikte på att kontrollera och begränsa sådana åtgärder som i integritetshänseende innebär särskilda risker. I avsnitt 13.2 föreslås bestämmelser som begränsar möjligheterna att använda känsliga personuppgifter som sökbegrepp. Därutöver finns det skäl att överväga om det bör förbjudas att känsliga personuppgifter används som enda grund för en behandling.

I polisdatalagen föreskrivs att uppgifter om en person inte får behandlas enbart på grund av vad som är känt i fråga om känsliga personuppgifter. Enligt förarbetena är det på grund av denna bestämmelse bl.a. förbjudet att föra register över eller på annat sätt göra anteckningar om enskilda enbart på den grunden att de utifrån etniskt ursprung, hälsa eller något annat i bestämmelsen angivet förhållande kan hänföras till en viss kategori av människor (prop. 2009/10:85 s. 325).

För domstolarna skulle en motsvarande bestämmelse ha en mer begränsad betydelse än vad den har inom polisen. Det beror på att domstolarna på grund av de processuella regelverken och de föreslagna ändamålsbestämmelserna, knappt torde ha något utrymme att registrera en uppgift om en person enbart på grund av vad som är känt i fråga om dennes etniska ursprung, hälsotillstånd, sexuella läggning eller liknande. Däremot kan en sådan bestämmelse ha betydelse för domstolarna i fråga om hur uppgifter får kategoriseras eller märkas i domstolarnas datorsystem.

Om det även i domstolsdatalagen införs en bestämmelse om att en uppgift om person inte får behandlas enbart på grund av vad som är känt i fråga om känsliga personuppgifter skulle det exempelvis bli otillåtet att vid en förvaltningsdomstol upprätta ett särskilt register över samtliga socialförsäkringsmål på grundval av vilken sjukdomsdiagnos som är aktuell i respektive mål. Det skulle också innebära ett förbud mot att i verksamhetsstödet Vera kategorisera en uppgift som en känslig personuppgift av visst slag, t.ex. att kategorisera ordet ”hindu” som en uppgift om

religiös övertygelse eller ”heterosexuell” som en uppgift om sexuell läggning. Det skulle således bli otillåtet att i verksamhetsstödet konstruera ett särskilt fält med benämningen ”religiös övertygelse” eller ”sexuell läggning”, i vilket domstolspersonal kunde fylla i relevanta uppgifter.

Att kategorisera eller märka de personuppgifter som finns hos domstolarna på sätt som beskrivs här innebär att uppgiftssamlingarna blir mer integritetskänsliga, eftersom sådan strukturering underlättar för den som vill göra en sammanställning utifrån känsliga personuppgifter. Samtidigt bedöms det inte finnas något påtagligt behov av att kunna behandla uppgifter om en person enbart på grund av vad som är känt i fråga om känsliga personuppgifter. Av dessa skäl bör det i domstolsdatalagen finnas en bestämmelse som hindrar sådan behandling.

Användningen av begreppet ras

I direktivet och rambeslutet, liksom i personuppgiftslagen och flertalet registerförfattningar, räknas som känslig personuppgift bl.a. ”uppgifter som avslöjar ras eller etniskt ursprung”. Användningen av begreppet ras har varit föremål för diskussioner i olika sammanhang. Enligt EU:s officiella ståndpunkt[2] bör begreppet ras undvikas i alla offentliga texter. Ståndpunkten har dock inte iakttagits konsekvent i de av EU antagna rättsakterna. Riksdagen har uttalat att det inte finns någon vetenskaplig grund för att dela in människor i skilda raser och ur biologisk synpunkt följaktligen heller ingen grund för att använda ordet ras om människor. Användningen av ordet ras i författningstexter riskerar enligt riksdagen att underblåsa fördomar (jfr även prop. 2007/08:95 s. 117 f.). I regeringsformen har sedan den 1 januari 2011 begreppet ras utmönstrats och i stället används uttrycket ”etniskt ursprung, hudfärg eller annat liknande förhållande”

[2] EGT C 152, 27.05.199 , s. 57.

(2 kap. 12 och 14 §§ RF samt prop. 2009/10:80 s. 152). Regeringen har dock ansett att begreppet, trots ändringen i regeringsformen, inte bör utmönstras endast i vissa registerförfattningar och därmed rubba den vedertagna beskrivningen av känsliga personuppgifter som finns bl.a. i personuppgiftslagen. Regeringen har i stället för avsikt att i ett annat sammanhang överväga frågan om begreppet ska utmönstras ur all lagstiftning (prop. 2011/12:45 s. 94). Av detta skäl används begreppet även i förslaget till ny domstolsdatalag.

12.2 Personnummer

Bedömning: Ingen särskild begränsning bör gälla för behandling av personnummer.

Skälen för bedömningen: I dataskyddsdirektivet anges att medlemsstaterna ska bestämma på vilka villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas (artikel 8.7). Direktivet innebär alltså att det måste finnas en reglering som gäller för behandling av personnummer. Däremot ställer direktivet inte något krav på hur denna reglering ska se ut.

Vid personuppgiftslagens införande valde lagstiftaren att i princip oförändrat föra över reglerna om användning av personnummer i den dåvarande datalagen (1973:289) till den nya lagen (prop. 1997/98:44 s. 76 f.). Därmed gäller fortfarande att personnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av säker identifiering eller något annat beaktansvärt skäl (22 §). Denna bestämmelse i personuppgiftslagen gäller numera också sådant samordningsnummer som i stället för personnummer tilldelas personer som inte är eller har varit folkbokförda här i landet. I Vera-förordningarna finns bestämmelser om att bl.a. parters, ställföreträdares och vittnens personnummer får

finnas i domstolarnas verksamhetsstöd (se bilagan till respektive förordning).

Allmänt sett kan behandling av personnummer i sig innebära vissa integritetsrisker eftersom varje personnummer är unikt för en person och eftersom personnumren används för att registrera information om enskilda i många, vitt skilda sammanhang. Samtidigt innebär just det faktum att personnumret är unikt att risken för felaktigheter minskar om de personuppgifter som behandlas knyts till personnummer. Personnummer kan således också vara integritetsfrämjande.

Med hänsyn till de långtgående rättsverkningar för enskilda som normalt är förknippade med domstolarnas verksamhet måste domstolarna kunna säkerställa inblandade personers identitet på ett så entydigt sätt som möjligt. Vid behandling av personuppgifter i den rättskipande och rättsvårdande verksamheten är det av rättssäkerhetsskäl därför nödvändigt att använda personnummer för att kunna eliminera risken för fel vid behandlingen av uppgifter om enskilda vid handläggningen och inte minst avgörandet av mål och ärenden.

Som föreslås i avsnitt 10.2 ska uppgifter få behandlas endast om det behövs för handläggningen av mål och ärenden eller för att fullgöra författningsenligt uppgiftslämnande. Detta i sig utesluter att personnummer används slentrianmässigt, t.ex. när det inte finns någon risk för förväxling mellan personer.

Domstolarna bör därför få använda personnummer vid den behandling som är tillåten enligt domstolsdatalagen. Någon särskild bestämmelse om detta är inte nödvändig

13 Sökning

13.1 Sökning – ett nödvändigt verktyg

Bedömning: Sökning bland personuppgifter bör som utgångspunkt vara tillåten i domstolarna.

Skälen för bedömningen

Allmänt om sökning

Med sökning avses en åtgärd genom vilken ett urval uppgifter tas fram ur en samlad informationsmängd enligt vissa kriterier, s.k. sökbegrepp.[1] Det urval som tas fram, dvs. sökresultatet, kan bestå av alltifrån enstaka uppgifter (t.ex. ett namn) eller dokument (t.ex. en dom) till en sammanställning av uppgifter eller dokument.

Sökning är en form av behandling, och i de fall en sökning innefattar personuppgifter innebär sökning därför en personuppgiftsbehandling. Sökningar får således endast ske i enlighet med de allmänna begränsningar som gäller för sådan behandling, t.ex. ändamålsbestämmelserna. Sökning är ett speciellt och kraftfullt verktyg som kan medföra integritetsrisker (jfr avsnitt 13.2). Av den anledningen förekommer i många registerförfattningar särskilda begränsningar av vilka sökbegrepp som

[1] Sökbegrepp har i förarbetena till patientdatalagen beskrivits som ”bokstäver, koder eller siffror med vilkas hjälp man, tillsammans med en sökmotor eller liknande funktion, kan ta fram ett önskat urval lagrade personuppgifter om en eller flera personer ur en samlad informationsmängd (prop. 2007/08:126 s. 68).

får användas och vilka sökningar som får utföras i en myndighets datorsystem. Genom sådana begränsningar kan ett ökat integritetsskydd uppnås. Samtidigt kan det innebära att datasystemets användbarhet inte kan utnyttjas till fullo.

Behov av att kunna söka

I domstolarnas verksamhet finns det ett behov av att på ett effektivt sätt kunna ta fram relevant information och därmed ett behov av att kunna söka bland de uppgifter som finns i datorsystemen. Genom sökning i partsinlagor och andra handlingar som lagras elektroniskt är det möjligt att snabbt hitta alla ställen i processmaterialet där en viss fråga berörs. Detta underlättar för den som behöver orientera sig i den tillgängliga utredningen. Dessa typer av sökningar är särskilt värdefulla i mål med omfattande utredning, t.ex. vissa skattemål, el- och telemål samt mål rörande ekonomisk brottslighet.

Vidare är möjligheten att söka mycket värdefull för att kunna planera och organisera domstolsarbetet på ett effektivt och ändamålsenligt sätt. Mål som lämpligen handläggs vid samma tillfälle, av samma beredningsorganisation eller av samma domare kan med hjälp av sökningar identifieras och föras samman. Domstolarna behöver också söka bland elektronisk lagrad information för att kontrollera att samma fråga inte prövas flera gånger. Detta kan ske genom sökning efter pågående och avgjorda mål i vilka en viss person eller en viss frågeställning förekommer (s.k. konferering). Vidare behöver sökning ske för att hitta relevanta adressuppgifter m.m. att användas vid delgivning.

En viktig aspekt av rättsäkerhet är att lika fall behandlas lika. Sökningar behövs för att domstolarna ska kunna identifiera och ta fram tidigare avgöranden som rör samma eller liknande frågeställningar som de i ett pågående mål. Därigenom kan bedömningar av rättsfrågor i tidigare avgöranden återfinnas, och rättsutredningar från avgjorda mål återanvändas. Om en domare t.ex. ställs inför en ovanlig måltyp eller ett mål som innehåller

sällsynta rättsfrågor har han eller hon behov att kunna genom sökfunktioner identifiera avgöranden. Den enhetliga rättstillämpningen underlättas därför om domstolarnas personal snabbt och effektivt kan söka bland tidigare domar och beslut som lagras elektroniskt.

Slutligen har sökningar betydelse för domstolarnas möjlighet att på olika sätt bistå allmänheten och att uppfylla sin serviceskyldighet. Genom att söka bland mål och ärenden kan domstolspersonalen ge snabbare och bättre service till parter men även till allmänheten, t.ex. journalister, som vänder sig till domstolen och begär att med stöd av offentlighetsprincipen få upplysningar om eller ta del av allmänna handlingar som förvaras hos domstolen. Den som t.ex. undrar i vilka mål ett visst företag förekommer kan snabbt få svar. Likaså kan snabb hjälp erbjudas den som vill veta vilka mål som t.ex. berör en viss fastighet eller en viss upphandling.

Sammanfattningsvis är sökning bland elektroniskt lagrade uppgifter ett praktiskt verktyg som domstolarna har ett stort och frekvent behov av att kunna använda i skiftande situationer. Efter hand som allt fler uppgifter lagras elektroniskt i domstolarna blir sökfunktionernas betydelse dessutom större.

Som anförs i avsnitt 6.2 bör domstolsdatalagen ta sin utgångspunkt i att personuppgiftsbehandling inom vissa angivna ramar är tillåten och att de överväganden som görs i första hand därför bör ta sikte på vilka former av behandling som bör begränsas eller inte tillåtas alls. I linje härmed, och mot bakgrund av de ovan redovisade behoven av att kunna använda sökfunktioner, bör sökning som utgångspunkt vara tillåtet i domstolarnas rättskipande och rättsvårdande verksamhet.

13.2 Begränsningar avseende integritetskänsliga sökbegrepp

Förslag: Uppgift som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i en fackförening liksom uppgifter som rör hälsa eller sexualliv (känsliga personuppgifter) samt uppgift som avslöjar nationell anknytning ska få användas som sökbegrepp endast vid sökning bland uppgifter hos allmän förvaltningsdomstol.

Uppgift som avslöjar brott eller misstanke om brott ska få användas som sökbegrepp endast vid sökning endast bland uppgifter hos allmän domstol.

Sökning med hjälp av ovan angivna sökbegrepp ska få ske endast om det är absolut nödvändigt för handläggning av mål och ärenden.

Skälen för förslaget

Integritetskänsliga sökningar

Genom sökningar är det möjligt att utifrån ett eller flera sökbegrepp på ett ögonblick sila fram ett väldefinierat urval av uppgifter ur en stor mängd information, som annars skulle vara oöverblickbar. Ju större mängd information sökningen sker i, desto mer kraftfullt blir ett sådant sökverktyg. Detta är ett viktigt skäl till att sökning är ett så användbart verktyg för domstolarna i det dagliga arbetet. Hur stora integritetsriskerna är med ett sådant urval styrs till stor del av vilka sökbegrepp som används. Vissa sökbegrepp medför särskilda risker i integritetshänseende.

Sökbegrepp som avser känsliga personuppgifter

Enligt Vera-förordningarna är det i fråga om domstolarnas verksamhetsregister inte tillåtet att använda känsliga person-

uppgifter som sökbegrepp. I fråga om uppgifter som behandlas i löpande text vid sidan av eller i anslutning till verksamhetsregistret finns däremot ingen motsvarande begränsning. Med känsliga personuppgifter avses uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i en fackförening samt uppgifter som rör hälsa eller sexualliv. Det är fråga om förhållanden som historiskt sett i olika sammanhang har legat till grund för förföljelse, diskriminering eller andra liknande åtgärder mot enskilda.

Genom en sökning som innefattar känsliga personuppgifter kan det tas fram domar eller andra handlingar i vilka t.ex. en viss sjukdomsdiagnos eller en viss etnisk tillhörighet nämns. På så sätt kan uppgifter om sjukdom eller etnicitet kopplas ihop med enskilda personer. Sådan kartläggning kan beroende på omständigheterna vara svår att försvara med hänsyn till det integritetsintrång som den innebär. Integritetsriskerna blir särskilt tydligt i de fall sökningen förfinas ytterligare genom att den känsliga personuppgiften kombineras med andra, i sig själva harmlösa sökbegrepp, såsom ett postnummer eller en gatuadress.

Sökbegrepp som avslöjar brott eller misstanke om brott

Enligt gällande rätt är det förbjudet att i de allmänna domstolarnas verksamhetsregister använda uppgifter om brottspåföljd, frihetsberövande eller tvångsmedel vid sökningar i verksamhetsstödet (4 § förordningen [2001:639] om registerföring m.m. vid allmänna domstolar med hjälp av automatiserad behandling). I fråga om uppgifter som behandlas i löpande text vid sidan av eller i anslutning till verksamhetsregistret finns däremot ingen motsvarande begränsning. Uppgifter som direkt eller indirekt avser brott anses i många sammanhang vara särskilt skyddsvärda på grund av att de är integritetskänsliga. Ett exempel är Rikspolisstyrelsens belastningsregister, som bl.a. innehåller uppgifter om dem som har ålagts påföljd för brott

eller har förklarats fria från påföljd på grund av en allvarlig psykisk störning (3 § lagen [1998:620] om belastningsregister). För uppgifterna i belastningsregistret gäller absolut sekretess (35 kap. 3 § OSL).

Information motsvarande de uppgifter som finns i belastningsregistret behandlas i domstolarna men är där som regel inte skyddad av sekretess. Exempelvis finns i de flesta brottmålsakter ett belastningsregisterutdrag avseende den tilltalade, vilket är offentligt. Intresset av offentlighet och insyn har av lagstiftaren ansetts väga tungt i fråga om rättegångar och domar. När uppgifter om brott sammanställs genom sökningar tillkommer dock integritetsaspekter som bör beaktas särskilt.

Sökbegrepp som avslöjar nationell anknytning

Enligt Vera-förordningarna är det i fråga om domstolarnas verksamhetsregister förbjudet att som sökbegrepp använda uppgifter om nationalitet och – såvitt gäller de allmänna förvaltningsdomstolarna – uppgifter om utfärdandeland för körkort (se t.ex. 4 § första stycket förordningen [2001:641] om registerföring m.m. vid Högsta förvaltningsdomstolen och kammarrätterna med hjälp av automatiserad behandling). Som anges ovan får det anses vara förenat med särskilda integritetsrisker att som sökbegrepp använda uppgifter som avslöjar etniskt ursprung. Detta begrepp anses emellertid som regel inte omfatta uppgifter om en persons nationalitet, eftersom en uppgift om nationalitet i sig inte ger upplysning om etniskt ursprung. Uppgifter om att en viss person närmast kommer från en viss världsdel eller ett visst land har också i de flesta fall ansetts inte vara uppgifter som avslöjar etniskt ursprung (prop. 2009/10:85 s. 325 och 2001/02:144 s. 41).

I domstolarnas verksamhet behandlas många uppgifter som avslöjar nationell anknytning, såsom uppgifter om nationalitet, födelseort, utfärdandeland för körkort, utländsk bakgrund m.m. I migrationsmål förekommer det att domstolen förordnar om

sekretess till skydd för denna typ av uppgifter i domar och beslut i de fall det finns ett känt behov av sekretesskydd. Uppgifter om nationell anknytning förekommer dock i andra sammanhang, såväl i migrationsmål som i andra måltyper, utan att skyddas av sekretess. Möjligheterna att genom sökningar sammanställa ett urval av personuppgifter utifrån sådana uppgifter kan innebära särskilda integritetsrisker, även om varje uppgift för sig själv inte nödvändigtvis är så känslig att den behöver skyddas av sekretess. Genom att använda sökbegrepp som avslöjar en aspekt av nationell anknytning skulle den som så önskar kunna kartlägga människor på ett sätt som måste anses utgöra påtagligt intrång i deras personliga integritet. Sådan kartläggning kan i värsta fall användas för förföljelse av de berörda. Möjligheten att utifrån denna typ av sökbegrepp ta fram ett urval av personuppgifter skulle också kunna missbrukas av stater som ägnar sig åt flyktingspionage eller av främlingsfientliga grupper.

Det har i fråga om vissa andra verksamheter, i vilka offentliga uppgifter behandlas, ansetts nödvändigt att genom bestämmelser om sökbegränsningar förhindra denna typ av sökningar. I folkbokföringsdatabasen är det t.ex. inte tillåtet att använda sådana sökbegrepp som kan matchas mot uppgifter i registret som avslöjar nationell anknytning.[2]

Berättigad användning av integritetskänsliga sökbegrepp

Som redovisas ovan får känsliga personuppgifter, uppgifter som avslöjar nationell anknytning samt uppgifter som avslöjar brott eller misstanke om brott anses vara sådana sökbegrepp som kan medföra särskilda risker i integritetshänseende. Som anges i avsnitt 13.1 är sökning ett viktigt verktyg för domstolarna för att kunna ta fram relevant information och på så sätt säkerställa att

[2] Enligt 2 kap. 10 § lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverkamhet är det (med vissa undantag) förbjudet att använda medborgarskap, födelseort och födelsehemort som sökbegrepp.

mål och ärenden kan handläggas på ett effektivt och rättssäkert sätt. Domstolarnas behov av att söka för att på ett effektivt sätt kunna ta fram relevant information gäller i samma utsträckning för sökningar som tar sin utgångspunkt i ett av de nu aktuella sökbegreppen.

För domstolspersonalen kan det exempelvis vara nödvändigt att använda de aktuella sökbegreppen för att snabbt och effektivt kunna orientera sig i domstolspraxis. Inom socialförsäkringsområdet finns det ett uttalat behov av att använda sjukdomsdiagnoser som sökbegrepp. I denna typ av mål räcker det för domstolen inte alltid att skaffa sig en bild av Högsta förvaltningsdomstolens avgöranden. Eftersom lagstiftningen inom detta område ändras relativt ofta är det för domaren angeläget att även ta del av aktuella kammarrättsavgöranden och ibland också avgöranden från förvaltningsrätterna. Vid handläggningen av migrationsmål finns det behov av att kunna använda nationell anknytning, etniskt ursprung, politiska åsikter, religiös övertygelse, och sexualliv som sökbegrepp, eftersom sådana uppgifter många gånger kan vara relevanta för domstolarnas avgöranden. Detta beror på att förhållandena i ursprungsländerna – vilka kan ha direkt betydelse för utgången i målet – ofta förändras drastiskt på kort tid i fråga om länder som är politisk instabila. I praktiken spelar underrätternas avgöranden en särskilt viktig roll inom migrationsområdet, eftersom vägledande avgöranden från Migrationsöverdomstolen rörande sådana frågor är begränsad (se SOU 2009:56 s. 201). Även i fråga om brottmål är sökbegrepp som på olika sätt rör brott mycket betydelsefulla för att relevanta avgöranden ska kunna återfinnas och för att en enhetlig ska kunna garanteras.

Behoven av att söka bland uppgifter i mål begränsar sig inte alltid till de dokument som innehåller domar och beslut. Ibland behöver domstolarna återfinna andra handlingar, såsom exempelvis rättsutredningar eller utredningar om innehållet i utländsk rätt.

Domstolarna har vidare behov av att använda de aktuella sökbegreppen för att med hjälp av de datoriserade verksamhets-

stöden planera och organisera verksamheten på det mest effektiva sättet. Genom att exempelvis använda en viss sjukdomsdiagnos som sökbegrepp kan mål vid en domstol som rör den sjukdomen identifieras och handläggningen av dessa mål samordnas i syfte att uppnå en mer effektiv och rättssäker prövning.

Alternativa sätt att tillgodose behoven

För att det ska kunna komma i fråga att tillåta domstolarna att använda de integritetskänsliga sökbegreppen bör först konstateras att det inte finns några andra, mindre integritetskänsliga sätt att tillgodose domstolarnas behov av att effektivt kunna ta fram relevant information. I viss utsträckning skulle behoven tillgodoses genom sökning med hjälp av de aktuella sökbegreppen i externa offentliga rättsdatabaser som inte omfattas av domstolsdatalagens tillämpningsområde. På webbsidan Vägledande avgöranden publicerar Domstolsverket med stöd av rättsinformationsförordningen (1999:175) avgöranden som har bedömts vara vägledande. Webbsidan får endast omfatta avgöranden från överinstanserna. En förutsättning för att avgörandena ska få publiceras är att personuppgifter maskas. Detta är resurskrävande och innebär dessutom att publiceringen fördröjs. Med hänsyn till dessa omständigheter samt att innehållet begränsas till ett urval av överinstansavgöranden bedöms webbsidan Vägledande avgöranden inte i tillräcklig utsträckning kunna tillgodose de behov som finns i domstolarna av att snabbt och effektivt kunna ta fram relevant information.

Det finns numera även privat affärsverksamhet inom området juridisk information där olika rättsdatabaser byggs upp. De företag som driver dessa begär hos domstolarna ut stora mängder allmänna handlingar, t.ex. samtliga domar och beslut som meddelas i landet, varefter kunderna erbjuds möjlighet att söka fritt i denna växande informationsmängd. Det vore inte rimligt om domstolarna skulle vara hänvisade till att använda sådana externa betaltjänster för att kunna söka bland vad som i

grunden är domstolarnas egna uppgifter. Dessutom har domstolarna kontroll över informationssäkerheten så länge det är fråga om sökningar bland domstolarnas egna databaser, till skillnad från vad som är fallet i fråga om externa privata rättsdatabaser.

Det ska också framhållas att det inte enbart är avgöranden som domstolarna behöver kunna återfinna med hjälp av sökning. Uppgifter som finns i ett mål (exempelvis ett rättsutlåtande) kan vara till stor nytta vid handläggningen av ett helt annat mål. Långtifrån all sådan information kan för närvarande sökas fram med hjälp av externa databaser.

Traditionellt informationsutbyte inom och mellan domstolarna bidrar till att hålla domare och föredragande à jour med den senaste rättsutvecklingen. Genom sådant samarbete kan ett urval av avgöranden som är av generellt intresse identifieras och presenteras i en promemoria eller vid ett föredrag. Detta har naturligtvis ett stort värde för domstolarnas verksamhet. Att kunna söka elektroniskt bland samtliga avgöranden fyller dock en annan funktion eftersom det därigenom är möjligt att snabbt och effektivt plocka fram avgöranden enligt mycket precisa kriterier ur en stor informationsmängd. Det traditionella informationsutbytet är jämfört med en situationsanpassad sökning resurskrävande, ineffektivt och långsamt. Dessutom är risken för ett ofullständigt resultat påtaglig. Att manuellt sammanställa avgöranden utifrån alla tänkbara relevanta kriterier är inte möjligt.

Vad gäller användningen av sökning som ett stöd vid planeringen och organisationen av arbetet vid domstolen finns det visserligen manuella metoder att tillgå för att handläggningen ska ske så effektivt som möjligt. En beredningsansvarig domare eller föredragande kan exempelvis ta sig tid att gå igenom målen på domstolen och identifiera de mål som rör liknande frågeställningar. Detta är dock avsevärt mer resurskrävande än att med hjälp av sökning bland uppgifterna i partsinlagorna identifiera denna typ av samband och lär inte vara praktiskt genomförbart, i vart fall inte vid de större domstolarna.

Sammanfattningsvis görs bedömningen att domstolarnas berättigade behov av att på ett effektivt sätt kunna ta fram viss

typ av information inte på ett tillfredsställande sätt kan tillgodoses på något annat sätt än med användning av de aktuella sökbegreppen (dvs. sökbegrepp som avser känsliga personuppgifter, som avslöjar brott eller misstanke om brott eller som avslöjar nationell anknytning), i vart fall inte på något annat sätt som skulle innebära mindre integritetsrisker.

Restriktiv användning av de integritetskänsliga sökbegreppen

De beskrivna behoven av att använda integritetskänsliga sökbegrepp avser sådan användning som syftar till att säkerställa att handläggningen är effektiv och rättssäker. Det finns redan på grund av det allmänna regelverk som omgärdar domstolarnas verksamhet samt de övriga skyddsbestämmelser som föreslås gälla enligt domstolsdatalagen ett gott skydd mot missbruk av integritetskänsliga sökbegrepp. De anställda kommer att vara lagligen förhindrade att göra en sökning om åtgärden inte ryms inom de tillåtna ändamål som föreslås gälla enligt domstolsdatalagen. I detta ligger att domstolspersonalen är förhindrad att vidta sökningar som inte behövs för arbetet och att sökningar därför inte får göras av t.ex. ren nyfikenhet. Till detta kommer att domstolsanställda ska agera i enlighet med god förvaltningssed och andra normer som gäller för domare och andra offentliga tjänstemän. Det kan också noteras att överträdelser av dessa bestämmelser skulle kunna leda till en disciplinpåföljd enligt lagen (1994:260) om offentlig anställning. Som föreslås i avsnitt 11.2 ska vidare den interna tillgången till personuppgifter vara begränsad till vad var och en behöver för att fullgöra sina arbetsuppgifter.

Trots dessa generella skyddsmekanismer finns det på grund av de integritetsrisker som är förknippade med de aktuella sökbegreppen skäl att genom specifika bestämmelser säkerställa att sökbegreppen används restriktivt.

Det bör ankomma på den anställde som vill använda ett särskilt känsligt sökbegrepp att i varje enskilt fall göra en

prövning av om sökningen verkligen är motiverad. Detta kan lämpligen komma till uttryck genom att det i domstolsdatalagen anges att de aktuella sökbegreppen endast får användas om sökningen är *absolut nödvändig* för handläggning av mål och ärende. Detta är ett begrepp som brukar användas i registerförfattningar för att signalera att det ställs högre krav än vad som följer av de allmänna ändamålsbestämmelserna. Begreppet har också använts för att rättsligt förhindra att åtgärder vidtas rutinmässigt (jfr prop. 2009/10:85, s. 371). En liknande bestämmelse avseende sökning i Säkerhetspolisens brottsbekämpande verksamhet finns i 5 kap. 11 § polisdatalagen. Med hänsyn till de ovan redovisade behoven finns det vidare anledning att begränsa sökmöjligheterna till *handläggning av mål och ärenden*. Detta innebär att sökning endast får ske inom domstolarnas kärnområde, men däremot inte om sökningen sker enbart för att fullgöra ett s.k. sekundärt ändamål, t.ex. att lämna uppgifter till en myndighet utan att det är nödvändigt för handläggningen.

Kravet på att en sökning ska vara absolut nödvändig innebär att det är domaren i det enskilda fallet som får avgöra om en sökning får ske. Behovet ska vara tydligt och det är lämpligt att i författning så långt som möjligt konkretisera vad som ligger i kravet på att endast sökningar som är absolut nödvändiga för handläggning av mål och ärenden är tillåtna. Såvitt framkommit hänför sig behoven av att kunna använda sökbegrepp som avser känsliga personuppgifter eller nationell anknytning framför allt till de allmänna förvaltningsdomstolarna, även om det finns vissa behov även i allmänna domstolar, t.ex. vid sökning efter praxis i mål om hatbrott, försäkringsmål eller diskrimineringsmål. Behoven av att använda sökbegrepp som avser brott eller misstanke om brott kan på motsvarande sätt framför allt hänföras till de allmänna domstolarna, även om det kan finnas något undantag, såsom sökning bland domar i körkortsmål vid en förvaltningsrätt utifrån en uppgift om brott. I hyres- och arrendenämnderna torde det överhuvudtaget inte finnas något påtagligt behov av att använda nämnda sökbegrepp. Det bör mot denna bakgrund anges i domstolsdatalagen att sökbegrepp som avser

känsliga personuppgifter eller nationell anknytning endast får användas bland uppgifter vid de allmänna förvaltningsdomstolarna samt att sökbegrepp som avser brott eller misstanke om brott endast får användas vid sökning bland uppgifter vid de allmänna domstolarna. Härigenom blir det exempelvis förbjudet att använda ett sökbegrepp som avser etnicitet eller nationalitet vid sökning bland brottmålsdomar vid en tingsrätt, eller att använda en brottsrubricering vid sökning bland skatte- eller sjukförsäkringsdomar vid en kammarrätt.

Genom förordningsbestämmelser kan utrymmet att använda de aktuella sökbegreppen preciseras ytterligare utifrån principen att endast absolut nödvändiga sökningar ska få ske, t.ex. genom att det föreskrivs att de aktuella sökbegreppen endast får användas vid sökning bland uppgifter i mål av en viss typ. Sådana föreskrifter bör inte tas in i domstolsdatalagen eftersom de behöver kunna anpassas då nya måltyper tillkommer eller försvinner, eller då domstolarnas inre organisation och arbetsformer utvecklas. För att bestämmelserna ska bli verkningsfulla behöver de ha den detaljeringsgrad som gör att de inte lämpar sig för lag. Regeringen bör därför ha ett utrymme att meddela föreskrifter i förordning som ytterligare förtydligar och inskränker möjligheterna att använda de aktuella sökbegreppen.

Till skillnad från vad som gäller enligt Vera-förordningarna kommer de föreslagna sökbegränsningar att gälla för sökning bland såväl strukturerad information i verksamhetsstödet som uppgifter i löpande text i exempelvis domar och partsinlagor.

13.3 Offentlighet och sekretess

Bedömning: Det bör inte införas någon särskild sekretessbestämmelse avseende uppgifter som tas fram med hjälp av sökning.

Skälen för bedömningen: Offentlighetsprincipen, såsom den kommer till uttryck i 2 kap. TF, innebär i huvudsak att allmänheten och massmedierna har rätt att ta del av offentliga allmänna handlingar hos en myndighet. Enligt 2 kap. 2 § första stycket TF får rätten att ta del av allmänna handlingar begränsas endast om det är påkallat med hänsyn till vissa angivna intressen, t.ex. skyddet för enskilds personliga och ekonomiska förhållanden. En sådan begränsning ska enligt 2 kap. 2 § andra stycket TF anges noga i en bestämmelse i en särskild lag eller, om det i visst fall är lämpligare, i en annan lag som den särskilda lagen hänvisar till. Den särskilda lagen är offentlighets- och sekretesslagen.

Handlingsoffentligheten enligt 2 kap. TF omfattar fysiska handlingar och elektroniskt lagrade uppgifter som ingår i s.k. *färdiga elektroniska handlingar*, dvs. uppgiftssammanställningar som redan har ett fixerat innehåll och därför inte förutsätter någon sökning för att återskapas, t.ex. e-postmeddelanden, domar och beslut i elektronisk form samt partsinlagor. Offentlighetsprincipen omfattar emellertid också uppgifter som ännu inte sammanställts men som kan sammanställas med hjälp av tillgänglig teknik och rutinbetonade åtgärder, t.ex. en sökning (2 kap. 3 § andra stycket TF). Sådana sammanställningar kallas *potentiella elektroniska handlingar*. Skälet till att enskilda har rätt att ta del av potentiella allmänna handlingar är att det anses följa av den s.k. *likställighetsprincipen* att enskilda bör ha samma möjligheter som aktuell myndighet att ta del av sammanställningar av uppgifter ur upptagningar för automatiserad behandling (dir. 2011:86 s. 16, se även SOU 2012:90 s. 93 f.).

I 2 kap. 3 § tredje stycket TF finns den s.k. *begränsningsregeln*, vilken anger att en sammanställning av uppgifter ur en upptag-

ning för automatiserad behandling inte anses förvarad hos myndigheten om sammanställningen innehåller personuppgifter och myndigheten enligt lag eller förordning saknar befogenhet att göra den tillgänglig[3]. Att en handling anses förvarad hos myndigheten är en förutsättning för att den ska omfattas av allmänhetens rätt att ta del av densamma enligt offentlighetsprincipen.

Begränsningsregeln innebär att dataskyddsbestämmelser indirekt kan få betydelse för hur omfattande begreppet allmän handling är i praktiken. Bestämmelser i registerförfattningar om för vilka ändamål myndigheten får behandla uppgifterna (s.k. ändamålsbegränsningar), anses i och för sig inte inskränka myndighetens skyldighet enligt offentlighetsprincipen att sammanställa personuppgifter. Samma sak gäller sökbegränsningar i de fall de tillåter sökning under särskilt angivna förutsättningar. En sökbegränsning som är absolut formulerad och som under inga omständigheter tillåter användningen av ett visst sökbegrepp har däremot ansetts kunna få genomslag enligt begränsningsregeln (jfr prop. 2007/08:126 s. 120 f., prop. 2007/08:160 s. 66 f., dir. 2011:86 samt SOU 2012:90 s. 93 f.).

Den i avsnitt 13.2 föreslagna bestämmelsen om att vissa integritetskänsliga sökbegrepp (bl.a. känsliga personuppgifter) får användas för sökning endast om det är absolut nödvändigt för handläggning av mål och ärenden är inte ovillkorlig, utan förutsätter att en behovsprövning sker i varje enskilt fall. Denna sökbegränsning är således inte av det slag som avses i begränsningsregeln. Den i samma avsnitt föreslagna bestämmelsen om att de aktuella sökbegrepp får användas för sökning endast bland uppgifter vid vissa domstolar innebär däremot en sådan ovillkorlig begränsning som i enlighet med begränsningsregeln får genomslag i förhållande till offentlighetsprincipen. Således finns det exempelvis ingen rätt för allmänheten att med stöd av offentlighetsprincipen ta del av det sökresultatet som skulle

[3] Färdiga elektroniska handlingar omfattas inte av begränsningsregeln.

uppstå vid sökning med hjälp av ett sökbegrepp som avslöjar brott om sökningen avser uppgifter som finns vid en förvaltningsrätt. På motsvarande sätt finns det ingen rätt för allmänheten att ta del av den uppgiftssammanställning som skulle kunna tas fram genom sökning med hjälp av ett sökbegrepp som avslöjar nationell anknytning om sökningen sker bland uppgifter som finns vid en hovrätt.

Enskildas tillgång till de uppgifter som tas fram med hjälp av sökning kan medföra särskilda integritetsrisker eftersom en enskild inte i samma utsträckning som de domstolsanställda begränsas i sitt agerande av domstolsdatalagens sökbegränsningar. När det gäller begränsning av allmänhetens tillgång till allmänna handlingar är det i stället sekretessbestämmelser i offentlighets- och sekretesslagen som ska tillämpas. Utlämnande till allmänheten av allmänna handlingar som tagits fram med användning av nu aktuella sökbegrepp ska således vägras om sekretess i ett enskilt fall bedöms föreligga (jfr 43 kap. OSL och de sekretessbestämmelser i lagens fjärde och femte avdelningar som är direkt tillämpliga hos domstolarna).

I domstolarna anses sedan gammalt intresset av insyn och öppenhet vara särskilt starkt. Det starka insynsintresset i domstolarnas rättskipande och rättsvårdande verksamhet kommer till uttryck bl.a. i regleringen av det s.k. offentlighetsdopet (jfr 43 kap. 5 och 8 §§ OSL). Allmänheten ska tillförsäkras en långtgående insyn i domstolarnas verksamhet. En viktig del i detta är massmedias journalistiska granskning av domstolarna. Precis som domstolarna har ett berättigat intresse av att använda automatiserade sökfunktioner för att hitta relevanta avgöranden m.m. får det anses finnas det ett betydande värde i att journalister kan söka fram avgöranden efter bestämda kriterier för att exempelvis jämföra hur olika domstolar dömer. Det kan också noteras att det enligt de nu gällande Vera-förordningarna inte finns några bestämmelser om att vissa sökbegrepp inte får användas såvitt gäller sökning bland elektroniskt lagrade domar eller andra fritextdokument, även om sådana sökningar för närvarande i många fall inte är tekniskt möjliga att utföra.

Som beskrivs i avsnitt 13.2 finns det numera privata aktörer som för allmänheten tillgängliggör mycket omfattande databaser med domar, partsinslagor och andra offentliga handlingar från domstolarna. I dessa databaser kan vem som helst som betalar det pris som gäller för tjänsten söka utan några begränsningar avseende vilka sökbegrepp som får användas. Ytterligare sekretess förhindrar därför inte allmänheten från att få fram samma sökresultat på annat sätt.

Mot den angivna bakgrund finns det inte tillräckliga skäl att föreslå några inskränkningar av offentlighetsprincipen i syfte att begränsa allmänhetens tillgång till uppgifter som tas fram med hjälp av sökning i domstolarnas rättskipande och rättsvårdande verksamhet. Någon ny sekretessbestämmelse bör således inte införas.

13.4 Undantag från sökbegränsningarna

Förslag: Sökbegränsningarna ska inte omfatta sökningar som endast sker i en viss handling eller i ett visst mål eller ärende.

Skälen för förslaget: Sökning som sker bland en tydligt begränsad mängd uppgifter innebär mindre integritetsrisker än sökningar som sker bland större uppgiftsmängder. Att någon använder sökfunktionen i ett ordbehandlingsprogram för att orientera sig i ett enskilt textdokument, t.ex. en dom eller en aktbilaga, framstår som ofarligt i integritetshänseende. På motsvarande sätt är det svårt att se några beaktansvärda integritetsrisker med sökningar som endast avser uppgifter i ett enskilt mål eller ärende. Detta är standardmässiga sökfunktioner som personalen vid domstolarna, liksom vilken datoranvändare som helst, behöver för att kunna bedriva sitt arbete på ett rationellt sätt. Mot denna bakgrund bör de sökbegränsningar som nu föreslås inte omfatta sökningar som endast avser uppgifterna i en

viss handling eller ett visst mål eller ärende (jfr 3 kap. 7 § polisdatalagen).

14 Elektroniskt utlämnande av personuppgifter

14.1 Inledning

Begreppen direktåtkomst och utlämnande på medium för automatiserad behandling

Personuppgifter kan lämnas ut på olika sätt, t.ex. via kopia av en handling eller en utskrift från dator. Utlämnande kan också göras i elektronisk form, s.k. *elektroniskt utlämnande*[1]. Att personuppgifter utlämnas innebär att de lämnas ut till eller görs tillgängliga för en mottagare utanför myndigheten. Eftersom varje domstol är en egen myndighet är det fråga om utlämnande även när uppgifter lämnas mellan domstolarna. Detsamma gäller när en domstol lämnar uppgifter till Domstolsverket.

I många registerförfattningar finns bestämmelser där det framgår inte bara i vilken utsträckning personuppgifter får behandlas genom att utlämnas utan även när det får göras i elektronisk form. Motivet för denna särreglering av sättet eller den särskilda tekniken för utlämnandet är att själva den elektroniska formen anses kunna medföra risker för otillbörliga integritetsintrång. Som regel innebär nämligen just den elektroniska formen att mottagaren efter utlämnandet har större möjligheter att bearbeta och sprida informationen än om utlämnandet

[1] I prop. 2008/09:96 definieras elektroniskt utlämnande som alla former av utlämnande av personuppgifter i binär form, dvs. som ettor och nollor (s. 85).

sker på papper. Inom datalagstiftningen används för denna typ av utlämnande ofta begreppen direktåtkomst och utlämnande på medium för automatiserad behandling (jfr prop. 2008/09:96 s. 8 och 2009/10:85 s. 168 f. samt SOU 2007:64 s. 160). Begreppen har inga legala definitioner.

Den grundläggande innebörden av begreppet *direktåtkomst* är att någon utomstående (en annan domstol, en förvaltningsmyndighet eller en enskild) har direkt tillgång till en domstols register eller databas och på egen hand kan ta fram information och på så sätt få den utlämnad till sig. I begreppet direktåtkomst ligger också att den domstol som är ansvarig för registret eller databasen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst tillfälle tar del av och domstolen har därför t.ex. inte någon möjlighet att göra en sekretessprövning i det enskilda fallet. Direktåtkomsten medges efter en förhandsprövning av den utlämnande domstolen, som sedan måste försäkra sig om att mottagaren endast kan få tillgång till uppgifter som får lämnas ut.

Med begreppet *utlämnande på medium för automatiserad behandling* avses annat elektroniskt utlämnande än genom direktåtkomst. Sådant utlämnande kan innebära t.ex. att elektronisk information överförs via e-post, genom utlämnande av uppgifter på flyttbart lagringsmedium – t.ex. flashminne (s.k. usb-minne) – eller genom direkt överföring från ett datorsystem till ett annat via allmänna kommunikationsnät. Vid utlämnande på medium för automatiserad behandling tar den utlämnade domstolen i varje enskilt fall ställning till vilka uppgifter som ska lämnas ut. En eventuell sekretessprövning kan därmed ske i samband med utlämnandet.

Den tekniska utvecklingen har inneburit att det numera finns betydligt fler sätt att överföra uppgifter elektroniskt än tidigare och nya åtkomstmetoder tillkommer alltjämt. Detta har medfört att tillämpningen av begreppen direktåtkomst och utlämnande på medium för automatiserad behandling på modernare metoder för informationsutbyte kommit att uppfattas som oklar (se t.ex. prop. 2007/08:160 s. 58 och 2009/10:85 s. 168 f. samt SOU

2010:4 s. 364 f.). Regeringen har mot denna bakgrund tillsatt Informationshanteringsutredningen som bl.a. ska ta ställning till om det finns skäl att i registerförfattningarna upprätthålla en skillnad mellan direktåtkomst och andra former av elektroniskt utlämnande och, om så bedöms vara fallet, vilka begrepp som bör användas samt hur dessa bör definieras (dir. Ju2011:86). Det skulle kunna leda till tolkningsproblem om domstolsdatalagen i fråga om terminologi avvek från registerförfattningar på närliggande områden. I avvaktan på den generella översyn i frågan som pågår bör därför tills vidare begreppen direktåtkomst och utlämnande på medium för automatiserad behandling användas i domstolsdatalagen.

Nuvarande ordning

I personuppgiftslagen regleras det inte särskilt på vilket sätt – elektroniskt eller på annat sätt, t.ex. muntligt eller på papper – som personuppgifter får lämnas ut. I den Vera-förordning som gäller för Högsta förvaltningsdomstolen och kammarrätterna anges att dessa domstolar får ha direktåtkomst till varandras register samt att även förvaltningsrätterna, Domstolsverket och Riksdagens ombudsmän får ha direktåtkomst till registren. Dessutom föreskrivs att Skatteverket och länsstyrelserna får ha direktåtkomst till registren för återsökning av vägledande avgöranden (3 § förordningen [2001:641] om registerföring m.m. vid Högsta förvaltningsdomstolen och kammarrätterna med hjälp av automatiserad behandling, jfr även SOU 2001:32 s. 108). I övriga Vera-förordningar saknas uttryckliga bestämmelser om direktåtkomst (jfr SOU 2012:90, s 210 f.). Vad gäller andra former av elektroniskt utlämnande än direktåtkomst finns det inga bestämmelser i Vera-förordningarna om detta. Det har blivit allt vanligare att domstolarna lämnar ut uppgifter på det sättet till såväl myndigheter som enskilda.

14.2 Utlämnande på medium för automatiserad behandling

Förslag: Personuppgifter ska få lämnas ut till myndigheter på medium för automatiserad behandling.

Personuppgifter i ett mål eller ärende ska få lämnas ut på medium för automatiserad behandling till parter och deras ombud, biträden och försvarare.

I övrigt ska endast enstaka personuppgifter få lämnas ut på medium för automatiserad behandling. Regeringen eller den myndighet som regeringen bestämmer har dock möjlighet att meddela föreskrifter om att utlämnande får ske även i andra fall.

Bedömning: Det behövs inga sekretessbrytande bestämmelser i domstolsdatalagen.

Skälen för förslaget och bedömningen

Utgångspunkter

Domstolarna har i sin rättskipande och rättsvårdande verksamhet ett regelmässigt behov av att kommunicera uppgifter med t.ex. parter, andra myndigheter och allmänheten. Traditionellt har domstolarnas uppgiftslämnande skett huvudsakligen med post, dvs. i pappersform. I takt med att allt fler uppgifter skapas eller lagras i domstolarnas datorsystem och möjligheterna att förmedla uppgifter till andra på elektronisk väg ökar framstår det som naturligt och allt mer nödvändigt att också i så stor utsträckning som möjligt överge pappershanteringen och i stället använda sig av olika sätt för elektroniskt utlämnande. Ett elektroniskt utlämnande av personuppgifter förenklar och effektiviserar tillgången till en myndighets offentliga information. Därigenom ökar möjligheterna till insyn och kontroll av myndigheternas verksamhet. Möjligheten till ett elektroniskt utlämnande blir i allmänhet också enklare och billigare för myndigheterna.

Ett utlämnande på medium för automatisk behandling är en form av behandling av personuppgifter. Varken personuppgiftslagen eller dataskyddsdirektivet innehåller regler om under vilka förutsättningar uppgifter får lämnas ut i elektronisk form. Någon åtskillnad mellan elektroniskt utlämnande av personuppgifter och utlämnande som sker på papper görs således inte. Ett utlämnande av uppgifter på medium för automatiserad behandling innebär dock som regel att mottagaren kan vidarebearbeta den utlämnade informationen på olika sätt, t.ex. genom strukturering och samkörning med andra uppgifter, och sprida den. Ett utlämnande på medium för automatiserad behandling kan därmed innefatta särskilda risker från integritetssynpunkt. Med hänsyn härtill framstår det som rimligt att författningsreglera förutsättningarna för utlämnande av uppgifter på medium för automatiserad behandling i domstol. Vid utformning av en sådan reglering bör utgångspunkten vara att utlämnande ska vara tillåtet om det kan försvaras av framför allt effektivitetsskäl och om det kan ske utan otillbörliga risker för den personliga integriteten.

Den reglering som övervägs i detta avsnitt gäller i vilken utsträckning domstolarna ska ha möjlighet att lämna ut personuppgifter på medium för automatiserad behandling. De bestämmelser som föreslås innebär således ingen skyldighet att lämna ut uppgifter på ett sådant medium. Eftersom spridningsrisken är större när uppgifter lämnas ut i elektroniskt format får det förutsättas att domstolspersonalen alltid utnyttjar denna möjlighet med omdöme. I fråga om utlämnande av särskilt känsligt material bör den som lämnar ut uppgifterna överväga om ett pappersutlämnande i det enskilda fallet är lämpligare för att försvåra vidarespridning och internetpublicering på ett som sätt som kan vara kränkande för de berörda.

Utlämnande till myndigheter

Domstolarna är enligt olika författningar skyldiga att tillställa vissa andra myndigheter kopior av domar. Av effektivitetsskäl bör detta kunna ske elektroniskt. Vidare bör domstolarna naturligtvis kunna använda vardagliga funktioner såsom e-post i sina kontakter med andra domstolar, Domstolsverket och andra myndigheter.

I takt med att myndigheterna inom den offentliga förvaltningen i allt större utsträckning övergår till fullständigt elektronisk informationshantering framstår begränsningar av möjligheten till elektroniskt informationsutbyte mellan myndigheterna i motsvarande grad som mindre lämpliga. Arbetet inom rättsväsendets informationsförsörjning syftar till att förbättra den elektroniska kommunikationen mellan rättskedjans myndigheter. En viktig del i det arbetet är att uppgifter som registreras elektroniskt hos en myndighet ska kunna skickas elektroniskt till andra myndigheter och där återanvändas. När samma uppgifter således endast behöver matas in manuellt i datorsystemen en enda gång, och inte en gång vid varje myndighet i rättskedjan, minskar risken för fel. En förutsättning för denna utveckling är att relevanta registerförfattningar medger sådant elektroniskt informationsutbyte mellan domstolar och övriga deltagande myndigheter.

Under förutsättning att den tekniska säkerheten i samband med överföringen är tillräckligt god bör ett utlämnande på medium för automatiserad behandling till myndigheter i de flesta fall inte innebära större risker för otillbörliga integritetsintrång än när utlämnandet sker på papper. Behandlingen av personuppgifter vid de myndigheter som tar emot uppgifterna styrs oftast av särskilda registerförfattningar, vilket innebär ett förstärkt integritetsskydd jämfört med mottagare vilkas personuppgiftsbehandling sker med stöd av endast personuppgiftslagen. I fråga om utlämnande från en domstol till en annan domstol kommer det inte att finnas några särskilda integritetsrisker, eftersom det är samma författning, domstolsdatalagen,

som föreslås reglera personuppgiftsbehandlingen både vid den avsändande och mottagande myndigheten.

Myndighetspersonal har att rätta sig efter förvaltningslagen och andra allmänna regler som gäller i offentlig verksamhet. I kombination med det tjänsteansvar som åvilar offentligt anställda bidrar detta till att minimera riskerna för att uppgifter som tas emot i elektroniskt format missbrukas. Till det totala integritetsskyddet bidrar också den omständigheten att den mottagande myndigheten inte får lämna ut de mottagna uppgifterna, varken elektroniskt eller på annat sätt, utan föregående sekretessprövning. I många fall finns det regler om elektroniskt utlämnande i den registerförfattning som gäller för den mottagande myndigheten så att den vidare spridningen i elektronisk form inte kan ske okontrollerat.

Sammanfattningsvis finns det starka effektivitetsskäl som talar för att inte begränsa elektroniskt utlämnande till andra myndigheter, inklusive andra domstolar. Med hänsyn till att de integritetsrisker som är förknippade med utlämnande till andra myndigheter på medium för automatiserad behandling inte är påtagliga görs bedömningen att några särskilda begränsningar avseende sådant utlämnande inte behöver föreslås.

Utlämnande till enskilda

Domstolarna har ett behov av att lämna ut uppgifter på medium för automatiserad behandling även till enskilda, såsom privatpersoner, journalister, företag och organisationer. Domar, partsinlagor, förelägganden och liknande dokument bör av effektivitetsskäl kunna skickas till enskilda på elektronisk väg. Det kan också vara till stor hjälp för parter och de som företräder dem i processen att ha tillgång till processmaterialet i elektronisk form, vilket bl.a. möjliggör sökningar bland uppgifterna i förundersökningsprotokoll, inlagor, myndighetsakter m.m. Vidare behöver domstolspersonalen kunna kommunicera med utomstående med hjälp av e-post. I de flesta fall är det ganska begränsade

mängder personuppgifter som behöver skickas till enskilda, om man jämför med den mängd uppgifter som exempelvis tingsrätterna behöver utbyta med Åklagarmyndigheten eller förvaltningsdomstolarna med Försäkringskassan eller Skatteverket.

Till skillnad från vad som gäller vid utlämnande till myndigheter saknas normalt särskilda bestämmelser om hur personuppgifter får behandlas hos de enskilda som tar emot uppgifter. Enskildas behandling av uppgifterna begränsas då endast av personuppgiftslagens bestämmelser. Hos enskilda gäller heller inga sekretessbestämmelser som förhindrar vidare spridning av uppgifterna. Av dessa skäl får integritetsriskerna anses vara större när utlämnande på medium för automatiserad behandling sker till enskilda än när det sker till myndigheter.

Av det s.k. utskriftsundantaget i tryckfrihetsförordningen följer att en domstol inte är skyldig att i större utsträckning än vad som följer av lag lämna ut en upptagning för automatiserad behandling i annan form än utskrift (2 kap. 13 § TF). Bestämmelsen syftar till att minimera riskerna för otillbörliga integritetsintrång. E-offentlighetskommittén anförde i sitt slutbetänkande att det långsiktiga målet bör vara att myndigheterna har en i lag reglerad skyldighet att – i den mån det inte finns särskilda förbud mot det i lag eller förordning – lämna ut allmänna handlingar i elektronisk form om sökanden så önskar. Kommittén ansåg dock att en sådan skyldighet inte kan införas förrän en grundlig genomgång och bearbetning har genomförts av samtliga registerförfattningar (SOU 2010:4 s. 306 f.). Denna fråga är nu även föremål för överväganden av Informationshanteringsutredningen (Ju2011:11). Utredningen ska även belysa den problematik som begränsningar i möjligheterna till elektroniskt utlämnande kan innebära för medias möjligheter att granska hur makten utövas och förvaltas och utforma förslag efter en avvägning mellan intresset av skydd för den personliga integriteten och intresset av insyn i myndigheternas verksamhet.

Ett alternativ är att, i likhet med Vera-förordningarna, helt avstå från att begränsa möjligheterna till att lämna ut personuppgifter på medium för automatiserad behandling till enskilda.

Som nämns ovan är dock integritetsriskerna inte obetydliga och det framstår som angeläget att på något sätt begränsa utrymmet för s.k. massuttag.

Ett annat alternativ är då att möjliggöra utlämnande på medium för automatiserad behandling efter en behovsprövning i det enskilda fallet. Domstolarna skulle då i det enskilda fallet t.ex. kunna ta ställning till om ett utlämnande är lämpligt med hänsyn till exempelvis personuppgifternas art, struktur och antal.

Ett ytterligare alternativ är den typ av reglering som finns i polisdatalagen och kustbevakningsdatalagen. Enligt dessa lagar får som utgångspunkt endast enstaka personuppgifter lämnas ut på medium för automatiserad behandling till enskilda (2 kap. 20 § respektive 2 kap. 8 §). I avvaktan på Informationshanteringsutredningens översyn framstår det som lämpligast att förslagen i domstolsdatalagen ansluter till den lösning som valts i dessa lagar. Det bör således föreslås att det som utgångspunkt ska gälla en begränsning till enstaka personuppgifter i fråga om utlämnande på medium för automatiserad behandling till enskilda. Det bör dock framhållas att begreppet enstaka personuppgifter i registerförfattningssammanhang har fått en något vidare innebörd än i vanligt språkbruk. Detta bör i synnerhet gälla när det är fråga om uppgifter som i sig själva är harmlösa (se t.ex. prop. 2009/10:85 s. 333).

Det kan framöver komma att bedömas nödvändigt att i vissa fall tillåta utlämnande av mer än enstaka personuppgifter i elektroniskt format till en enskild. Det kan också finnas behov av att anpassa regleringen när den tekniska utvecklingen går framåt och formerna för elektroniskt utlämnande förändras. Regeringen eller den myndighet som regeringen bestämmer bör av dessa skäl kunna meddela föreskrifter om att utlämnande på medium för automatiserad behandling får ske i andra fall än vad som följer av domstolsdatalagen.

När det gäller utlämnande till parter och deras ombud, biträden eller försvarare gör sig särskilda hänsyn gällande. Av förordningen (2003:234) om tiden för tillhandahållande av domar och beslut, m.m. framgår att en dom eller ett beslut får

skickas till parter med telefax eller elektronisk post eller på annat sätt tillhandahållas i elektronisk form, om det är lämpligt (10 §). Flera skäl talar för att domstolsdatalagen inte bör hindra elektroniskt kommunikation med parter och deras ombud, biträden eller försvarare. Intresset av en transparent domstolsprocess är särskilt starkt när det gäller dessa personer. Insynen i processen underlättas om domstolen kan använda e-post och liknande kommunikationssätt för att översända handlingar till parterna. Domstolarna har vidare en långtgående skyldighet att se till att parterna får ta del av skriftligt material i målet och effektivitetsvinsterna är därför stora om detta kan ske på elektronisk väg. Att parter, ombud, biträden och försvarare får tillgång till processmaterial i elektronisk form möjliggör ett modernt och effektivt arbetssätt, t.ex. genom att dessa personer kan ha tillgång till handlingar i en läsplatta under förhandlingen, att de enkelt kan hitta relevanta delar i ett omfattande material och att de kan hålla sakframställning och förhör med elektroniska hjälpmedel under en muntlig förhandling. Att enskilda parter och deras ombud, biträden eller försvarare har samma möjlighet som myndigheter som uppträder som parter i domstol att få del av uppgifter på elektronisk väg kan sägas vara ett utslag av principen att parterna ska vara likställda i processen (equality of arms) och säkerställer att enskilda har lika goda möjligheter att utföra sin talan i domstolen som företrädare för det allmänna.

Mot den angivna bakgrunden bör enligt domstolsdatalagen personuppgifter utan någon särskild begränsning få lämnas ut på medium för automatiserad behandling till parter samt till deras ombud, biträden och försvarare. Utlämnande bör naturligtvis endast få ske avseende uppgifter i det egna målet. Förslaget innebär inte någon skyldighet att lämna ut uppgifter i elektroniskt format. Domstolarna bör utifrån omständigheterna i det enskilda fallet avgöra om ett pappersutlämnande är lämpligare med hänsyn till risken för att uppgifterna sprids på ett sätt som kan vara kränkande för enskilda. Särskild försiktighet kan t.ex. göra sig gällande avseende fotografier i en förundersökning som i och för sig inte är sekretessbelagda men som har ett innehåll som

gör att det är stötande för brottsoffret om de sprids. I fråga om myndigheter görs ovan bedömningen att utlämnande ska kunna ske till dem på medium för automatiserad behandling, oavsett om de är parter eller inte.

Sekretessbrytande bestämmelser

I en del registerförfattningar finns det sekretessbrytande bestämmelser. I 2 kap. 16 § polisdatalagen föreskrivs det exempelvis att vissa brottsbekämpande myndigheter trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 § OSL ska ha rätt att ta del av personuppgifter under närmare angivna förutsättningar. Vad gäller domstolarnas rättskipande och rättsvårdande verksamhet har det inte framkommit något behov för domstolarna att kunna lämna ut uppgifter i större utsträckning än vad som medges enligt gällande rätt. Det bör därför inte införas några sekretessbrytande bestämmelser i domstolsdatalagen.

14.3 Direktåtkomst

Förslag: En domstol ska få medge en annan domstol direktåtkomst. En domstol ska även kunna medge en part och en parts ombud, biträde eller försvarare direktåtkomst till sitt mål eller ärende.

Regeringen eller den myndighet som regeringen bestämmer meddelar ytterligare föreskrifter om begränsning av direktåtkomsten samt om behörighet och säkerhet.

Skälen för förslaget

Närmare om direktåtkomst

I begreppet direktåtkomst ligger att den som är personuppgiftsansvarig för registret eller databasen inte har någon

kontroll över vilka uppgifter som mottagaren vid ett visst söktillfälle tar del av. Den myndighet som lämnar ut uppgifter genom direktåtkomst fattar således inte beslut om utlämnande av de uppgifter som mottagaren tar del av i varje enskilt fall. I stället måste en förhandsprövning göras av förutsättningarna för utlämnande. En sådan prövning innefattar alla de uppgifter som mottagaren har möjlighet att ta del av genom sin direktåtkomst. Även om personuppgiftsregleringen medger direktåtkomst är det inte tillåtet för en myndighet att medge direktåtkomst till uppgifter som omfattas av sekretess om det inte står klart att mottagaren vid en prövning enligt offentlighets- och sekretesslagen med säkerhet skulle ha rätt att ta del av uppgifterna.

Vid författningsreglering av direktåtkomst till uppgifter anges ofta att någon får medges direktåtkomst. Innebörden av detta är inte att någon skulle ha en ovillkorlig rätt att få ut uppgifterna, utan att den myndighet som innehar informationen har rätt att medge sådan åtkomst. Den utlämnande myndigheten har ett principiellt ansvar för att förvissa sig om att den som beviljas direktåtkomst vidtar de åtgärder som bedöms vara nödvändiga ur säkerhetssynpunkt (prop. 2011/12:45 s. 133).

De uppgifter som mottagaren har direktåtkomst till får i normalfallet anses utlämnade i offentlighets- och sekretesslagens mening i och med att direktåtkomst finns. Det spelar i det avseendet ingen roll om mottagaren faktiskt tar del av en viss uppgift eller inte (jfr SOU 2007:45 s. 192 f.). Sedan några år tillbaka finns det en bestämmelse i offentlighets- och sekretesslagen som innebär att sekretess som gäller hos en myndighet kan överföras till en annan myndighet som har direktåtkomst (11 kap. 4 § OSL).

Utgångspunkter

Vid bedömningen av vilka som bör få ha direktåtkomst till uppgifter som behandlas i domstolarnas verksamhet bör utgångspunkten vara att sådan åtkomst bör tillåtas när nyttan av

åtkomsten är klart påvisbar samtidigt som den inte innebär några beaktansvärda försämringar av skyddet för den personliga integriteten.

I de databaser och register som förs av domstolarna finns det ofta stora mängder personuppgifter. Många av dessa kan vara av känslig karaktär. Ju fler personer som har omedelbar tillgång till sådana uppgiftssamlingar, desto mera påtaglig är risken för intrång. Direktåtkomst kan också minska möjligheterna att kontrollera den vidare användningen av uppgifterna. Dessa förhållanden utgör skäl för en restriktiv hållning i fråga om direktåtkomst till uppgifter som domstolarna behandlar.

Enligt kustbevakningsdatalagen har regeringen getts möjlighet att besluta om vilka myndigheter som ska kunna medges direktåtkomst till personuppgifter i kustbevakningens operativa verksamhet som inte är brottsbekämpande (5 kap. 7 §). Det framgår dock av den aktuella bestämmelsen att sådan direktåtkomst inte får avse känsliga personuppgifter. Vad gäller domstolarna förekommer det känsliga personuppgifter i många typer av mål och det skulle i många fall inte vara meningsfullt att medge direktåtkomst som inte får omfatta känsliga personuppgifter. Ett annat alternativ är att ge regeringen rätt att utvidga möjligheten till direktåtkomst till alla typer av uppgifter, utan begränsningar avseende känsliga personuppgifter. Det alternativet är dock tveksamt med hänsyn till de svåra avvägningar mellan integritetsskydd och effektivitetsintressen som bör ske. Det kan också ifrågasättas om en sådan vid möjlighet för regeringen att meddela föreskrifter om direktåtkomst skulle vara förenligt med 2 kap. 6 § RF. Det bör av dessa skäl regleras i domstolsdatalagen i vilka fall direktåtkomst får medges.

Direktåtkomst för myndigheter som omfattas av domstolsdatalagen

Det tydligaste behovet av direktåtkomst finns domstolarna emellan. De allmänna förvaltningsdomstolarna har möjlighet att med hjälp av direktåtkomst söka bland överrättsavgöranden i

Vera. Det är uppenbart att detta är till stor nytta för förvaltningsrätterna och kammarrätterna. I avsnitt 13.2 görs bedömningen att domstolarna bör kunna söka bland avgöranden för att säkerställa en enhetlig rättstillämpning och effektiv handläggning. Det är ofta lika viktigt att en domstol kan söka bland andra domstolars avgöranden som bland sina egna. Åtkomstbehovet gäller väsentligen inom varje domstolsslag, men det torde mer sällan vara nödvändigt att komma åt information mellan domstolsslagen. Det saknas således normalt anledning för en domstol inom ett domstolsslag att ha direktåtkomst till avgöranden i det andra domstolsslaget. Överrätternas behov av att ha tillgång till lägre instansers avgöranden är mindre än vice versa. Hyres- och arrendenämnder behöver i första hand få tillgång till varandras avgöranden samt till Svea hovrätts domar och beslut, eftersom nämndernas avgöranden kan överklagas dit. Utöver själva avgörandedokumenten behöver direktåtkomsten också omfatta sådana uppgifter som behövs för återsökning av avgörandena, t.ex. sammanfattningar och sökord.

Domstolarna kan vidare ha behov av direktåtkomst till vissa uppgifter för att kunna konferera mål. Med konferering menas att domstolarna genom sökningar säkerställer att samma fråga inte redan är föremål för prövning i någon domstol (litis pendens) samt att frågan inte redan är rättskraftigt avgjord (res judicata). Det är också angeläget att mål som av olika skäl inletts i olika domstolar trots att de borde handläggas tillsammans kan identifieras och sammanföras. Detta är inte minst viktigt i brottmål, eftersom en rättssäker straffmätning i många fall förutsätter att alla pågående mål som rör en viss tilltalad kan identifieras.

En av tankarna med RIF-samarbetet är att partsuppgifter, uppgifter om misstänkta brott och annan strukturerad information ska kunna återanvändas av en överrätt när ett mål eller ärende överklagas så att uppgifterna inte behöver matas in manuellt i datorsystemen flera gånger. När ett mål överklagas behöver överrätten vidare kunna ta del av ljud- och bildupptagningar som lagras elektroniskt i underrättens datorsystem. Utan denna möjlighet skulle ljud- och bildfilerna behöva lagras

parallellt i flera domstolar. En underrätt bör av dessa skäl kunna medge en överrätt direktåtkomst till uppgifter i underrättens datorsystem.

Direktåtkomst till andra domstolars uppgifter kan också behövas för delgivningsändamål. Att parter och ombud kan delges handlingar är avgörande för att domstolarna överhuvudtaget ska kunna handlägga mål och ärenden. Dessvärre har domstolarna svårigheter att nå enskilda för delgivning. Detta leder bl.a. till att förhandlingar måste ställas in eller att handläggningen i övrigt fördröjs. Det innebär en onödig psykisk påfrestning för parter, vittnen och andra aktörer att tvingas infinna sig i rätten flera gånger innan den förhandling de kallats till kan genomföras. Fördröjda domstolsprocesser leder också till stora kostnader.[2] Det är således angeläget att domstolarna får bästa tänkbara förutsättningar att genomföra delgivningar. Om en domstol sedan tidigare har bevarat uppgifter om var en viss person brukar uppehålla sig eller vederbörande arbetar bör övriga domstolar vid behov kunna ta del av dessa uppgiften i syfte att kunna delge honom eller henne handlingar. Domstolarna bör därför kunna medge varandra direktåtkomst till adressuppgifter och andra uppgifter som kan vara till hjälp i samband med delgivning.

Mot denna bakgrund finns det alltså flera skäl för att möjliggöra för domstolarna att medge varandra direktåtkomst. Integritetsriskerna med ett sådant medgivande är begränsade, framför allt med hänsyn till att samtliga inblandade myndigheter kommer att tillämpa domstolsdatalagens skyddsbestämmelser. De sökbegränsningar som föreslås i avsnitt 13 är utformade på ett sådant sätt att det avgörande för vilka sökbegränsningar som ska gälla vilken domstol uppgifterna behandlas vid – inte vid vilken domstol den som utför sökningen är anställd. Om en anställd vid en domstol med hjälp direktåtkomst söker bland uppgifter som finns vid en annan domstol är han eller hon

[2] Se t.ex. Riksrevisionens rapport Inställda huvudförhandlingar i brottmål, RiR 2010:7.

således bunden av sökbegränsningarna i samma utsträckning som de anställda vid den domstol där uppgifterna lagras. Sammanfattningsvis bör de domstolar och nämnder som omfattas av domstolsdatalagen ha möjlighet att medge varandra direktåtkomst.

Som framgår av redogörelsen är behovet av direktåtkomst olika starkt beroende på bl.a. hur den avsändande och mottagande domstolen förhåller sig till varandra i domstolsorganisationen. Behoven ser också olika ut beroende på om det är fråga om åtkomst till domar, till uppgifter som behövs för konferering eller till uppgifter för delgivningsändamål. Dessa behov varierar över tiden och är bl.a. beroende av hur domstolarnas inre och yttre organisation utformas, arbetsrutiner, målsammansättningen i domstolarna, forumregler m.m. De närmare villkoren för direktåtkomsten bör därför beslutas av regeringen eller den myndighet som regeringen bestämmer. Det kan därvid finnas skäl att begränsa möjligheterna att medge direktåtkomst till i huvudsak domstolar inom samma domstolsslag. Vidare kan regeringen överväga andra begränsningar som exempelvis tar sikte på vilken typ av uppgifter som får bli föremål för direktåtkomst.

Direktåtkomst för övriga myndigheter

Fråga är om domstolarna bör kunna medge myndigheter som inte omfattas av domstolsdatalagen direktåtkomst. Åklagarmyndigheten och vissa andra förvaltningsmyndigheter fullgör uppgifter och funktioner där ökade möjligheter att söka efter avgöranden skulle vara till viss nytta. Dessa behov kan dock i allt väsentligt tillgodoses på andra sätt. Myndigheterna har möjlighet att söka efter avgöranden i Domstolsverkets offentliga, internetbaserade rättsfallssamling Vägledande avgöranden (se avsnitt 13.1). Vidare kan myndigheterna ha en möjlighet att internt bygga upp egna elektroniska rättsfallssamlingar. Det blir allt vanligare att domstolarna expedierar domar elektroniskt till parter och till andra mottagare som enligt gällande rätt ska

tillställas kopior av alla domar i vissa måltyper. Detta underlättar för den myndighet som vill skapa en elektronisk rättsfallssamling. Huruvida det är tillåtet för myndigheter utanför domstolsdatalagens tillämpningsområde att bygga upp sådana rättsfallssamlingar styrs av den personuppgiftsreglering som gäller för respektive myndighet. Detta är en lämplig ordning eftersom det därigenom kan ske en anpassad avvägning mellan integritets- och effektivitetsintressen utifrån varje myndighets förutsättningar.

Den nuvarande planen för utvecklingen av RIF-samarbetet förutsätter inte att andra myndigheter än domstolar behöver beredas direktåtkomst till en domstols datorsystem. Om t.ex. en enskild polisman i framtiden ska få möjlighet att genom datorsystemen följa vad som händer med ett ärende som han eller hon tidigare har handlagt, bör detta i första hand kunna lösas genom elektroniskt utlämnande som inte innefattar direktåtkomst.

Domstolsverket intar i fråga om domstolarnas personuppgiftsbehandling en särställning jämfört med andra myndigheter. Verket konstruerar och underhåller de datorsystem som domstolarna använder sig av. För att kunna utföra sådana åtgärder kan Domstolsverket inta rollen av personuppgiftsbiträde (avsnitt 9.2) och i denna roll ha direkt tillgång till personuppgifter i domstolarnas verksamhet utan att det rättsligt sett blir fråga om direktåtkomst. Det saknas därför anledning att göra det möjligt för domstolarna att medge Domstolsverket direktåtkomst.

Domar i vissa mål överklagas från tingsrätt till Arbetsdomstolen och Marknadsdomstolen. Det kan inte uteslutas att dessa domstolar skulle ha en viss nytta av att få direktåtkomst. Med hänsyn till att de inte använder samma datorsystem som de domstolar som omfattas av domstolsdatalagen och inte deltar i RIF-samarbetet framstår dock behoven av direktåtkomst som mer begränsade.

Behoven av att kunna medge direktåtkomst till myndigheter som inte omfattas av domstolsdatalagen är sammanfattningsvis inte påtagliga samtidigt som integritetsriskerna med sådan direktåtkomst är större eller mer svårbedömda. Om direkt-

åtkomst medges kan t.ex. enskilda vända sig till den myndighet som har direktåtkomst och med stöd av offentlighetsprincipen begära att få ta del av de uppgifter som myndigheten har direktåtkomst till. (jfr prop. 2007/08:126 s. 122 och prop. 2007/08:160 s. 68). Det finns med hänsyn härtill inte tillräckliga skäl att skapa möjligheter till direktåtkomst för dessa myndigheter i andra fall än i deras egenskap av part (se nedan). Det bör dock framhållas att denna bedömning kan komma att behöva omprövas om det i framtiden uppkommer tydligare behov av direktåtkomst för vissa myndigheter, t.ex. på grund av den utveckling som kan komma att ske inom RIF-samarbetet.

Direktåtkomst för parter

Parter i mål och ärenden behöver ofta få uppgifter från domstolarna, framför allt i fråga om handläggningen. Det gäller t.ex. information om när ett mål beräknas bli avgjort eller när en förhandling ska hållas. En parts ombud, biträde eller försvarare har motsvarande behov.

Om dessa aktörer ges möjlighet att ha direktåtkomst till uppgifter i egna mål och ärenden kan tid sparas både för dem själva och för domstolarna. Direktåtkomsten är till hjälp för dem som regelbundet är i rätten, dvs. advokater och åklagare i allmän domstol och förvaltningsmyndigheter i allmän förvaltningsdomstol. För enskilda parter skulle direktåtkomsten kunna leda till ökad tillgänglighet till domstolarna. Likaså främjas insynen i domstolarnas verksamhet. En sådan utveckling är positiv och ligger i linje med regeringens allmänna strävan att utveckla bl.a. domstolarna i fråga om e-förvaltning.

I fråga om enskilda parter skulle det i de flesta fall röra sig om en ganska begränsad mängd personuppgifter. I förvaltningsdomstolarna är det oftast fråga om personuppgifter som avser den enskilde själv, varvid direktåtkomsten knappast innebär några risker. Myndigheter som är part i många mål (Åklagarmyndigheten, Skatteverket, Försäkringskassan m.fl.) skulle i och

för sig kunna få tillgång till en betydande mängd personuppgifter. Till största delen rör det sig dock om uppgifter som redan behandlas i dessa myndigheters egna datorsystem. Vidare kan det genom rättsliga och tekniska begränsningar säkerställas att dessa myndigheter inte använder direktåtkomsten till att göra avancerade eller integritetskänsliga sammanställningar.

De beskrivna intressena av effektivitet, tillgänglighet och insyn väger tungt, samtidigt som integritetsriskerna är begränsade om direktåtkomsten endast avser uppgifter i de egna målen. Domstolarna bör därför ha möjlighet att medge parter direktåtkomst till sitt eget mål i de fall domstolen bedömer att det är lämpligt. Samma sak gäller i förekommande fall parternas ombud, biträden eller försvarare.

En part eller ett ombud bör dock inte ha möjlighet att utföra sökningar som på en gång omfattar uppgifter i flera mål. Den som är part i många mål skulle annars kunna göra avancerade sammanställningar ur mycket stora informationsmängder. Avsikten med direktåtkomsten för parter är att de ska få insyn och kunna agera i sitt pågående mål i egenskap av part. Det bör därför inte vara möjligt för den som är part i många mål att göra sökningar som avser alla dessa mål eller att göra avancerade sammanställningar avseende uppgifterna i dessa mål. Att sådana åtgärder förhindras bör säkerställas genom att regeringen meddelar föreskrifter om särskilda sökbegränsningar.

Domstolarna är generellt skyldiga att genom tekniska och organisatoriska åtgärder skydda de personuppgifter som behandlas (se avsnitt 11.1). Innan en domstol medger någon utomstående direktåtkomst bör domstolen därför utifrån rådande förhållanden bedöma om den datasäkerhet som kan åstadkommas vid direktåtkomst är tillräckligt hög för att det ska vara lämpligt att medge sådan åtkomst. Innan direktåtkomst medges bör domstolen alltid överväga om det av något skäl är olämpligt. Det åligger också domstolarna att genom tekniska åtgärder eller på annat sätt se till att de parter m.fl. som har direktåtkomst inte kan utföra sökningar som är förbjudna enligt domstolsdatalagen. För att säkerställa ett i alla avseenden fullgott integritetsskydd

bör regeringen ha möjlighet att meddela föreskrifter om ytterligare begränsningar av möjligheterna att meddela direktåtkomst, om vem som ska ha behörighet att kunna använda sådan åtkomst och om säkerhet.

Direktåtkomst för allmänheten

Med hänsyn till integritetsriskerna brukar direktåtkomst oftast förbehållas myndigheter. Det är i fråga om domstolarnas rättskipande och rättsvårdande verksamhet inte aktuellt att tillåta direktåtkomst för enskilda som varken är parter eller ombud.

Enligt 6 kap. 6 § OSL ska en myndighet på begäran ge en enskild tillfälle att själv använda tekniska hjälpmedel för automatiserad behandling som myndigheten förfogar över för att ta del av upptagningar för automatiserad behandling. Lagen medger undantag från denna skyldighet i vissa fall, bl.a. om den enskilde skulle få tillgång till upptagningar som inte är allmänna handlingar. För att tillgodose detta krav ställer många domstolar en datorterminal till allmänhetens förfogande i sina offentliga utrymmen (”allmänhetens terminal”). Vid denna terminal är det möjligt för allmänheten att på egen hand ta del av uppgifter i domstolens verksamhetsstöd Vera. Det är endast offentliga uppgifter som kan visas på terminalen. Det finns ingen möjlighet för användaren att ta med sig uppgifterna i elektronisk form, t.ex. genom att med e-post skicka uppgifterna till sig själv eller spara uppgifterna på ett flyttbart lagringsmedium. Att på detta sätt erbjuda allmänheten möjlighet att läsa elektroniskt lagrade offentliga uppgifter brukar inte betraktats som direktåtkomst. Det saknas därför skäl att föreslå några särskilda regler i domstolsdatalagen om detta. ”Allmänhetens terminal” förekommer även hos Skatteverket.

14.4 Överföring till tredje land

Förslag: Domstolsdatalagen ska hänvisa till föreskrifterna i 33–35 §§ PUL om överföring av personuppgifter till tredje land.

Skälen för förslaget: Enligt 33 § PUL får personuppgifter som är under behandling inte föras över till tredje land, dvs. en stat som inte är medlem av EU eller är ansluten till Europeiska ekonomiska samarbetsområdet, om inte det mottagande landet har en adekvat nivå för skyddet av personuppgifter. Från förbudet finns vissa undantag och regeringen har också möjlighet att föreskriva ytterligare undantag från förbudet, bl.a. om det behövs med hänsyn till ett viktigt allmänt intresse (34 och 35 §§ PUL, se även 12–14 §§ PUF).

Dessa regler har sin grund i de krav som gäller enligt EU:s dataskyddsdirektiv. Även om överföring till tredje land inte är särskilt vanligt förekommande i domstolarnas rättskipande och rättsvårdande verksamhet kan det dock förekomma. Exempelvis kanske en domstol som en förberedande åtgärd inför ett telefonförhör med någon som befinner sig utomlands skickar ett e-postmeddelande med personuppgifter. Det saknas skäl att i domstolsdatalagen avvika från personuppgiftslagens reglering i denna del. Dessa bestämmelser bör därför gälla även inom domstolsdatalagens tillämpningsområde.

15 Bevarande i arkiv m.m.

15.1 Inledning

Allmänt om arkivering och gallring av allmänna handlingar

Domstolarna är liksom andra myndigheter skyldiga att bevara allmänna handlingar för arkivändamål. I 2 kap. 18 § TF föreskrivs att grundläggande bestämmelser om hur allmänna handlingar ska bevaras samt om gallring och annat avhändande av sådana handlingar ska meddelas i lag. Av 3 § tredje stycket arkivlagen (1990:782) framgår att myndigheternas arkiv ska bevaras, hållas ordnade och vårdas så att de tillgodoser rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen samt forskningens behov.

Varje myndighet är enligt 3 § arkivförordningen (1991:446) skyldig att arkivera allmänna handlingar i ett ärende sedan ärendet har slutbehandlats. I samband därmed ska myndigheten pröva i vilken omfattning sådana handlingar som avses i 2 kap. 9 § TF (minnesanteckningar, utkast och koncept) ska tas om hand för arkivering. Det framgår också av samma bestämmelse att varje anteckning i diarier och journaler samt register och förteckningar som förs fortlöpande (t.ex. dagboksfunktionen i Vera) ska anses arkiverad i och med att anteckningen har gjorts.

Huvudregeln är alltså att de allmänna handlingar som utgör en myndighets arkiv *ska bevaras*. Undantag från detta medges genom bestämmelserna om bl.a. gallring i 10 § arkivlagen, som anger att vid gallring enligt arkivlagen ska alltid beaktas att arkiven utgör en del av kulturarvet och att det arkivmaterial som

återstår ska kunna tillgodose arkivbildningens syften. Arkivlagstiftningen är teknikneutral och ställer alltså inga krav på att handlingarna t.ex. ska sparas i pappersform. Så länge uppgifter ändå bevaras i pappersform har det framför allt varit på grund av intresset av att spara kostnader samt att undvika ohanterligt stora arkiv som myndigheter gallrar uppgifter ur arkiven (jfr prop. 1989/90:72 bil. I s. 39 f.).

Om det finns avvikande bestämmelser om gallring av vissa allmänna handlingar i annan lag eller i förordning, gäller dessa bestämmelser (10 § tredje stycket arkivlagen). Enligt 14 § arkivförordningen får statliga myndigheter gallra allmänna handlingar endast i enlighet med föreskrifter eller beslut av Riksarkivet, om inte särskilda gallringsföreskrifter finns i lag eller förordning.

För domstolarnas del har Riksarkivet meddelat sådana föreskrifter.[1] Bestämmelserna innebär att domen i ett mål ska bevaras för alltid, men i fråga om uppgifter i akterna finns det bestämmelser om att gallring får ske. Exempelvis får förundersökningsmaterial hos tingsrätt gallras fem år efter att det aktuella målet vann laga kraft. Hos hovrätt och Högsta domstolen är tiden i stället tio år (9 § RA-MS 2010:3). Ett annat exempel är att det hos förvaltningsrätt och kammarrätt är tillåtet att gallra akterna i en rad måltyper när det gått sex år från utgången av det år när målet avgjordes (8 och 10 §§ RA-MS 2008:82). I denna promemoria skapas förutsättningar i fråga om personuppgiftsregleringen för att domstolarna ska kunna övergå till en fullständigt elektronisk uppgiftshantering. Det är därför lämpligt att Riksarkivet i samarbete med Domstolsverket ser över de

[1] RA-MS 1998:57 (omtryckt i RA-MS 2010:3) avseende brottmål i de allmänna domstolarna, RA-MS 2008:83 avseende tvistemål och ärenden hos de allmänna domstolarna, RA-MS 2008:82 (ändrad genom RA-MS 2010:16, 2010:81 och 2011:13) avseende de allmänna förvaltningsdomstolarna, RA-MS 2008:6 avseende hyres- och arrendenämnderna, RA-MS 2003:19 avseende hyres- och arrendenämnderna i Stockholm, Göteborg och Malmö, RA-MS 2006:26 avseende Hyres- och arrendenämnden i Gävle samt RA-MS 1994:25 för registret HDREFER hos Högsta domstolen som inte längre används.

gallringsföreskrifter som gäller för domstolarna och anpassar dem till den pågående och förestående tekniska utvecklingen.

Utöver Riksarkivets föreskrifter finns det förordningsbestämmelser som gör det möjligt för domstolarna att gallra. Dubbletter, missiv, delgivningsbevis m.m. får exempelvis gallras i samband med att ett mål eller ärende avslutas (se t.ex. 37 § mål och ärendeförordningen). För de allmänna domstolarna är denna gallring obligatorisk. I fråga om ljud- och bildupptagningar gäller att dessa ska gallras redan sex veckor efter det att målet eller ärendet har avgjorts genom en dom eller ett beslut som har vunnit laga kraft (se t.ex. 20 § mål och ärendeförordningen).

Gällande personuppgiftsregler om bevarande

I personuppgiftslagen föreskrivs i 9 § första stycket i) att personuppgifter inte får bevaras elektroniskt under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Denna bestämmelse går tillbaka på de krav som följer av dataskyddsdirektivet (artikel 6). Personuppgiftslagen innehåller dock två viktiga undantag.

För det första hindrar personuppgiftslagens bestämmelser aldrig att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet (8 § andra stycket PUL). Detta generella undantag från personuppgiftslagens krav att uppgifter ska tas bort från datorsystemen har tillkommit för att offentlighetsprincipen i 2 kap. TF ska kunna uppfylla sina syften (prop. 1997/98:44 s. 118). Om personuppgifter i allmänna handlingar inte skulle få bevaras längre än vad som allmänt gäller för personuppgifter skulle rätten att ta del av allmänna handlingar i enlighet med offentlighetsprincipen riskera att urholkas.

För det andra finns det ett undantag som gäller för alla personuppgifter, oavsett om de utgör en allmän handling hos en myndighet. Det följer av 9 § tredje stycket PUL att personuppgifter får bevaras så länge det sker för historiska, statistiska

eller vetenskapliga ändamål. Vid sådant bevarande gäller dock den begränsningen att personuppgifterna får användas för att vidta åtgärder i fråga om den registrerade bara om den registrerade har lämnat sitt samtycke eller det finns synnerliga skäl med hänsyn till den registrerades vitala intressen (9 § fjärde stycket PUL).

Ytterligare bestämmelser om bevarande, vilka kompletterar personuppgiftslagen, finns i två av de fyra Vera-förordningarna, nämligen de förordningar som gäller för de allmänna domstolarna respektive förvaltningsrätterna. Bestämmelserna innebär att personuppgifter som behandlas i verksamhetsregistren ska tas bort ur verksamhetsregistret högst nio år efter avgörandeåret. För brottmål och de flesta förvaltningsrättsliga mål utom skattemål är fristen i stället fem år. Enligt de Vera-förordningar som gäller för Högsta förvaltningsdomstolen och kammarrätterna samt hyres- och arrendenämnderna gäller i stället att personuppgifter ska tas bort ur verksamhetsregistren enligt föreskrifter som Riksarkivet kan meddela. Denna möjlighet har Riksarkivet endast utnyttjat i fråga om ett datorsystem som inte längre används. Det torde innebära att personuppgiftslagens bestämmelser gäller. Beträffande rättsfallsregister saknas det bevaranderegler i Vera-förordningarna och uppgifter i dessa register får därför bevaras så länge det är tillåtet enligt personuppgiftslagen. Fristerna i Vera-förordningarna gäller inte för uppgifter som – vid sidan av eller i anslutning till verksamhets- eller rättsfallsregistren – behandlas i löpande text, i ljudupptagningar eller i ljud- och bildupptagningar. För sådana uppgifter tillämpas i stället personuppgiftslagens regler, om inte annat är särskilt föreskrivet (se t.ex. 8 § förordningen [2001:639] om registerföring m.m. vid allmänna domstolar med hjälp av automatiserad behandling).

Domstolsverkets skrivelser

Domstolsverket har i skrivelser till regeringen[2] hemställt om att bl.a. tidsfristerna i Vera-förordningarna för bevarande i verksamhetsstödet och fristerna för gallring enligt arkivlagstiftningen bör synkroniseras samt att bevarandetiden för systemgallring i brottmål ska räknas från tiden för laga kraft i stället för från tiden för avgörandet. Det är enligt verket nämligen viktigt att undvika en situation där elektroniskt lagrade handlingar på grund av personuppgiftsregleringen måste skrivas ut i pappersform för att arkivlagstiftningens krav på bevarande ska kunna följas. Enligt Domstolsverket bör vidare reglerna vara enhetliga mellan domstolarna och domstolsslagen.

För att de elektroniskt förvarade handlingar som inte ska gallras ska kunna tas om hand för framtiden bör enligt Domstolsverket ett system för e-arkivering av handlingar finnas på plats. Eftersom det av Domstolsverket inte bedöms möjligt att få till stånd ett sådant system för Sveriges Domstolar inom de närmaste åren anser verket att domstolarna under en övergångsperiod bör tillåtas att bevara uppgifterna i verksamhetssystemet en något längre tid än vad som annars är motiverat i avvaktan på att ett e-arkiv finns på plats.

Elektroniskt bevarande och konsekvenserna för integritetsskyddet

Så länge uppgifter bevaras i pappersform är det framför allt intresset av att spara kostnader samt att undvika ohanterligt stora arkiv som domstolarna gallrar uppgifter ur arkiven. När mer eller mindre all skriftlig uppgiftshantering, inklusive aktbilagor, sker i elektroniskt format blir det möjligt att bevara uppgifter på hårddiskar eller andra databärare, vilket gör att arkivkostnaderna blir avsevärt mindre jämfört med pappersarkivering. När uppgifter bevaras elektroniskt är det tack vare

[2] Dnr Ju2006/7183/DOM, Ju2010/1564/SI, Ju2010/10147/SI och Ju2011/6800/SI.

datoriserade sökfunktioner oftast lätt att orientera sig även i mycket omfattande material. Elektroniskt bevarande innebär således att de incitament som funnits för att gallra i pappersarkiv inte gör sig gällande på samma sätt.

Att bevara information elektroniskt i stället för i pappersformat innebär integritetsrisker. Var och en har ett berättigat intresse av att inte för all framtid kunna kopplas ihop med olika känsliga förhållanden som framgår av domstolsakter, såsom sjukdomar eller brott. När uppgifter om en persons domstolskontakter finns sparade elektroniskt är det enklare att kartlägga personen. Uppgifter från olika akter och olika tidpunkter kan då kombineras med hjälp av automatiserade sökningar. När det gäller domstolarna måste det särskilt beaktas att de uppgifter som bevaras till största delen är offentliga och därmed åtkomliga för vem som helst. Detta är en väsentlig skillnad mot exempelvis polisens verksamhet.

Tillgången till bevarade uppgifter kan emellertid också vara integritetsfrämjande. Ju mer information som sparas och finns åtkomlig, desto lättare är det också att verifiera eller falsifiera andra uppgifter. Bevarande av uppgifter bidrar på ett generellt plan till att äktheten och tillförlitligheten hos uppgifter som åberopas i olika sammanhang kan kontrolleras. Tillgången till skriftlig dokumentation kan också vara en förutsättning för att rekonstruera historiska händelseförlopp. Bevarande av uppgifter kan således bidra till att den som utsatts för ett integritetsintrång i ett senare skede kan få skadestånd eller annan upprättelse (jfr bl.a. SOU 2001:100 s. 163 f samt SOU 1992:2 och SOU 2000:20).

15.2 Elektroniskt bevarande

Förslag: Domstolsdatalagen ska hänvisa till 8 § andra stycket samt 9 § första stycket i) och tredje stycket PUL om bevarande av personuppgifter. Detta innebär att elektroniskt bevarande av allmänna handlingar ska regleras genom arkivlagen, arkivförordningen och Riksarkivets föreskrifter samt att övriga personuppgifter ska få bevaras så länge det är nödvändigt med hänsyn till ändamålen med behandlingen eller om bevarandet sker för historiska, statistiska eller vetenskapliga ändamål.

Skälen för förslaget: Genom domstolsdatalagen läggs grunden för att domstolarna på sikt ska kunna helt övergå till en ordning med s.k. e-akter (dvs. mål- och ärendeakter som består av elektroniska handlingar) samt att diarier och annan skriftlig information i den rättskipande och rättsvårdande verksamheten ska kunna hanteras elektroniskt. För att en sådan elektronisk hantering ska vara möjlig krävs en anpassning även av den reglering som styr bevarande av uppgifter efter det att ett mål eller ärende avgjorts genom en lagakraftvunnen dom eller beslut. Det vore mycket svårt att försvara en ordning där domstolarna i och för sig kan hantera aktbilagor och andra handlingar elektroniskt så länge handläggningen pågår men sedan måste skriva ut de elektroniska handlingarna på papper när handläggningen avlutats, med det enda syftet att kunna arkivera handlingarna. Ett grundläggande och oavvisligt krav i fråga om den reglering som nu föreslås bör därför vara att domstolarna ska ha möjlighet att genom elektroniskt bevarande tillgodose de behov som finns av att spara uppgifter i mål och ärenden efter det att handläggningen avslutats och avgörandet vunnit laga kraft. Nödvändigt integritetsskydd bör åstadkommas på annat sätt än att domstolarna av integritetsskäl hindras från datorbaserad arkivbildning eller annat elektroniskt bevarande som är nödvändigt i verksamheten.

Med denna utgångspunkt finns det i huvudsak två sätt att reglera frågan om bevarande. Ett alternativ är att i domstolsdatalagen uttömmande reglera frågan om elektroniskt bevarande av uppgifter i mål och ärenden och därigenom ersätta bestämmelserna om gallring i Riksarkivets föreskrifter. En fördel med en sådan lösning är att det blir tydligt vad som gäller och att det blir möjligt att göra en samlad integritetsbedömning. Mot denna lösning talar emellertid det faktum att Riksarkivet är den instans som är bäst skickad att överblicka och bedöma de intressen för vilka allmänna handlingar behöver bevaras (dvs. rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen samt forskningens behov). Riksarkivet är också den instans som bäst kan bedöma i vilken utsträckning allmänna handlingar kan gallras utan att nämnda intressen åsidosätts. Offentligheten har en särskilt stark ställning inom domstolarnas verksamhet och vikten av att nämnda arkivintressen får ett starkt genomslag gör sig särskilt gällande i denna verksamhet.

Ett annat alternativ är att låta frågan om elektroniskt bevarande av uppgifter i mål och ärenden regleras av det arkivrättsliga regelverket (framför allt arkivlagen, arkivförordningen och Riksarkivets föreskrifter). Även denna lösning innebär att det blir tydligt vad som gäller. Dessutom saknar detta alternativ de nackdelar som det första alternativet är förknippat med. Eftersom behovet av information för rättskipningen är särskilt beaktat i arkivlagen kan domstolarnas behov av att kunna bevara uppgifter bli väl tillgodosedda med detta alternativ, i synnerhet som Riksarkivets föreskrifter rörande domstolarna tas fram i samråd med Domstolsverket och domstolarna. En nackdel är att Riksarkivets gallringsföreskrifter inte utformas med särskild hänsyn till de integritetsrisker som kan vara förknippade med bevarande av personuppgifter. I avsnitt 15.3 föreslås emellertid en ordning för att begränsa dessa risker på annat sätt. Det nu beskrivna alternativet återspeglar vad som gäller enligt Vera-förordningarna i fråga om uppgifter i löpande text (se t.ex. 7 och 8 §§ förordningen [2001:640] om registerföring m.m. vid

förvaltningsrätt med hjälp av automatiserad behandling). Det är också den lösning som har valts i polisdatalagen och kustbevakningsdatalagen när det gäller bevarande av uppgifter i ärenden om utredning eller beivrande av brott (2 kap. 13 § respektive 3 kap. 5 §, se även prop. 2011/12:45 s. 207 och 216).

Mot den angivna bakgrunden görs bedömningen att frågan om elektroniskt bevarande av uppgifter i mål och ärenden bör hanteras i enlighet med det andra alternativet, vilket innebär att frågan regleras genom det arkivrättsliga regelverket. För att åstadkomma detta bör domstolsdatalagen hänvisa till 8 § andra stycket PUL. Den bestämmelsen innebär nämligen att personuppgifter i allmänna handlingar kan bevaras elektroniskt samt överlämnas till arkivmyndighet utan hinder av domstolsdatalagen. Det är avgörande för detta ställningstagande att det elektroniska bevarandet inte leder till otillbörliga integritetsrisker. Att så inte sker säkerställs genom de särskilda skyddsregler som redovisas i avsnitt 15.3.

Den övervägande delen av alla personuppgifter i domstolarnas rättskipande och rättsvårdande verksamhet torde utgöra allmänna handlingar eller bli allmänna handlingar under handläggnings- och arkiveringsprocessen i enlighet med bestämmelserna i 2 kap. TF. Det skulle därför eventuellt vara tillräckligt att i domstolsdatalagen hänvisa till 8 § andra stycket PUL, men för att säkerställa en heltäckande bevaranderegelering bör en hänvisning till bestämmelserna i 9 § första stycket i) och tredje stycket också inkluderas. Det innebär att personuppgifter som inte finns i en allmän handling (t.ex. personuppgifter i en föredragningspromemoria eller ett domsutkast) kan bevaras elektroniskt så länge det är nödvändigt med hänsyn till ändamålen med behandlingen eller om bevarandet sker för historiska, statistiska eller vetenskapliga ändamål.

15.3 Ett förstärkt integritetsskydd för elektroniskt bevarade uppgifter

Förslag: Regeringen eller den myndighet som regeringen bestämmer meddelar särskilda föreskrifter om villkoren för bevarande av uppgifter som hänför sig till ett mål eller ärende som har avgjorts genom en dom eller ett beslut som har vunnit laga kraft.

Bedömning: I förordning bör tillgången till personuppgifter i avslutade mål och ärenden begränsas. Direktåtkomst och sökning bör i huvudsak endast tillåtas för domstolarna och då endast när det behövs för handläggning av mål och ärenden. Sådan tillgång bör vidare vara begränsad i tid och till vissa uppgifter. Särskilda krav bör också gälla i fråga om säkerhet och intern åtkomst.

Skälen för förslaget och bedömningen: I föregående avsnitt föreslås att frågan om elektroniskt bevarande av personuppgifter i mål och ärenden ska styras av det arkivrättsliga regelverket. Det konstateras också att dessa regler inte är utformade med någon särskild hänsyn till de integritetsrisker som är förknippade med elektroniskt bevarande. Som framgår ovan uppstår riskerna framför allt om uppgifterna blir åtkomliga för automatiserade sökningar och sammanställningar (avsnitt 15.1). Möjligheterna till direktåtkomst och annan spridning av uppgifterna utgör också en risk för integritetsintrång.

Ett viktigt skäl till att domstolarna bevarar uppgifter från avslutade mål och ärenden är att domstolarna har ett eget behov av att kunna komma åt uppgifterna. Detta återspeglas i arkivlagen, enligt vilken syftet med domstolars och andra myndigheters arkivbildning bl.a. är att tillgodose behovet av information för rättskipningen (3 §). Domstolarna kan dock med hänsyn till integritetsintresset inte tillåtas ha en oförändrad åtkomst till uppgifter i mål och ärenden när handläggningen avslutats genom lagakraftvunnen dom eller beslut.

Mot denna bakgrund bör det inte vara möjligt för domstolarna att fortsätta hantera elektroniska personuppgifter på samma sätt efter det att handläggningen av ett mål eller ärende har avslutats och avgörandet har vunnit laga kraft. Det är påkallat att föreskriva begränsningar som innebär att domstolarnas möjligheter att bevara personuppgifter elektroniskt närmar sig den verklighet som alltid har gällt i fråga om pappersarkiv. Samtidigt är det inte rimligt att låta begränsningarna få en utformning som omöjliggör för domstolarna att i rimlig utsträckning utnyttja de möjligheter till ökad effektivitet, rättssäkerhet och insyn som erbjuds tack vare övergången till elektroniskt bevarande.

För det första bör möjligheterna till direktåtkomst begränsas ytterligare i förhållande till vad som gäller generellt enligt domstolsdatalagen. I traditionella pappersarkiv finns överhuvudtaget inte några möjligheter till sådan elektronisk fjärrtillgång. Eftersom domstolarna har ett berättigat behov av att söka efter domar och beslut (avsnitt 13.1 och 13.2) bör dock domstolar kunna medges direktåtkomst till just sådana handlingar under ett begränsat antal år efter det domen eller beslutet vunnit laga kraft. Vidare bör domstolarna under en begränsad tid kunna medges direktåtkomst till de specifika uppgifter som behövs för konferering och för att underlätta delgivning. Dessa behov beskrivs i avsnitt 14.3.

För det andra finns det skäl att begränsa sökmöjligheterna ytterligare i förhållande till vad som annars föreslås gälla enligt domstolsdatalagen. I ett pappersarkiv är det normalt nödvändigt att känna till mål- eller ärendenummer, eller i vart fall dagen för avgörande, för att en dom eller akt ska kunna identifieras. I de fall uppgifter bevaras elektroniskt, i stället för i ett pappersarkiv, är det därför rimlig utgångspunkt att endast sökbegrepp som avser mål- eller ärendenummer och datum för avgörande ska vara tillåtna. Det framgår av avsnitt 13 att domstolarna har ett omfattande och berättigat behov av att kunna söka efter uppgifter. Domar och beslut bör mot denna bakgrund vara åtkomliga för sökning inom domstolarna under ett antal år efter

tidpunkten för laga kraft. Domstolarna bör också kunna utföra sökningar som behövs för konferering och för att underlätta delgivning. När denna begränsade tid har förflutit bör endast de ovan angivna mer begränsade sökmöjligheterna kunna användas.

För det tredje finns det skäl att föreskriva särskilda begränsningar avseende hur uppgifter som hör till avslutade mål och ärenden ska bevaras (exempelvis i ett separat datorsystem) och vilka personalkategorier inom domstolen som ska ha elektronisk tillgång till vilka uppgifter.

Sammanfattningsvis bör det gälla särskilda begränsningar avseende sökning, direktåtkomst, säkerhet, intern åtkomst m.m. för uppgifter som är hänförliga till mål eller ärenden som avgjorts genom en dom eller beslut som har vunnit laga kraft. Ju längre tid som förflutit sedan ett mål eller ärende avgjorts rättskraftigt, desto mindre påtagliga blir behoven av att på ett enkelt sätt kunna komma åt uppgifter som hör till målet eller ärendet. De begränsningarna som nu övervägs bör därför kopplas till tidsfrister, så att regleringen blir mer rigorös när ett antal år förflutit sedan målet eller ärendet vann laga kraft.

Mot den ovan angivna bakgrunden kan det konstateras att regleringen bör vara relativt detaljerad och att det är fråga om regler som kan behöva justeras ganska ofta, exempelvis när domstolarnas arbetssätt utvecklas eller då nya måltyper tillkommer i verksamheterna. Det talar för att regleringen av de aktuella frågorna bör ske i förordning och i myndighetsföreskrifter, snarare än i lag. En mer detaljerad reglering ger också bättre förutsättningar för att optimera den avvägning som ska ske mellan integritets- och effektivitetsintressena. Av dessa skäl bör det överlåtas på regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om de särskilda begränsningar som ska gälla för bevarande av personuppgifter som är hänförliga till mål och ärenden vilka avgjorts genom en dom eller ett beslut som har vunnit laga kraft.

16 Insyn och tillsyn

16.1 Inledning

För att uppnå ett starkt integritetsskydd vid personuppgiftsbehandling i domstolarnas rättskipande och rättsvårdande verksamhet det viktigt att behandlingarna sker med omsorg och att domstolsdatalagen tillämpas på ett korrekt sätt. Detta kan säkerställas på flera sätt.

Öppenhet och transparens kring vilka personuppgiftsbehandlingar som domstolarna utför är i detta sammanhang viktigt. Genom att registrerade och andra enskilda får insyn i vilka behandlingar som en domstol genomför har var och en möjlighet att försäkra sig om att felaktiga behandlingsåtgärder inte genomförs (avsnitt 16.2).

Ansvaret för domstolsdatalagens tillämpning ligger ytterst på den personuppgiftsansvarige, dvs. varje enskild domstol (avsnitt 9.1). Interna kontrollfunktioner, exempelvis ett personuppgiftsombud, utgör en ytterligare garant för att inga oberättigade integritetsintrång sker (avsnitt 16.4). En extern tillsynsmyndighet, som Datainspektionen, kan i egenskap av utomstående expertmyndighet säkerställa att domstolarnas personuppgiftsbehandling underkastas en objektiv kontroll samt att domstolarna får råd och stöd rörande tillämpningen av domstolsdatalagen (avsnitt 16.3).

I avsnitt 17 förslås att enskilda ska kunna begära skadestånd och rättelse. Dessa rättsmedel bidrar till att undvika att otillbörliga integritetsintrång sker.

16.2 Enskildas insyn i personuppgiftsbehandlingen

Förslag: Den personuppgiftsansvarige ska vara skyldig att föra en särskild förteckning över de personuppgiftsbehandlingar som sker med stöd av domstolsdatalagen. Den personuppgiftsansvarige ska också vara skyldig att på begäran lämna sådan information till enskilda.

Domstolsdatalagen ska hänvisa till 23 och 25–27 §§ PUL om information till den enskilde.

Skälen för förslaget

Bakgrund

Enskildas insyn i domstolarnas personuppgiftsbehandling är en viktig aspekt av personuppgiftsskyddet eftersom insynen möjliggör för enskilda att försäkra sig om att domstolarnas personuppgiftsbehandling sker på ett korrekt sätt i enlighet med gällande regler, t.ex. att uppgifterna ska vara riktiga och behandlas för tillåtna ändamål. Den insyn som enskilda har i praktiken påverkas av flera faktorer. Det finns därför anledning att på ett samlat sätt överväga hur enskildas insyn i domstolarnas personuppgiftsbehandling ska säkerställas.

Det kan inledningsvis konstateras att domstolarnas verksamhet kännetecknas av att den i hög grad styrs av de processuella regelverken, t.ex. rättegångsbalken och förvaltningsprocesslagen. Inom det tillämpningsområde som föreslås för domstolsdatalagen, dvs. domstolarnas rättskipande och rättsvårdande verksamhet, utförs de flesta personuppgiftsbehandlingar med stöd av, eller i vart fall som ett utflöde av, dessa regelverk. Tack vare att domstolarnas verksamhet är så genomreglerad har en utomstående förhållandevis goda möjligheter att bilda sig en uppfattning om vilka personuppgiftsbehandlingar som en domstol utför. Möjligheterna till insyn underlättas naturligtvis också av att en så stor del av uppgifterna som behandlas i domstolarna är offentliga samt att den enskilde som är part har en mycket

långtgående rätt till insyn och dessutom bidrar själv med många av de uppgifter som tillförs målet. Fråga är vilka ytterligare mekanismer som bör införas i syfte att stärka enskildas insyn i domstolarnas personuppgiftsbehandling.

Årlig information

Enligt personuppgiftslagen gäller att den personuppgiftsansvarige till var och en som ansöker om det en gång per kalenderår utan kostnad ska lämna besked om huruvida personuppgifter som rör den sökande behandlas. Om så är fallet ska information lämnas om vilka uppgifter det rör sig om, varifrån uppgifterna har hämtats, ändamålen med behandlingen och till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut. Information behöver dock inte lämnas om personuppgifter i löpande text som inte har fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande, under förutsättning att uppgifterna inte har lämnats ut till tredje man (26 § PUL). Rätten till information gäller inte om det i lag eller annan författning eller i beslut som har meddelats med stöd av författning särskilt har föreskrivits att uppgifter inte får lämnas ut till den registrerade (27 § PUL). Dessa bestämmelser har sin grund i dataskyddsdirektivet (artiklarna 12 a och 13.1 g). Enligt gällande rätt är de tillämpliga i domstolarnas verksamhet.

De angivna bestämmelserna ger den enskilde en möjlighet att kontrollera om han eller hon är registrerad och, om så är fallet, att de registrerade personuppgifterna är riktiga. Detta bidrar på ett praktiskt sätt till den enskildes skydd mot felaktig personuppgiftsbehandling. Såvitt framkommit har bestämmelserna inte medfört några problem eller betungande administration i domstolarnas verksamhet. Mot denna bakgrund bör en hänvisning till 26 och 27 §§ PUL tas in i domstolsdatalagen.

En förteckning över personuppgiftsbehandlingar

Enligt 36 § första stycket PUL gäller en skyldighet att anmäla personuppgiftsbehandlingar till tillsynsmyndigheten (Datainspektionen). Som anförs i avsnitt 16.3 bör någon hänvisning inte göras i domstolsdatalagen till denna bestämmelse. Detta hänger samman med att anmälningsskyldigheten enligt personuppgiftslagen inte gäller för behandlingar som regleras genom särskilda föreskrifter i lag eller förordning såsom domstolsdatalagen och att en hänvisning därför skulle bli meningslös (se 3 § PUF). Det finns dock anledning att överväga om domstolarna bör vara skyldiga att sammanställa och göra tillgänglig den information som en sådan anmälan skulle ha innehållit.[1] Det rör sig som följande uppgifter:

- den personuppgiftsansvariges namn, adress, telefonnummer och organisationsnummer,
- ändamålet eller ändamålen med behandlingen,
- en beskrivning av den eller de kategorier av registrerade som berörs av behandlingen,
- en beskrivning av de uppgifter eller kategorier av uppgifter som ska behandlas om de registrerade,
- uppgift om mottagarna eller de kategorier av mottagare till vilka uppgifterna kan komma att lämnas ut,
- upplysning om överföringar av uppgifter till tredje land,
- en allmän beskrivning av de åtgärder som har vidtagits för att trygga säkerheten i behandlingen.[2]

Fördelen med att ålägga domstolarna en skyldighet att föra en sådan förteckning är att såväl den registrerade som andra kan få tillgång till en uppdaterad beskrivning som innehåller mer preci-

[1] En sådan skyldighet föreligger enligt personuppgiftslagen i vissa situationer och avseende vissa personuppgiftsbehandlingar, närmare bestämt i de fall ett personuppgiftsombud utses (39 §), men förteckningen behöver då ändå inte avse personuppgiftsbehandling som regleras genom särskilda föreskrifter, såsom exempelvis domstolsdatalagen (39 § PUL jämförd med 36 § PUL och 3 § tredje punkten personuppgiftsförordningen).

[2] Se 6 § Datainspektionens föreskrifter (DIFS 1998:2) i fråga om skyldigheten att anmäla behandlingar av personuppgifter till Datainspektionen, omtryckta genom DIFS 2001:1.

serad information om vilka personuppgiftsbehandlingar som sker vid en domstol än vad som kan utläsas ur domstolsdatalagen. Detta är särskilt värdefullt med tanke på att domstolsdatalagen, till skillnad från Vera-förordningarna, inte bör innehålla några uppräkningar av vilka personuppgiftsbehandlingar som ska vara tillåtna (se avsnitt 6.2). En förteckning som domstolarna själva ansvarar för kan, jämfört med författningsbestämmelser, justeras relativt formlöst och anpassas till de vid varje tillfälle rådande förhållandena hos varje enskild domstol. Sådana justeringar kan förväntas bli nödvändiga när t.ex. ny teknik tas i bruk inom domstolarnas verksamhet och när arbetet med rättsväsendets informationsförsörjning utvecklas.

Förteckningar av nu aktuellt slag har också andra fördelar. De kan bli ett stöd för domstolarna i arbetet med att säkerställa att deras personuppgiftsbehandling uppfyller de säkerhetskrav som uppställs genom domstolsdatalagen. Vidare kan domstolarna med hjälp av förteckningen på ett enklare och snabbare sätt efterkomma enskildas begäran om information enligt 26 § PUL. I de fall den personuppgiftsansvarige väljer att publicera förteckningen på internet kan enskilda dessutom i många fall få den information de efterfrågar utan att ens behöva kontakta domstolen.

Om domstolarna åläggs en skyldighet att föra en förteckning över sina personuppgiftsbehandlingar innebär det naturligtvis visst merarbete och kostnader för att initialt upprätta förteckningen samt att fortlöpande uppdatera den. Detta arbete kan effektiviseras genom att Domstolsverket hjälper domstolarna att ta fram relevanta förteckningar. Innehållet i förteckningarna är till stor del beroende av hur domstolarnas datorstöd utformas, vilket Domstolsverket i praktiken har stort inflytande över.

Sammanfattningsvis skulle en generell skyldighet för domstolarna att föra en förteckning över sina personuppgiftsbehandlingar innebära tydliga fördelar bl.a. i fråga om enskildas insyn. En sådan skyldighet bör därför gälla enligt domstolsdatalagen. En lämplig utgångspunkt är att förteckningarna ska omfatta samma kategorier av uppgifter som en anmälan enligt 36 § PUL

till Datainspektionen. De närmare kraven på innehållet i förteckningarna bör regleras av regeringen eller den myndighet som regeringen bestämmer.

Uppgiftsskyldighet i förhållande till allmänheten

Det främsta syftet med skyldigheten att föra en förteckning är att underlätta för allmänheten att få kunskap om vilka personuppgiftsbehandlingar som utförs vid en domstol. Den som så önskar bör därför kunna få ta del av förteckningen. Därigenom tillgodoses kravet i artikel 21.3 i dataskyddsdirektivet att de personuppgiftsansvariga ska åläggas att på lämpligt sätt tillhandahålla var och en som begär det information av nu aktuellt slag. Artikel 21.3 i dataskyddsdirektivet har genomförts genom bestämmelserna i 42 § PUL. Av denna paragraf framgår bl.a. att den personuppgiftsansvarige till var och en som begär det skyndsamt och på lämpligt sätt ska lämna upplysningar om sina behandlingar av personuppgifter och att upplysningarna ska omfatta i princip samma information som ska framgå av den förteckning som domstolarna förslås bli skyldiga att föra. En motsvarande skyldighet bör gälla även enligt domstolsdatalagen. Av lagtekniska skäl är det dock inte lämpligt att hänvisa till 42 § PUL. En uttrycklig bestämmelse med motsvarande innehåll bör därför tas in i domstolsdatalagen. Det bör vidare, i linje med regleringen i 42 § PUL, förtydligas att skyldigheten att lämna upplysningar inte omfattar sekretessbelagda uppgifter eller uppgifter om vilka säkerhetsåtgärder som har vidtagits.

Uppgiftsskyldighet i förhållande till den registrerade

En ytterligare möjlighet att åstadkomma starkare insyn i domstolarnas personuppgiftsbehandling skulle vara att föreslå bestämmelser av det slag som finns i 23–25 §§ PUL eller göra dessa paragrafer tillämpliga genom en hänvisning. Dessa bestäm-

melser är enligt nuvarande ordning tillämpliga i domstolarnas rättskipande och rättsvårdande verksamhet.

Enligt 23 § PUL ska den personuppgiftsansvarige i samband med att personuppgifter samlas in självmant lämna den registrerade information om behandlingen av uppgifterna. Av 25 § första stycket PUL framgår att informationen ska omfatta

a) uppgift om den personuppgiftsansvariges identitet,
b) uppgift om ändamålen med behandlingen, och
c) all övrig information som behövs för att den registrerade ska kunna ta tillvara sina rättigheter i samband med behandlingen, såsom information om mottagarna av uppgifterna, skyldighet att lämna uppgifter och rätten att ansöka om information och få rättelse.

Enligt 25 § andra stycket PUL behöver information enligt 23 § inte lämnas om sådant som den registrerade redan känner till. I domstolarnas rättskipande och rättsvårdande verksamhet torde de registrerade som skickar in uppgifter till domstolarna (exempelvis parterna) i de flesta fall anses känna till den information som avses i 23 § PUL eftersom denna information framgår direkt av domstolsdatalagen, av den förteckning som domstolarna föreslås vara skyldig att sammanställa och av de processuella regelverken som styr domstolarnas verksamhet. Följden blir att domstolarna i praktiken sällan torde behöva lämna särskild information till den registrerade även om det i domstolsdatalagen tas in en hänvisning till 23 och 25 §§ PUL. Bestämmelserna i 23 och 25 §§ PUL har sin grund i dataskyddsdirektivet. För att det inte ska råda någon tvekan om att domstolsdatalagen lever upp till de krav som följer av unionsrätten bör dessa bestämmelser även fortsättningsvis vara tillämpliga i domstolarnas rättskipande och rättsvårdande verksamhet. Det bör därför i domstolsdatalagen tas in en hänvisning till bestämmelserna i 23 och 25 §§ PUL.

I 24 § PUL föreskrivs en skyldighet för den personuppgiftsansvarige att självmant lämna information till den registrerade i de fall personuppgifter samlas in från någon annan än den registrerade själv. Det är fråga om samma information

som enligt 23 §. Av 24 § andra stycket följer emellertid att informationsskyldigheten enligt 24 §, till skillnad från 23 §, inte gäller om det finns bestämmelser om registrerandet eller utlämnandet av personuppgifterna i en lag eller någon annan författning. I fråga om domstolarnas rättskipande och rättsvårdande verksamhet kommer det att finnas sådana bestämmelser dels i domstolsdatalagen och dels i rättegångsbalken, förvaltningsprocesslagen och övrig lagstiftning som styr domstolarnas verksamhet. I likhet med vad som gäller enligt polisdatalagen bör det därför inte tas in någon hänvisning till 24 § PUL i domstolsdatalagen.

16.3 Tillsynsmyndighet

Förslag: Domstolsdatalagen ska hänvisa till 32, 43–45 och 47 §§ PUL om tillsynsmyndighetens befogenheter att utöva tillsyn, med undantag för möjligheten att utfärda vitesföreläggande, samt till 41 § PUL om att regeringen har möjlighet att föreskriva att vissa särskilt känsliga behandlingar ska anmälas till tillsynsmyndigheten för förhandskontroll.

Skälen för förslaget: För att kunna säkerställa att personuppgifter behandlas på ett korrekt sätt har Datainspektionen i egenskap av tillsynsmyndighet enligt personuppgiftslagen vissa befogenheter gentemot den personuppgiftsansvarige.

Enligt 32 § första stycket PUL får Datainspektionen i enskilda fall besluta om vilka säkerhetsåtgärder som den personuppgiftsansvarige ska vidta enligt 31 § PUL, dvs. lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas (se avsnitt 11.1).

Enligt 43 § PUL har Datainspektionen möjlighet att på begäran få tillgång till de personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen och säkerheten vid denna samt tillträde till lokaler.

Om Datainspektionen efter en begäran enligt 43 § PUL inte kan få tillräckligt underlag för att konstatera att personuppgiftsbehandlingen är laglig, får myndigheten enligt 44 § förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än genom att lagra dem.

Enligt 45 § första stycket PUL ska Datainspektionen genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse om inspektionen konstaterar att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt. Om det inte går att få rättelse på något annat sätt eller saken är brådskande, får inspektionen vidare förbjuda den personuppgiftsansvarige att fortsätta att behandla personuppgifterna på något annat sätt än genom att lagra dem.

De redovisade bestämmelserna i 32 och 43–45 §§ PUL om tillsyn är enligt nuvarande ordning tillämpliga i domstolarnas rättskipande och rättsvårdande verksamhet och tillsynsmyndigheten bör även i fortsättningen ha samma befogenheter. Därigenom får Datainspektionen goda möjligheter att stödja domstolarna i deras arbete med att säkerställa integritetsskyddet i verksamheten. En hänvisning till de aktuella paragraferna bör därför tas in i domstolsdatalagen. Att förbjuda en domstol att behandla personuppgifter på något annat sätt än genom att lagra dem skulle i många fall innebära att verksamheten blockeras, vilket kan ha allvarliga följer för rättsäkerheten, tilltron till rättsväsendet och för enskildas möjligheter att ta tillvara sin rätt. Datainspektionen bör därför i det längsta undvika att tillgripa denna åtgärd.

Bestämmelserna i 32, 44 och 45 §§ PUL innehåller även en möjlighet för Datainspektionen att förena sina beslut med vite. I flera lagstiftningsärenden har en lösning valts som inte ger Datainspektionen någon sådan möjlighet. Detta har motiverats med grundsatsen att regler om vite inte bör tillämpas i förhållandet mellan statliga myndigheter (prop. 2004/05:164 s. 54 och 2006/07:46 s. 105, se även prop. 2009/10:85 s. 90). Domstolsdatalagen bör mot denna bakgrund inte möjliggöra för

Datainspektionen att vid vite förbjuda en domstol att behandla personuppgifter enligt domstolsdatalagen.

Enligt 47 § första stycket PUL har Datainspektionen rätt att hos allmän förvaltningsdomstol ansöka om att sådana uppgifter som har behandlats på ett olagligt sätt ska utplånas. I andra stycket anges att beslut om utplånande inte får meddelas om det är oskäligt. Bestämmelsen har sin grund i dataskyddsdirektivet (artikel 28.3). Där anges att varje nationell tillsynsmyndighet ska ha befogenheter att inleda rättsliga förfaranden när de nationella bestämmelser som antagits till följd av direktivet har överträtts, alternativt att uppmärksamma de rättsliga myndigheterna på dessa överträdelser. För att tillgodose direktivets krav bör Datainspektionen ha möjlighet att ansöka om utplåning av uppgifter i domstolarnas rättskipande och rättsvårdande verksamhet vilket åstadkoms genom en hänvisning till 47 § PUL, i likhet med vad som gäller enligt polisdatalagen (prop. 2009/10:85 s. 90). Beslut om utplåning får enligt 47 § andra stycket PUL inte meddelas om det är oskäligt, vilket innebär att det inte bör komma i fråga att utplåna uppgifter som behövs för handläggningen av mål och ärenden eller som på grund av processrättsliga regler eller allmänna rättsprinciper bör bevaras.

Automatiserade behandlingar av personuppgifter ska anmälas till Datainspektionen, om inte regeringen föreskriver om undantag från den skyldigheten (36 § första och tredje styckena PUL). Enligt 3 § PUF behöver anmälan inte göras för behandlingar som regleras genom särskilda föreskrifter i lag eller förordning, såsom den nya domstolsdatalagen. Det finns därför inget behov av att i denna lag hänvisa till 36 § första stycket PUL.

Det följer av 41 § PUL att regeringen har möjlighet att föreskriva att vissa särskilt känsliga behandlingar ska anmälas till Datainspektionen för förhandskontroll. Bestämmelsen har sin grund i artikel 20.1 i dataskyddsdirektivet som innehåller krav på att medlemsstaterna ska bestämma vilka behandlingar som kan innebära särskilda risker för den registrerades fri- och rättigheter samt säkerställa att dessa behandlingar kontrolleras innan de påbörjas. Även om regeringen inte har meddelat några sådana

föreskrifter som avses i 41 § PUL såvitt gäller domstolarnas verksamhet, saknas det skäl att inte behålla denna möjlighet i den lag som nu föreslås. En hänvisning till nämnda bestämmelse bör därför, precis som i polisdatalagen, införas i domstolsdatalagen.

I avsnitt 17.4 avhandlas frågan om överklagande av Datainspektionens beslut.

16.4 Personuppgiftsombud

Förslag: Varje domstol ska utse ett eller flera personuppgiftsombud. Detta – liksom entledigande av sådana ombud – ska anmälas till tillsynsmyndigheten.

Personuppgiftslagens bestämmelser om ombudets uppgifter i 38 och 40 §§ PUL ska tillämpas i domstolarnas rättskipande och rättsvårdande verksamhet.

Skälen för förslaget: I personuppgiftslagen föreskrivs en möjlighet för den personuppgiftsansvarige att utse ett personuppgiftsombud. Den personuppgiftsansvarige ska anmäla ombudet till Datainspektionen(36 § andra stycket PUL). Även entledigande ska anmälas till inspektionen. Ombudet har till uppgift att självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed. Till skillnad från ett personuppgiftsbiträde kan en anställd vara personuppgiftsombud, förutsatt att denne har en sådan ställning att arbetsuppgifterna som ombud kan utövas på ett självständigt sätt i förhållande till arbetsgivaren. I första hand ska personuppgiftsombudet påpeka brister i uppgiftsbehandlingen till den personuppgiftsansvarige, men om den ansvarige inte rättar till bristerna är ombudet skyldigt att anmäla förhållandet till Datainspektionen. Personuppgiftsombudet ska också hjälpa registrerade personer att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga (38 och 40 §§ PUL).

I polisdatalagen har det föreskrivits en skyldighet för polisen att utse personuppgiftsombud, medan personuppgiftslagens bestämmelser innebär att varje personuppgiftsansvarig själv får göra en bedömning om ett sådant ombud bör utses. Som skäl för att i fråga om polisens verksamhet göra det obligatoriskt att ha ett personuppgiftsombud anförde regeringen att behandlingen av personuppgifter i polisens brottsbekämpande verksamhet i stor utsträckning rör uppgifter som får anses integritetskänsliga, vilket gör det särskilt angeläget med den kontroll som kan utövas av ett personuppgiftsombud (prop. 2009/10:85 s. 93). Vad gäller domstolarnas rättskipande och rättsvårdande verksamhet begränsas hanteringen av personuppgifter indirekt av de processuella regelverken. Jämfört med polisen har domstolarna därför ett mindre utrymme att styra över vilka personuppgifter som ska samlas in och behandlas på andra sätt inom verksamheten. Risken för att det i verksamheten företas alltför integritetskänsliga behandlingar avseende personuppgifter får därför anses vara mindre än inom polisen.

Inte desto mindre skulle en skyldighet för domstolarna att utse ett personuppgiftsombud bidra till att skapa ett allsidigt personuppgiftsskydd. Ett personuppgiftsombud torde ofta få särskilda kunskaper om personuppgiftsfrågor och kan då ge god service åt enskilda som behöver hjälp för att kunna ta tillvara sin rätt. Enskilda får genom personuppgiftsombudet en tydlig kontaktpunkt vid varje domstol i frågor som rör bl.a. information om behandlingen och rättelse av felaktiga uppgifter. Personuppgiftsombudet kan också bidra till kunskapsspridningen inom sin domstol och vara ett stöd för andra medarbetare. I syfte att åstadkomma ett förstärkt integritetsskydd bör det av dessa skäl vara obligatoriskt för domstolarna att utse ett eller flera personuppgiftsombud. Skyldigheten att utse personuppgiftsombud och anmäla dessa till Datainspektionen bör framgå direkt av domstolsdatalagen.

Det finns inte anledning att utforma arbetsuppgifter och skyldigheter för ett personuppgiftsombud som utses med stöd av domstolsdatalagen annorlunda än vad som gäller enligt

personuppgiftslagen. Domstolsdatalagen bör därför hänvisa till 38 och 40 §§ PUL. I 39 § samma lag finns en bestämmelse som innebär att personuppgiftsombud i vissa fall är skyldiga att föra en förteckning över de behandlingar som genomförs. I avsnitt 16.2 föreslås att det ska finnas en generell skyldighet för domstolarna att föra motsvarande förteckningar. Någon hänvisning till 39 § PUL bör därför inte tas in i domstolsdatalagen.

17 Rättsmedel

17.1 Rättelse

Förslag: Domstolsdatalagen ska hänvisa till 28 § PUL om rättelse av personuppgifter.

Skälen för förslaget: Enligt 9 § första stycket h) PUL, till vilken domstolsdatalagen ska hänvisa (se avsnitt 10.1), ska den personuppgiftsansvarige se till att alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen. Det finns också en möjlighet för den registrerade att begära att sådana åtgärder vidtas. Enligt 28 § PUL är den personuppgiftsansvarige skyldig att på begäran av den registrerade rätta, blockera eller utplåna sådana personuppgifter som inte behandlats i enlighet med personuppgiftslagens bestämmelser. Vidare följer av denna bestämmelse att när den personuppgiftsansvarige rättar en personuppgift ska han eller hon underrätta dem som fått del av uppgiften om den registrerade begär det eller om mer betydande skada eller olägenhet därigenom kan undvikas. Sådan underrättelse behöver dock inte lämnas om det visar sig vara omöjligt eller om det skulle innebära en oproportionerligt stor arbetsinsats.

Bestämmelserna i 28 § PUL är redan enligt nuvarande ordning tillämpliga på domstolarnas rättskipande och rättsvårdande verksamhet. Felaktig behandling av personuppgifter innebär ett integritetsintrång och för att i så stor utsträckning

som möjligt begränsa sådana intrång är det viktigt att personuppgifter som behandlas felaktigt i domstolarna även i fortsättningen rättas, blockeras eller utplånas. En hänvisning till 28 § PUL bör därför tas in i domstolsdatalagen.

Det är den personuppgiftsansvarige som själv får avgöra vilken åtgärd – rättelse, blockering eller utplånande – som är lämpligast i varje enskilt fall (prop. 1997/98:44 s. 86). Rättelse anses härvid innebära att den ursprungliga, felaktiga eller ofullständiga uppgiften ersätts av en uppgift om de rätta förhållandena eller att uppgiften på annat sätt kompletteras. Vid rättelse behöver den ursprungliga uppgiften alltså inte utplånas (se Öman och Lindblom, Personuppgiftslagen – En kommentar, 4 uppl., s. 418).

Rättelse, blockering eller utplåning ska inte nödvändigtvis ske enbart av det skälet att uppgifter som framstod som riktiga eller rimliga när behandlingen påbörjades, senare har visat sig vara oriktiga (prop. 2009/10:85 s. 312). En utgångspunkt är att en uppgift trots att den inte återger en korrekt bild av ett sakförhållande inte är oriktig i den bemärkelsen att den ska rättas om uppgiften korrekt återger ett händelseförlopp i verksamheten och dessutom behövs i verksamheten (SOU 1999:105 s. 286). De aktuella bestämmelserna innebär således inte att t.ex. en tjänsteanteckning som på ett korrekt sätt återger vad som framkommit vid ett telefonsamtal måste rättas, även om det som sades under samtalet är felaktigt.

17.2 Skadestånd

Förslag: Domstolsdatalagen ska hänvisa till 48 § PUL om skadestånd.

Skälen för förslaget: Om behandling av personuppgifter i strid med personuppgiftslagen orsakar skada för den registrerade har han eller hon rätt till skadestånd (48 § PUL). Rätten till

ersättning omfattar varje typ av skada eller kränkning av den personliga integriteten orsakad genom en behandling i strid med reglerna i personuppgiftslagen eller föreskrifter som har meddelats med stöd av den lagen. Det är den personuppgiftsansvarige som ska ersätta den registrerade. Skadestånd kan komma i fråga vid varje brott mot lagen och utgår trots att ingen har skadats fysiskt eller ekonomiskt och trots att den personuppgiftsansvarige inte haft uppsåt att göra fel eller varit försumlig vid behandlingen. Bakgrunden till denna reglering är att bestämmelsen om skadestånd, precis som enskildas rättigheter i övrigt enligt lagen har till syfte att skydda människor mot kränkning av den personliga integriteten genom behandling av personuppgifter (jfr prop. 1997/98:44 s. 106 och SOU 1997:39 s. 432).

Personuppgiftslagens bestämmelser om skadestånd är enligt gällande rätt tillämpliga i domstolarnas rättskipande och rättsvårdande verksamhet (se t.ex. 10 § förordningen [2001:641] om registerföring m.m. vid Högsta förvaltningsdomstolen och kammarrätterna med hjälp av automatiserad behandling). Om personuppgifter skulle behandlas i strid med domstolsdatalagen är det principiellt viktigt att den som drabbas av skada eller kränkning på ett rimligt sätt kan kompenseras genom skadestånd. En hänvisning till 48 § PUL bör därför tas in i domstolsdatalagen.

17.3 Straffansvar

Bedömning: Domstolsdatalagen bör inte innehålla några bestämmelser om straffansvar.

Skälen för bedömningen: I personuppgiftslagen har i första hand valts andra sanktioner än straff. Straffansvar föreskrivs dock för överträdelser av vissa bestämmelser (49 § PUL). Det är fråga om sådana uppsåtliga brott eller grova oaktsamma förfaranden som har ansetts svåra att åtgärda på annat sätt än

genom straff, t.ex. att någon lämnar osanna uppgifter i den information till den registrerade som lagen föreskriver eller i anmälan till Datainspektionen. Vidare tillämpas straffbestämmelserna om någon i strid med lagen för över uppgifter till tredje land eller underlåter att göra föreskriven anmälan om behandling till Datainspektionen. Straffbestämmelsernas tillämplighet är begränsade genom att det inte ska dömas till ansvar om en förseelse är ringa. Vera-förordningarna innehåller inga bestämmelser om straffansvar.

Lagrådet har i ett tidigare lagstiftningsärende (prop. 2000/01:33 s. 346) ansett att legalitetsprincipen medför att 49 § PUL inte kan ges motsvarande tillämpning på bestämmelser som avviker från personuppgiftslagen och som har tagits in i särlagstiftning. Straffansvaret enligt 49 § PUL kan alltså inte ges en generell tillämpning på de regler som förs in i domstolsdatalagen genom en hänvisning i domstolsdatalagen till den paragrafen. Det skulle således krävas att det införs en särskild straffbestämmelse i domstolsdatalagen.

Det kan konstateras att behandlingen av personuppgifter enligt domstolsdatalagen kommer att utföras av personer som är anställda vid statliga myndigheter. För felaktig behandling av personuppgifter som sker vid myndighetsutövning kan därför tjänstefelsansvar enligt 20 kap. 1 § brottsbalken komma i fråga. Det gäller om gärningen inte är belagd med straff enligt någon annan bestämmelse. Även bestämmelserna om disciplinansvar för tjänsteförseelse enligt lagen (1994:260) om offentlig anställning, liksom straff för dataintrång i 4 kap. 9 c § brottsbalken, kan ha betydelse i sammanhanget.

Vid tillkomsten av flera andra författningar som gäller personuppgiftsbehandling vid statliga myndigheter har bedömningen gjorts att det inte finns behov av några särskilda bestämmelser om straff vid överträdelser av författningarna, se t.ex. förarbetena till lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet (prop. 2004/05:164 s. 55) och till polisdatalagen (prop. 2009/10:85 s. 91). Det finns inte skäl att för domstolarna göra någon annan

bedömning. Några bestämmelser om straffansvar bör således inte tas in i domstolsdatalagen.

17.4 Överklagande

Förslag: Beslut av domstol om upplysningar till allmänheten, om information samt om rättelse och underrättelse till tredje man ska kunna överklagas. Högsta domstolens och Högsta förvaltningsdomstolens beslut ska dock inte kunna överklagas.

Beslut av en hovrätt, tingsrätt och förvaltningsrätt ska överklagas till kammarrätten. Beslut av en kammarrätt ska överklagas till Högsta förvaltningsdomstolen.

Beslut av en hyres- och arrendenämnd ska överklagas till allmän förvaltningsdomstol, varvid prövningstillstånd ska krävas vid överklagande till kammarrätten.

Domstolsdatalagen ska hänvisa till 51 § PUL om överklagande av Datainspektionens beslut, med undantag för möjligheten för den myndigheten att bestämma att dess beslut ska gälla även om det överklagas.

Skälen för förslaget

Beslut av den personuppgiftsansvarige

Enligt 52 § PUL får en myndighets beslut om information enligt 26 § PUL, om rättelse och underrättelse till tredje man enligt 28 § PUL, om information enligt 29 § andra stycket PUL och om upplysningar enligt 42 § PUL överklagas till allmän förvaltningsdomstol (förvaltningsrätt). Andra beslut enligt personuppgiftslagen får inte överklagas (53 § PUL).

Fråga är inledningsvis vilka beslut som ska kunna överklagas med stöd av domstolsdatalagen. En principiell utgångspunkt bör vara att beslut angående behandling av personuppgifter som direkt berör den enskilde ska kunna överklagas medan beslut

som kan betecknas som interna eller administrativa och som inte direkt berör den enskilde, t.ex. ett beslut att inte medge direktåtkomst, inte ska kunna överklagas (jfr prop. 2005/06:173 s. 52). Beslut enligt 26 och 28 §§ PUL, till vilka domstolsdatalagen hänvisar, bör mot denna bakgrund kunna överklagas. Även beslut om upplysningar till allmänheten, som enligt vad som föreslås i avsnitt 16.2 ska regleras särskilt i domstolsdatalagen, bör på motsvarande sätt som gäller enligt personuppgiftslagen kunna överklagas (jfr 42 och 52 §§ PUL). Övriga beslut som kan meddelas av den personuppgiftsansvarige enligt domstolsdatalagen bedöms däremot inte vara av sådan karaktär att de bör kunna överklagas. Detta är i linje med vad som gäller enligt många registerförfattningar (se t.ex. 2 kap. 2 § polisdatalagen och 2 kap. 2 § kustbevakningsdatalagen).

Att tillämpa den vanliga överklagandeordningen i fråga om ärenden som har inletts hos en allmän domstol eller en allmän förvaltningsdomstol är inte lämpligt i detta fall. Det skulle nämligen innebära att t.ex. en kammarrätts beslut skulle överklagas till en förvaltningsrätt, att en förvaltningsrätts beslut skulle överklagas till samma förvaltningsrätt, och att en hovrätts beslut skulle överklagas till en förvaltningsrätt. För att förvaltningsrätterna inte ska behöva överpröva sina egna eller högre instansers beslut har det i Vera-förordningarna införts en avvikande instansordning i fråga om överklagande av domstolars beslut. Enligt dessa förordningar gäller att en förvaltningsrätts beslut överklagas till kammarrätten, en kammarrätts beslut till Högsta förvaltningsdomstolen samt att en tingsrätts eller hovrätts beslut överklagas till kammarrätten.[1] Det är också vad som gäller för beslut om utlämnande av handling i domstolarnas administrativa verksamhet enligt offentlighets- och sekretesslagen (6 kap. 8 §

[1] 10 § första stycket förordningen (2001:639) om registerföring m.m. vid allmänna domstolar med hjälp av automatiserad behandling, 10 § första stycket förordningen (2001:640) om registerföring m.m. vid förvaltningsrätt med hjälp av automatiserad behandling och 11 § första stycket förordningen (2001:641) om registerföring m.m. vid Högsta förvaltningsdomstolen och kammarrätterna med hjälp av automatiserad behandling.

OSL). Motsvarande ordning finns även i 15 § första stycket lagen (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen. Den nu redovisade instansordningen framstår som ändamålsenlig även vid överklagande av beslut enligt domstolsdatalagen.

De beslut som är överklagbara utgör administrativa beslut i respektive domstol. Kammarrätten dit beslutet överklagas kommer därmed i realiteten att vara första domstolsinstans. Mot den angivna bakgrunden och i enlighet med vad som gäller enligt Vera-förordningarna bör det därför inte gälla något krav på prövningstillstånd vid överklagande till kammarrätten.

Högsta domstolen är högsta allmänna domstol och Högsta förvaltningsdomstolen är högsta förvaltningsdomstol (11 kap. 1 § RF). Av detta följer att dessa domstolars avgöranden inte kan överklagas (jfr prop. 2009/10:175 s. 185). Högsta domstolens och Högsta förvaltningsdomstolens beslut enligt domstolsdatalagen bör därför inte kunna överklagas. Detta överensstämmer med vad som gäller enligt offentlighets- och sekretesslagen och Vera-förordningarna.

När det gäller beslut som meddelas av en hyres- och arrendenämnd finns det inte skäl att avvika från den vanliga ordningen för överklagande av förvaltningsbeslut. Det bör således anges i domstolsdatalagen att nämndernas beslut överklagas till allmän förvaltningsdomstol samt att prövningstillstånd krävs vid överklagande till kammarrätten.

Beslut av tillsynsmyndigheten

I 51 § första stycket PUL föreskrivs att Datainspektionens beslut enligt lagen om annat än föreskrifter får överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten. I avsnitt 16.3 föreslås att Datainspektionen ska kunna meddela säkerhetsåtgärder enligt 32 § PUL och förbud enligt 44 eller 45 § PUL, vilket innebär att en hänvisning bör göras till 51 § första stycket PUL för att

möjliggöra ett överklagande av sådana beslut. Enligt 51 § andra stycket PUL får Datainspektionen bestämma att dess beslut ska gälla även om det överklagas. Det är svårt att se något egentligt praktiskt behov av en sådan möjlighet när det gäller domstolarnas personuppgiftsbehandling. Datainspektionen bör därför inte ges möjlighet att meddela sådana beslut. Hänvisningen i domstolsdatalagen till personuppgiftslagen bör därför endast avse första stycket i paragrafen (jfr prop. 2011/12:45 s. 87 angående motsvarande bedömning för Kustbevakningen).

18 Ikraftträdande- och övergångsbestämmelser

Förslag: Domstolsdatalagen ska träda i kraft den 1 april 2014.
Bedömning: Några särskilda övergångsbestämmelser behövs inte.

Skälen för förslaget och bedömningen: Domstolarnas personuppgiftsbehandling regleras för närvarande genom Vera-förordningarna. De tillkom som en provisorisk lösning för drygt tio år sedan och datortekniken har sedan dess utvecklats i snabb takt. Som redovisas i avsnitt 6.1 ställer vidare den nya integritetsskyddsbestämmelsen i regeringsformen krav på lagstiftning. Det finns alltså ett behov av att anpassa såväl integritetsskyddet som de rättsliga möjligheterna att utnyttja den nya tekniken så snart som möjligt. De föreslagna bestämmelserna i domstolsdatalagen bedöms inte förutsätta några mer omfattande anpassningar av verksamheten eller datorsystemen. Mot den angivna bakgrunden bör domstolsdatalagen träda i kraft den 1 april 2014. Domstolsdatalagen ersätter Vera-förordningarna, vilka därför bör upphävas när lagen träder i kraft.

Det bedöms inte finnas behov av några särskilda övergångsbestämmelser.

19 Konsekvenser av förslagen

Bedömning: Förslagen kommer att ge förutsättningar för domstolarna att bedriva sin verksamhet effektivt och med ett rationellt datorstöd. Förslagen innebär en flexibel reglering som ger domstolarna möjlighet att fortlöpande utveckla och anpassa sina system för automatiserad behandling utan att det krävs ändringar i regelverket.

De kostnader som inledningsvis kan uppkomma hos domstolarna bedöms rymmas inom domstolarnas befintliga ekonomiska ramar.

Skälen för bedömningen: Förslagen innebär att en modern, teknikneutral och ändamålsenlig reglering av domstolarnas personuppgiftsbehandling införs. Särskild hänsyn har tagits till integritetsaspekterna av omfattande automatiserade uppgiftssamlingar i myndighetsverksamhet och regleringen säkerställer ett långsiktigt hållbart integritetsskydd.

Domstolarna kommer med stöd av domstolsdatalagen att mer effektivt kunna utnyttja sökfunktioner och direktåtkomst till varandras datorsystem. Detta främjar domstolarnas effektivitet och bidrar till en enhetlig rättstillämpning. Förslagen innebär vidare att domstolarna kan effektivisera sin delgivningsverksamhet genom att spara och strukturera information som behövs för att delgivning ska kunna genomföras med personer som av olika skäl är svåra att få kontakt med.

Ett annat syfte med förslagen är att underlätta domstolarnas samverkan med andra myndigheter inom rättsväsendet. Därtill

skapar förslagen förutsättningar för att parter ska kunna beredas elektronisk åtkomst till uppgifter i sina egna mål och ärenden. Förslagen kan således ligga till grund för att enskildas insyn i domstolsprocesserna förbättras ytterligare samt att parter och ombud kan föra sina processer mer effektivt. Det ska dock understrykas att förslaget inte innebär några skyldigheter att inrätta sökfunktioner eller att möjliggöra direktåtkomst.

Genom förslagen genomförs nödvändiga justeringar av personuppgiftsregleringen för att domstolarna ska kunna övergå till elektronisk arkivering. Detta är på sikt kostnadsbesparande. Förslagen innebär att domstolarnas dokumenthantering i pappersform i allt större utsträckning kommer att kunna ersättas av elektronisk informationshantering. Även detta innebär i sig kostnadsbesparingar. Dessutom leder det till att miljöbelastningen kan minska då pappersutskrifter och transporter kan minimeras.

Även om förslagen på olika sätt leder till effektiviseringar och andra förbättringar kan Sveriges Domstolar inledningsvis komma att orsakas vissa begränsade merkostnader på grund av tekniska anpassningar. Vidare ställs det krav på domstolarna att upprätta en förteckning över de personuppgiftsbehandlingar som utförs med stöd av domstolsdatalagen. Även vissa utbildningsinsatser kan behövas. Dessa insatser är inte mer omfattande än att de får anses utgöra en del av det ordinarie utvecklingsarbetet och bedöms därför rymmas inom befintliga anslag.

Förslagen bedöms inte ha några ekonomiska konsekvenser för övriga myndigheter, kommuner, landsting, företag eller andra enskilda. Den nya lagstiftningen bedöms inte heller ha någon påverkan på jämställdheten mellan män och kvinnor eller möjligheterna att nå de integrationspolitiska målen.

20 Författningskommentar

Förslaget till domstolsdatalag

Lagens tillämpningsområde

1 § Denna lag gäller vid behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas samt hyres- och arrendenämndernas rättskipande och rättsvårdande verksamhet.

Lagen gäller om behandlingen är helt eller delvis automatiserad eller om personuppgifter ingår i eller är avsedda att ingå i en strukturerad samling av uppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Paragrafen anger tillämpningsområdet för domstolsdatalagen. Övervägandena finns i avsnitt 7.

I *första stycket* anges inledningsvis att lagen gäller vid behandling av personuppgifter. Med begreppet personuppgifter avses detsamma som i 3 § PUL, dvs. all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet (jfr 4 § första stycket 1). Även begreppet behandling har samma innebörd som i personuppgiftslagen. Därmed avses således varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, t.ex. insamling, registrering, organisering, lagring, bearbetning, användning, spridning eller annat tillhandahållande, sammanställning eller samkörning samt utplåning eller förstöring. Lagen gäller för de allmänna domstolarna, de allmänna förvaltningsdomstolarna samt hyres- och arrendenämnderna i deras rättskipande och rättsvårdande verksamhet.

Utanför lagens tillämpningsområde faller således behandling av personuppgifter i samband med de interna och administrativa åtgärder som kan förekomma i domstolarnas och nämndernas verksamhet. För behandling av uppgifter som rör sådana frågor, t.ex. i personal- och löneregister, gäller i stället personuppgiftslagen. Även de särskilda domstolarna, dvs. migrationsdomstol och mark- och miljödomstol, omfattas av domstolsdatalagens tillämpningsområde.

I *andra stycket* anges att lagen endast är tillämplig om behandlingen av personuppgifter är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier (jfr 5 § PUL). Utanför lagens tillämpningsområde faller således helt manuell behandling av personuppgifter som inte ingår i någon sådan samling.

Lagens syfte

2 § Syftet med denna lag är att ge de allmänna domstolarna, de allmänna förvaltningsdomstolarna samt hyres- och arrendenämnderna möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin rättskipande och rättsvårdande verksamhet och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

I paragrafen anges det övergripande syftet med lagen. Övervägandena finns i avsnitt 8.1.

I paragrafen anges att syftet med lagen är ge domstolarna och nämnderna möjlighet att behandla personuppgifter på ett ändamålsenligt sätt samt att skydda den personliga integriteten vid sådan behandling. Intrång i den personliga integriteten ska alltid stå i rimlig proportion till det intresse som ska tillgodoses med behandlingen av personuppgifterna. Bestämmelsen har utformats med förebild i 1 kap. 1 § polisdatalagen (2010:361) och 1 kap. 1 § kustbevakningsdatalagen (2012:145).

Förhållandet till personuppgiftslagen m.m.

3 § Om inte annat anges i 4 § gäller denna lag i stället för personuppgiftslagen (1998:204).

I paragrafen regleras förhållandet till personuppgiftslagen. Övervägandena finns i avsnitt 8.2.

Bestämmelsen innebär att domstolsdatalagen inom sitt tillämpningsområde helt ersätter personuppgiftslagen, utom i de fall som uttryckligen anges i 4 §. Vid sådan personuppgiftsbehandling som omfattas av lagen ska alltså bestämmelser i personuppgiftslagen tillämpas endast om det finns en hänvisning till dem i 4 §. Polisdatalagen och kustbevakningsdatalagen bygger på samma lagtekniska lösning.

4 § När personuppgifter behandlas enligt denna lag eller enligt föreskrifter som har meddelats i anslutning till lagen, gäller följande bestämmelser i personuppgiftslagen (1998:204):

1. 3 § om definitioner,
2. 8 § om förhållandet till offentlighetsprincipen,
3. 9 § om grundläggande krav på behandling av personuppgifter,
4. 23 och 25–27 §§ om information till den registrerade,
5. 28 § om rättelse,
6. 30 och 31 §§ samt 32 § första stycket om säkerheten vid behandling,
7. 33–35 §§ om överföring av personuppgifter till tredje land,
8. 38, 40 och 41 §§ om personuppgiftsombud m.m.,
9. 43 och 44 §§, 45 § första stycket och 47 § om tillsynsmyndighetens befogenheter,
10. 48 § om skadestånd, samt
11. 51 § första stycket och 53 § om överklagande.

Förbud enligt 44 eller 45 § personuppgiftslagen får inte förenas med vite.

Paragrafen innehåller hänvisningar till tillämpliga bestämmelser i personuppgiftslagen. Övervägandena finns i avsnitt 8.2, 8.3, 8.5, 9.2, 10.1, 11.1, 14.4, 15.2, 16.2–16.4, 17.1, 17.2 och 17.4.

I *första stycket* anges i elva punkter uttömmande vilka bestämmelser i personuppgiftslagen som ska gälla vid tillämpningen av domstolsdatalagen.

Enligt *punkten 1* ska de definitioner som anges i 3 § PUL tillämpas även vid behandling av personuppgifter som omfattas av domstolsdatalagen. Därigenom klargörs vad som menas med begreppen personuppgifter, behandling, personuppgiftsansvarig, personuppgiftsombud, personuppgiftsbiträde m.m. I 9 § finns dock en särskild bestämmelse om personuppgiftsansvar för den behandling som domstolen respektive nämnden utför.

I *punkten 2* hänvisas till 8 § PUL, i vilken det i första stycket anges att bestämmelserna i personuppgiftslagen inte ska tillämpas i den utsträckning det skulle inskränka en myndighets skyldighet enligt 2 kap. TF att lämna ut handlingar. Genom domstolsdatalagens hänvisning till denna bestämmelse klargörs att bestämmelserna i domstolsdatalagen – liksom de andra bestämmelser i personuppgiftslagen som domstolsdatalagen hänvisar till – inte ska tillämpas om det skulle inskränka den skyldigheten. Det innebär t.ex. att en myndighet inte kan vägra att ta fram och lämna ut uppgifter i enlighet med tryckfrihetsförordningens bestämmelser enbart med hänvisning till att utlämnandet inte ryms inom de enligt domstolsdatalagen tillåtna ändamålen för behandling. I sammanhanget bör dock understrykas att offentlighetsprincipen inte innebär någon skyldighet att lämna ut uppgifter i elektronisk form. Vid bedömningen av om en uppgift kan lämnas ut i elektronisk form måste alltså lagens regler beaktas.

Vidare följer av hänvisningen till 8 § andra stycket PUL att bestämmelserna i domstolsdatalagen inte hindrar att personuppgifter i allmänna handlingar arkiveras och bevaras eller att arkivmaterial tas om hand av en arkivmyndighet. För personuppgifter som inte finns i en allmän handling gäller att uppgifterna som huvudregel inte får bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen (se punkten 3 nedan). Regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela särskilda föreskrifter om bevarande av uppgifter som hänför sig till mål eller ärende som avslutats genom ett lagakraftvunnet avgörande (se författningskommentaren till 22 §).

I *punkten 3* hänvisas till 9 § PUL. Hänvisningen innebär att den personuppgiftsansvarige (se författningskommentaren till 9 §) ska se till att uppgifterna behandlas enbart om det är lagligt och att de behandlas på ett korrekt sätt och i enlighet med god sed (9 § första stycket a och b PUL). I förarbetena till personuppgiftslagen uttalas att vad som är god sed vid behandling av personuppgifter får avgöras i rättstillämpningen mot bakgrund av bl.a. de mer preciserade föreskrifter som kan utfärdas med stöd av personuppgiftslagen, de branschregler på området som kan ha utarbetats av etablerade branschorganisationer eller andra representativa sammanslutningar och hur ansvarsfulla personuppgiftsansvariga som regel beter sig (prop. 1997/98:44 s. 143).

Hänvisningen innebär också att den personuppgiftsansvarige ska se till att de behandlade personuppgifterna är adekvata och relevanta i förhållande till ändamålen för behandlingen, att inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen för behandlingen, att de behandlade personuppgifterna är riktiga och, om det är nödvändigt, aktuella, samt att alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen (9 § första stycket e–h PUL). Vid tillämpningen av de aktuella bestämmelserna måste hänsyn tas till den särskilda karaktären hos de uppgifter som förekommer i domstolarnas och nämndernas rättskipande och rättsvårdande verksamhet (jfr prop. 2011/12:45 s. 194). Bedömningen av om en uppgift ska anses vara oriktig eller inte, dvs. om uppgiften ska rättas, måste göras mot bakgrund av vilka krav verksamheten ställer på uppgiftsbehandlingen (prop. 2000/01:33 s. 107 f.). Det är naturligt att parterna under en domstolsprocess ifrågasätter riktigheten i varandras utsagor. Detta utgör naturligtvis inget hinder för domstolarna att behandla uppgifterna i utsagorna elektroniskt. En utgångspunkt är att en uppgift, trots att den inte återger en korrekt bild av ett sakförhållande, inte är oriktig i den bemärkelsen att den ska rättas, om den korrekt återger ett händelseförlopp i

verksamheten och dessutom behövs i densamma (se SOU 1999:105 s. 286 och SOU 2001:100 s. 175 f., jfr även RH 2008:87). Rättelse ska inte ske enbart därför att uppgifter som framstod som riktiga eller rimliga när de samlades in, t.ex. brottsmisstankar, senare har visat sig vara oriktiga (jfr prop. 2011/12:45 s. 196).

Hänvisningen innebär vidare att den personuppgiftsansvarige ska se till att personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål (9 § första stycket c PUL). Den insamling av uppgifter som domstolarna och nämnderna företar i den rättskipande och rättsvårdande verksamheten lever normalt upp till de aktuella kraven, eftersom insamlandet av uppgifter för domstolarnas och nämndernas del styrs av andra bestämmelser, såsom förvaltningslagen, rättegångsbalken, förvaltningsprocesslagen samt andra handläggnings- och förfaranderegler. Av dessa regelverk framgår det i vilka fall och under vilka förutsättningar uppgifter ska tillföras verksamheten vid handläggning av mål och ärenden. På så sätt tydliggörs det för vilka ändamål som uppgifter samlas in. När en domstol eller nämnd samlar in uppgifter är det i det enskilda fallet oftast klart för vilket ändamål uppgifterna samlas in.

Genom hänvisningen gäller dessutom att personuppgifter inte får behandlas för ett ändamål som är oförenligt med det ändamål för vilket de samlades in (9 § första stycket d PUL). Detta är ett uttryck för den s.k. finalitetsprincipen. Genom bestämmelsen uppställs en begränsning i fråga om hur uppgifter som redan finns i verksamheten får behandlas för nya ändamål. Generellt gäller dock att behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål inte ska anses som oförenliga med de ändamål för vilka uppgifterna samlades in (9 § andra stycket PUL). Vid behandling för historiska, statistiska och vetenskapliga ändamål gäller emellertid särskilda begränsningar för hur uppgifterna får användas (9 § fjärde stycket PUL).

Slutligen innebär hänvisningen att personuppgiftslagens bestämmelser rörande bevarande av uppgifter som inte finns i allmänna handlingar ska tillämpas. Således gäller som huvudregel

att personuppgifter inte får bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen (9 § första stycket i PUL). Personuppgifter får dock bevaras längre om det behövs för historiska, statistiska eller vetenskapliga ändamål, men då gäller särskilda begränsningar för hur uppgifterna får användas (9 § tredje stycket PUL).

Genom hänvisningen i *punkten 4* till 23 och 25–27 §§ PUL säkerställs den registrerades rätt till information. Enligt 23 § PUL ska den personuppgiftsansvarige i samband med att personuppgifter samlas in självmant lämna den registrerade information om behandlingen av uppgifterna. Av 25 § första stycket PUL framgår att informationen ska omfatta uppgift om den personuppgiftsansvariges identitet, uppgift om ändamålen med behandlingen, och all övrig information som behövs för att den registrerade ska kunna ta tillvara sina rättigheter i samband med behandlingen, såsom information om mottagarna av uppgifterna, skyldighet att lämna uppgifter och rätten att ansöka om information och få rättelse. Av 25 § andra stycket PUL framgår emellertid att information inte behöver lämnas om sådant som den registrerade redan känner till. I domstolarnas rättskipande och rättsvårdande verksamhet torde de registrerade som skickar in uppgifter till domstolarna (exempelvis parterna) i de flesta fall anses känna till den information som avses i 23 § PUL eftersom denna information framgår direkt av domstolsdatalagen, av den förteckning som domstolarna föreslås vara skyldig att sammanställa och av de processuella regelverken som styr domstolarnas verksamhet. Följden blir att domstolarna i praktiken sällan torde behöva lämna särskild information till den registrerade.

Av 26 och 27 §§ PUL följer att den personuppgiftsansvarige är skyldig att en gång per år efter skriftlig ansökan lämna gratis information om huruvida personuppgifter som rör den sökande behandlas. Om sådan behandling sker, ska upplysning också lämnas om bl.a. ändamålet med behandlingen. Under vissa förutsättningar gäller undantag från informationsskyldigheten i fråga om personuppgifter i löpande text som inte fått sin slutliga utformning, minnesanteckningar och liknande. Informations-

plikten gäller inte heller i den utsträckning det råder sekretess eller tystnadsplikt för informationen. Bestämmelserna innebär inga skyldigheter för domstolarna att inrätta sök- eller andra sammanställningsfunktioner endast för att kunna lämna så fullständig information som möjligt till den registrerade. För att fullgöra sina skyldigheter enligt bestämmelserna är det tillräckligt att den personuppgiftsansvarige utnyttjar de sök- och sammanställningsmöjligheter som han eller hon har tillgång till för att få fram information att lämna till den registrerade (jfr prop. 1997/98:44 s. 81 f.)

Enligt hänvisningen i *punkten 5* till 28 § PUL ska den lagens bestämmelser om rättelse tillämpas. Den personuppgiftsansvarige är alltså skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med domstolsdatalagen, inklusive de bestämmelser i personuppgiftslagen som domstolsdatalagen hänvisar till. Vad gäller frågan om när uppgifter är att betrakta som oriktiga, se punkten 3. Det är den personuppgiftsansvarige som själv får avgöra vilken åtgärd – rättelse, blockering eller utplånande – som är lämpligast i varje enskilt fall (prop. 1997/98:44 s. 86). Rättelse anses härvid innebära att den ursprungliga, felaktiga eller ofullständiga uppgiften ersätts av en uppgift om de rätta förhållandena eller att uppgifterna på annat sätt kompletteras. Vid rättelse behöver den ursprungliga uppgiften alltså inte utplånas. Rättelse, blockering eller utplåning ska inte ske enbart därför att uppgifter som framstod som riktiga eller rimliga när behandlingen påbörjades, senare har visat sig vara oriktiga (prop. 2009/10:85 s. 312). De aktuella bestämmelserna innebär alltså inte att t.ex. en tjänsteanteckning som på ett korrekt sätt återger vad som framkommit vid ett telefonsamtal ska rättas, även om det som sades under samtalet är felaktigt.

I *punkten 6* görs en hänvisning till 30 och 31 §§ samt 32 § första stycket PUL. Enligt 30 § första stycket PUL får ett personuppgiftsbiträde (dvs. den som behandlar personuppgifter för den personuppgiftsansvariges räkning) och den eller de personer som arbetar under biträdets eller den personuppgifts-

ansvariges ledning behandla personuppgifter enbart i enlighet med instruktioner från den personuppgiftsansvarige. Bestämmelser om tystnadsplikt och sekretess har dock företräde framför sådana instruktioner som den personuppgiftsansvarige lämnar (30 § tredje stycket PUL och prop. 1997/98:44 s. 136). Enligt 30 § andra stycket PUL ska det i fråga om personuppgiftsbiträden finnas ett skriftligt avtal om biträdets behandling för den personuppgiftsansvariges räkning. Det ska i avtalet särskilt föreskrivas att biträdet får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige och att biträdet är skyldigt att vidta de åtgärder som avses i 31 § första stycket PUL. Domstolsverket har en central roll i uppbyggnaden och driften av domstolarnas och nämndernas datorsystem. När Domstolsverket utför personuppgiftsbehandlingar för domstolarnas räkning behöver alltså domstolarna och Domstolsverket ingå ett avtal. Av 31 § PUL följer bl.a. att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de behandlade personuppgifterna. Enligt 32 § PUL första stycket får Datainspektionen i enskilda fall besluta om vilka åtgärder som den personuppgiftsansvarige ska vidta enligt 31 § samma lag.

En hänvisning görs i *punkten 7* till 33–35 §§ PUL. Enligt 33 § PUL är det förbjudet att överföra personuppgifter till tredje land om landet inte har en adekvat nivå för skyddet av personuppgifter. Frågan om en skyddsnivå är adekvat ska bedömas med hänsyn till samtliga omständigheter som har samband med överföringen. Särskild vikt ska fästas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen ska pågå, ursprungslandet, det slutliga bestämmelselandet och reglerna för behandlingen i tredje land. I 34 och 35 §§ PUL föreskrivs undantag från förbudet enligt 33 § samma lag. Enligt 34 § PUL får uppgifter trots förbudet överföras dels om den registrerade har lämnat sitt samtycke till överföringen, dels om överföringen är nödvändig med hänsyn till vissa uppräknade omständigheter. Det är också enligt den paragrafen tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit

sig till dataskyddskonventionen. I 35 § PUL föreskrivs att regeringen, och för vissa fall även den myndighet som regeringen bestämmer, meddelar föreskrifter om undantag från förbudet i 33 § PUL.

I *punkten 8* görs en hänvisning till 38 och 40 §§ PUL, där det framgår vilka närmare uppgifter ett personuppgiftsombud har. Domstolarna är enligt 10 § skyldiga att utse ett eller flera personuppgiftsombud. Dessa ska självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed samt påpeka eventuella brister. Har ett personuppgiftsombud anledning att misstänka att den personuppgiftsansvarige bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och vidtas inte rättelse så snart det kan ske efter påpekande, ska personuppgiftsombudet anmäla förhållandet till Datainspektionen. Även i övrigt ska personuppgiftsombuden samråda med Datainspektionen vid tveksamhet rörande tillämpningen av Domstolsdatalagen. Slutligen har personuppgiftsombuden också till uppgift att hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga. En hänvisning görs i punkten 8 också till 41 § PUL. Enligt den paragrafen har regeringen möjlighet att föreskriva att vissa särskilt känsliga behandlingar ska anmälas till Datainspektionen för förhandskontroll.

Genom hänvisningen i *punkten 9* till 43 och 44 §§, 45 § första stycket och 47 § PUL görs det klart vilka befogenheter tillsynsmyndigheten har, utöver möjligheten att besluta om säkerhetsåtgärder med stöd av hänvisningen till 32 § PUL. Enligt 43 § PUL har Datainspektionen möjlighet att på begäran få tillgång till de personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen och säkerheten vid denna samt tillträde till lokaler. Om Datainspektionen efter en begäran enligt 43 § PUL inte kan få tillräckligt underlag för att konstatera att personuppgiftsbehandlingen är laglig, får myndigheten enligt 44 § PUL förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än genom att lagra

dem. Enligt 45 § första stycket PUL ska Datainspektionen genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse om inspektionen konstaterar att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt. Om det inte går att få rättelse på något annat sätt eller om saken är brådskande, får inspektionen vidare förbjuda den personuppgiftsansvarige att fortsätta att behandla personuppgifterna på något annat sätt än genom att lagra dem. Möjligheten för Datainspektionen att enligt 43 och 44 §§ PUL förbjuda en domstol eller nämnd att behandla personuppgifter på något annat sätt än genom att lagra dem skulle i många fall innebära att verksamheten blockeras, vilket kan ha allvarliga följer för rättsäkerheten, tilltron till rättsväsendet och för enskildas möjligheter att ta tillvara sin rätt. Datainspektionen bör därför i det längsta undvika att tillgripa denna åtgärd. Datainspektionen har också möjlighet att hos förvaltningsrätten ansöka om att personuppgifter som har behandlats på ett olagligt sätt ska utplånas (47 § PUL). Beslut om utplåning får dock inte fattas om det är oskäligt. Det är i praktiken uteslutet att utplåna uppgifter som behövs för handläggningen av mål och ärenden eller som på grund av processrättsliga regler eller allmänna rättsprinciper ska bevaras.

Genom hänvisningen i *punkten 10* till 48 § PUL regleras den registrerades rätt till skadestånd. Den personuppgiftsansvarige (domstolen eller nämnden) ska ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med domstolsdatalagen har orsakat. Detta gäller även om en behandling har skett i strid med de bestämmelser i personuppgiftslagen som domstolsdatalagen hänvisar till. I vissa fall kan ersättningen jämkas.

Hänvisningen i *punkten 11* till 51 § första stycket PUL innebär att Datainspektionens beslut enligt domstolsdatalagen får överklagas till allmän förvaltningsdomstol. Av 23 § följer att även vissa beslut av de personuppgiftsansvariga domstolarnas och nämndernas får överklagas. Av hänvisningen till 53 § PUL följer att andra beslut än dessa inte får överklagas.

Av *andra stycket* framgår det att Datainspektionen inte får förena ett förbud med vite.

5 § Om det i lagen (2013:000) om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen eller i föreskrifter som regeringen har meddelat i anslutning till den lagen finns avvikande bestämmelser, ska de tillämpas i stället för bestämmelserna i denna lag.

I paragrafen anges förhållandet till den föreslagna lagen om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen. Övervägandena finns i avsnitt 8.4.

I paragrafen klargörs att om det i den föreslagna lagen eller i föreskrifter som har meddelats i anslutning till den lagen finns bestämmelser som avviker från bestämmelser i domstolsdatalagen ska de förstnämnda bestämmelserna tillämpas.

Tillåtna ändamål

6 § Personuppgifter får behandlas om det behövs för handläggning av mål och ärenden.

I paragrafen anges de primära ändamålen för personuppgiftsbehandlingen i den rättskipande och rättsvårdande verksamheten. Övervägandena finns i avsnitt 10.2.

Enligt bestämmelsen får domstolarna och nämnderna behandla personuppgifter om det behövs för handläggning av mål och ärenden. Det är fråga om s.k. primära ändamål, dvs. ändamål för vilka domstolarna och nämnderna inte enbart får vidarebehandla lagrade uppgifter, utan även får samla in uppgifter, t.ex. genom att motta partsinlagor, föra protokoll vid förhandlingar eller göra tjänsteanteckningar. I 7 § regleras de s.k. sekundära ändamålen.

Under förevarande ändamålsbestämmelse faller alla åtgärder som behöver vidtas inom ett ärende eller ett mål, från mottagande av uppgifter, konferering (dvs. kontroll av att målet

inte gäller något som redan är eller har varit föremål för domstolens eller nämndens prövning), diarieföring, kommunicering, protokollföring, sökning efter relevant praxis till upprättande av dom samt expediering. Det förutsätts emellertid inte att en behandling är nödvändig för ett visst mål eller ärende, utan även behandlingar som behövs för handläggningen av mål och ärenden i stort omfattas av den aktuella ändamålsbestämmelsen. Planering, uppföljning och utvärdering anses vara en integrerad del av själva verksamheten och omfattas också av den nu aktuella ändamålsbestämmelsen (prop. 2004/05:164 s. 66 f. och 162 samt prop. 2009/10:85 s. 116).

Genom hänvisning i 4 § första stycket 3 är personuppgiftslagens grundläggande bestämmelser om ändamål tillämpliga i domstolarnas och nämndernas rättskipande och rättsvårdande verksamhet. En grundläggande förutsättning för personuppgiftsbehandling är således att personuppgifter får samlas in endast för särskilda och uttryckligt angivna ändamål (9 § första stycket c PUL). Ytterligare en grundläggande förutsättning är att personuppgifter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (finalitetsprincipen, 9 § första stycket d PUL).

7 § Personuppgifter som behandlas enligt 6 § får även behandlas om det behövs för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning.

Paragrafen innehåller bestämmelser om de sekundära ändamål för vilka personuppgifter får behandlas. Övervägandena finns i avsnitt 10.2.

Enligt bestämmelsen får personuppgifter som samlats in eller på annat sätt behandlats för handläggningen av mål och ärenden enligt 7 § även behandlas om det behövs för att fullgöra uppgiftslämnande. Det är fråga om en s.k. sekundär ändamålsbestämmelse. Bestämmelsen ger inte stöd för att samla in personuppgifter till den rättskipande verksamheten, utan det kan enbart bli fråga om att vidarebehandla personuppgifter som

behandlas i verksamheten med stöd av 6 §. Bestämmelsen är tillämplig oavsett om uppgiftslämnandet sker genom utskrift på ett papper som lämnas ut, genom att e-post skickas eller genom att information publiceras på internet.

Det följer redan av domstolsdatalagens hänvisning till 8 § första stycket PUL (jfr 4 § första stycket 2) att det alltid är tillåtet att utföra sådana behandlingar som är nödvändiga för att fullgöra skyldigheten enligt 2 kap. TF att lämna ut personuppgifter i allmänna handlingar. Genom den nu aktuella bestämmelsen tillåts domstolarna och nämnderna att även i andra fall behandla personuppgifter för att kunna lämna uppgifter till utomstående eller till en annan del av verksamheten. Det kan röra sig om situationer där domstolarna och nämnderna enligt bestämmelser i olika författningar är skyldiga att lämna uppgifter till utpekade myndigheter, t.ex. uppgifter om brottmålsdomar till Rikspolisstyrelsen och Kriminalvården eller om domar i upphandlingsmål till Konkurrensverket. En domstol eller nämnd är också enligt 6 kap. 5 § OSL, med vissa undantag, skyldiga att på begäran av en annan myndighet lämna uppgift som domstolen eller nämnden förfogar över. Bestämmelsen tillåter emellertid även att personuppgifter behandlas för att kunna lämnas ut i situationer då det inte finns någon uttrycklig skyldighet att lämna ut uppgifterna. Det kan t.ex. vara fråga om en åtgärd som vidtas för att fullgöra serviceskyldigheten gentemot enskilda enligt 4 § förvaltningslagen eller skyldigheten att hjälpa andra myndigheter enligt 6 § samma lag. Bestämmelsen ger också stöd för uppgiftslämnande till sådan verksamhet vid domstolen eller nämnden som inte omfattas av domstolsdatalagen, dvs. till den administrativa verksamheten. Det kan exempelvis röra sig om rapportering av nämndemäns tjänstgöring i syfte att administrationen ska kunna betala ut ersättning. Bestämmelsen har utformats med förebild i 2 kap. 5 § patientdatalagen.

Genom hänvisning i 4 § första stycket 3 är personuppgiftslagens grundläggande bestämmelser om ändamål tillämpliga i domstolarnas och nämndernas rättskipande och rättsvårdande verksamhet. En grundläggande förutsättning för personuppgifts-

behandling är således att personuppgifter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (finalitetsprincipen, 9 § första stycket d PUL).

Tillgången till personuppgifter

8 § Tillgången till personuppgifter ska begränsas till vad varje anställd behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om tillgången till personuppgifter.

Paragrafen reglerar den interna tillgången till personuppgifter för domstolens eller nämndens personal. Övervägandena finns i avsnitt 11.2.

I *första stycket* slås det fast att tillgången till personuppgifter i domstolarna och nämnderna alltid ska begränsas till vad varje anställd behöver för att kunna fullgöra sina arbetsuppgifter. Bestämmelsen riktar sig inte bara till dem som arbetar i domstolarnas och nämndernas dagliga verksamhet. Den får också betydelse vid t.ex. utformningen av nya datasystem och när den personuppgiftsansvarige har att avgöra vilken tillgång till personuppgifter respektive anställd ska ha för att kunna fullgöra sina uppgifter. Vid utformningen av de tekniska systemen är det i allmänhet inte möjligt att förutse i detalj vilken information varje anställd behöver få tillgång till i alla situationer. Avsikten med bestämmelsen är inte att fullständiga tekniska spärrar ska behöva etableras för allt som kan betecknas som överskottsinformation. En motsvarande bestämmelse finns bl.a. i 2 kap. 11 § polisdatalagen.

I *andra stycket* finns en upplysning om att regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela närmare föreskrifter om förutsättningarna för tillgången till personuppgifter.

Personuppgiftsansvar

9 § En allmän domstol, allmän förvaltningsdomstol eller hyres- och arrendenämnd är personuppgiftsansvarig för den behandling av personuppgifter som den domstolen eller nämnden utför.

Paragrafen innehåller bestämmelser om personuppgiftsansvar. Övervägandena finns i avsnitt 9.1.

Enligt 3 § PUL är den personuppgiftsansvarig som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Domstolsdatalagen hänvisar i 4 § första stycket 1 till denna definition. I paragrafen förtydligas att varje enskild domstol eller nämnd ska vara personuppgiftsansvarig för den behandling som den domstolen eller nämnden utför. Flera bestämmelser i personuppgiftslagen, till vilka domstolsdatalagen hänvisar, innebär särskilda skyldigheter för den personuppgiftsansvarige. Enligt domstolsdatalagen gäller vidare att den personuppgiftsansvarige ska utse ett eller flera personuppgiftsombud (10 §). Det är vidare den personuppgiftsansvariges uppgift att föra en förteckning över de personuppgiftsbehandlingar som utförs med stöd av denna lag (11 §).

Personuppgiftsombud

10 § Den personuppgiftsansvarige ska utse ett eller flera personuppgiftsombud.

Den personuppgiftsansvarige ska enligt personuppgiftslagen (1998:204) anmäla till tillsynsmyndigheten när ett personuppgiftsombud utses eller entledigas.

Paragrafen innehåller bestämmelser om personuppgiftsombud. Övervägandena finns i avsnitt 16.4.

Enligt *första stycket* är den personuppgiftsansvarige skyldig att utse personuppgiftsombud. Personuppgiftsombudets uppgifter framgår av 38 och 40 §§ PUL, vilka domstolsdatalagen hänvisar till (4 § första stycket 8).

Enligt *andra stycket* ska den personuppgiftsansvarige anmäla till tillsynsmyndigheten enligt personuppgiftslagen, dvs. Datainspektionen, när ett personuppgiftsombud utses eller entledigas. En motsvarande bestämmelse om personuppgiftsombud återfinns bl.a. i 2 kap. 5 § polisdatalagen.

Förteckning över personuppgiftsbehandlingar

11 § Den personuppgiftsansvarige ska föra en förteckning över de behandlingar som utförs med stöd av denna lag.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om vilka uppgifter en sådan förteckning ska innehålla.

I paragrafen regleras skyldigheten att föra en förteckning över personuppgiftsbehandlingar. Övervägandena finns i avsnitt 16.2.

I *första stycket* första stycket föreskrivs att den personuppgiftsansvarige är skyldig att föra en förteckning över de personuppgiftsbehandlingar som utförs med stöd av domstolsdatalagen.

Det förtydligas i *andra stycket* att regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om vilka uppgifter förteckningen ska innehålla. En utgångspunkt är att förteckningen bör innehålla samma kategorier av uppgifter som en anmälan enligt 36 § PUL ska innehålla. Det rör sig som bl.a. om en beskrivning av den personuppgiftsansvarige och dennes kontaktuppgifter, ändamålen med behandlingen, de kategorier av registrerade som berörs av behandlingen, de uppgifter som ska behandlas om de registrerade, de kategorier av mottagare till vilka uppgifterna kan komma att lämnas ut samt de åtgärder som har vidtagits för att trygga säkerheten i behandlingen (se vidare DIFS 2001:1). Förteckningen kan publiceras på domstolens eller nämndens hemsida, så att registrerade och andra enskilda lätt kan bilda sig en uppfattning om på vilka sätt personuppgifter behandlas i respektive domstol eller nämnd.

Upplysningar till allmänheten

12 § Den personuppgiftsansvarige ska till var och en som begär det skyndsamt och på lämpligt sätt lämna upplysningar om de behandlingar som utförs med stöd av denna lag. Upplysningarna ska omfatta de uppgifter som en förteckning enligt 11 § ska innehålla. Den personuppgiftsansvarige är dock inte skyldig att lämna ut sekretessbelagda uppgifter eller uppgifter om vilka säkerhetsåtgärder som har vidtagits.

Paragrafen innehåller bestämmelser om skyldigheten att lämna upplysningar till allmänheten. Övervägandena finns i avsnitt 16.2.

Enligt paragrafens bestämmelser har var och en, oavsett om vederbörande själv är registrerad, rätt att få information om vilka personuppgiftsbehandlingar som en domstol eller nämnd utför. Bestämmelsen motsvarar vad som gäller enligt 42 § PUL, men till skillnad från den bestämmelsen gäller inget undantag för uppgifter som anmälts till Datainspektionen, eftersom någon sådan anmälan inte ska ske enligt domstolsdatalagen. Enligt 26 § PUL, som enligt 4 § första stycket 4 är tillämplig, har därutöver den som ansöker om det rätt att en gång per år få information från den personuppgiftsansvarige om huruvida personuppgifter som rör honom eller henne behandlas.

Känsliga personuppgifter

13 § Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.

Paragrafen innehåller en begränsning avseende behandlingen av känsliga personuppgifter. Övervägandena finns i avsnitt 12.1.

I paragrafen uppställs ett förbud mot att behandla uppgifter om en person enbart på grund av vad som är känt om personens etniska ursprung, politiska åsikter, hälsa m.m. (känsliga personuppgifter). Det är således inte tillåtet att föra ett register över

eller på annat sätt göra anteckningar om enskilda enbart på den grunden att de utifrån etniskt ursprung, politiska åsikter, hälsa eller något annat i paragrafen angivet kriterium kan hänföras till en viss kategori av människor. Bestämmelsen innebär begränsningar i fråga om hur domstolarna och nämnderna får kategorisera eller märka uppgifter i domstolarnas datorsystem. Det är således inte tillåtet att vid en förvaltningsdomstol upprätta ett särskilt register över samtliga socialförsäkringsmål på grundval av vilken sjukdomsdiagnos som är aktuell i respektive mål. Bestämmelsen innebär också att det är förbjudet att i verksamhetsstödet kategorisera en uppgift som en känslig personuppgift av visst slag, t.ex. att kategorisera ordet ”kurd” som en uppgift om etniskt ursprung eller ”heterosexuell” som en uppgift om sexuell läggning. Det är inte heller tillåtet att i verksamhetsstödet konstruera ett särskilt fält med benämningen ”etniskt ursprung” eller ”sexuell läggning”, i vilket en anställd kan fylla i relevanta uppgifter. Paragrafen hindrar inte sådana sökningar som uttryckligen är tillåtna enligt 14–17 §§. Åtgärder som involverar känsliga personuppgifter begränsas på ett generellt plan av den ram som uppställs genom ändamålsbestämmelserna i 6 och 7 §§.

Sökning

14 § Uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening liksom uppgifter som rör hälsa eller sexualliv får användas som sökbegrepp endast vid sökning som avser uppgifter hos allmän förvaltningsdomstol. Detsamma gäller uppgifter som avslöjar nationell anknytning.

En sökning enligt första stycket får ske endast om det är absolut nödvändigt för handläggning av mål och ärenden.

Paragrafen innehåller bestämmelser om användningen av känsliga personuppgifter och uppgifter om nationell anknytning som sökbegrepp. Övervägandena finns i avsnitt 13.

Genom bestämmelserna *i första stycket* begränsas möjligheterna att som sökbegrepp använda känsliga personuppgifter och uppgifter som avslöjar nationell anknytning till uppgifter som finns vid allmän förvaltningsdomstol. Bestämmelsen innebär alltså att det inte är tillåtet att använda sådana sökbegrepp vid sökning bland uppgifter som finns vid en allmän domstol eller en hyres- och arrendenämnd. Detta gäller oavsett om den som utför sökningen själv arbetar vid den domstol där uppgifterna finns, eller om sökningen utförs på distans via direktåtkomst. Uttrycket uppgifter som avslöjar nationell anknytning syftar bl.a. på uppgifter om medborgarskap, om födelseort eller om utlandsfödda föräldrar. Varje form av nationell anknytning omfattas dock inte av bestämmelsen utan det krävs att uppgifterna tyder på en anknytning till ett land, vilken inte är alltför svag. En uppgift om att en person har besökt ett land eller att vederbörande känner någon i landet är inte uppgifter som kan anses utgöra uppgifter om nationell anknytning i lagens mening. Normalt torde uppgifter om språkkunskaper eller om behov av tolk inte vara att anse som en uppgift om nationell anknytning. Om det exempelvis är fråga om ett språk som endast talas i ett enda land och som få personer lär sig som andraspråk, kan dock bedömningen bli annorlunda. Övriga begrepp i paragrafen, såsom uppgifter om etnicitet, hälsa osv., har samma innebörd som enligt personuppgiftslagen.

I *andra stycket* anges att de sökningar som tillåts enligt första stycket endast får ske om det är absolut nödvändigt för handläggning av mål och ärenden. Redan de allmänna begränsningar som gäller för personuppgiftsbehandling enligt domstolsdatalagen, t.ex. ändamålsbestämmelserna, innebär begränsningar för vilka sökningar som är tillåtna. Genom kravet på att sökningen endast får utföras om det är absolut nödvändigt för handläggning av mål och ärenden uppställs en extra spärr mot obefogad användning av vissa särskilt integritetskänsliga sökbegrepp. Bestämmelsen innebär i praktiken att den anställde som vill använda ett sökbegrepp av nu aktuellt slag i varje enskilt fall måste göra en prövning av om sökningen är motiverad utifrån

verksamhetsbehoven. Slentrianmässig användning av sådana sökbegrepp är inte tillåten. Bestämmelsen i stycket utgör inte en sådan ovillkorlig begränsning som påverkar myndigheters skyldighet att sammanställa uppgifter ur allmänna handlingar enligt 2 kap. 3 § tredje stycket TF. En motsvarande bestämmelse finns i 15 § andra stycket.

15 § Uppgifter som avslöjar brott eller misstanke om brott får användas som sökbegrepp endast vid sökning som avser uppgifter hos allmän domstol.

En sökning enligt första stycket får ske endast om det är absolut nödvändigt för handläggning av mål och ärenden.

Paragrafen innehåller bestämmelser om användningen av uppgifter som avslöjar brott eller misstanke om brott som sökbegrepp. Övervägandena finns i avsnitt 13.

Genom bestämmelsen i *första stycket* begränsas möjligheterna att som sökbegrepp använda uppgifter som avslöjar brott eller misstanke om brott till uppgifter som finns vid allmän domstol. Bestämmelsen innebär alltså att det inte är tillåtet att använda sådana sökbegrepp vid sökning bland uppgifter som finns vid en allmän förvaltningsdomstol eller en hyres- och arrendenämnd. Detta gäller oavsett om den som utför sökningen själv arbetar vid den domstol där uppgifterna finns, eller om sökningen utförs på distans via direktåtkomst. Med uppgifter om brott och misstanke om brott avses även uppgifter om frihetsberövande på grund av brott eller misstanke om brott, uppgifter om brottspåföljder och liknande uppgifter.

I *andra stycket* anges att de sökningar som tillåts enligt första stycket endast får ske om det är absolut nödvändigt för handläggning av mål och ärenden. Redan de allmänna begränsningar som gäller för personuppgiftsbehandling enligt domstolsdatalagen, t.ex. ändamålsbestämmelserna, innebär begränsningar för vilka sökningar som är tillåtna. Genom kravet på att sökningen endast får utföras om det är absolut nödvändig för handläggning av mål och ärenden uppställs en extra spärr mot obefogad användning av vissa särskilt integritetskänsliga sökbegrepp.

Bestämmelsen innebär i praktiken att den anställde som vill använda ett sökbegrepp av nu aktuellt slag i varje enskilt fall måste göra en prövning av om sökningen är motiverad utifrån verksamhetsbehoven. Slentrianmässig användning av sådana sökbegrepp är inte tillåten. Bestämmelsen i stycket utgör inte en sådan ovillkorlig begränsning som påverkar myndigheters skyldighet att sammanställa uppgifter ur allmänna handlingar enligt 2 kap. 3 § tredje stycket TF. En motsvarande bestämmelse finns i 14 § andra stycket.

16 § Bestämmelserna i 14 och 15 §§ gäller inte vid sökning i en viss handling eller i ett visst mål eller ärende.

I paragrafen föreskrivs undantag från sökbegränsningarna enligt 14 och 15 §§. Övervägandena finns i avsnitt 13.4.

Bestämmelsen innebär att sökningar som sker enbart bland uppgifter i en viss handling eller i ett visst mål är undantagna från de begränsningar som annars gäller i fråga om sökning. För alla åtgärder som innebär att personuppgifter behandlas med stöd av domstolsdatalagen, inklusive sökningar, gäller dock att åtgärden endast får äga rum om den ryms inom de ramar som uppställs genom ändamålsbestämmelserna i 6 och 7 §§.

17 § Regeringen meddelar ytterligare föreskrifter om begränsning av möjligheterna att söka.

Paragrafen innehåller en bestämmelse om möjligheterna för regeringen att meddela strängare sökbegränsningar. Övervägandena finna i avsnitt 13.2.

I paragrafen tydliggörs att regeringen har möjlighet att meddela ytterligare föreskrifter som begränsar möjligheterna att söka i förhållande till vad som gäller enligt domstolsdatalagen. Det kan röra sig om ytterligare sökbegrepp som ska vara förbjudna, att vissa sökbegrepp får användas endast vid sökning bland uppgifter i en viss måltyp eller andra begränsningar som ska gälla i fråga om sökningar.

Utlämnande på medium för automatiserad behandling

18 § Personuppgifter får lämnas ut till en myndighet på medium för automatiserad behandling.

Personuppgifter i ett mål eller ärende får även lämnas ut till en part och till en parts ombud, biträde eller försvarare på medium för automatiserad behandling.

I övrigt får enstaka personuppgifter lämnas ut på medium för automatiserad behandling.

Paragrafen reglerar i vilka fall personuppgifter får lämnas ut på medium för automatiserad behandling, Övervägandena finns i avsnitt 14.2.

Med utlämnade på medium för automatiserad behandling avses sådant elektroniskt utlämnande som inte är direktåtkomst, t.ex. utlämnande genom e-post, på ett USB-minne eller elektronisk överföring. Direktåtkomst regleras i 20 och 21 §§. I förevarande paragraf regleras i vilken utsträckning personuppgifter får lämnas ut på medium för automatiserad behandling. Av 19 § följer att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om att uppgifter får lämnas ut på sådant medium även i andra fall. Ingen av de nämnda bestämmelserna har någon sekretessbrytande verkan. Ingen av bestämmelserna innebär heller någon skyldighet för domstolarna att använda sig av elektroniskt utlämnande, ens om mottagaren uttryckligen begär det. Det är domstolens ansvar att ytterst bedöma om det är lämpligt att använda den typen av utlämnande. Innan personuppgifter lämnas ut i elektroniskt format behöver domstolen överväga de integritetsrisker som ett sådan utlämnande kan medför i förlängningen, t.ex. risken för att känsliga fotografier sprids genom att publiceras på internet. Som vid all personuppgiftsbehandling enligt domstolsdatalagen har domstolarna att förhålla sig till personuppgiftslagens bestämmelser om säkerheten vid behandlingen (30 och 31 §§ samt 32 § första stycket PUL, vilka 4 § hänvisar till). Enligt dessa bestämmelser är domstolarna bl.a. skyldiga att genom tekniska och organisatoriska åtgärder se till att personuppgifter skyddas och att det åstadkoms en säkerhetsnivå som är lämplig med hänsyn till

tillgänglig teknik, kostnader, särskilda risker och uppgifternas känslighet.

I *första stycket* föreskrivs att personuppgifter får lämnas ut på medium för automatiserad behandling till domstolar och andra myndigheter.

Enligt *andra stycket* tillåts domstolarna vidare att använda sig av medium för automatiserad behandling vid kommunikation i mål och ärenden med parter och deras ombud, biträde eller försvarare. Om en part för sin talan genom förvaltare, god man särskild ställföreträdare för barn eller någon annan form av ställföreträdare får domstolarna använda sig av medium för automatiserad behandling i samma utsträckning som skulle varit möjligt i förhållande till parten själv.

Det följer av *tredje stycket* att enstaka personuppgifter får lämnas ut på medium för automatiserad behandling även till andra än dem som nämns i första och andra styckena. Begränsningen till enstaka uppgifter innebär att en större mängd personuppgifter, t.ex. ett helt register eller delar av ett register, inte får lämnas ut på medium för automatiserad behandling med stöd av denna bestämmelse. Ordet enstaka används i paragrafen, liksom i 2 kap. 20 § polisdatalagen och 2 kap. 8 § kustbevakningsdatalagen, med en annan innebörd än i vanligt språkbruk. I synnerhet i de fall då det är fråga om uppgifter som i sig själva är harmlösa bör begränsningen till enstaka uppgifter inte innebära att antalet uppgifter behöver begränsas så strängt. En lista med ett större antal telefonnummer har exempelvis bedömts kunna rymmas inom begreppet enstaka personuppgifter (prop. 2009/10:85 s. 333 och prop. 2006/07:46 s. 124).

19 § Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om att uppgifter får lämnas ut på medium för automatiserad behandling även i andra fall än som avses i 18 §.

Paragrafen innehåller bestämmelser om möjligheterna för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om att utlämnande på medium för auto-

matiserad behandling ska vara tillåtet i andra fall än som följer av 18 §. Övervägandena finns i avsnitt 14.2.

I paragrafen tydliggörs att regeringen eller den myndighet som regeringen bestämmer har möjlighet att utvidga möjligheterna för domstolarna att lämna ut personuppgifter på medium för automatiserad behandling. Det kan exempelvis vara befogat att medge utlämnande av mer än endast enstaka uppgifter till enskilda i vissa fall.

Direktåtkomst

20 § Direktåtkomst till personuppgifter får medges en allmän domstol, en allmän förvaltningsdomstol eller en hyres- och arrendenämnd.

En part och en parts ombud, biträde eller försvarare får medges direktåtkomst till personuppgifter i sitt mål eller ärende.

Paragrafen innehåller bestämmelser om direktåtkomst. Övervägandena finns i avsnitt 14.3.

Enligt *första stycket* får direktåtkomst till de personuppgifter som behandlas i den rättskipande och rättsvårdande verksamheten medges vissa myndigheter, nämligen de myndigheter som omfattas av domstolsdatalagens tillämpningsområde.

Av *andra stycket* följer en särskild möjlighet för domstolarna att medge parter och deras ombud, biträde eller försvarare direktåtkomst till personuppgifter i sina egna mål. Direktåtkomsten får bara avse ett visst mål eller ärende i taget. Bestämmelsen omfattar både enskilda parter och parter som företräder det allmänna.

I de fall som en domstol har möjlighet att medge direktåtkomst innebär det inte någon rätt för mottagarna att få sådan åtkomst. Det är den domstol som innehar informationen som bestämmer om sådan åtkomst ska beviljas eller inte. Denna domstol har ett principiellt ansvar för att förvissa sig om att den som beviljas direktåtkomst vidtar de åtgärder som bedöms vara nödvändiga ur säkerhetssynpunkt (prop. 2011/12:45 s. 133).

Direktåtkomst bör endast beviljas om det i det enskilda fallet bedöms lämpligt. De uppgifter som mottagaren har direktåtkomst till får i normalfallet anses utlämnade i offentlighets- och sekretesslagens mening i och med att direktåtkomst finns. Det spelar i det avseendet ingen roll om mottagaren faktiskt tar del av en viss uppgift eller inte (jfr SOU 2007:45 s. 192 f.). Paragrafen, liksom övriga bestämmelser om elektroniskt utlämnande i domstolsdatalagen, saknar sekretessbrytande verkan. För att en domstol ska kunna medge direktåtkomst räcker det därför inte att det är tillåtet enligt domstolsdatalagen. Direktåtkomst till uppgifter som omfattas av sekretess får bara medges om det står klart att mottagaren vid en prövning enligt offentlighets- och sekretesslagen med säkerhet skulle ha rätt att ta del av uppgifterna. I 11 kap. 4 § OSL finns en särskild bestämmelse om direktåtkomst som innebär att sekretess som gäller hos en myndighet kan överföras till en annan myndighet som har direktåtkomst.

21 § Regeringen eller den myndighet som regeringen bestämmer meddelar ytterligare föreskrifter om begränsning av direktåtkomsten enligt 20 § samt om behörighet och säkerhet vid sådan åtkomst.

Paragrafen innehåller bestämmelser om möjligheterna för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om direktåtkomst. Övervägandena finns i avsnitt 14.3.

I paragrafen förtydligas att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter som ytterligare begränsar möjligheterna att medge direktåtkomst till personuppgifter. Det kan röra sig om att bara tillåta direktåtkomst inom samma domstolsslag i vissa fall. Genom sådana föreskrifter kan det också preciseras vilka uppgifter som direktåtkomsten får avse och vilka personalkategorier som får medges direktåtkomst. I paragrafen förtydligas också att regeringen eller den myndighet som regeringen bestämmer kan meddela före-

skrifter om behörighets- och säkerhetsfrågor såvitt avser direktåtkomst.

Bevarande i arkiv m.m.

22 § Regeringen eller den myndighet som regeringen bestämmer meddelar ytterligare föreskrifter om bevarande av personuppgifter som hänför sig till ett mål eller ärende som har avgjorts genom dom eller beslut som har vunnit laga kraft.

Paragrafen innehåller bestämmelser om bevarande av personuppgifter. Övervägandena finns i avsnitt 15.3.

Enligt 4 § första stycket 2 och 3 gäller att frågan om hur länge personuppgifter får bevaras i elektroniskt format styrs av personuppgiftslagens bestämmelser. Det innebär att personuppgifter i allmänna handlingar kan bevaras elektroniskt (8 § andra stycket PUL). Även andra personuppgifter kan bevaras, men endast så länge som det är nödvändigt med hänsyn till ändamålet med behandlingen (9 § PUL). För uppgifter som bevaras gäller bestämmelserna i domstolsdatalagen. I förevarande paragraf förtydligas att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om vilka ytterligare villkor som ska gälla för sådant bevarande. Regeringen eller den myndighet som regeringen bestämmer har således möjlighet att föreskriva hur lång tid personuppgifter ska få vara åtkomliga för olika former av sökning och direktåtkomst, hur uppgifterna ska bevaras och vilka andra begränsningar som ska gälla för personuppgifter som är hänförliga till mål och ärenden, vilka har avslutats genom ett lagakraftvunnet avgörande.

Överklagande

23 § En hovrätts, tingsrätts eller förvaltningsrätts beslut om upplysningar enligt 12 §, information enligt 26 § personuppgiftslagen (1998:204) samt om rättelse och underrättelse till tredje man enligt 28 § samma lag får överklagas till kammarrätten. En kammarrätts beslut i sådana frågor får överklagas till Högsta förvaltningsdomstolen. Högsta domstolens och Högsta förvaltningsdomstolens beslut i sådana frågor får inte överklagas.

En hyres- och arrendenämnds beslut i sådana frågor som avses i första stycket får överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen reglerar frågor om överklagande. Övervägandena finns i avsnitt 17.4.

I paragrafen anges vilka beslut av en personuppgiftsansvarig domstol eller nämnd som får överklagas. Det är beslut om upplysningar till allmänheten enligt 12 § samt beslut om information, rättelse och underrättelse till tredje man enligt 26 och 28 §§ PUL, vilka enligt 4 § är tillämpliga vid personuppgiftsbehandling i domstolarnas och nämndernas rättskipande och rättsvårdande verksamhet. Genom hänvisning i 4 § till 53 § PUL framgår att andra beslut än de som anges i denna paragraf och i 51 § PUL inte får överklagas.

Enligt *första stycket* får de nämnda besluten av en personuppgiftsansvarig hovrätt, tingsrätt eller förvaltningsrätt överklagas till kammarrätt. Det krävs inte prövningstillstånd i kammarrätten vid ett sådant överklagande. Ett beslut som meddelats av en personuppgiftsansvarig kammarrätt får i stället överklagas till Högsta förvaltningsdomstolen, varvid det inte krävs prövningstillstånd (35 § FPL, jfr även prop. 1979/80:2 Del A s. 364). Högsta domstolens och Högsta förvaltningsdomstolens beslut i nu aktuella frågor som domstolarna meddelat i egenskap av personuppgiftsansvarig får inte överklagas.

Av *andra stycket* följer att beslut i nämnda frågor av en personuppgiftsansvarig hyres- och arrendenämnds får överklagas till allmän förvaltningsdomstol samt att prövningstillstånd krävs vid överklagande till kammarrätten.

Sammanfattning av Domstolsdata-utredningens förslag

En ny reglering för behandling av personuppgifter i domstolarna och nämnderna

Domstolsdatautredningen överlämnade i januari 2002 sitt slutbetänkande, Informationshantering och behandling av uppgifter vid domstolar, En rättslig översyn (SOU 2001:100).

Enligt utredningen visar utvecklingen inom datorområdet att lagstiftning som reglerar användningen av datorstöd måste vara teknikoberoende och flexibel för att inte hindra den effektivisering av verksamheterna i de allmänna domstolarna, de allmänna förvaltningsdomstolarna samt hyres- och arrendenämnderna som kontinuerligt pågår. Samtidigt är det mycket viktigt att det i lagstiftningen hela tiden tas hänsyn till enskildas personliga integritet.

För att garantera såväl integritetsskyddet som möjligheterna till fortlöpande effektivisering av verksamheterna, är det nödvändigt med en lagstiftning som tar sikte på principiellt viktiga frågor, men så långt som möjligt lämnar detaljregleringen därhän. Utredningen föreslår därför att de grundläggande principerna för behandling av personuppgifter i domstolarnas och nämndernas rättskipande och rättsvårdande verksamhet ska regleras särskilt i lag, medan kompletterande bestämmelser ska meddelas av regeringen eller den myndighet som regeringen bestämmer.

Med hänsyn till de skilda verksamhetsområdena anser utredningen att det inte är lämpligt med en enda gemensam lag och en förordning. I stället föreslås en sammanhållen reglering för de allmänna domstolarna, en för de allmänna förvaltningsdomstolarna samt en för hyres- och arrendenämnderna. För behandling av personuppgifter i domstolarnas och nämndernas administrativa verksamhet anser utredningen att det är tillräckligt med personuppgiftslagens bestämmelser och det föreslås därför ingen särskild reglering inom det området.

De föreslagna lagarna ska alla bestå av tre delar. I den första delen finns allmänna bestämmelser om hur uppgifter ska behandlas vid domstolarna och nämnderna. I den andra delen regleras särskilt behandling av uppgifter i databaser. I den tredje delen finns bestämmelser om enskildas rättigheter gentemot de personuppgiftsansvariga domstolarna och nämnderna. Till varje lag föreslår utredningen en förordning där regeringen meddelar närmare bestämmelser som kompletterar lagarna.

Allmänna bestämmelser

Elektronisk informationshantering och behandling av uppgifter kan förekomma såväl i form av e-postfunktioner och ordbehandling som användning av register och avancerade datorsystem. Lagarna föreslås vara tillämpliga på all sådan behandling av personuppgifter i domstolarnas och nämndernas rättskipande och rättsvårdande verksamhet. Även behandling av personuppgifter i strukturerade manuella register ska omfattas av lagarnas tillämpningsområde.

Personuppgiftslagen gäller bara för behandling av uppgifter om levande fysiska personer. Ett flertal grundläggande bestämmelser i de föreslagna lagarna ska enligt utredningen vara tillämpliga även på uppgifter om juridiska personer och avlidna.

Bestämmelser i personuppgiftslagen ska tillämpas på behandling av personuppgifter vid domstolar och nämnder endast när det anges särskilt.

De ändamål för vilka personuppgifter ska få behandlas automatiserat eller i manuella register är handläggning av mål och ärenden, fullgörande av underrättelseskyldighet som följer av lag eller förordning, återsökning av vägledande avgöranden samt planering, uppföljning och utvärdering av verksamheten. Uppgifter ska också få användas för att framställa statistik.

En domstol eller nämnd ska vara personuppgiftsansvarig för behandling som den utför eller som det åligger den att utföra.

Behandling av personuppgifter som utförs med hjälp av persondatorer och som andra inte har tillgång till, t.ex. vanlig ordbehandling och e-posthantering, omfattas inte av bestämmelserna om databaser. Vid sådan behandling ska känsliga personuppgifter få användas endast om uppgifterna har lämnats automatiserat i ett mål eller ärende eller om uppgiften behövs för handläggningen, för fullgörande av underrättelseskyldighet eller för återsökning av vägledande avgöranden. Uppgifter som behandlas automatiserat i ett mål eller ärende utanför databasen, ska gallras senast ett år efter det att målet eller ärendet har avslutats, om inte regeringen eller Riksarkivet har meddelat föreskrifter om att uppgifter ska gallras vid en senare tidpunkt eller bevaras.

Behandling av personuppgifter i databaser

Utredningen föreslår att begreppet databas införs i regleringen för domstolar och nämnder, som en benämning på samlingar av uppgifter och handlingar som med hjälp av automatiserad behandling används gemensamt i verksamheterna. Avgörande för att viss behandling av personuppgifter ska omfattas av de särskilda bestämmelserna om databaser är att uppgifter eller handlingar hanteras för gemensamt bruk inom eller mellan domstolar och nämnder.

I databaser bör enligt utredningen en åtskillnad göras mellan uppgifter och handlingar. Med uppgifter avses enskilda ord eller mindre sammanställningar av ord som är bärare av en begränsad

informationsmängd och som enligt fastställda rutiner kan registreras på ett bestämt sätt i ett datorsystem. Med handlingar avses sammanställningar av uppgifter utan en i förväg fastställd struktur i datorsystemet, t.ex. ordbehandlingsdokument, e-postmeddelanden, digitala ljud- och bildupptagningar eller skannade pappershandlingar.

I en databas ska uppgifter om personer som omfattas av handläggningen av mål och ärenden eller som berörs av författningsreglerad underrättelseskyldighet få behandlas under förutsättning att det sker för de i lagstiftningen uttryckligen angivna ändamålen. I lag bör endast anges vilka kategorier av uppgifter som får hanteras i databaserna, medan den närmare preciseringen av vilka uppgifter som omfattas kan beslutas av regeringen eller Domstolsverket. Undantag görs dock för känsliga personuppgifter, som får behandlas endast om det uttryckligen anges i lag. Utredningen föreslår att parters nationalitet och språktillhörighet ska få anges som identitets-uppgifter samt att känsliga personuppgifter ska få användas vid angivande av saken i ett mål eller ärende, om det är nödvändigt för att saken ska kunna återges på ett ändamålsenligt sätt. Regeringen eller Domstolsverket meddelar närmare föreskrifter om vilka uppgifter som får behandlas.

Elektroniska handlingar ska få behandlas i stor omfattning i databaserna, vilket är nödvändigt för att effektiva mål- och ärendehanteringssystem ska kunna användas. Handlingar som har kommit in till en domstol eller nämnd i ett mål eller ärende ska få lagras i en databas utan begränsningar. I en upprättad elektronisk handling ska känsliga personuppgifter däremot få behandlas endast om det behövs för handläggningen av ett mål eller ärende, för fullgörande av författningsreglerad underrättelseskyldighet eller för återsökning av vägledande avgöranden.

Elektroniskt utlämnande av personuppgifter i databaser

Utredningen anser att uppgifter utan begränsningar ska få lämnas ut elektroniskt på medium för automatiserad behandling till myndigheter, om det behövs för handläggningen av ett mål eller ärende eller för författningsreglerad underrättelseskyldighet. Uppgifter ska även få lämnas ut till andra än myndigheter på detta sätt, om regeringen meddelar föreskrifter om det. Utredningen föreslår att det i förordning anges att avidentifierade rättsfall får lämnas ut till enskilda på elektronisk väg. Även uppgifter och handlingar i övrigt bör få lämnas ut, om det är uppenbart att det kan ske utan risk för intrång i enskildas personliga integritet.

Utredningen föreslår att en allmän domstol ska få ha direktåtkomst till samtliga uppgifter i andra allmänna domstolars mål och ärenden. Detsamma ska gälla en allmän förvaltningsdomstols direktåtkomst till andra förvaltningsdomstolars mål samt en hyres- och arrendenämnds direktåtkomst till andra nämnders ärenden. Direktåtkomst till identitetsuppgifter ska dock få förekomma endast i pågående mål och ärenden. Direktåtkomst ska över huvud taget inte få förekomma till elektroniska handlingar. Domstolsverket ska för framställning av statistik få ha direktåtkomst till avidentifierade uppgifter i domstolarnas och nämndernas databaser.

Utredningen föreslår att en part ska få ha direktåtkomst till uppgifter i egna mål och ärenden vid domstolar och nämnder, om regeringen meddelar föreskrifter om det.

Sökning efter uppgifter och handlingar i databaser

Utredningen anser att sökning i en databas i princip bör vara så fri som möjligt för att ett effektivt utnyttjande av datorsystemen ska kunna åstadkommas. I vissa avseenden är det dock av integritetsskäl viktigt att det finns begränsningar. Vid sökning efter identitetsuppgifter, t.ex. för att få fram ett namn eller en

adress, ska känsliga personuppgifter inte få användas som sökbegrepp. Det ska däremot vara tillåtet att använda sådana uppgifter vid sökning på saken, dvs. beskrivningen av ett mål eller ärende, för att få information om intressanta avgöranden.

Vid sökning efter elektroniska handlingar får som sökbegrepp endast användas uppgifter om datum när en handling kom in eller upprättades, diarienummer eller annan beteckning på en handling samt från vem handlingen har kommit in eller till vem den har expedierats.

Regeringen ska kunna föreskriva att andra sökbegrepp får användas efter det att uppgifter eller handlingar har överlämnats till en arkivmyndighet. Utredningen föreslår att det tjugofem år efter att ett mål eller ärende har avslutats ska vara möjligt att vid en arkivmyndighet söka efter uppgifter och handlingar utan begränsningar i fråga om sökbegrepp.

Gallring av uppgifter i databaser

Av integritetsskäl bör uppgifter och handlingar som huvudregel inte få bevaras utan tidsgräns. Utredningen anser att uppgifter och handlingar i ett mål eller ärende ska, beroende på mål- eller ärendetyp, gallras antingen två eller sex år efter utgången av det kalenderår då målet eller ärendet avslutades.

Uppgifter som behövs för återsökning av vägledande avgöranden och innehållet i avidentifierade domar och beslut får gallras vid en senare tidpunkt, dock senast tio år efter utgången av det kalenderår då målet eller ärendet avslutades.

Regeringen eller Riksarkivet ska få föreskriva att uppgifter eller handlingar ska gallras vid en senare tidpunkt eller bevaras.

Avgifter

Användningen av elektronisk mål- och ärendehantering kommer att underlätta arbetet för domstolar och nämnder. Samtidigt

finns det risk för att förfrågningar från myndigheter och enskilda att i elektronisk form få ta del av handlingar kan leda till att domstolar och nämnder får lägga tid på att göra olika sammanställningar av uppgifter. Utredningen föreslår därför att en domstol eller nämnd ska få ta ut avgifter för att lämna ut uppgifter eller handlingar ur en databas.