

Lagrådsremiss

Domstolsdatalag

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 11 juni 2015

Morgan Johansson

Per Lennerbrant
(Justitiedepartementet)

Lagrådsremissens huvudsakliga innehåll

Regeringen föreslår en lag om behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas och hyres- och arrendenämndernas rättskipande och rättsvårdande verksamhet.

Syftet med lagen är att ge domstolarna och nämnderna möjlighet att behandla personuppgifter på ett effektivt och ändamålsenligt sätt och att skydda människor mot att deras personliga integritet kränks vid sådan behandling. En utgångspunkt är att skapa en teknikneutral och flexibel lag som innehåller de bestämmelser som är av central betydelse för integritetsskyddet, däribland ändamålen med behandlingen och de begränsningar som ska gälla för behandlingen av vissa uppgifter.

Lagen ska gälla i stället för personuppgiftslagen (1998:204), men innehåller hänvisningar till de bestämmelser i personuppgiftslagen som ska vara tillämpliga i domstolarnas och nämndernas verksamhet.

Den nya lagen föreslås träda i kraft den 1 januari 2016.

Innehållsförteckning

1	Beslut	4
2	Förslag till domstolsdatalag	5
3	Ärendet och dess beredning	9
4	Övergripande rättslig reglering	9
4.1	Regeringsformen	9
4.2	Internationella konventioner.....	10
4.3	EU-rättslig reglering.....	11
4.4	Personuppgiftslagen	14
5	Nuvarande reglering av personuppgiftsbehandlingen i domstolarna och nämnderna	16
5.1	Inledning	16
5.2	Vera-förordningarna.....	16
6	En lag om domstolarnas behandling av personuppgifter	19
6.1	Behovet av en ny reglering.....	19
6.2	Lagens tillämpningsområde	25
6.3	Lagens syfte.....	28
6.4	Lagens förhållande till personuppgiftslagen.....	29
6.5	Lagens förhållande till offentlighetsprincipen.....	30
6.6	Beteckningar och definitioner	30
6.7	Lagens förhållande till viss annan lagstiftning	31
7	Personuppgiftsansvarig och personuppgiftsbiträden	32
7.1	Varje domstol är personuppgiftsansvarig	32
7.2	Domstolarna får anlita personuppgiftsbiträden	35
8	Ramarna för domstolarnas personuppgiftsbehandling	36
8.1	Grundläggande krav på domstolarnas personuppgiftsbehandling	36
8.2	Verksamhets specifika ändamålsbestämmelser	38
9	Säkerhet och intern åtkomst	43
9.1	Säkerheten vid behandlingen.....	43
9.2	Tillgång till personuppgifter.....	44
10	Behandling av känsliga personuppgifter och personnummer	47
10.1	Känsliga personuppgifter	47
10.2	Personnummer.....	51
11	Sökbegränsningar.....	51
11.1	Allmänt om sökning	51
11.2	Utgångspunkter för sökregleringens utformning	53
11.3	Någon särskild sekretessbestämmelse föreslås inte.....	55
11.4	Integritetskänsliga sökningar ska begränsas	57
11.5	Generella undantag från sökbegränsningarna.....	63
12	Elektroniskt utlämnande	64
12.1	Utlämnande genom direktåtkomst.....	64

12.2	Utlämnande på medium för automatiserad behandling	73
12.3	Överföring till tredjeland	78
13	Bevarande av personuppgifter	80
14	Insyn och tillsyn	84
14.1	Enskildas insyn i personuppgiftsbehandlingen	84
14.2	Tillsynsmyndighet	88
14.3	Personuppgiftsombud	91
15	Rättsmedel	92
15.1	Åtgärder vid felaktig personuppgiftsbehandling	92
15.2	Överklagande	93
16	Ikraftträdande- och övergångsbestämmelser	96
17	Konsekvenser av förslagen	97
18	Författningskommentar	100
Bilaga 1	Sammanfattning av promemorian Domstolsdatalog (Ds 2013:10)	118
Bilaga 2	Promemorians lagförslag	119
Bilaga 3	Förteckning över remissinstanserna	123

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till domstolsdatalag.

2 Förslag till domstolsdatalag

Härigenom föreskrivs följande.

Lagens syfte

1 § Syftet med denna lag är att ge de allmänna domstolarna, de allmänna förvaltningsdomstolarna och 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.

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas och hyres- och arrendenämndernas rättskipande och rättsvårdande verksamhet. Lagen gäller också när personuppgifterna vidarebehandlas i den administrativa verksamheten för att lämnas ut efter begäran.

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

3 § Om det i lagen (2013:329) med vissa bestämmelser 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.

Förhållandet till personuppgiftslagen

4 § Om inte något annat anges i 5 §, gäller denna lag i stället för personuppgiftslagen (1998:204).

5 § 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. 22 § om behandling av personnummer,
5. 23 och 25–27 §§ om information till den registrerade,
6. 28 § om rättelse,
7. 30 och 31 §§ samt 32 § första stycket om säkerheten vid behandling,
8. 33–35 §§ om överföring av personuppgifter till tredjeland,
9. 38, 40 och 41 §§ om personuppgiftsombud m.m.,
10. 43 och 44 §§, 45 § första stycket och 47 § om tillsynsmyndighetens befogenheter, och

11. 48 § om skadestånd.

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

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 det som varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om tillgången till personuppgifter.

Personuppgiftsansvar

9 § En allmän domstol, en allmän förvaltningsdomstol eller en 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 anmäla till tillsynsmyndigheten enligt personuppgiftslagen (1998:204) när ett personuppgiftsombud utses eller entledigas.

Förteckning över personuppgiftsbehandlingar

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

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om vilka uppgifter en sådan förteckning ska innehålla.

Upplysningar till allmänheten

12 § Den personuppgiftsansvarige ska skyndsamt och på lämpligt sätt lämna upplysningar om de behandlingar som utförs med stöd av denna lag till var och en som begär det. 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.

Behandling av 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.

Sökbegränsningar

14 § Vid sökning i personuppgifter är det förbjudet att som sökbegrepp använda uppgifter som avslöjar

1. ras eller etniskt ursprung,
2. politiska åsikter,
3. religiös eller filosofisk övertygelse,
4. medlemskap i fackförening,
5. hälsa,
6. sexualliv,
7. nationell anknytning, eller
8. brott eller misstanke om brott.

Användning av särskilda beteckningar för identifiering av en viss mål- eller ärendetyp som sökbegrepp omfattas inte av förbudet i första stycket.

15 § Förbudet i 14 § första stycket gäller inte användning

1. i allmän domstol av sökbegrepp som avslöjar brott eller misstanke om brott, och
2. i allmän förvaltningsdomstol av sökbegrepp som avslöjar hälsa, brott eller misstanke om brott.

Förbudet i 14 § första stycket gäller inte heller vid sökning i en viss handling eller i ett visst mål eller ärende.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om begränsningar av möjligheten att använda de sökbegrepp som anges i första stycket.

Elektroniskt utlämnande av personuppgifter

16 § Personuppgifter får lämnas ut på medium för automatiserad behandling om det inte är olämpligt.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter på medium för automatiserad behandling.

17 § Direktåtkomst får endast medges

1. en allmän domstol,

2. en allmän förvaltningsdomstol,
3. en hyres- och arrendenämnd, eller
4. en part eller partens ombud, biträde eller försvarare.

Direktåtkomst enligt första stycket 4 får endast avse personuppgifter i partens mål eller ärende.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar av direktåtkomst enligt första stycket och om behörighet och säkerhet vid sådan åtkomst.

Personuppgifter i avgjorda mål och ärenden

18 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar för behandling av personuppgifter som hänför sig till ett mål eller ärende som har avgjorts genom en dom eller ett beslut som har fått laga kraft.

Överklagande

19 § Tillsynsmyndighetens beslut enligt denna lag eller enligt de bestämmelser i personuppgiftslagen (1998:204) som anges i 5 § om annat än föreskrifter får överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.

20 § En hovrätts, tingsrätts eller förvaltningsrätts beslut om upplysningar enligt 12 § eller om information till den registrerade enligt 26 § personuppgiftslagen (1998:204) och 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 frågor som avses i första stycket får inte överklagas.

21 § En hyres- och arrendenämnds beslut i frågor som avses i 20 § första stycket får överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.

22 § Andra beslut än sådana som avses i 19–21 §§ eller i 47 § personuppgiftslagen (1998:204) får inte överklagas.

Vid överklagande av förvaltningsrättens beslut i frågor som avses i 47 § personuppgiftslagen krävs prövningstillstånd vid överklagande till kammarrätten.

Denna lag träder i kraft den 1 januari 2016.

3 Ärendet och dess beredning

Sedan flera år är modern informationsteknik en naturlig del av de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas och hyres- och arrendenämndernas verksamhet. Den nuvarande regleringen av den automatiserade behandlingen av personuppgifter vid domstolarna och nämnderna tillkom år 2001 som en provisorisk lösning för att tillgodose de behov av regler som uppstod då datalagen (1973:289) upphörde att gälla. Sedan dess har de sätt på vilka personuppgifter behandlas i domstolarnas och nämndernas verksamhet förändrats. Mot bakgrund av den digitala teknikens utveckling finns ett behov av att modernisera det nuvarande regelverket som styr den automatiserade behandlingen av personuppgifter i domstolarnas och nämndernas verksamhet. Inom Justitiedepartementet har därför upprättats en departementspromemoria (Ds 2013:10 Domstolsdatalag) med förslag till en ny lag om behandling av personuppgifter i domstolarna och nämnderna. Syftet med regleringen är att ge domstolarna och nämnderna möjlighet att behandla personuppgifter på ett effektivt och ändamålsenligt sätt i den rättskipande och rättsvårdande verksamheten och att skydda människor mot att deras personliga integritet kränks vid sådan behandling. En sammanfattning av promemorian finns i *bilaga 1*. Promemorians lagförslag finns i *bilaga 2*.

Promemorian har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. Remissyttrandena finns tillgängliga i Justitiedepartementet (Ju2013/1684/DOM).

I februari 2015 anordnande Domstolsverket ett seminarium för att kartlägga behovet av att kunna utföra sökningar med integritetskänsliga sökbegrepp i domstolarna och nämndernas verksamhet. Minnesanteckningar från seminariet finns tillgängliga i Justitiedepartementet (Ju2013/1684/DOM).

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 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. Efter detta datum kommer det

således inte vara möjligt att behålla förordningsregler som är av den angivna karaktären i förhållande till den personliga integriteten.

4.2 Internationella konventioner

Europakonventionen

Enligt artikel 8 i den europiska konventionen om skydd för de mänskliga rättigheterna och grundläggande friheterna (Europakonventionen) har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. En offentlig myndighet får inte inskränka 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 finnas ett angeläget samhällligt 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 få rättelse. Prövningen kan göras av domstol, men även prövning av en stats regering eller av en förvaltningsmyndighet kan vara tillräcklig.

Europakonventionen gäller som lag i Sverige. Av regeringsformen framgår att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av 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).

Dataskyddskonventionen

Reglering om automatiserad behandling av personuppgifter finns i bl.a. Europarådets konvention från år 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. Ett arbete med att se över konventionen har inletts.

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 iakttä 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 och 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, och för att skydda enskildas fri- och rättigheter.

4.3 EU-rättslig reglering

Stadgan om de grundläggande rättigheterna

Lissabonfördraget innebär att Europeiska unionens stadga om de grundläggande rättigheterna 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 och 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 tillgång till insamlade uppgifter som rör honom eller henne och att få dem rättade. En oberoende myndighet ska kontrollera att reglerna

efterlevs. Av artikel 51 i stadgan framgår att den riktar sig till verksamhet som utförs av EU:s egna organ och institutioner och att den blir tillämplig för medlemsstaterna endast i de fall där de tillämpar EU-rätten. Stadgan är följaktligen inte tillämplig på nationell lagstiftning inom områden där EU inte har lagstiftningskompetens.

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. Av artikel 53 följer att stadgans artiklar inte får tolkas som att de inskränker eller inkräktar på rättigheter enligt andra konventioner eller överenskommelser om fri- och rättigheter.

Dataskyddsdirektivet

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 (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 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 och 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 tredjeland.

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 baserat på den reglering som redan gäller enligt dataskyddsdirektivet. Förhandlingarna om dataskyddsförordningen pågår.

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. De återstående delarna av rambeslutet har genomförts i svensk rätt genom lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen. Lagen trädde i kraft den 1 juli 2013.

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 har kommissionen föreslagit att rambeslutet ska ersättas av ett särskilt dataskyddsdirektiv för de brottsbekämpande myndigheterna (KOM(2012) 10). Förhandlingarna om direktivet pågår.

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).

Personuppgiftslagen syftar till att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter (1 §). Lagen är tekniskneutral 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. 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 uppräknning 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.

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

ling 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 som 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 lagöverträdelse som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden och 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, blockeras eller utplånas av den personuppgiftsansvarige (28 §). Lagen innehåller vidare bestämmelser om säkerheten vid behandling av personuppgifter (30–32 §§).

Enligt personuppgiftslagen är det förbjudet att till tredjeland 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 tredjeland 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 personliga integritet.

5 Nuvarande reglering av personuppgiftsbehandlingen i domstolarna och nämnderna

5.1 Inledning

Sveriges Domstolar utgörs av de allmänna domstolarnas (tingsrätt, hovrätt och Högsta domstolen) och de allmänna förvaltningsdomstolarnas (förvaltningsrätt, kammarrätt och Högsta förvaltningsdomstolen). I Sveriges Domstolar ingår även hyres- och arrendenämnderna, Domstolsverket och Rättshjälpsmyndigheten. I Sveriges Domstolar ingår däremot inte de fyra specialdomstolarna Försvarsunderrättelsesdomstolen, Patentbesvärsträtten, Marknadsdomstolen och Arbetsdomstolen.

Behandlingen av personuppgifter i domstolarnas och nämndernas verksamhet reglerades tidigare för de allmänna domstolarnas och länsrätternas del i förordning och för Regeringsrättens, kammarrätternas och 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 arrendenämnderna med hjälp av automatiserad behandling.

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

Samtliga fyra förordningar gäller utöver personuppgiftslagen (1998:204) 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 och 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 och för framställning av statistik. För de allmänna domstolarna finns ett ytterligare ändamål, nämligen att fullgöra författningsenlig underrättskyldighet. 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 uppräkningsbilaga 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 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 en dom eller ett beslut som har fått 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 en kammarrätt överklagas till Högsta förvaltningsdomstolen. Beslut av Högsta domstolen eller Högsta förvaltningsdomstolen får inte överklagas. Beslut av en 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

Regeringens förslag: Personuppgiftsbehandling i de allmänna domstolarna, de allmänna förvaltningsdomstolarna och hyres- och arrendenämnderna regleras i en ny, flexibel och teknikneutral lag som anger ramarna och de grundläggande principerna för personuppgiftsbehandlingen. Lagen benämns domstolsdatalag.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: Samtliga remissinstanser tillstyrker promemorians förslag eller har ingen invändning mot det, med undantag av *Förvaltningsrätten i Härnösand* som anser att integritetsskyddssyftet bör kunna tillgodoses genom en ytterligare utveckling av nuvarande Vera-förordningar och föreskrifter tillsammans med personuppgiftslagen (1998:204, PUL). Vidare kan det enligt förvaltningsrätten ifrågasättas om förslaget till ny lag bör aktualiseras i nuvarande skede mot bakgrund av den pågående tekniska utvecklingen och andra utredningar. Förvaltningsrätten ser dock positivt på att lagstiftningen ges en flexibel och teknikneutral utformning.

Borås tingsrätt framhåller att det är en lämplig utgångspunkt att i lag reglera vilka former av personuppgiftsbehandling som ska begränsas eller förbjudas i stället för att i detalj peka ut vilka behandlingar som är tillåtna.

Skälen för regeringens förslag

Regelverket behöver moderniseras

Vera-förordningarna tar i huvudsak sikte på den behandling som sker i myndigheternas automatiserade register och innehåller detaljerade och uttömmande uppräknings av vilka uppgifter som får behandlas i registren (se avsnitt 5.2). Sedan den nuvarande regleringen infördes har den digitala tekniken utvecklats och fortsätter att utvecklas i betydande omfattning. Detta har medfört att allt mer avancerade automatiserade behandlingar kan utföras och att tekniken får nya användningsområden. Denna utveckling skapar nya förutsättningar att effektivisera samtliga myndigheters arbete och ytterligare stärka rättssäkerheten och kvaliteten i deras verksamhet.

Sedan flera år är 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. i stämningar, förelägganden, kallelser och domar). Domstolarna tar dessutom i allt större uträkning 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 informationsförsörjningen mellan Sveriges Domstolar och övriga myndigheter fungerar på ett bra sätt. Regeringen har en uttalad målsättning att skapa ett helt elektroniskt och strukturerat informationsutbyte mellan rättsväsendets myndigheter. Rättsväsendets myndigheter, däribland Domstolsverket, bedriver sedan ett antal år ett arbete för att utveckla brottmålshanteringen. Syftet med arbetet är att skapa ett elektroniskt flöde av information såväl framåt i rättskedjan som bakåt. Arbetet leds och samordnas av Justitiedepartementet. För arbetet finns ett särskilt inrättat råd, Rådet för rättsväsendets informationsförsörjning (RIF-rådet), som består av verkscheferna för samtliga deltagande myndigheter. Varje myndighet genomför sin del av de gemensamma överenskommelser som träffas.

Den pågående utvecklingen skapar alltså goda möjligheter att ytterligare effektivisera domstolarnas och hyres- och arrendenämndernas verksamheter, att stärka rättssäkerheten samt att förbättra kommunikationen med andra myndigheter och med enskilda. Att återanvända uppgifter som redan finns registrerade hos andra myndigheter är arbetsbesparande och främjar effektiviteten i domstolarna. 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 personuppgiftsbehandling möjliggör detta. Eftersom Vera-förordningarna tillkommit som en provisorisk lösning och de inte är anpassade för den beskrivna utvecklingen i fråga om användandet av modern teknik, anser regeringen att regelverket behöver moderniseras.

Ett starkt och hållbart 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.

Den grundläggande bestämmelsen till skydd för den personliga integriteten återfinns sedan den 1 januari 2011 i 2 kap. 6 § regeringsformen (RF). 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, se propositionen En reformerad grundlag (prop. 2009/10:80 s. 175).

Integritetsskyddscommittén 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). Av ovan nämnda proposition framgår att bestämmelsen i 2 kap. 6 § RF är avsedd att endast omfatta vissa kvalificerade intrång i den personliga integriteten. Vid bedömningen av hur ingripande intrånget i den personliga integriteten kan anses vara i samband med insamling, lagring och bearbetning eller utlämnande av uppgifter om enskildas personliga förhållanden är det naturligt att stor vikt läggs vid uppgifternas karaktär och ändamålet med behandlingen. Därutöver kan även mängden uppgifter vara en betydelsefull faktor i sammanhanget. Även omfattningen av utlämnandet av uppgifter till andra som sker utan omedelbart stöd av offentlighetsprincipen kan vara av betydelse. Det kan också beaktas på vilket sätt och för vilka syften mottagaren av uppgifterna hanterar utlämnande uppgifter (nämnda prop. s. 183 f.).

Regeringen konstaterar att flera av de kriterier som enligt förarbetena ska ligga till grund för bedömningen av vad som kan anses innebära ett betydande intrång vid behandlingen av personuppgifter kan vara uppfyllda vid den personuppgiftsbehandling som behöver ske i domstolarna och nämnderna i olika mål- och ärendetyper. I domstolarnas

och nämndernas verksamhet behandlas ett stort antal uppgifter som rör enskildas personliga förhållanden. I flera mål- och ärendetyper, t.ex. brottmål, migrationsmål och mål om tvångsvård, behandlas dessutom regelmässigt känsliga personuppgifter. Mot denna bakgrund gör regeringen bedömningen att en stor del av den personuppgiftsbehandling som behöver ske i domstolarna och nämnderna omfattas av regeringsformens bestämmelse om integritetsskydd.

Detta skydd mot integritetsintrång kan begränsas i lag under förutsättning att begränsningen görs för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle (2 kap. 20 § första stycket 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 en 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 behövs en 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 och hyres- och arrendenämnderna regleras såvitt gäller dessa myndigheters rättskipande och rättsvårdande verksamhet dels genom personuppgiftslagen, dels genom de fyra Vera-förordningarna, som 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 lagstiftningsärendet 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, se propositionen Personuppgiftslag (prop. 1997/98:44 s. 40 f.).

Det är vanligt att den personuppgiftsbehandling som utförs vid en viss myndighet regleras av en registerförfattning, som innehåller bestämmelser som i större eller mindre utsträckning 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 i fråga om domstolarnas och nämndernas verksamhet. Regeringen anser att det därför även i fortsättningen ska gälla särskilda

regler för den personuppgiftsbehandling som sker i domstolarnas och nämndernas verksamhet.

En ny reglering i lag

Personuppgiftsbehandlingen i domstolarna och hyres- och arrendenämnderna regleras för närvarande huvudsakligen i förordning. Den 1 januari 2011 infördes den tidigare nämnda bestämmelsen i regeringsformen om förstärkt skydd mot intrång i den personliga integriteten (2 kap. 6 § RF). Som redovisas ovan gör regeringen bedömningen att en stor del av den personuppgiftsbehandling som behöver ske i domstolarna och nämnderna omfattas av denna integritetsskyddsbestämmelse. 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. Härigenom åstadkoms ett förstärkt integritetsskydd i förhållande till vad som gäller för närvarande. Samtidigt är det enligt regeringen olämpligt att tynga lagen med alltför detaljerade bestämmelser. Lagregleringen avseende domstolarnas och nämndernas personuppgiftsbehandling bör därför kompletteras med bestämmelser som meddelas genom förordning. De föreskrifter regeringen meddelar får dock inte innebära ett betydande intrång i den personliga integriteten (2 kap. 6 § andra stycket RF).

Regleringen bör vara flexibel och teknikneutral

De nuvarande Vera-förordningarna utgår i stor utsträckning från att personuppgifter lagras och struktureras i särskilda register. 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 därför inte vara beroende av att vissa tekniska lösningar används, utan ska tillåta användningen av ny teknik. Det krävs alltså 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 eller tillgänglighet för allmänheten. Likaså bör den vara flexibel såtillvida att den i möjligaste mån ska vara oberoende av nya faktiska, organisatoriska eller rättsliga förutsättningar som påverkar domstolarnas och nämndernas verksamhet. Regeringen anser sammanfattningsvis att det bör skapas ett rättsligt utrymme för att välja olika tekniska lösningar, arbetssätt och kommunikationsvägar inom verksamheterna.

Att lagstiftningen är teknikneutral och flexibel är 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 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 enligt regeringen återspeglas i hur lagen utformas. Till skillnad från nuvarande registerförordningar bör lagen ta sin utgångspunkt i att personuppgiftsbehandling är tillåten inom vissa ramar. I likhet med *Borås tingsrätt* anser regeringen därför att regeringens förslag i första hand bör ta sikte på vilka former av personuppgiftsbehandling som ska begränsas eller förbjudas i stället för att i detalj peka ut vilka behandlingar som är tillåtna. Detta innebär att den nya regleringen bör vara uppbyggd på ett i grunden annat sätt än Vera-förordningarna. En sådan reform kan enligt regeringen inte åstadkommas om den nuvarande regleringen i Vera-förordningarna skulle behållas och utvecklas, såsom *Förvaltningsrätten i Härnösand* föreslår.

Domstolsdatalagen – en gemensam lag för domstolar och hyres- och arrendenämnder

Personuppgiftsbehandlingen i de allmänna domstolarna, de allmänna förvaltningsdomstolarna och i hyres- och arrendenämnderna regleras i dag i Vera-förordningarna, (se avsnitt 5.2). Dessa fyra förordningar är i stort sett identiska. Hyres- och arrendenämnderna fullgör rättskipande och rättsvårdande uppgifter. De ingår i Sveriges Domstolar och flera hyres- och arrendenämnders administration är sedan år 2006 samordnad med en tingsrätt på samma ort och nämnderna använder samma datorsystem som domstolarna. Även om hyres- och arrendenämnderna inte är domstolar i formell mening anser regeringen mot denna bakgrund att den nya regleringen också i fortsättningen bör omfatta dessa nämnder.

För enkelhetens skull används i fortsättningen domstolarna som samlingsbegrepp. Om inget annat särskilt anges så avses med detta de allmänna domstolarna, de allmänna förvaltningsdomstolarna och hyres- och arrendenämnderna. Den reglering som nu föreslås bör enligt regeringen samlas i en enda gemensam lag. Därigenom undviks att i princip identiska bestämmelser upprepas i olika lagar och det blir lättare att tillämpa reglerna på ett enhetligt sätt.

Vad gäller namnet på den nya lagen anser regeringen att den bör benämnas domstolsdatalag. Detta ligger i linje med de korta men informativa namn på lagar inom personuppgiftsområdet som tillkommit under senare år, t.ex. patientdatalagen (2008:355), polisdatalagen (2010:361) och kustbevakningsdatalagen (2012:145).

6.2 Lagens tillämpningsområde

Regeringens förslag: Domstolsdatalagen gäller vid behandling av personuppgifter i domstolarnas rättskipande och rättsvårdande verksamhet. Lagen gäller också när personuppgifterna vidarebehandlas i domstolarnas administrativa verksamhet för att lämnas ut efter begäran.

Lagen gäller endast 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.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorian innehåller dock ingen uttrycklig bestämmelse rörande personuppgifter som vidarebehandlas i domstolarnas administrativa verksamhet för att lämnas ut efter begäran.

Remissinstanserna: Samtliga remissinstanser tillstyrker eller har ingen invändning mot att lagens tillämpningsområde i och för sig avgränsas till domstolarnas rättskipande och rättsvårdande verksamhet. *Domstolsverket* och flera domstolar, bl.a. *Svea hovrätt* och *Kammarrätten i Sundsvall*, efterfrågar ett klargörande av om domstolsdatalagen ska tillämpas i fråga om publicering på internet av exempelvis domar och uppslagslistor. Många remissinstanser framhåller att det kan uppstå gränsdragningsproblem och efterfrågar klargöranden angående hur den rättskipande och rättsvårdande verksamheten ska avgränsas gentemot den administrativa verksamheten. Som exempel på åtgärder som kan vara svåra att bedöma uppmärksammas behandlingar som avser register över advokater och över domstolspersonal och åtgärder avseende nämndemän och tolkar, såsom exempelvis behörighetskontroller och indelning. Vidare nämns in- och utbetalningar av avgifter och ersättningar samt omlottnings- och förtursförklaring av mål.

Många domstolar efterlyser, i likhet med *Domstolsverket*, förtydliganden i fråga om huruvida domstolsdatalagen ska vara tillämplig när personuppgifter har förts över från den rättskipande och rättsvårdande verksamheten till den administrativa verksamheten för att behandlas vidare där, exempelvis för att sekretessprövas och lämnas ut enligt offentlighetsprincipen.

Domstolsverket väcker frågan om domstolsdatalagens tillämpningsområde är avsett att bli annorlunda än Vera-förordningarnas tillämpningsområde.

Hovrätten över Skåne och Blekinge anser att 5 a § PUL, som handlar om undantag för behandling av personuppgifter i ostrukturerat material, ska göras tillämplig även på behandling av personuppgifter i domstolarnas rättskipande och rättsvårdande verksamhet. Hovrätten pekar på att det i den enskilde domarens arbete med ett mål ofta uppkommer skiftande behov av att göra sammanställningar, textbearbetningar osv. och att dessa behandlingar sällan är förknippade med några integritetsrisker. Enligt hovrätten är behoven skiftande och svåra att förutse, men generellt är behoven större ju mer omfattande och komplicerat ett mål är.

Skälen för regeringens förslag

Rättskipande och rättsvårdande verksamhet

Regeringens skäl för att föreslå en ny domstolsdatalag hänför sig i allt väsentligt till de särskilda förhållanden som råder inom domstolarnas rättskipande och rättsvårdande verksamhet, framför allt 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 [1971:291]) och att enskildas möjligheter till insyn är särskilt goda tack vare den offentlighet som ofta råder för uppgifter i denna verksamhet. I fråga om de personuppgifter som samlas in och behandlas i domstolarnas övriga verksamhet, dvs. den administrativa verksamheten, råder dock inte sådana särskilda förhållanden. Personuppgifter i exempelvis personalärenden eller handlingar avseende lokalförsörjningen skiljer sig inte i något väsentligt hänseende från de personuppgifter som hanteras i motsvarande verksamhet hos andra myndigheter eller hos privata företag. Något behov av särreglering finns därför inte i den delen. Det kan noteras att registerförfattningarna som gäller för polisen och Kustbevakningen inte omfattar personuppgiftsbehandlingen i dessa myndigheters administrativa verksamhet (1 kap. 2 § polisdatalagen och 1 kap. 2 § kustbevakningsdatalagen).

Regeringen anser således att domstolsdatalagens tillämpningsområde som utgångspunkt bör begränsas till domstolarnas rättskipande och rättsvårdande verksamhet. I likhet med nu gällande Vera-förordningarna bör domstolsdatalagen därför gälla för hanteringen av personuppgifter som samlas in och behandlas i domstolarnas rättskipande och rättsvårdande verksamhet, medan behandlingen av personuppgifter som samlas in och behandlas i den administrativa verksamheten även i fortsättningen bör regleras av personuppgiftslagen. Bland andra *Domstolsverket* anför att det förekommer att domstolarna som en service till allmänheten publicerar domar och andra handlingar från den rättskipande och rättsvårdande verksamheten på sin webbplats. Avgränsningen av domstolsdatalagens tillämpningsområde innebär att sådan publicering faller utanför tillämpningsområdet.

Tillämpningsområdet för domstolsdatalagen kommer alltså i huvudsak att formuleras på samma sätt som i Vera-förordningarna. *Domstolsverket* väcker även frågan om domstolsdatalagens tillämpningsområde är avsett att bli annorlunda än Vera-förordningarnas tillämpningsområde. Regeringen konstaterar att domstolsdatalagen i grunden är konstruerad på ett annat sätt än Vera-förordningarna. Till skillnad från dessa förordningar ska domstolsdatalagen vara teknikneutral och inte ta sikte på den behandling som sker i vissa utpekade datorsystem. En annan grundläggande skillnad i förhållande till Vera-förordningarna är att domstolsdatalagen är en självständig reglering som helt ersätter personuppgiftslagen, medan Vera-förordningarna gäller utöver personuppgiftslagen. Av dessa skäl blir gränsdragningen för domstolsdatalagens tillämpningsområde inte i alla situationer identisk med den som har gällt i fråga om Vera-förordningarna.

Många remissinstanser, bl.a. *Svea hovrätt*, *Kammarrätten i Sundsvall* och *Domstolsverket*, har efterfrågat förtydliganden avseende hur

domstolsdatalagens tillämpningsområde ska avgränsas i olika praktiska situationer. För att uppnå syftet att domstolsdatalagen ska vara teknikneutral och inte ta sikte på behandlingen i vissa bestämda register bör lagen utformas så att det inte är avgörande vilket datorsystem som används för en viss behandling. Bedömningen av om en personuppgiftsbehandling omfattas av domstolsdatalagen bör enligt regeringen ta sin utgångspunkt i om de aktuella personuppgifterna har samlats in i eller behandlats på annat sätt i den rättskipande och rättsvårdande verksamheten. Begreppet rättskipande och rättsvårdande verksamhet inskränker sig i detta sammanhang inte enbart till handläggningsåtgärder som vidtas enligt en processuell bestämmelse, utan är avsett att ha en vidare innebörd. Exempelvis är hanteringen av ansökningsavgifter, liksom omlotning och förtursförklaring av mål, åtgärder som har en omedelbar koppling till mål- och ärendehantering och som därför bör betraktas som en del av den rättskipande och rättsvårdande verksamheten. Detta gäller både insamlandet av personuppgifter och den vidare hanteringen av uppgifterna. Insamling av personuppgifter avseende ombud, tolkar, vittnen och andra aktörer samt den fortsatta hanteringen av dessa uppgifter i samband med registerföring, kallelser och utbetalning av ersättningar är andra exempel på personuppgiftsbehandlingar som också är avsedda att rymmas i begreppet rättskipande och rättsvårdande verksamhet.

Personuppgifter avseende anställda vid domstolen behandlas enligt regeringens bedömning såväl i den administrativa som i den rättskipande och rättsvårdande verksamheten. I den administrativa verksamheten hanteras sådana personuppgifter exempelvis i samband med löneutbetalning, vid indelning på avdelningar eller enheter och när beredskapslistor upprättas. Sådan behandling är inte avsedd att omfattas av den nya lagen. Personuppgifter som avser domstolens anställda behandlas emellertid också i direkt anslutning till hanteringen av mål och ärenden, exempelvis i domar, uppslagslistor och förelägganden. Behandlingen av personuppgifter i sådana fall får enligt regeringen anses ske i den rättskipande och rättsvårdande verksamheten.

När det gäller nämndemän behandlar domstolarna också personuppgifter i flera olika sammanhang. Insamling av sådana personuppgifter, liksom den fortsatta hanteringen i form av exempelvis behörighetskontroller, kontroll av utdrag ur belastningsregistret, upprättande av adressregister och indelningsbeslut sker i den administrativa verksamheten som styrs av personuppgiftslagen. Samma sak gäller utbetalning av ersättning till nämndemän för deras medverkan i handläggningen. Nämndemäns personuppgifter behandlas emellertid också i direkt anslutning till hanteringen av mål och ärenden, t.ex. vid upprättande av domar. Denna behandling sker i den rättsvårdande och rättskipande verksamheten och i dessa fall blir således domstolsdatalagen tillämplig.

Utlämnande efter begäran

Flera remissinstanser, bl.a. *Svea hovrätt* och *Domstolsverket*, lyfter fram frågan om domstolsdatalagen ska fortsätta att vara tillämplig när en domstol vidarebehandlar personuppgifter från den rättskipande och

rättsvårdande verksamheten i den administrativa verksamheten i syfte att på begäran lämna ut uppgifterna till en enskild eller en myndighet. Ett typexempel är utlämnande av en allmän handling från ett mål, t.ex. en partsinlägga eller en dom med stöd av offentlighetsprincipen. Denna hantering – inklusive avsändande av handlingarna och debitering av eventuella avgifter – brukar anses hänförlig till den administrativa verksamheten.

Regeringen anser att sådan vidarebehandling av personuppgifter som nu beskrivits bör omfattas av domstolsdatalagen. Skälet till det är att domstolsdatalagens bestämmelser om sökning och utlämnande på medium för automatiserad behandling (se avsnitt 11 respektive 12) bör gälla vid utlämnande av personuppgifter som behandlas i den rättskipande och rättsvårdande verksamheten. Såsom *Sundsvalls tingsrätt*, *Kammarrätten i Stockholm* och Domstolsverket uppmärksammar framgår det också indirekt av promemorian att domstolsdatalagen är avsedd att tillämpas även när en domstol vidarebehandlar personuppgifter i sin administrativa verksamhet för att efter en begäran lämna ut uppgifterna. Lagens tillämpningsområde bör förtydligas så att det framgår att den gäller även i dessa fall.

Automatiserade behandlingar och manuella register

Domstolsdatalagen bör omfatta sådan behandling av personuppgifter som är helt eller delvis automatiserad eller viss manuell behandling, närmare bestämt sådan manuell behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier. En sådan reglering stämmer överens med vad som gäller enligt personuppgiftslagen, polisdatalagen och flertalet andra registerförfattningar samt de krav som följer av dataskyddsdirektivet.

Personuppgiftslagen innehåller sedan år 2007 en särskild regel om behandling av personuppgifter i ostrukturerat material som gör undantag från ett flertal av lagens bestämmelser, samtidigt som bestämmelsen innehåller ett generellt skydd mot att den registrerades personliga integritet kränks (5 a §). Samtliga bestämmelser i domstolsdatalagen bör utformas med hänsyn till domstolarnas behov av att kunna behandla personuppgifter effektivt, inte minst i ostrukturerat material såsom i domar, protokoll och andra ordbehandlingsdokument. Regeringen anser därför att det undantag som bestämmelsen i 5 a § PUL innebär inte behövs i domstolsdatalagen.

6.3 Lagens syfte

Regeringens förslag: Syftet med domstolsdatalagen är att ge domstolarna 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.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: Samtliga remissinstanser tillstyrker promemorian förslag eller har ingen invändning mot det.

Skälen för regeringens förslag: En utgångspunkt vid utformningen av bestämmelserna i domstolsdatalagen är bestämmelsen i 2 kap. 21 § RF. Av denna bestämmelse följer att begränsningar av det grundlagsfästa skyddet mot integritetsintrång inte får gå utöver vad som är nödvändigt med hänsyn till det ändamål som föranlett dem. I domstolarnas rättskipande och rättsvårdande verksamhet måste personuppgifter kunna få behandlas på ett ändamålsenligt sätt, vilket bl.a. innefattar användandet av ett modernt och rationellt datorstöd. Detta är nödvändigt för att samhällets rättmätiga krav på en rättssäker och effektiv dömande verksamhet ska kunna tillgodoses. Samtidigt måste det beaktas att hanteringen av personuppgifter kan medföra en risk för intrång i den personliga integriteten. Skyddet för den enskildes personliga integritet måste därför värnas genom bestämmelserna i domstolsdatalagen. Vid utformningen av den närmare regleringen i domstolsdatalagen är det viktigt att hitta en väl avvägd balans mellan å ena sidan skyddet för den personliga integriteten och å andra sidan behovet av att på ett effektivt och rättssäkert sätt kunna handlägga och avgöra mål och ärenden i domstolarna.

Mot den angivna bakgrunden kan syftet med domstolsdatalagen sägas vara tvådelat: att möjliggöra en ändamålsenlig personuppgiftsbehandling i domstolarna och att skydda enskilda mot integritetsintrång. Regeringen anser att detta dubbla syfte bör komma till tydligt uttryck i lagen.

6.4 Lagens förhållande till personuppgiftslagen

<p>Regeringens förslag: Domstolsdatalagen gäller i stället för personuppgiftslagen. I lagen anges vilka bestämmelser i personuppgiftslagen som ändå ska tillämpas.</p>

Promemorian förslag överensstämmer med regeringens.

Remissinstanserna: Samtliga remissinstanser tillstyrker promemorian förslag eller har ingen invändning mot det.

Skälen för regeringens förslag: 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). 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 utöver den lagen. I den utsträckning som en fråga inte är reglerad i Vera-förordningarna gäller alltså personuppgiftslagens bestämmelser.

Vad gäller domstolsdatalagen instämmer regeringen i promemorian bedömning att förhållandet till personuppgiftslagen bör vara tydligare än vad som är fallet med den nuvarande regleringen. Regleringen bör vara så tydlig att bestämmelserna i domstolsdatalagen inte först måste jämföras med bestämmelserna i personuppgiftslagen för att det ska kunna fastställas vilka bestämmelser som är tillämpliga i ett enskilt fall.

Regeringen anser därför att domstolsdatalagen helt ska ersätta personuppgiftslagen inom sitt tillämpningsområde. I de fall en viss fråga bör regleras på samma sätt i domstolsdatalagen som i personuppgiftslagen bör det i domstolsdatalagen tas in en uttrycklig hänvisning till den aktuella bestämmelsen i personuppgiftslagen. Såsom framhålls i promemorian innebär denna lagtekniska lösning att regleringen blir tydlig och att förutsättningarna för en enhetlig rättstillämpning blir goda. Den lagtekniska lösningen är i linje med vad som gäller enligt lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet, polisdatalagen och kustbevakningsdatalagen.

6.5 Lagens förhållande till offentlighetsprincipen

Regeringens förslag: I likhet med personuppgiftslagen ska domstolsdatalagen inte tillämpas i den utsträckning det skulle inskränka skyldigheten att lämna ut personuppgifter enligt 2 kap. tryckfrihetsförordningen.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: Samtliga remissinstanser tillstyrker promemorians förslag eller har ingen invändning mot det.

Skälen för regeringens förslag: 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 offentlighetsprincipen, såsom den kommer till uttryck i 2 kap. tryckfrihetsförordningen. 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). Enligt regeringen bör det av tydlighetsskäl komma till uttryck att detta även gäller i fråga om domstolsdatalagen genom att lagen innehåller en hänvisning till 8 § första stycket 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 12.

I avsnitt 13 behandlas frågan om huruvida domstolsdatalagen även bör hänvisa till 8 § andra stycket PUL, enligt vilken myndigheter ges möjlighet att bevara allmänna handlingar.

6.6 Beteckningar och definitioner

Regeringens förslag: Domstolsdatalagen hänvisar till personuppgiftslagens definitioner av beteckningar.

Promemorians förslag överensstämmer med regeringens.

Reminstanserna: Samtliga remissinstanser tillstyrker promemorians förslag eller har ingen invändning mot det.

Skälen för regeringens förslag: I personuppgiftslagen definieras vissa beteckningar som är centrala vid behandling av personuppgifter, bl.a.

behandling, personuppgifter, personuppgiftsansvarig, den registrerade och tredje man (3 §). Dessa beteckningar är avsedda att ha samma innebörd som motsvarande uttryck har i dataskyddsdirektivet (artikel 2).

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. Beteckningen 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 är fråga om behandling av personuppgifter t.ex. även när sådana skrivs ut på papper.

För en enhetlig rättstillämpning är det viktigt att domstolsdatalagens terminologi överensstämmer med personuppgiftslagens. Regeringen föreslår därför att en hänvisning till 3 § PUL tas in i domstolsdatalagen.

6.7 Lagens förhållande till viss annan lagstiftning

Regeringens förslag: Det anges i domstolsdatalagen att avvikande bestämmelser i lagen med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen har företräde framför bestämmelserna i domstolsdatalagen.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: Samtliga remissinstanser tillstyrker promemorians förslag eller har ingen invändning mot det, utom *Kammarrätten i Stockholm* som konstaterar att den föreslagna bestämmelsen inte är lika lätt att tillämpa som den bestämmelse i förslaget till domstolsdatalag som innehåller hänvisningar till personuppgiftslagen.

Skälen för regeringens förslag: I lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen finns särskilda bestämmelser avseende behandling av personuppgifter i verksamhet som har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller verkställa straffrättsliga påföljder. En förutsättning för lagens tillämpning är att personuppgifterna, inom ramen för polissamarbete eller straffrättsligt 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. Det innebär att lagen i vissa fall även kan bli tillämplig vid domstolarnas handläggning av exempelvis brottmål i fråga om uppgifter som utbyts med utländska stater och organisationer.

Bestämmelserna i den aktuella lagen avser bl.a. för vilka ändamål personuppgifter får behandlas och vad som gäller för den fortsatta behandlingen av uppgifterna. Lagen anger vidare i vilka situationer personuppgifter får överföras till enskilda, till tredjeland och till internationella organ. Svenska myndigheter är därför skyldiga att följa de villkor om användningen av personuppgifter som ställts upp av den som överfört uppgifterna eller gjort dem tillgängliga.

Den aktuella lagen har tillkommit för att genomföra rambeslutet 2008/977/RIF om skydd för personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete. I de fall den aktuella lagen avviker från domstolsdatalagens bestämmelser ska den först nämnda lagen därför ges företräde. Enligt regeringen bör detta förhållande komma till tydligt uttryck i domstolsdatalagen genom en bestämmelse som klargör att avvikande bestämmelser i den aktuella lagen eller föreskrifter som regeringen har meddelat i anslutning till den lagen har företräde framför domstolsdatalagens bestämmelser. Som *Kammarrätten i Stockholm* konstaterar blir en sådan bestämmelse mindre användarvänlig än den bestämmelse i domstolsdatalagen som innehåller hänvisningar till personuppgiftslagen. Samtidigt är det en fördel om regleringen på den här punkten överensstämmer med motsvarande bestämmelser för andra myndigheter som berörs av den aktuella lagen. På så sätt blir det tydligt att det är fråga om ett enhetligt regelsystem. Regeringen föreslår därför att den aktuella bestämmelsen i sak utformas i enlighet med vad som även gäller enligt bl.a. polisdatalagen. Med hänsyn till att bestämmelsen inte torde aktualiseras lika ofta i domstolarnas verksamhet som i t.ex. polisens, kan bestämmelsen i domstolsdatalagen ges en mer kortfattad utformning, dvs. på det i promemorian föreslagna sättet.

7 Personuppgiftsansvarig och personuppgiftsbiträden

7.1 Varje domstol är personuppgiftsansvarig

Regeringens förslag: Varje domstol är personuppgiftsansvarig för den behandling som den utför.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanserna tillstyrker promemorians förslag eller har ingen invändning mot det. Flera remissinstanser, bl.a. *Göta hovrätt*, *Hovrätten för Västra Sverige*, *Attunda tingsrätt*, *Kammarrätten i Göteborg* och *Datainspektionen*, framhåller att domstolarnas faktiska möjligheter att påverka om och hur en enskild personuppgiftsbehandling ska företas kan vara begränsade eftersom det är Domstolsverket som utformar datorsystemen. *Datainspektionen* anser att promemorians förslag inte helt stämmer med grundtanken att det är den som styr över behandlingen som också har

ansvaret. Vidare efterlyser Datainspektionen en analys av de enskilda myndigheternas faktiska möjligheter att leva upp till de krav som ställs på personuppgiftsansvariga i fråga om säkerheten vid personuppgiftsbehandling. *Göta hovrätt* föreslår, i likhet med *Kammarrätten i Göteborg*, ett delat personuppgiftsansvar där domstolarna respektive Domstolsverket tar ansvar för vad de i praktiken kan påverka. *Hovrätten för Västra Sverige* ifrågasätter om inte varje domstol tillsammans med Domstolsverket ska vara ansvarig för den personuppgiftsbehandling som är knuten till den egna domstolens verksamhet. *Ekobrottsmyndigheten* menar att det finns uppgifter som behandlas i enlighet med de överenskommelser Domstolsverket träffat med övriga myndigheter inom RIF, utan att domstolarna har någon reell möjlighet att påverka behandlingen eller ibland ens är medvetna om vilka uppgifter som faktiskt behandlas. Det kan enligt myndigheten leda till komplikationer i RIF-samarbetet om domstolarna och Domstolsverket har olika uppfattningar om hur personuppgifter får behandlas. *Borås tingsrätt* ser positivt på promemorians förslag och framhåller att det delade ansvar som enligt den nuvarande ordningen råder mellan de enskilda domstolarna och Domstolsverket skapar gränsdragningsproblem och en olycklig otydlighet gentemot den som exempelvis vill vända sig till den personuppgiftsansvarige för att få en viss personuppgift rättad.

Skälen för regeringens förslag: Personuppgiftslagen (1998:204, PUL) definierar en personuppgiftsansvarig som den vilken ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter (3 §). Den personuppgiftsansvarige har ett ansvar för att all behandling av personuppgifter sker i överensstämmelse med tillämpliga personuppgiftsbestämmelser. Personuppgiftsansvaret innebär bl.a. en skyldighet att kontrollera och ansvara för att de behandlingar som utförs är korrekta, vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas och rätta uppgifter. 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.

I registerförfattningar anges vanligtvis att den myndighet som registerförfattningen gäller för är personuppgiftsansvarig för personuppgiftsbehandlingen i den myndighetens verksamhet. Exempelvis är Polismyndigheten ansvarig för den behandling av personuppgifter som myndigheten utför enligt polisdatalagen (2010:361) och Tullverket är ansvarigt för den behandling som verket utför enligt lagen (2001:185) om behandling av uppgifter i Tullverkets verksamhet. Genom en bestämmelse som pekar ut personuppgiftsansvaret blir det tydligt att den myndighet som registerförfattningen avser är personuppgiftsansvarig trots att det är riksdagen som genom lag – eller regeringen som genom förordning – i registerförfattningen faktiskt bestämmer för vilka ändamål personuppgifter får behandlas hos myndigheten.

En fördel med att låta den aktuella domstolen vara personuppgiftsansvarig är att en enskild som vill framföra ett klagomål slipper att analysera och ta ställning till vem som ska anses som personuppgiftsansvarig för en viss behandling. Att det råder klarhet i frågan om vem som är ansvarig för de behandlingar som en domstol utför innebär också

att det skapas goda förutsättningar för en effektiv tillsyn av Datainspektionen. Med hänsyn till domstolarnas självständighet skulle det vidare väcka principiella betänkligheter att peka ut någon annan myndighet, exempelvis Domstolsverket, som personuppgiftsansvarig för de behandlingar som en domstol utför i den rättskipande och rättsvårdande verksamheten. Regeringen anser därför, i likhet med promemorian, att det är respektive domstol som bör vara personuppgiftsansvarig för den behandling som domstolen utför. *Datainspektionen* anser att en sådan ordning inte helt stämmer med grundtanken att det är den som styr över behandlingen som också har ansvaret. Regeringen vill dock framhålla att eftersom varje domstol är självständig och på ett formellt plan är den som styr vilka åtgärder som vidtas i den rättskipande och rättsvårdande verksamheten är det naturligt att det formella personuppgiftsansvaret också ligger på den berörda domstolen.

Det stämmer som *Ekobrottsmyndigheten* uppmärksammar att domstolarna på ett praktiskt plan är styrda av de överenskommelser som Domstolsverket träffar med andra myndigheter inom RIF-samarbetet. Att domstolarna i vissa avseenden är styrda av omständigheter som helt eller delvis ligger bortom den egna kontrollen är emellertid inget unikt. Många andra personuppgiftsansvariga myndigheter är i praktiken styrda av författningsbestämmelser, myndighetsinstruktioner, samarbetsavtal samt andra praktiska realiteter och yttre faktorer. I personuppgiftsansvaret ligger då en skyldighet att sammanjämka dessa olika krav och vidta nödvändiga åtgärder, inom de ramar som föreligger, för att på bästa sätt säkerställa att gällande personuppgiftsbestämmelser följs och samtidigt leva upp till gällande åtaganden och förpliktelser.

Några remissinstanser invänder att Domstolsverket i praktiken har ett stort inflytande över domstolarnas datorsystem och att respektive domstol därför i praktiken har begränsade möjligheter att vidta åtgärder för att garantera säkerheten vid behandlingarna och att påverka vilka behandlingar som över huvud taget utförs. *Göta hovrätt*, *Hovrätten för Västra Sverige* och *Kammarrätten i Göteborg* förespråkar i linje med detta att en domstols personuppgiftsansvar ska delas eller vara gemensamt med Domstolsverket. *Datainspektionen* efterlyser en analys av de enskilda myndigheternas faktiska möjligheter att leva upp till kraven i fråga om säkerheten vid personuppgiftsbehandling.

Varje domstol förväntas självklart samarbeta på olika sätt med Domstolsverket för att kunna uppfylla de krav som följer av domstolsdatalagen. Om en personuppgiftsansvarig domstol skulle upptäcka att datorsystemen i något avseende är utformade på ett sådant sätt att domstolen inte kan leva upp till dessa krav är det naturligt att den domstolen kontaktar Domstolsverket för att komma till rätta med problemen. Detta gäller även i de fall en domstol blir varse brister i datorsystemet eller otillåtna behandlingar genom ett påpekande från någon utomstående, exempelvis genom ett tillsynsbeslut från Datainspektionen eller en begäran om rättelse från en registrerad. Regeringen utgår från att Domstolsverket kommer att göra det möjligt för domstolarna att fullgöra sitt personuppgiftsansvar. Fördelarna med att varje enskild domstol ska vara personuppgiftsansvarig är som nämns ovan bl.a. att det blir tydligt för den enskilde vem han eller hon ska vända sig till med klagomål och att det skapas förutsättningar för en

effektiv tillsyn av Datainspektionen. Enligt regeringen skulle ett delat eller gemensamt personuppgiftsansvar medföra beaktansvärda nackdelar, inte minst gränsdragningsproblem och otydligheter, som *Borås tingsrätt* uppmärksammar.

7.2 Domstolarna får anlita personuppgiftsbiträden

Regeringens förslag: Den personuppgiftsansvariga domstolen får, på samma sätt som enligt personuppgiftslagen, anlita ett personuppgiftsbiträde för att utföra behandlingar för den egna domstolens räkning.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanserna tillstyrker promemorians förslag eller har ingen invändning mot det. *Göta hovrätt*, *Attunda tingsrätt*, *Borås tingsrätt* och *Kammarrätten i Göteborg*, är dock kritiska till att förslaget förutsätter att varje domstol ska vara beredd att ingå ett skriftligt avtal med Domstolsverket för att verket ska kunna utföra personuppgiftsbehandlingar för domstolarnas räkning. Attunda tingsrätt ifrågasätter om Domstolsverkets roll som central förvaltningsmyndighet, med bemyndigande att meddela föreskrifter för hur domstolarna ska använda tekniska system, är förenlig med att vara avtalspart i fråga om hantering av personuppgifter, och anser att en bättre lösning hade varit att i lag eller förordning bestämma att Domstolsverket är personuppgiftsbiträde åt domstolarna när verket behandlar personuppgifter i domstolarnas rättskipande och rättsvårdande verksamhet.

Skälen för regeringens förslag: Av 3 § PUL framgår att ett personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning. 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 vanligtvis ett externt organ som anlitas för att utföra uppgifter för den personuppgiftsansvariges räkning, vilket innebär att personuppgifter behandlas.

Av 30 § PUL följer att ett personuppgiftsbiträde och den eller de personer som arbetar under bitrådets eller den personuppgiftsansvariges ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige. Det ska finnas ett skriftligt avtal om personuppgiftsbitrådets behandling av personuppgifter för den personuppgiftsansvariges räkning. Av 31 § andra stycket PUL framgår vidare att den personuppgiftsansvarige ska förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas för att skydda uppgifterna och se till att biträdet verkligen vidtar åtgärderna.

Den personuppgiftsansvariga domstolen bör, på samma sätt som enligt personuppgiftslagen, kunna anlita personuppgiftsbiträden för att utföra personuppgiftsbehandlingar för domstolens räkning. Respektive domstol bör därmed kunna anlita Domstolsverket och andra utomstående, t.ex. tekniska konsulter, som personuppgiftsbiträden. För att det ska finnas rättsligt stöd för Domstolsverket och andra utomstående att utföra

personuppgiftsbehandlingsmedel med stöd av domstolsdatalagen för en eller flera domstolars räkning bör domstolsdatalagen hänvisa till bestämmelserna i 3, 30 och 31 §§ PUL.

Bland andra *Göta hovrätt* och *Kammarrätten i Göteborg* ifrågasätter lämpligheten i att låta domstolarna teckna avtal med Domstolsverket för att verket ska kunna fungera som personuppgiftsbiträde åt domstolarna. *Attunda tingsrätt* anser att Domstolsverkets roll som personuppgiftsbiträde kan komma i konflikt med verkets roll som systemansvarig för de verksamhetsstöd som domstolarna använder och med en möjlig föreskriftsrätt för verket. Enligt regeringen finns det inga principiella hinder mot att två offentlighetsorgan ingår ett sådant avtal, även om den ena parten har föreskriftsrätt. Ett personuppgiftsbiträde är en fysisk eller juridisk person som utför uppgifter på grundval av ett uppdragsavtal. Det ligger i själva definitionen av ett personuppgiftsbiträde att det är en funktion som skapas genom avtal mellan den personuppgiftsansvarige och den som ska behandla personuppgifter för den personuppgiftsansvariges räkning. Det finns även ett värde i att dokumentera instruktionerna och relationen i övrigt mellan den personuppgiftsansvarige och personuppgiftsbiträdet i det aktuella avtalet. Att som *Attunda tingsrätt* föreslår reglera rollen som personuppgiftsbiträde i författning framstår därför inte som lämpligt. Något sådant förslag lämnas således inte.

8 Ramarna för domstolarnas personuppgiftsbehandling

8.1 Grundläggande krav på domstolarnas personuppgiftsbehandling

Regeringens förslag: Domstolsdatalagen hänvisar till personuppgiftslagens bestämmelser om grundläggande krav för personuppgiftsbehandling. Det innebär bl.a. att

- de behandlingar som utförs måste vara lagliga och göras på ett korrekt sätt och i enlighet med god sed,
- personuppgifterna som behandlas måste vara nödvändiga, adekvata, relevanta och riktiga,
- personuppgifter får samlas in endast för särskilda och uttryckligt angivna ändamål, och
- insamlade personuppgifter inte får vidarebehandlas för ett ändamål som är oförenligt med det ändamål som uppgifterna samlades in för.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: *Hovrätten för Västra Sverige* påpekar att de verksamhetspecifika ändamålsbestämmelserna i domstolsdatalagen torde täcka in flertalet av de grundläggande krav som personuppgiftslagen (1998:204, PUL) ställer på personuppgiftsbehandlingsmedel. I

övrigt ställer sig samtliga remissinstanser bakom promemorians förslag eller har ingen invändning mot det.

Skälen för regeringens förslag: I personuppgiftslagen slås det fast ett antal grundläggande krav som gäller för all behandling av personuppgifter. Syftet med dessa krav är att behandlingar som på ett otillbörligt sätt kränker den personliga integriteten inte ska få förekomma. Kraven gäller enligt Vera-förordningarna och personuppgiftslagen även i domstolarnas rättskipande och rättsvårdande verksamhet.

De aktuella kraven riktar sig mot den personuppgiftsansvarige, som ska se till att personuppgifter endast behandlas om det är lagligt och att personuppgifter alltid 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 vad som är nödvändigt inte behandlas, att de personuppgifter som behandlas är riktiga och om nödvändigt aktuella, och 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). Ett ytterligare grundläggande krav är att personuppgifter får samlas in endast för särskilda och uttryckligt angivna ändamål (9 § första stycket c PUL). Slutligen är det otillåtet att behandla personuppgifter för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (9 § första stycket d PUL). Detta brukar kallas finalitetsprincipen. Denna princip begränsar dock inte möjligheterna att behandla personuppgifter för historiska, statistiska eller vetenskapliga ändamål (9 § andra stycket PUL).

Regeringen anser, i likhet med promemorian, att de nu redovisade grundläggande kraven bör gälla för sådan personuppgiftsbehandling som sker med stöd av domstolsdatalagen och att detta bör åstadkommas genom att det i domstolsdatalagen tas in hänvisningar till de relevanta bestämmelserna i personuppgiftslagen.

Hovrätten för Västra Sverige påpekar att flertalet av bestämmelserna om grundläggande krav också torde täckas av de verksamhetsspecifika ändamålsbestämmelserna som föreslås i avsnitt 8.2. Även om dessa olika bestämmelser i viss mån kan sägas överlappa varandra anser regeringen att bestämmelserna fyller en funktion var för sig. De grundläggande kraven utgör de yttre gränserna för vilken behandling som får ske samtidigt som de verksamhetsspecifika ändamålsbestämmelserna klargör att bestämmelserna om grundläggande krav ska tillämpas på ett sätt som är anpassat till den rättskipande och rättsvårdande verksamheten. Det kan tilläggas att både polisdatalagen (2010:361) och kustbevakningsdatalagen (2012:145) är uppbyggda enligt denna struktur.

8.2 Verksamhetsspecifika ändamålsbestämmelser

Regeringens förslag: Personuppgifter får behandlas om det behövs för handläggning av mål och ärenden. Personuppgifter som behandlas på denna grund får även vidarebehandlas om det behövs för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanserna tillstyrker promemorians förslag eller har ingen invändning mot det. *Hovrätten för Västra Sverige* ifrågasätter om alla de sökningar som domstolarna utför i dag kan sägas falla inom de föreslagna ändamålsbestämmelserna. Som exempel nämner hovrätten sökningar som görs för att få en uppfattning om gällande praxis, för att göra praxissammanställningar eller för att ta fram underlag till olika utbildningar och praxisdiskussioner. *Göta hovrätt* betonar att en strikt tolkning av ändamålsbestämmelserna kan förhindra domstolarna från att använda äldre domar och beslut i det interna kompetensutvecklingsarbetet (praxisdiskussioner, domskrivningsarbete m.m.). *Riksdagens ombudsmän (JO)* väcker frågan om det bör införas någon bestämmelse som uttryckligen tillåter behandlingar i syfte att kontrollera nämndemäns behörighet. *Stockholms tingsrätt* uppmärksammar ett antal åtgärder som utförs vid domstolarna och som det behöver finnas stöd för i domstolsdatalagens ändamålsbestämmelser, såsom kallelse och indelning av nämndemän, utlämnande av handlingar till parter, in- och utbetalningar av avgifter och ersättningar samt framtagande av uppgifter som växeltelefonister behöver tillgång till. *Västmanlands tingsrätt* menar att man genom den föreslagna lagen inte kan skydda människors integritet mer än marginellt eftersom offentlighetsprincipen alltid har företräde.

Rikspolisstyrelsen påpekar att det krävs en regelbunden elektronisk återkoppling för att polisen ska kunna fullgöra sina skyldigheter enligt 3 kap. polisdatalagen och efterlyser en tydlig reglering som gör RIF-samarbetet till ett ändamål för utlämnande. *Brottsförebyggande rådet* framhåller att ändamålsbestämmelserna måste ge tillräcklig höjd för behandling av uppgifter som är nödvändig för framställning av rättsstatistik av god kvalitet och för att genomföra de överenskommelser som finns inom ramen för RIF-samarbetet. Enligt *Datainspektionen* är det för den enskilde alltför otydligt att de primära ändamålen även omfattar vidarebehandling av personuppgifter för planering, uppföljning och utvärdering hos de enskilda myndigheterna. *Domstolsverket* uppmärksammar att domstolarna ofta får ta emot uppgifter eller handlingar som saknar betydelse för handläggningen utan att de är att betrakta som felskickade.

Skälen för regeringens förslag

Ändamålsbestämmelsernas utformning

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 (avsnitt 8.1). I likhet med polisdatalagen, Vera-förordningarna och många andra registerförfattningar bör domstolsdatalagen dessutom innehålla en mer verksamhetsanpassad ram i form av verksamhetsspecifika ändamålsbestämmelser. Därigenom 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 de ändamål för vilka personuppgifter behandlas i verksamheten. För det andra blir det genom sådana verksamhetsspecifika ändamålsbestämmelser tydligare vilka åtgärder som är tillåtna respektive otillåtna.

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. Uttrycket insamling avser inte bara situationer då uppgifter lämnas till en domstol på begäran av domstolen, utan även andra tillvägagångssätt genom vilka domstolen får del av personuppgifter. Exempel på sådana situationer är att en åklagare skickar in stämningsansökan eller att en enskild lämnar in ett överklagande. Bestämmelser om primära ändamål ger rättsligt stöd både för insamling av uppgifter och för vidarebehandling av uppgifterna, exempelvis genom lagring eller utlämning. Bestämmelser om sekundära ändamål medger inte insamling, utan tillåter endast att uppgifter som redan behandlas i verksamheten får vidarebehandlas. Bestämmelserna i domstolsdatalagen bör utformas utifrån denna distinktion mellan primära och sekundära ändamål.

Primära ändamål

Som framgår av avsnitt 6.2 ska domstolsdatalagen gälla för den rättskipande och rättsvårdande verksamheten, som är domstolarnas kärnverksamhet. Domstolarna behöver samla in och vidarebehandla personuppgifter i de fall då handläggningen av mål och ärenden kräver det. Insamlingen kan exempelvis bestå i att en part med e-post skickar in uppgifter till domstolen eller att en myndighet skickar uppgifter till domstolen med hjälp av de kanaler som har etablerats genom RIF-samarbetet. En väsentlig skillnad mot t.ex. polisens verksamhet är att domstolarnas insamlade av personuppgifter i hög grad styrs av andra regelverk än personuppgiftsregleringen såsom rättegångsbalken, förvaltningsprocesslagen (1971:291) och lagen (1996:242) om domstolsärenden samt 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 således styrs främst av processrätten och som inte ska regleras genom domstolsdatalagen eller andra personuppgiftsbestämmelser. 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. I domstolsdatalagen bör det därför anges att domstolarna får behandla (dvs. samla in eller vidarebehandla) personuppgifter om det behövs för handläggning av mål och ärenden. En sådan bestämmelse är tillräckligt flexibel för att domstolarnas organisation och arbetssätt ska kunna fortsätta att utvecklas och för att domstolarna ska kunna hantera nya måltyper. Samtidigt innebär bestämmelsen ett skydd mot integritetskränkning genom att bestämmelsen inte medger behandling av personuppgifter som inte är befogad i domstolarnas verksamhet.

Avsikten är inte att en bestämmelse med det beskrivna innehållet ska tolkas alltför snävt. *Göta hovrätt* och *Hovrätten för Västra Sverige* befarrar att bestämmelsen inte i tillräcklig utsträckning skulle medge sökning efter tidigare avgöranden eller hantering av sådana avgöranden i samband med praxisdiskussioner, domskrivningsarbete eller annat kompetensutvecklingsarbete. Regeringen delar inte denna farhåga, bl.a. eftersom det av bestämmelsens utformning kommer framgå att bedömningen av om en viss behandling är nödvändig ska göras i förhållande till mål- och ärendehandläggningen i stort och inte i förhållande till handläggningen av ett specifikt mål eller ärende. Sökning efter tidigare avgöranden och hantering av sådana avgöranden kommer således att rymmas inom vad som är tillåtet enligt ändamålsbestämmelserna, oavsett om åtgärderna sker i syfte att underlätta praxisdiskussioner, domskrivningsarbete eller annat kompetensutvecklingsarbete.

Domstolsverket påpekar att det ofta ges in handlingar till domstolarna som saknar betydelse för handläggningen utan att de är att betrakta som felskickade. Verket menar att det inte vore rimligt att domstolarna ska sälla bland det ingivna materialet så att endast det som är av faktisk betydelse för handläggning behandlas automatiserat. Regeringen gör samma bedömning. Den föreslagna bestämmelsen bör ge utrymme för domstolarna att elektroniskt hantera personuppgifter i handlingar som ges in i mål och ärenden utan att det i det enskilda fallet sker någon bedömning av hur relevant uppgiften är för ett visst mål eller ärende.

Regeringen har i fråga om bl.a. lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet och polisdatalagen gjort bedömningen att personuppgifter som får användas i myndighetens verksamhet också får användas för planering, uppföljning och utvärdering av verksamheten utan att detta uttryckligen anges i lagen, se propositionerna Tullverkets brottsbekämpning – Effektivare uppgiftsbehandling (prop. 2004/05:164 s. 66 f.) och Integritet och effektivitet i polisens brottsbekämpande verksamhet (prop. 2009/10:85 s. 116). Någon särskild bestämmelse om att planering m.m. är ett tillåtet ändamål finns därför inte i dessa lagar. *Datainspektionen* föreslår att en sådan bestämmelse ändå ska tas in i domstolsdatalagen för att det ska bli tydligt för enskilda att deras personuppgifter kan komma att användas för planering, uppföljning och utvärdering. Det saknas enligt regeringen skäl att reglera denna fråga annorlunda i domstolsdatalagen än vad som har skett i exempelvis lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet och polisdatalagen. Någon särskild ändamålsbestämmelse om planering m.m. föreslås därför inte.

En del tingsrätter använder målregistret för att söka information i syfte att kontrollera nämndemäns behörighet och *JO* väcker frågan om det bör införas någon särskild bestämmelse som uttryckligen tillåter sådan behandling. *Stockholms tingsrätt* uppmärksammar att domstolarna kan behöva behandla personuppgifter för att bl.a. hantera in- och utbetalningar. Såsom anförs i avsnitt 6.2 bör behandling av sådana personuppgifter räknas till den administrativa verksamheten. Behandlingen kommer därmed inte att omfattas av domstolsdatalagens tillämpningsområde utan av personuppgiftslagen.

Det saknas enligt regeringen skäl att tillåta insamlande av personuppgifter för 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.

Sekundära ändamål

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 ut 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 en 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.

En allmän förutsättning för sådan behandling som sker för utlämnande till andra bör vara att uppgiftslämnandet sker i överensstämmelse med lag eller förordning, dvs. med stöd av bestämmelser som påbjuder eller tillåter utlämnande. När bestämmelser som påbjuder eller tillåter utlämnande 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, och att man vid denna avvägning funnit att uppgiften ska eller får lämnas ut, jfr propositionen Patientdatalag m.m. (prop. 2007/08:126 s. 60). Bestämmelser av detta slag som berör domstolarnas verksamhet finns i många olika sammanhang, vilket framgår av det följande.

För det första är domstolarna enligt olika författningsbestämmelser skyldiga att på begäran lämna ut uppgifter. Domstolarna är t.ex. enligt 6 kap. 5 § offentlighets- och sekretesslagen (2009:400) skyldiga 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.

För det andra är domstolarna enligt bestämmelser i olika författningar skyldiga att lämna uppgifter till utpekade myndigheter. Genom de reformer som följer av RIF-samarbetet kommer en del av denna hantering att bli helt automatiserad. Som *Rikspolisstyrelsen* och *Brottsförebyggande rådet* påpekar är det viktigt att domstolsdatalagens ändamålsbestämmelser inte förhindrar en sådan effektivisering.

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 domstolar, myndigheter eller andra utomstående. Det kan t.ex. vara fråga om en åtgärd som vidtas för att fullgöra serviceskyldigheten gentemot enskilda enligt 4 § förvaltningslagen (1986:223). Såsom *Stockholms tingsrätt* påpekar kan också exempelvis växeltelefonister – vid en viss domstol eller vid en växel som är gemensam för flera domstolar – behöva ta fram uppgifter ur målhanteringssystemen.

Domstolsdatalagens bestämmelse om sekundära ändamål bör enligt regeringen formuleras så att den ger stöd för samtliga dessa former av utlämnande. Det kan konstateras att domstolarnas uppgiftsutlämnande styrs av flera andra regelverk med mer eller mindre detaljerade bestämmelser om utlämnande. För att undvika dubbelreglering är det därför lämpligast att bestämmelsen om uppgiftslämnande som sekundärt ändamål i domstolsdatalagen får en generell utformning, i likhet med regleringen i t.ex. patientdatalagen (2008:355). Med en generell formulerad bestämmelse blir det överflödigt att uttryckligen nämna RIF-samarbetet som ett tillåtet ändamål på sätt som *Rikspolisstyrelsen* efterlyser. Regeringen föreslår mot denna bakgrund, i likhet med promemorian, en sekundär 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. Därmed omfattas alla de former av utlämnande som redovisas ovan av den sekundära ändamålsbestämmelsen.

Avslutningsvis bör det av tydlighetsskäl framhållas att 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 själva utlämnandet ska få ske i elektroniskt format övervägs i avsnitt 12. Det bör också sägas, såsom *Västmanlands tingsrätt* påpekar, att varken ändamålsbestämmelserna eller några andra bestämmelser i domstolsdatagen kan förhindra sådana åtgärder som är nödvändiga för att leva upp till offentlighetsprincipen enligt 2 kap. tryckfrihetsförordningen (se avsnitt 6.5).

9 Säkerhet och intern åtkomst

9.1 Säkerheten vid behandlingen

Regeringens förslag: Den personuppgiftsansvarige ansvarar, på samma sätt som enligt personuppgiftslagen, för säkerheten vid personuppgiftsbehandlingen.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanserna tillstyrker promemorians förslag eller har ingen invändning mot det. Enligt *Göta hovrätt* aktualiserar förslaget frågan om avgränsningen av ansvar mellan domstolarna och Domstolsverket, eftersom verket tillhandahåller de system för personuppgiftsbehandling som domstolarna använder. Hovrätten menar att det med hänsyn till domstolarnas beroende av Domstolsverkets system inte är möjligt för domstolarna att fullgöra personuppgiftsansvaret utan verkets medverkan.

Skälen för regeringens förslag: I 30 och 31 §§ personuppgiftslagen (1998:204, 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. Regeringen anser, i likhet med vad som anförs i promemorian, att dessa principer även bör gälla i domstolarnas rättskipande och rättsvårdande verksamhet. En hänvisning till dessa bestämmelser bör därför tas in i domstolsdatalagen. Detta innebär att ansvaret för säkerheten vid personuppgiftsbehandlingen kommer att ligga på respektive personuppgiftsansvarig domstol som utför behandlingen (avsnitt 7.1). *Göta hovrätt* anser att domstolarna inte kan fullgöra sitt personuppgiftsansvar utan Domstolsverkets medverkan eftersom det är verket som konstruerar och ansvarar för driften av de it-system som domstolarna använder. Frågan om förhållandet mellan de personuppgiftsansvariga domstolarna och Domstolsverkets funktion som konstruktör och driftsansvarig för systemen behandlas i avsnitt 7.1. Såsom anförs i det avsnittet förväntas varje domstol samarbeta med Domstolsverket för att uppfylla de krav som ställs på den personuppgiftsansvarige enligt domstolsdatalagen. Om exempelvis en domstol inte på egen hand kan vidta lämpliga säkerhetsåtgärder i enlighet med kraven i 30 och 31 §§ PUL till följd av brister i Domstolsverkets datorsystem får domstolen alltså kontakta verket för att få hjälp med att lösa denna situation. På så sätt bör den frågeställning som *Göta hovrätt* väcker kunna hanteras.

I avsnitt 14.2 föreslås 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 2009/10:85 s. 271). Det bör mot den bakgrunden inte införas några särskilda bestämmelser om informations säkerhet i domstolsdatalagen, vid sidan av hänvisningen till personuppgiftslagens bestämmelser om säkerheten vid behandlingen.

9.2 Tillgång till personuppgifter

Regeringens förslag: Tillgången till personuppgifter ska begränsas till det som varje tjänsteman behöver för att fullgöra sina arbetsuppgifter i domstolarna. I lagen upplyses det om att regeringen eller den myndighet som regeringen bestämmer kan meddela närmare föreskrifter om tillgången till personuppgifter.

Promemorians förslag överensstämmer i huvudsak med regeringens. I promemorians förslag används uttrycket ”varje anställd” i stället för ”varje tjänsteman”.

Remissinstanserna: En del remissinstanser, bl.a. *Västmanlands tingsrätt*, *Kammarrätten i Stockholm* och *Domstolsverket*, är positivt inställda till att en begränsningsregel tas in i domstolsdatalagen men poängterar samtidigt att regleringen inte får förhindra ett rationellt arbets sätt vid domstolarna. Många remissinstanser, bl.a. *Göta hovrätt*, *Hovrätten för Västra Sverige* och *Domstolsverket* ser svårigheter med hur bestämmelsen ska tillämpas eftersom flera personalkategorier inom domstolarna vid skilda tidpunkter kan behöva åtkomst till personuppgifter för att fullgöra sina arbetsuppgifter. Bland dessa remissinstanser poängteras det att den föreslagna regleringen inte bör få medföra en begränsning av de anställdas möjligheter att få tillgång till de personuppgifter som behövs för att de effektivt ska kunna fullgöra sina arbetsuppgifter. Vidare framhålls att behovet av en bestämmelse om att begränsa tillgången till personuppgifter, som bygger på motsvarande reglering i polisdatalagen (2010:361), är mindre i domstolarnas verksamhet än i polisens verksamhet. *Göta hovrätt*, *Attunda tingsrätt* och *Ekobrottsmyndigheten* lämnar förslag på förtydliganden i den föreslagna bestämmelsen. Några remissinstanser, bl.a. *Umeå tingsrätt*, *Kammarrätten i Jönköping* och *Förvaltningsrätten i Härnösand*, lyfter fram flera praktiska problem med förslaget. En synpunkt som förs fram är att förslaget kan leda till att verksamhetsstödet behöver byggas om och att domstolarnas arbetsrutiner behöver förändras. *Göteborgs tingsrätt* ser svårigheter med att genom tekniska och organisatoriska åtgärder begränsa varje anställds tillgång till personuppgifter. Skyddet för den enskilde bör snarare kunna tillgodoses genom en varnings- och loggningsfunktion. *Förvaltningsrätten i Malmö* framför en liknande synpunkt. *Justitiekanslern* anser att en ordning som innebär att bedömningen av en åtgärds tillåtlighet i praktiken överlämnas till den enskilde användaren inte skulle stämma överens med bestämmelsens utformning och kan medföra risk för missbruk. *Hyresnämnden i Stockholm* ifrågasätter om det krävs eller är motiverat med sådana

föreskrifter som enligt promemorians förslag ska få meddelas i förordning eller i myndighetsföreskrifter. *Datainspektionen* anser att den föreslagna bestämmelsen i domstolsdatalagen är mycket vid och bör kompletteras med mer preciserade bestämmelser, i första hand i förordningsform. Inspektionen menar att det finns integritetsrisker med att överlåta till varje domstol att säkerställa åtkomstbegränsningarna och att den enskilde bör åtnjuta samma integritetsskydd oavsett hos vilken domstol dennes personuppgifter behandlas. *Göta hovrätt* pekar på att skydd för uppgifter i domsutkast redan finns i rättegångsbalken och offentlighets- och sekretesslagen (2009:400).

Skälen för regeringens förslag

Behovet av en begränsningsregel i lag

I föregående avsnitt föreslås att personuppgiftslagens bestämmelser om hur den personuppgiftsansvarige ska organisera arbetet med behandling av personuppgifter för att garantera säkerheten ska vara tillämpliga i domstolarnas verksamhet (30 och 31 §§ PUL). Detta innebär bl.a. att den som arbetar med personuppgifter får behandla dessa endast i enlighet med instruktioner från den personuppgiftsansvarige och att den personuppgiftsansvarige är skyldig att vidta tekniska och organisatoriska åtgärder för att skydda personuppgifterna. I polisdatalagen och flera andra registerförfattningar har det, utöver en hänvisning till 30 och 31 §§ PUL, tagits in en särskild bestämmelse som föreskriver att enbart de som behöver uppgifterna för att fullgöra sina arbetsuppgifter ska ha tillgång till dem. Regeringen anser att en sådan bestämmelse bör tas in även i domstolsdatalagen. Syftet är att tydliggöra att personuppgifterna inte får spridas till obehöriga personer i domstolarna och att fler uppgifter än nödvändigt inte får behandlas vid varje tillfälle.

I polisdatalagen och kustbevakningsdatalagen (2012:145) anges att tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att fullgöra sina arbetsuppgifter. I promemorian föreslås i stället att begränsningen ska gälla varje anställd. Det är en fördel om regleringen i detta avseende överensstämmer med regleringen för andra myndigheter, t.ex. polisen och Kustbevakningen. Uttrycket ”varje tjänsteman” bör således användas i stället för ”varje anställd”.

Några remissinstanser ifrågasätter om behovet av en bestämmelse av detta slag i domstolarnas verksamhet är lika stort som i exempelvis polisens eftersom fler personalkategorier hos domstolarna än hos polisen kan behöva en bredare tillgång till personuppgifter för att i olika skeden av handläggningen av mål och ärenden kunna vidta nödvändiga åtgärder. Förutom den eller de domare och notarier som handlägger mål och ärenden kan även kanslipersonal, växeltelefonister och vaktmästare behöva ha tillgång till personuppgifter i mål och ärenden för att kunna fullgöra sina arbetsuppgifter. Regeringen delar remissinstansernas uppfattning att kretsen som behöver ha möjlighet att komma åt lagrade personuppgifter i domstolarna i många fall kan behöva göras tämligen vid och att en begränsningsregel inte bör få hindra ett rationellt arbetssätt vid domstolarna. Beroende på hur en domstol är organiserad är det inte alltid från början givet vilka personer som vid en viss tidpunkt kommer att vidta olika handläggningsåtgärder i ett mål eller ärende. Det är inte

heller ovanligt att personer som inte deltar i handläggningen ändå behöver kunna komma åt de personuppgifter som behandlas exempelvis för att kunna besvara förfrågningar från allmänheten. Den bestämmelse som föreslås – att tillgången till personuppgifter ska begränsas till det som varje tjänsteman behöver för att fullgöra sina arbetsuppgifter – har den fördelen att den innebär en hög grad av flexibilitet. Bestämmelsen utgår från de berättigade behov av åtkomst som finns eller som kan förutses i varje enskild verksamhet. Den ger utrymme för att åtkomst medges dem som potentiellt kan behöva åtkomst, även om det i efterhand kan konstateras att alla i den grupp som beviljas åtkomst faktiskt inte behövde utnyttja åtkomsten. Att bestämmelsen till sin ordalydelse ansluter nära till motsvarande bestämmelser i andra registerförfattningar, såsom exempelvis polisdatalagen, innebär inte att tillgången till personuppgifter i domstolarna ska begränsas på samma sätt som i polisens verksamhet. Bestämmelsen är således enligt regeringen tillräckligt flexibel för att inte stå i vägen för en effektiv verksamhet i domstolarna.

Några remissinstanser lyfter frågan om det ska krävas tekniska lösningar för att begränsa åtkomsten till personuppgifter i domstolarnas verksamhet. Det kan i detta sammanhang framhållas att modern teknik ger ständigt nya möjligheter att på ett mer sofistikerat sätt reglera tillgången till uppgifter som behandlas automatiserat. Det finns också olika sätt att leva upp till bestämmelsens krav – såväl genom föreskrifter och instruktioner som genom tekniska åtgärder. Vilka begränsningsåtgärder som bör vidtas får bedömas fortlöpande utifrån domstolarnas olika förutsättningar och behov och med beaktande bl.a. av vad det skulle kosta att genomföra åtgärderna (jfr 31 § PUL).

Detaljföreskrifter om tillgången till personuppgifter

Några remissinstanser uttrycker en oro för att en ytterligare begränsning av åtkomstregleringen i förordning eller myndighetsföreskrifter kommer att hindra domstolarna i deras arbete och *Hyresnämnden i Stockholm* anser att några närmare föreskrifter inte behövs. I kontrast till dessa synpunkter anser *Datainspektionen* att bestämmelsen i domstolsdatalagen är mycket vid och bör kompletteras med mer preciserade bestämmelser som, i syfte att skydda den enskildes personliga integritet, främst bör meddelas i förordningsform.

Regeringen vill i detta sammanhang framhålla följande. Domstolarna skiljer sig åt sinsemellan i fråga om vilka typer av mål, och därmed vilka typer av personuppgifter, som behandlas i verksamheten. Domstolarna är också olika stora och deras inre organisation varierar. Dessutom förändras dessa förutsättningar över tid. Ett bestående integritetsskydd förutsätter därför en flexibel reglering som kan anpassas efter skiftande förhållanden. Även om den nu föreslagna begränsningsregeln i domstolsdatalagen lämnar utrymme för en flexibilitet beträffande vilka personer vid domstolarna som tillgången till personuppgifter ska avse och vilka personuppgifter som omfattas av regleringen kan det enligt regeringen finnas behov av att i förordning och myndighetsföreskrifter förtydliga och konkretisera innebörden av bestämmelsen. Föreskrifterna bör ge utrymme för olika tekniska lösningar, arbetssätt och kommunikationsvägar inom domstolarna. Genom föreskrifterna kan det

bl.a. tydliggöras för domstolarna, och för de registrerade, hur behörighetsstilldelning ska ske och hur tillgången till personuppgifter i olika fall ska begränsas. Sådana föreskrifter kommer alltså, tvärtemot vad några remissinstanser anför, att kunna anpassas efter domstolarnas behov och därmed inte hindra ett rationellt arbetssätt i domstolarna. För att upplysa om att sådana föreskrifter kan komma att meddelas, bör det tas in en bestämmelse i domstolsdatalagen om detta på samma sätt som i polisdatalagen (2 kap. 11 §) och kustbevakningsdatalagen (2 kap. 3 §). Det är fråga om verkställighetsföreskrifter vilket innebär att föreskrifterna inte får förändra innehållet i lagbestämmelsen. Sådana detaljerade föreskrifter kan meddelas av regeringen eller den myndighet som regeringen bestämmer.

Övriga frågor

Såsom anføres i avsnitt 9.1 är det domstolarnas uppgift att tillsammans med Domstolsverket se till att personalen får tillräcklig utbildning i frågor som rör dataskydd och informationssäkerhet. *Justitiekanslern* anser att en ordning som innebär att bedömningen av en åtgärds tillåtlighet i praktiken överlämnas till den enskilde användaren inte skulle stämma överens med bestämmelsens utformning och kan medföra risk för missbruk. Domstolarna ska med hjälp av Domstolsverket eftersträva att sådan åtkomst som inte är berättigad förhindras. Detta kan bl.a. ske genom tekniska åtgärder. Det kommer dock aldrig att vara möjligt att enbart på teknisk väg förhindra varje form av åtkomst som inte är yrkesmässigt motiverad. Ett fullgott skydd mot obehörig tillgång till personuppgifter förutsätter med nödvändighet andra åtgärder än tekniska begränsningar, såsom att de anställda instrueras och utbildas i dessa frågor. Tekniska lösningar kan också ta tid att utarbeta.

Göta hovrätt påpekar att ett skydd för personuppgifter i domsutkast redan finns i rättegångsbalken och sekretesslagstiftningen. Enligt regeringen innebär detta dock inte att den föreslagna regleringen är överflödigt eftersom den syftar till att minska risken för att uppgifter som är offentliga men som ändå inte bör vara åtkomliga för vem som helst sprids till fler personer vid domstolarna än vad som är motiverat.

10 Behandling av känsliga personuppgifter och personnummer

10.1 Känsliga personuppgifter

Regeringens förslag: 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 (känsliga personuppgifter).

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanserna tillstyrker promemorians förslag eller har ingen invändning mot det. *Kammarrätten i Göteborg* menar att förslaget innebär att förvaltningsdomstolarna inte kommer att kunna upprätta praxissamlingar som grundar sig på sjukdomsdiagnoser i socialförsäkringsmål. Enligt kammarrätten bör förslaget inte få försvåra praxisbildningen och upprätthållandet av likabehandlingsprincipen inom socialförsäkringsområdet. *Förvaltningsrätten i Göteborg* anser att det krävs ett redskap för att i ett så tidigt skede som möjligt av målens handläggning kunna sammanföra mål av liknande beskaffenhet. Om detta inte kan göras vid målens registrering i verksamhetsstödet Vera bör andra möjligheter att sammanföra mål undersökas.

Skälen för regeringens förslag

Känsliga personuppgifter bör få behandlas i domstolarna

Känsliga personuppgifter förekommer i många måltyper och i olika sorters handlingar. Enligt 13 § personuppgiftslagen (1998:204, PUL) är känsliga personuppgifter uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i en fackförening och uppgifter som rör hälsa eller sexualliv. Känsliga personuppgifter definieras också på detta sätt i annan lagstiftning om personuppgiftsbehandling och definitionen används fortfarande i olika internationella instrument. Mot denna bakgrund bör definitionen användas i den nya lagen, trots att det finns befogade invändningar mot användningen av begreppet ras (jfr prop. 2009/10:85 s. 123). Det bör framhållas att användningen av uttrycket ras för närvarande är föremål för överväganden av Utredningen om transpersoners straffrättsliga skydd m.m. (dir. 2014:115).

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).

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 § första stycket 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 stora flertalet känsliga personuppgifter 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 formulering 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 uteslutet att genom bestämmelser i domstolsdatalagen inskränka domarnas frihet att formulera domskäl i syfte att undvika att känsliga personuppgifter behandlas (jfr även 8 § personuppgiftsförordningen [1998:1191]) 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, domskrivning, expediering av domar osv., bedöms typiskt sett inte medföra särskilt stora risker i 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 denna bakgrund anser regeringen att behovet av att kunna behandla känsliga personuppgifter och de effektivitetsvinster som elektronisk hantering medför väger tyngre än den risk för integritetsintrång som en sådan behandling kan innebära. Behandlingen av känsliga personuppgifter bör därför som utgångspunkt vara tillåten och endast begränsas genom den rättsliga ram som föreslås i avsnitt 8, vilken bl.a. består av verksamhetspecifika ändamålsbestämmelser. Detta är i linje med vad som gäller enligt polisdatalagen (2010:361) 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 (2008:355).

Personuppgifter bör dock inte utgöra enda grund för behandlingen

För att minimera riskerna för att känsliga personuppgifter missbrukas bör det enligt regeringen finnas bestämmelser som direkt tar sikte på att kontrollera och begränsa sådana åtgärder som i integritetshänseende innebär särskilda risker. I avsnitt 11.4 föreslås därför bestämmelser som begränsar möjligheterna att använda känsliga personuppgifter som sökbegrepp. Såsom föreslås i promemorian anser regeringen att det av tydlighetsskäl även bör införas ett uttryckligt förbud mot att känsliga personuppgifter används som enda grund för en behandling. En bestämmelse med liknande lydelse finns i polisdatalagen och den bestämmelsen innebär enligt förarbetena att polisen inte får 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).

Kammarrätten i Göteborg och Förvaltningsrätten i Göteborg uttrycker farhågor för att den bestämmelse som promemorian föreslår på socialförsäkringsområdet kan förhindra praxisbildningen eller göra det svårt att sammanföra mål av liknande beskaffenhet. Enligt regeringen ska bestämmelsen emellertid inte behöva innebära några problem i dessa avseenden. Så länge det finns en annan konkret grund för behandlingen – såsom att underlätta den enhetliga rättstillämpningen och tillgodose likabehandlingsprincipen – bör exempelvis en sammanställning över socialförsäkringsmål som rör en viss sjukdomsdiagnos betraktas som tillåten. Sjukdomsdiagnosen utgör i sådana fall inte den enda grunden för behandlingen. En förutsättning för tillåtligheten är naturligtvis att den konkreta grunden för behandlingen är godtagbar utifrån domstolsdatalagens ändamålsbestämmelser, dvs. att behandlingen behövs för handläggning av mål och ärenden eller för uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Att åstadkomma en enhetlig rättstillämpning är exempel på en sådan godtagbar grund. Motsvarande bedömning bör kunna göras i fråga om åtgärder som behövs för att sammanföra mål av liknande beskaffenhet så att de kan handläggas i ett sammanhang vid en domstol.

För domstolarna får förbudet mot att använda känsliga personuppgifter som enda grund för en behandling i praktiken en mer begränsad betydelse än vad motsvarande bestämmelse i polisdatalagen har för polisen. Det beror på att domstolarna med hänsyn till de processuella regelverken och de föreslagna ändamålsbestämmelserna, även utan den nu föreslagna bestämmelsen, är begränsade i vad de kan företa sig i fråga om personuppgiftsbehandling. För att det inte ska råda någon tvekan tydliggörs dock genom den föreslagna bestämmelsen att vissa åtgärder är förbjudna, exempelvis att konstruera ett register över personer med en viss sjukdomsdiagnos utan att det finns ett konkret och utifrån ändamålsbestämmelserna godtagbart syfte med registret.

10.2 Personnummer

Regeringens förslag: Personnummer och samordningsnummer får, på samma sätt som enligt personuppgiftslagen, behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Promemorians förslag innehåller ingen särskild bestämmelse om personnummer och samordningsnummer. Promemorian innehåller i stället en bedömning att någon särskild begränsning inte bör gälla för behandling av sådana uppgifter.

Remissinstanserna: Ingen remissinstans kommenterar promemorians bedömning.

Skälen för regeringens förslag: I 22 § personuppgiftslagen föreskrivs att uppgifter om personnummer eller samordningsnummer får behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Bestämmelserna innebär att den personuppgiftsansvarige ska göra en intresseavvägning mellan skälen för att behandla uppgifterna och de integritetsrisker det innebär. I polisdatalagen och flera andra registerförfattningar har det tagits in en hänvisning till 22 § PUL för att markera vikten av denna princip. I domstolarnas verksamhet är det självklart att personnummer måste kunna behandlas i många situationer. Domstolarna behöver exempelvis kunna lagra och vidarebefordra elektroniska partsinlagor som innehåller personnummer. Domstolarna måste också i många fall kunna använda personnummer och samordningsnummer i sitt verksamhetsstöd liksom i domar och beslut för att på ett tillförlitligt sätt identifiera personer. Det bör dock även i domstolsdatalagen, i likhet med bl.a. polisdatalagen, komma till uttryck att personnummer inte får behandlas rent slentrianmässigt. Regeringen gör bedömningen att 22 § PUL innebär en flexibel reglering som är väl anpassad för att förhindra omotiverad behandling av personnummer och samordningsnummer även i domstolarnas verksamhet. Regeringen föreslår därför, till skillnad från promemorian, att domstolsdatalagen ska hänvisa till 22 § PUL.

11 Sökbegränsningar

11.1 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. Med hjälp av exempelvis bokstäver, koder eller siffror kan man, tillsammans med en sökmotor eller liknande funktion, ta fram ett önskat urval lagrade personuppgifter om en eller flera personer ur en samlad informationsmängd. 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. Användningen av sökfunktioner är viktig för att domstolarna effektivt ska kunna hitta relevant information, t.ex. tidigare domar som kan tjäna till vägledning. Sökfunktionerna är också av betydelse för allmänhetens insyn i domstolarnas verksamhet, eftersom domstolarna med hjälp av sökning kan tillmötesgå specifika förfrågningar från allmänheten. Samtidigt finns det en risk att möjligheterna att söka leder till integritetsintrång, exempelvis genom att de framtagna uppgifterna används för kartläggning av vissa grupper av människor. Vissa sökbegrepp, såsom uppgifter om hälsa eller om brott, kan innebära särskilda integritetsrisker. Av den anledningen förekommer i en del registerförfattningar särskilda begränsningar av vilka sökbegrepp som får användas. Genom sådana begränsningar kan ett ökat integritetsskydd uppnås.

Möjligheterna att effektivt begränsa användningen av integritetskänsliga sökbegrepp påverkas emellertid av offentlighetsprincipen. Offentlighetsprincipen, såsom den kommer till uttryck i 2 kap. tryckfrihetsförordningen (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 enskilda 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 ett visst fall är lämpligare, i en annan lag som den särskilda lagen hänvisar till. Den särskilda lagen är offentlighets- och sekretesslagen (2009:400, OSL).

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 och 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 handlingar. Skälet till att enskilda har rätt att ta del av potentiella allmänna handlingar är att det följer 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.

I 2 kap. 3 § tredje stycket TF finns den s.k. begränsningsregeln, vilken anger att en sammanställning av uppgifter ur en upptagning för automatiserad behandling inte anses förvarad hos myndigheten om sammanställningen innehåller personuppgifter och myndigheten enligt lag eller förordning saknar befogenhet att göra den tillgänglig. 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 (2 kap. 1 § TF). 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 får däremot genomslag enligt begränsningsregeln.

Sammanfattningsvis innebär regleringen i tryckfrihetsförordningen att det finns två sätt att genom författningsbestämmelser reglera allmänhetens tillgång till potentiella allmänna handlingar i domstolarna, och därmed indirekt reglera allmänhetens tillgång till de sökfunktioner som används för att sammanställa sådana handlingar. Dels kan en sådan reglering åstadkommas genom sekretessbestämmelser i offentlighets- och sekretesslagen, dels genom sökbestämmelser i domstolsdatalagen som på ett ovillkorligt sätt förbjuder personalen att utföra vissa sökningar både för verksamhetens behov och på begäran av allmänheten. Bestämmelser som tillåter personalen att under vissa villkor utföra en sökning, t.ex. att söka om det är absolut nödvändigt, begränsar inte allmänhetens rätt att begära att sådana sökningar utförs och att de uppgifter som tas fram lämnas ut.

11.2 Utgångspunkter för sökregleringens utformning

Regeringens bedömning: Begränsningarna av möjligheterna att söka bör utformas så att de inte enbart gäller för domstolspersonalens användning av datorsystemen utan även skyddar mot de integritetsrisker som är förknippade med enskildas rätt att begära att sökningar utförs med stöd av offentlighetsprincipen.

Promemorians förslag överensstämmer inte med regeringens bedömning. I promemorian föreslås att integritetskänsliga sökbegrepp får användas av domstolens personal endast om det är absolut nödvändigt för handläggningen av mål och ärenden.

Remissinstanserna: Flera remissinstanser uppmärksammar att personalen enligt promemorians förslag ska få använda särskilt integritetskänsliga sökbegrepp endast om det är absolut nödvändigt samtidigt som denna spärr på grund av regleringen i tryckfrihetsförordningen inte kan tillämpas när en enskild begär att en integritetskänslig sökning ska utföras. *Hovrätten för Västra Sverige* och *Kammarrätten i Sundsvall* pekar särskilt på att detta innebär att enskilda kan få tillgång till sökfunktioner som personalen inte kan använda för domstolens egen verksamhet. Hovrätten menar att detta kan innebära integritetsrisker och att problematiken bör uppmärksammas ytterligare. *Kammarrätten i Jönköping* menar att skillnaden i sökmöjligheter mellan

domstolsanställda och enskilda framstår som märklig ur integritetssynpunkt. *Kammarätten i Stockholm* är kritisk till att stora resurser kan behöva tas i anspråk för att handlägga framställningar om att få ut sådana allmänna handlingar som myndigheterna inte får söka efter för egen del. *Förvaltningsrätten i Göteborg* och *Förvaltningsrätten i Malmö* gör bedömningen att risken för otillbörliga integritetsintrång måste vara potentiellt mindre när sökningar utförs av domstolspersonalen för handläggning av mål och ärenden än när sammanställningar utifrån de aktuella uppgifterna görs på begäran av allmänheten. Enligt förvaltningsrätterna är det under sådana förhållanden inte motiverat att införa en spärr som endast begränsar domstolspersonalens sökmöjligheter, men inte allmänhetens möjligheter att med stöd av offentlighetsprincipen begära att en sökning ska utföras. *Datainspektionen* saknar en analys av de konsekvenser som ett utlämnande av en sammanställning som utförs med integritetskänsliga sökbegrepp kan innebära. *Ekobrottsmyndigheten* anser att förslagen innebär så omfattande förändringar i tillgången till uppgifter att det kräver en betydligt djupare analys för att nytta och risk för rättsprocessen och den enskildes integritet ska kunna bedömas.

Nyköpings tingsrätt menar att begränsningen till absolut nödvändiga sökningar i fråga om sökbegrepp som avslöjar brott eller misstanke om brott innebär en avsevärd och betydelsefull inskränkning och att skälen för denna inskränkning inte uppväger nackdelarna. *Domstolsverket* förespråkar att bestämmelsen om att personalen endast får använda integritetskänsliga sökbegrepp när det är absolut nödvändigt ska utgå om domstolarnas verksamhetsstöd Vera ska kunna användas som en rättsdatabas. Ett stort antal domstolar är kritiska till begreppet ”absolut nödvändigt” och hänvisar till att förstärkningsordet absolut i språkligt hänseende inte medför någon skärpning i förhållande till begreppet ”nödvändigt”. *Hovrätten för Västra Sverige* tycker också att uttrycket är mindre väl valt, men anser att det kan godtas med hänsyn till att det redan använts i annan lagstiftning på området. *Kammarrätten i Jönköping* menar att kravet framstår som mycket restriktivt och föreslår i stället att det i lagtexten ska anges att de aktuella sökbegränsningarna ska få ske endast om det ”behövs för en effektiv och rättssäker handläggning”. *Borås tingsrätt*, *Förvaltningsrätten i Malmö* och *Justitiekanslern* ställer sig frågande till när en sökning kan anses vara absolut nödvändig. *Göta hovrätt*, *Förvaltningsrätten i Malmö* och *Justitiekanslern* väcker frågan om vem som ska vara behörig att pröva om en sökning är absolut nödvändig och *Justitiekanslern* menar att prövningen kan ge upphov till bedömnings-, avvägnings- och praktiska tillämpningssvårigheter.

Skälen för regeringens bedömning: De integritetsrisker som är förknippade med domstolspersonalens möjlighet att söka är av flera skäl relativt begränsade. De anställda kommer enligt regeringens förslag att vara lagligen förhindrade att göra en sökning om åtgärden inte rymms inom de tillåtna ändamål som ska gälla enligt domstolsdatalagen. I detta ligger bl.a. 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 disciplinåtgärd enligt lagen (1994:260) om offentlig anställning. Ytterst kan straffansvar för dataintrång aktualiseras (4 kap. 9 c § brottbalken). Som föreslås i avsnitt 9.2 ska vidare den interna tillgången till personuppgifter vara begränsad till det varje tjänsteman behöver för att fullgöra sina arbetsuppgifter. Genom loggning och andra tekniska säkerhetsåtgärder kan bestämmelsernas efterlevnad kontrolleras i efterhand och riskerna för att sökfunktionerna missbrukas därmed begränsas. Det bör i detta sammanhang också noteras att ingen av remissinstanserna anför att de domstolsanställdas användning av integritetskänsliga sökbegrepp i sig skulle innebära några särskilda risker, samtidigt som många remissinstanser uppmärksammar de integritetsrisker som följer av allmänhetens rätt att begära att tillgängliga sökfunktioner används (se avsnitt 11.4). Det är således inte motiverat att införa en spärr som endast begränsar domstolspersonalens sökmöjligheter, men inte allmänhetens möjligheter att med stöd av offentlighetsprincipen begära att en sökning ska utföras, vilket också *Förvaltningsrätten i Göteborg* och *Förvaltningsrätten i Malmö* lyfter fram.

I promemorian föreslås att domstolens personal ska få använda särskilt integritetskänsliga sökbegrepp endast om det är absolut nödvändigt. Denna typ av bestämmelse är inte ovillkorlig, och regeringen föreslår därför inte någon sådan bestämmelse. Detta är i linje med vad majoriteten av de remissinstanser som yttrat sig över promemorians förslag anför. Regeringen gör i stället bedömningen att sökregleringen i domstolsdatalagen bör ha en sådan utformning att sökspärrarna inte enbart träffar domstolspersonalens behandling i tjänsten utan att spärrarna mot integritetskänsliga sökningar också blir verksamma när sökningar utförs på begäran av enskilda med stöd av offentlighetsprincipen. Detta förutsätter att sökbestämmelserna är ovillkorliga.

I avsnitt 11.4 överväger regeringen ovillkorliga sök begränsningar som ska gälla såväl när domstolens personal utför sökningar för verksamhetens egna behov som när personalen utför sökningar på begäran av enskilda med stöd av offentlighetsprincipen.

11.3 Någon särskild sekretessbestämmelse föreslås inte

Regeringens bedömning: Det bör inte införas någon särskild sekretessbestämmelse för personuppgifter som tas fram med hjälp av sökning.

Promemorians bedömning överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna instämmer i promemorians bedömning eller kommenterar den inte närmare. *Sundsvalls tingsrätt*, *Kammarrätten i Stockholm*, *Kammarrätten i Jönköping*, *Förvaltningsrätten i Stockholm* och *Ekobrottsmyndigheten* anser att det finns skäl att ytterligare överväga en sekretessbestämmelse.

Som skäl hänvisas till de integritetsrisker som orsakas av allmänhetens tillgång till att begära integritetskänsliga sökningar och att sökmöjligheterna kan leda till att mycket resurser tas i anspråk för att hantera framställningar från allmänheten. *Attunda tingsrätt* uppmärksammar de integritetsrisker som följer av att mediaföretag, som inte omfattas av personuppgiftslagen (1998:204, PUL), hämtar in domstolshandlingar, bygger upp egna databaser och erbjuder uppgifterna till sina kunder. Om ingen reglering införs finns det möjlighet för bl.a. en arbetsgivare, en hyresvärd eller ett försäkringsbolag att inför ett beslut ta reda på om en person exempelvis varit åtalad.

Skälen för regeringens bedömning: *Sundsvalls tingsrätt, Kammarrätten i Stockholm, Kammarrätten i Jönköping, Förvaltningsrätten i Stockholm, Ekobrottsmyndigheten och Datainspektionen* efterlyser en närmare och djupare analys av behovet av en särskild sekretessbestämmelse för uppgifter som tas fram med hjälp av sökning. De flesta av dessa remissinstanser pekar i sammanhanget på de integritetsrisker som följer av allmänhetens möjligheter att begära att sökningar utförs med stöd av offentlighetsprincipen.

Enligt regeringen kan det ur integritetssynvinkel framstå som önskvärt med en sekretessbestämmelse som tar sikte på de uppgifter som plockas fram med hjälp av integritetskänsliga sökbegrepp, såsom exempelvis en sammanställning över personer som dömts för ett visst brott eller beviljats ersättning för viss typ av skada. Det finns dock principiella skäl som talar mot att införa någon ny sådan sekretessbestämmelse. I domstolarna anses sedan gammalt intresset av insyn och öppenhet vara särskilt starkt. En aspekt av insynsintresset i domstolarnas rättskipande och rättsvårdande verksamhet kommer exempelvis till uttryck bl.a. i regleringen av det s.k. offentlighetsdopet (jfr 43 kap. 5 och 8 §§ OSL och promemorian *Offentlighet och sekretess för uppgifter i domstolsavgöranden* [Ds 2014:33]), som något förenklat innebär att sekretess upphör att gälla för uppgifter som läggs fram vid en offentlig domstolsförhandling eller tas in i en dom. Den bakomliggande tanken är att allmänheten ska tillförsäkras en långtgående insyn i domstolarnas verksamhet. En viktig del i detta är massmedias journalistiska granskning av domstolarnas dömande verksamhet. Det finns ett betydande värde i att både journalister och andra enskilda kan begära att avgöranden söks fram efter bestämda kriterier för att exempelvis möjliggöra en jämförelse hur olika domstolar dömer. Det kan också noteras att det enligt *Veraförordningarna* 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.

En sekretessbestämmelse avseende uppgifter som tagits fram med hjälp av sökning skulle också medföra praktiska svårigheter för tillämparen. För det första skulle den innebära att uppgifter som finns i en dom utan sekretessförordnande, skulle omfattas av sekretess när de förekommer i ett annat sammanhang vid samma domstol, nämligen i en sammanställning som tagits fram med hjälp av sökning. För det andra kan det i den sammanställning som tas fram med hjälp av sökning finnas uppgifter som avser ett mycket stort antal personer. Att vid sekretessprövningen i det enskilda fallet ta ställning till vilken skada ett

utlämnande skulle innebära för var och en av dem skulle medföra en betydande resursåtgång i domstolarna. Vid en sammantagen bedömning anser regeringen att någon särskild sekretessbestämmelse för uppgifter i domstolarna som tagits fram med hjälp av vissa sökningar inte bör införas.

Attunda tingsrätt uppmärksammar de integritetsproblem som kan följa av att medieföretag med s.k. utgivningsbevis bygger upp databaser med uppgifter från domstolarna. Denna fråga ligger emellertid utanför ramen för detta lagstiftningsärende. Sedan promemorian remitterades har regeringen tillsatt en kommitté på det tryck- och yttrandefrihetsrättsliga området med uppdrag att bl.a. analysera om skyddet för den personliga integriteten i databaser med utgivningsbevis är tillräckligt (dir. 2014:97). Utredningen ska redovisa sina överväganden och förslag senast den 1 september 2016.

11.4 Integritetskänsliga sökningar ska begränsas

Regeringens förslag: Vid sökning i personuppgifter är det förbjudet att som sökbegrepp använda uppgifter som avslöjar

- ras eller etniskt ursprung,
- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening,
- hälsa,
- sexualliv,
- nationell anknytning, eller
- brott eller misstanke om brott.

Förbudet gäller inte användning av uppgifter som avslöjar brott eller misstanke om brott i de allmänna domstolarnas och de allmänna förvaltningsdomstolarnas verksamhet och användning av uppgifter som avslöjar hälsa i de allmänna förvaltningsdomstolarnas verksamhet. I lagen upplyses det om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om begränsningar av möjligheterna att använda dessa sökbegrepp.

Användning av särskilda beteckningar för identifiering av en viss mål- eller ärendetyp som sökbegrepp omfattas inte av förbudet.

Promemorians förslag överensstämmer delvis med regeringens. I promemorian föreslås att uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa, sexualliv och nationell anknytning ska få användas som sökbegrepp i de allmänna förvaltningsdomstolarna och att uppgifter som avslöjar brott eller misstanke om brott ska få användas i de allmänna domstolarna. Vidare föreslås att regeringen kan meddela ytterligare föreskrifter om begränsningar av möjligheterna att söka. Promemorian saknar en bestämmelse om att särskilda beteckningar för identifiering av mål- eller ärendetyp som sökbegrepp inte ska omfattas av förbudet.

Remissinstanserna: Remissutfallet är blandat. Samtliga kammarrätter, majoriteten av förvaltningsrätterna, *Nyköpings tingsrätt* och

Domstolsverket tillstyrker eller är övervägande positiva till förslaget. *Borås tingsrätt* är tveksam till om nyttan av förslagen väger upp integritetsriskerna. Med hänsyn till integritetsriskerna tillstyrker *Förvaltningsrätten i Stockholm* och *Förvaltningsrätten i Jönköping* förslaget endast under förutsättning att det införs en sekretessbestämmelse avseende uppgifter som tas fram med hjälp av sökning.

Sveriges advokatsamfund avstyrker förslaget av integritetsskyddsskal. Samfundet menar att domstolarna i stället bör kunna använda externa rättsdatabaser trots kostnaderna för det och att skälen för att tillåta användningen av integritetskänsliga sökbegrepp är mycket svaga. *Ekobrottsmyndigheten* lämnar synpunkter av liknande slag.

Borås tingsrätt framhåller att sökmöjligheterna i kombination med direktåtkomst kan utnyttjas för att få avgöranden från landets alla domstolar utlämnade för illvilliga syften. Även om *Domstolsverket* tillstyrker förslaget, lyfter verket fram att de nya sökmöjligheterna kan leda till integritetsrisker och en ökad arbetsbelastning för domstolarna när allmänheten begär att sökningar ska utföras.

Hovrätten för Västra Sverige och *Förvaltningsrätten i Malmö*, ifrågasätter om inte ändamålsbestämmelserna utgör en tillräcklig reglering avseende sökbegrepp som avslöjar brott eller misstanke om brott. *Västmanlands tingsrätt* menar att sökbegrepp som avslöjar brott eller misstanke om brott kan vara nödvändiga att använda även vid kartläggning och analys av målstrukturen vid en domstol. *Sundsvalls tingsrätt* pekar på att användningen av dessa sökbegrepp kan underlätta handläggningen hos en hyresnämnd, exempelvis för att bedöma betydelsen av den brottslighet som en hyresgäst har gjort sig skyldig till. Tingsrätten pekar också på att konsekvenserna för hyres- och arrendenämndernas rådgivnings- och upplysningsarbete inte har analyserats närmare i promemorian.

Ett stort antal förvaltningsdomstolar är kritiska till begränsningar i sökmöjligheterna. *Kammarrätten i Göteborg*, *Kammarrätten i Sundsvall*, *Kammarrätten i Jönköping*, *Förvaltningsrätten i Göteborg*, *Förvaltningsrätten i Malmö* och *Förvaltningsrätten i Jönköping* anser att det även i de allmänna förvaltningsdomstolarna kan finnas behov av att använda sökbegrepp som avslöjar brott eller misstanke om brott, exempelvis i körkortsmål, migrationsmål, vapenmål, LVU-mål, skattemål och mål om upphävande av allmän domstols beslut om utvisning på grund av brott. *Kammarrätten i Göteborg* framhåller att domar och beslut är offentliga och att behovet av att kunna söka bland uppgifter i sådana dokument för att hitta vägledande avgöranden är större än i fråga om uppgifter i elektroniska akter. *Kammarrätten* ser ingen anledning att begränsa återsökningsmöjligheterna i domar och beslut, i synnerhet som privata aktörer redan idag tillhandahåller databaser med samtliga domar och beslut utan sökbegränsningar. *Kammarrätten i Sundsvall* anser att det är en självklarhet att domstolarna behöver tillgång till sina egna och andra domstolars avgöranden för att verksamheten ska fungera. Om det genom den nya lagen införs begränsningar i hur de domstolsanställda får söka i verksamhetssystemet kommer domstolarna enligt *kammarrätten* att behöva köpa tillbaka sina egna uppgifter genom abonnemang hos olika rättsdatabaser.

Förvaltningsrätten i Härnösand anser att samordningsvinster sällan torde uppnås genom sökning på exempelvis en viss diagnos eftersom det sällan är själva diagnosen som är intressant vid bedömningen. Enligt förvaltningsrätten finns det inte behov av att använda de integritets-känsliga sökbegreppen på sätt som har föreslagits. Enligt *Riksdagens ombudsmän* bör möjligheten att som sökbegrepp använda nationell anknytning, etniskt ursprung, politiska åsikter, religiös övertygelse och sexualliv begränsas till migrationsdomstolarna och Migrationsöverdomstolen.

Hovrätten för Västra Sverige menar att behovet av att använda känsliga personuppgifter som sökbegrepp torde vara relativt begränsat och torde uteslutande finnas i de allmänna förvaltningsdomstolarna.

Justitiekanslern ifrågasätter om det inte skulle kunna finnas alternativa sätt att tillgodose domstolarnas behov som skulle innebära mer begränsade integritetsrisker, exempelvis genom att utveckla och anpassa Domstolsverkets webbsida Vägledande avgöranden.

Domstolsverket förespråkar ett förtydligande som innebär att det ska vara tillåtet i allmänna domstolar att som sökbegrepp använda brottsrubriceringar som också innefattar en uppgift om sexualliv eller någon annan känslig personuppgift.

Justitiekanslern anser att det i bestämmelsen om sökning av tydlighetsskäl bör anges uttryckligen att regeringen kan meddela föreskrifter om behörighet och säkerhetsfrågor.

Skälen för regeringens förslag

Integritetskänsliga sökbegrepp

I promemorian identifierades ett antal sökbegrepp som enligt bedömningen i promemorian medför särskilda integritetsrisker i domstolarnas verksamhet. Det rör sig dels om sökbegrepp som tar sikte på s.k. känsliga personuppgifter (uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening och uppgifter som rör hälsa eller sexualliv), dels sökbegrepp som består av uppgifter som avslöjar nationell anknytning, brott eller misstanke om brott. Regeringen delar bedömningen att dessa typer av sökbegrepp intar en särställning i fråga om integritetsrisker och noterar att ingen av remissinstanserna uppmärksammar någon annan typ av uppgifter som i domstolarnas verksamhet också bör betraktas som integritetskänsliga sökbegrepp.

Domstolarna har behov av att använda integritetskänsliga sökbegrepp

Att domstolarna kan bedriva den rättskipande och rättsvårdande verksamheten rättssäkert och effektivt är avgörande för tilltron till rättsväsendet. En viktig aspekt av rätts säkerheten är att lika fall behandlas lika. Det är därför viktigt att den domare som står inför att avgöra ett mål har goda möjligheter att återfinna tidigare avgöranden som rymmer identiska eller liknande frågeställningar. I effektivitetshänseende kan det vara värdefullt att hitta förebilder för domskrivningen genom att söka efter tidigare avgöranden. Av betydelse för effektiviteteten är också möjligheten att med hjälp av sökning kartlägga och analysera

målstrukturen vid en domstol såsom *Västmanlands tingsrätt* påpekar. Vidare är det möjligt att med hjälp av sökning identifiera öppna mål som innehåller likartade frågeställningar så att handläggningen kan samordnas, vilket kan främja såväl effektiviteten som rättssäkerheten. I vissa måltyper är det betydelsefullt att kunna använda också integritetskänsliga sökbegrepp. Exempelvis kan en uppgift om en viss sjukdomsdiagnos behöva användas för att identifiera avgöranden på socialförsäkringsområdet, eller en uppgift om brott för att sammanställa praxis avseende påföljder. Regeringen gör därför bedömningen att det, för att främja en effektiv och rättssäker verksamhet, finns ett behov i domstolarna att kunna utföra sökningar med integritetskänsliga sökbegrepp. Denna bedömning delas i stort också av remissinstanserna och har bekräftats ytterligare vid det seminarium som Domstolsverket anordnat i syfte att kartlägga behoven av att använda integritetskänsliga söksamhet i domstolarnas verksamhet.

Kan externa databaser tillgodose domstolarnas sökbehov?

I promemorian presenteras en analys av frågan om behoven av att söka skulle kunna tillgodoses på något annat sätt som innebär mindre integritetsrisker och det konstateras att några tillfredsställande alternativ inte står till buds. De flesta remissinstanser anför inga invändningar mot denna bedömning.

Justitiekanslern ifrågasätter dock promemorians bedömning i denna del och väcker frågan om inte Domstolsverkets webbsida *Vägledande avgöranden* skulle kunna utvecklas och anpassas för att tillgodose domstolarnas behov. Regeringen konstaterar att de sökningar som domstolarna behöver utföra framför allt avser offentliga uppgifter, såsom uppgifter i domar och beslut. Att försöka tillgodose detta behov genom att bygga ut denna webbsida, som enligt den nuvarande ordningen endast får innehålla utvalda avgöranden från överrätterna, framstår enligt regeringen inte som ett bättre alternativ jämfört med att tillåta domstolarna att söka bland sina egna avgöranden. Att utveckla den aktuella webbsidan till att omfatta domar och beslut mer generellt, inklusive underrätternas avgöranden, skulle såvitt kan bedömas ta stora resurser i anspråk, eftersom det då måste avsättas personal till att gå igenom och maskera personuppgifter i alla domar. Det skulle också leda till en fördröjning innan avgörandena blev tillgängliga och sökbara för domstolarna. Samtidigt skulle det medföra ökad spridning av integritetskänslig information till andra än domstolarna eftersom webbplatsen är direkt åtkomlig för vem som helst som har tillgång till internet.

Sveriges advokatsamfund anser att skälen för att tillåta användningen av integritetskänsliga sökbegrepp är mycket svaga och menar att domstolarna trots kostnaderna bör kunna använda externa rättsdatabaser i stället för att söka bland sina egna uppgifter. *Kammarrätten i Sundsvall* anser å sin sida att det är en självklarhet att domstolarna behöver tillgång till sina egna och andra domstolars avgöranden för att verksamheten ska fungera. Om det genom den nya lagen införs begränsningar i hur de domstolsanställda får söka i verksamhetssystemet kommer domstolarna enligt kammarrätten att behöva köpa tillbaka sina egna uppgifter genom

abonnemang hos olika rättsdatabaser. Som anges ovan anser regeringen att det är principiellt orimligt att domstolarna ska behöva teckna abonnemang med externa tillhandahållare av rättsdatabaser för att kunna söka bland vad som i grunden är domstolarnas egna uppgifter. Det ska också understrykas att sökning i sådana externa databaser inte betyder mindre risker. Tvärtom är det i sådana databaser ofta möjligt att använda integritetskänsliga sökbegrepp för att söka bland avgöranden från många olika domstolar på en gång.

Vidare måste det beaktas att det blir allt billigare och enklare att lagra stora mängder uppgifter och att göra dem tillgängliga efter hand som den tekniska utvecklingen går framåt. Regeringen kan därför inte ansluta sig till *Ekobrottsmyndighetens* antagande att det totala antalet personer som har tillgång till externa rättsdatabaser skulle vara och förbli färre än antalet personer som utnyttjar sökmöjligheterna hos domstolarna. Inte heller finns det fog för *Ekobrottsmyndighetens* bedömning att det sökbara materialet i de externa rättsdatabaserna skulle bli mindre omfattande än det material som är sökbart hos en domstol. Hos domstolarna kommer det sökbara materialet att inskränkas bl.a. genom bestämmelser som begränsar vilka handlingar som är sökbara. För att undvika integritetsintrång är det viktigt att de personuppgifter som behandlas är riktiga och aktuella (jfr 9 § första stycket g PUL som domstolsdatalagen hänvisar till). Till skillnad från externa rättsdatabaser, finns det hos domstolarna i princip alltid aktuell information tillgänglig angående vilka domar som har överklagats eller angående eventuella rättelser. Domstolarna har kontroll över informations säkerheten så länge det är fråga om sökningar i domstolarnas egna system, till skillnad från vad som är fallet i fråga om externa privata rättsdatabaser. Integritetsriskerna är alltså i vissa avseenden mindre om sökning efter domar och beslut sker direkt hos domstolarna, jämfört med om sökning sker i externa rättsdatabaser.

Sammanfattningsvis anser regeringen att externa rättsdatabaser inte utgör ett bättre alternativ än att tillåta användningen av integritetskänsliga sökbegrepp i domstolarna och att det, i likhet med promemorians bedömning, inte heller står några andra bättre alternativ till buds för att tillgodose domstolarnas behov av att söka efter information.

Förbud mot integritetskänsliga sökbegrepp men med vissa undantag

Det kan alltså konstateras att det i domstolarna finns behov av att i vissa fall använda även integritetskänsliga sökbegrepp för att säkerställa en rättssäker och effektiv verksamhet, och att dessa behov inte kan tillgodoses på något annat sätt som innebär mindre integritetsrisker än att domstolarna tillåts söka i de egna verksamhetssystemen. Några remissinstanser, däribland *Borås tingsrätt* och *Förvaltningsrätten i Stockholm*, anser att integritetsriskerna med att tillåta integritetskänsliga sökbegrepp i den omfattning som promorian föreslår är för stora och flera remissinstanser pekar på de risker som finns när personuppgifter kan tas fram med hjälp av ett integritetskänsligt sökbegrepp på begäran av en enskild och spridas. Det finns dock många remissinstanser, framför

allt förvaltningsdomstolar, som i olika avseenden anser att promemorians förslag innebär för långtgående begränsningar.

Regeringen konstaterar att det finns integritetsrisker förknippade med att tillåta domstolspersonalen att använda känsliga sökbegrepp. Detta gäller inte minst eftersom allmänheten med stöd av offentlighetsprincipen därigenom får möjlighet att begära att domstolspersonalen ska använda dessa sökbegrepp för att sammanställa och lämna ut personuppgifter. Vid den avvägning som måste göras mellan å ena sidan domstolarnas verksamhetsbetingade behov av att kunna använda integritetskänsliga sökbegrepp, och å andra sidan de integritetsrisker som vidsträckta sökmöjligheter kan innebära vid tillämpningen av offentlighetsprincipen, stannar regeringen för att det som huvudregel inte bör vara tillåtet att söka med användning av de integritetskänsliga sökbegrepp som det nu är fråga om. Denna huvudregel bör komma till uttryck i domstolsdatalagen.

Regeringen anser dock att det inom väl avgränsade ramar bör tillåtas att domstolarna i vissa fall använder integritetskänsliga sökbegrepp under förutsättning att det finns ett tydligt behov och att integritetsriskerna inte blir så stora att verksamhetsbehovet trots allt bör stå tillbaka. I de allmänna domstolarnas verksamhet finns ett sådant behov beträffande uppgifter som avslöjar brott eller misstanke om brott. Flera remissinstanser, bl.a. *Kammarrätten i Jönköping* och *Förvaltningsrätten i Göteborg*, framhåller att det också finns ett verksamhetsbehov av att kunna använda sådana sökbegrepp i de allmänna förvaltningsdomstolarna, exempelvis vid sökning bland domar i körkortsmål. Regeringen gör samma bedömning. Med hänsyn till att integritetsriskerna vid sökning på brott eller misstanke om brott i en allmän förvaltningsdomstol får anses begränsade anser regeringen sådana sökningar inom vissa ramar bör tillåtas. Det är enligt regeringen också tydligt att de allmänna förvaltningsdomstolarna behöver använda sökbegrepp som rör hälsa, främst inom socialförsäkringsområdet. Remissinstanserna i stort är av samma uppfattning och vid det seminarium som Domstolsverket anordnade har sökbehoven enligt regeringens nu gjorda bedömningar bekräftats.

Domstolsdatalagens generella sökförbud bör mot denna bakgrund förenas med undantag för användning av sökbegrepp i allmän domstol och allmän förvaltningsdomstol som avslöjar brott eller misstanke om brott och användning av sökbegrepp i allmän förvaltningsdomstol som avslöjar hälsa. Undantagen bör av integritetsskyddsskäl kunna avgränsas så specifikt som möjligt. Dessa ytterligare avgränsningar bör dessutom kunna anpassas kontinuerligt, efterhand som nya måltyper tillkommer och domstolarnas organisation förändras. Det är därför lämpligt att det i förordning preciseras vilka möjligheter till sökning som ska finnas. Mot denna bakgrund bör det tas in en upplysning i domstolsdatalagen om att regeringen kan meddela föreskrifter om begränsningar av möjligheten att använda de aktuella sökbegreppen. Regeringens möjlighet att delegera föreskrifträtten till myndighet bör också återspeglas i bestämmelsen. I förordningsbestämmelserna kan det t.ex. specificeras i vilka måltyper som sökbegreppen får användas, vilka handlingar som då får vara sökbara och vilka särskilda begränsningar som ska gälla i fråga om direktåtkomst. Bestämmelserna i förordning som begränsar

möjligheterna att använda de aktuella sökbegreppen bör utformas som ovillkorliga bestämmelser så att de får genomslag när allmänheten begär att en sökning ska utföras med stöd av offentlighetsprincipen (se avsnitt 11.2).

I avsnitt 13 görs bedömningen att det utöver de nu aktuella sökförbuden bör gälla särskilda begränsningar avseende hur länge uppgifterna i ett mål ska vara sökbara efter det att målet har fått laga kraft och handlingarna i målet har arkiverats.

Behörighet och säkerhet

Justitiekanslern anser att det i bestämmelsen om sökning av tydlighets skull bör anges uttryckligen att regeringen kan meddela föreskrifter om behörighet och säkerhetsfrågor. I avsnitt 9.2 föreslås att det i domstolsdatalagen ska tas in en upplysningsbestämmelse om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela närmare föreskrifter om tillgången till personuppgifter. Enligt regeringen behövs det inte något ytterligare förtydligande av regeringens behörighet att meddela föreskrifter om behörighet och säkerhetsfrågor vid sökning. Den sökreglering som föreslås är en rättsligt bindande reglering och det förutsätts naturligtvis att personalen utbildas i vad som är tillåtet respektive förbjudet så att efterlevnaden kan garanteras.

Särskilda beteckningar för identifiering av en viss mål- eller ärendetyp

Domstolarna använder i många olika sammanhang särskilda beteckningar för identifiering av en viss mål- eller ärendetyp, s.k. målgrupps- och måltypskoder. Dessa fastställs i de flesta fall av Domstolsverket och varje målgrupps- eller måltypskod anknyter till mål eller ärenden inom ett visst ämnesområde (t.ex. inkomst- och förmögenhetstaxering) eller en författning (t.ex. mål enligt vapenlagen). Målgrupps- och måltypskoder används i mycket stor utsträckning i den dagliga verksamheten och det har inte framkommit att detta skulle medföra några särskilda risker i integritetshänseende. Det är regeringens uppfattning att sökning med användning av nu aktuella koder bör vara tillåten. Med regeringens förslag till sökreglering kan det dock i något enstaka fall anses oklart om användningen av en viss målgrupps- eller måltypskod är tillåten. Regeringen föreslår därför att det i lagen tas in en bestämmelse som förtydligar att användningen av målgrupps- och måltypskoder som sökbegrepp inte omfattas av förbudet i sökbestämmelsen.

11.5 Generella undantag från sökbegränsningarna

<p>Regeringens förslag: Förbudet att använda vissa sökbegrepp omfattar inte sökningar som endast görs i en viss handling eller i ett visst mål eller ärende.</p>

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna tillstyrker promemorians förslag eller har ingen invändning mot det.

Skälen för regeringens förslag: 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 det sökförbud 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 [2010:361]).

12 Elektroniskt utlämnande

12.1 Utlämnande genom direktåtkomst

Regeringens förslag: Direktåtkomst får endast medges

- en allmän domstol,
- en allmän förvaltningsdomstol,
- en hyres- och arrendenämnd,
- en part eller
- en parts ombud, biträde eller försvarare.

Direktåtkomst för en part eller en parts ombud, biträde eller försvarare får endast avse personuppgifter i partens mål eller ärende.

I lagen upplyses det om att regeringen eller den myndighet som regeringen bestämmer kan meddela ytterligare föreskrifter om begränsningar av direktåtkomsten samt om behörighet och säkerhet vid sådan åtkomst.

Regeringens bedömning: Den kommande förordningsregleringen bör vara uppbyggd så att direktåtkomst som huvudregel är förbjuden och undantag endast tillåts inom noggrant avgränsade ramar.

Promemorians förslag överensstämmer i huvudsak med regeringens. I promemorian föreslås en annan lagteknisk lösning.

Remissinstanserna: Remissutfallet är blandat. *Svea hovrätt*, *Nyköpings tingsrätt* och *Kammarrätten i Stockholm* tillstyrker promemorians förslag.

Justitiekanslern kan i avsaknad av närmare analyser av de frågeställningar som Justitiekanslern uppmärksammar, som framför allt rör direktåtkomst för parter, inte tillstyrka förslaget. *Datainspektionen* avstyrker förslaget att parter enligt domstolsdatalagen ska kunna medges direktåtkomst. *Sveriges advokatsamfund* anser att de skäl som anförs i promemorian inte motiverar att domstolarna kan medge varandra direktåtkomst och avstyrker förslaget. *Ekobrottsmyndigheten* anser att konsekvenserna av förslagen behöver analyseras betydligt djupare.

Hovrätten över Skåne och Blekinge anser att direktåtkomsten för andra domstolar bör begränsas till att gälla underinstansernas material i ett mål eller ärende som är eller har varit anhängigt vid den domstol som får direktåtkomst. Enligt hovrätten är behoven av att söka efter vägledande avgöranden och att konferera mål begränsade. Integritetsriskerna skulle vara betydande om de allmänna domstolarna får generell direktåtkomst till varandras uppgifter, exempelvis om allmänheten kan få ut uppgifter från en tingsrätt om huruvida en person har åtalats vid någon annan domstol. *Förvaltningsrätten i Malmö* anser att direktåtkomst mellan underrätterna inte är nödvändig.

Göta hovrätt, Hovrätten för Västra Sverige, Borås tingsrätt och Kammarrätten i Sundsvall ifrågasätter om de tekniska systemen kommer att medge att varje domstol individuellt kan styra över vem som får direktåtkomst. *Göta hovrätt, Hovrätten för Västra Sverige, Attunda tingsrätt, Kammarrätten i Sundsvall och Kammarrätten i Jönköping* ifrågasätter om det är lämpligt att låta varje individuell domstol styra vem som får direktåtkomst, bl.a. med hänsyn till att RIF-samarbetet förutsätter att uppgifter kan återanvändas elektroniskt i rättskedjan. *Hovrätten för Västra Sverige, Attunda tingsrätt, Kammarrätten i Göteborg och Migrationsverket* förordar en skyldighet att bereda direktåtkomst och att den författningsregleras. *Domstolsverket* anser att direktåtkomsten inte ska bygga på frivillighet och att verket bör ha föreskriftsrätt avseende skyldigheten att bereda direktåtkomst. Enligt verket förutsätter hanteringen i domstolarnas verksamhetstöd Vera och i RIF-samarbetet att underrätterna har tillgång till underrätternas information och vid övergång till helt elektroniska akter blir behovet större. Om direktåtkomsten är frivillig ser verket en risk att domstolarna ska anses ha rätt att kunna medge direktåtkomst. Kostnadsskäl talar mot att låta varje domstol bestämma självständigt över direktåtkomsten. *Förvaltningsrätten i Malmö* anser å sin sida att det är av avgörande principiell betydelse att möjligheten till direktåtkomst bygger på frivillighet. *Svea hovrätt* förutsätter att underinstanserna i praktiken kommer att ge överinstanserna direktåtkomst i överklagade mål och ärenden. *Kammarrätten i Stockholm* anser att det saknas skäl att ifrågasätta att direktåtkomst är beroende av den enskilda domstolens medgivande i egenskap av personuppgiftsansvarig. Enligt kammarrätten är de integritetsrisker som finns begränsade med hänsyn till att samtliga myndigheter som berörs kommer att tillämpa domstolsdatalagens skyddsbestämmelser.

Hovrätten för Västra Sverige påpekar att sekretess som är direkt tillämplig hos den mottagande myndigheten, s.k. primär sekretess, har företräde framför överförd sekretess, även om den primära sekretessen är svagare. Hovrätten menar att det kan finnas anledning att överväga behovet av ytterligare sekretess till följd av möjligheten till direktåtkomst liksom behovet av sekretessbrytande regler vid direktåtkomst. *Borås tingsrätt och Kammarrätten i Sundsvall* uppmärksammar att den domstol som har direktåtkomst till en annan domstol kan bli skyldig att sekretesspröva och lämna ut uppgifter från den andra domstolen. De efterlyser en närmare analys av denna fråga. *Göteborgs tingsrätt och Kammarrätten i Sundsvall* anser att det är orimligt att en annan domstol än den som har handlagt ett mål ska sekretesspröva handlingar i målet.

Med hänsyn till att sekretessprövningar i denna typ av situationer kan bli av sämre kvalitetet och medföra ett administrativt merarbete anser *Förvaltningsrätten i Malmö* att underrätterna inte bör ha direktåtkomst till varandras uppgifter. *Göteborgs tingsrätt* anser att det bör utredas vidare om en annan domstols handling ska behöva ingå i direktåtkomsten när den domstol som beviljats direktåtkomst faktiskt inte tagit del av handlingen. *Justitiekanslern* anser att domstolarnas ansvar för personuppgifterna genom direktåtkomsten riskerar att bli otydligare och bedömningar gällande tillåtligheten att behandla personuppgifter kan bli svårare att genomföra, eftersom den domstol som medger direktåtkomst förlorar kontrollen över vilka uppgifter mottagaren vid ett visst söktillfälle tar del av. Vidare menar *Justitiekanslern* att en förutsättning för direktåtkomst för enskilda bör vara att åtkomsten endast avser uppgifter för vilka det inte gäller sekretess i förhållande till mottagaren. Det saknas överväganden avseende hur domstolarna ska hantera sekretesskyddade uppgifter i förhållande till parterna samt en analys av förslaget ur sekretessperspektiv.

Göteborgs tingsrätt anser att direktåtkomsten inte får innebära att domstolarna, utan ytterligare överväganden, åläggs en skyldighet att utföra kontroller avseende om en fråga redan är anhängiggjord vid en domstol eller rättskraftigt avgjord. *Ekobrottsmyndigheten* menar att direktåtkomst kan leda till att en domstol eller åklagare får del av överskottsinformation som har beröring med ett mål som handläggs av dem utan att det är fråga om processmaterial. Direktåtkomsten kan därför enligt *Ekobrottsmyndigheten* leda till att det blir otydligt för en tilltalad vilka uppgifter domstolen och åklagaren faktiskt tagit del av. *Domstolsverket* anser att det behöver belysas ytterligare under vilka förutsättningar en domstol är skyldig att till ett eget mål föra de uppgifter som domstolen har tagit del av via direktåtkomsten.

Domstolsverket är positivt inställt till att det i domstolsdatalagen skapas möjlighet för parter m.fl. att i framtiden få direktåtkomst till personuppgifter i sitt eget mål eller ärende. En sådan direktåtkomst är ett effektivt sätt för parter att få tillgång till uppgifter i de egna målen och kan leda till en ökad insyn i domstolarnas verksamhet. Det krävs dock ett omfattande utvecklingsarbete och komplicerade analyser av autenticitet och säkerhet för att få fram en fungerande teknisk lösning för en sådan direktåtkomst, eftersom det inte finns någon befintlig systemstruktur att bygga vidare på för att skapa en sådan direktåtkomst. *Migrationsverket* anser att möjligheten till direktåtkomst till de egna målen sannolikt kommer att underlätta och påskynda verkets ärendehandläggning. Det är viktigt för verket att kunna fortsätta utveckla den elektroniska kommunikationen med domstolarna via direktåtkomst. *Försäkringskassan* anser att direktåtkomst till de egna målen kommer att öka effektiviteten för myndigheten i dess egenskap av part i allmän förvaltningsdomstol och allmän domstol. *Kammarrätten i Sundsvall* menar att parter och andra s.k. aktörer skulle uppskatta att få direktåtkomst som motsvarar funktionen ”allmänhetens PC” (tidigare ”allmänhetens terminal”). *Datainspektionen* anser att direktåtkomst för parter skulle kunna innebära att myndigheter, försvarare, ombud och biträden skulle få tillgång till en betydande mängd personuppgifter som ofta är känsliga. Det är enligt inspektionen svårt att införa annat än

generella åtkomstbegränsningar utifrån vad varje myndighet behöver för sin verksamhet och sådana begränsningar ger inte ett fullgott skydd. Dainspektionen pekar också på att det i mål hos domstolarna ofta kan förekomma personuppgifter som avser andra än den enskilde parten själv. *Attunda tingsrätt* anser att det bör klargöras vad som avses med "biträde" och ifrågasätter om ett rättgångsbiträde enligt 12 kap. 22 § rättegångsbalken, som endast får handla på partens vägnar i hans eller hennes närvaro, ska kunna medges direktåtkomst. *Förvaltningsrätten i Härnösand* anser att direktåtkomst för parter kan underlätta arbetet, men befarar omfattande tekniska och säkerhetsmässiga svårigheter, särskilt rörande sekretesskyddade uppgifter.

Domstolsverket anser att det bör övervägas om domstolarnas expedieringsskyldighet ska ersättas med en möjlighet för andra myndigheter att ha direktåtkomst.

Skälen för regeringens förslag och bedömning

Begreppet direktåtkomst

Begreppet direktåtkomst har ingen legaldefinition men den grundläggande innebörden är att någon utomstående har direkt tillgång till uppgifter som behandlas hos en myndighet, t.ex. en domstol. I begreppet direktåtkomst ligger att den utomstående på egen hand kan ta fram uppgifter och på så sätt få uppgifterna utlämnade till sig. Vid direktåtkomst fattas beslutet om överföring i varje enskilt fall av mottagaren. Prövningen av om ett utlämnande är förenligt med offentlighets- och sekretesslagen (2009:400, OSL) måste därför ske redan då uppgifterna görs tillgängliga genom direktåtkomst, oavsett om någon mottagare vid den tidpunkten tar del av dem. Den direktåtkomst som en myndighet medger någon utomstående är vanligtvis avgränsad så att mottagaren endast har tillgång till vissa bestämda uppgifter, såsom uppgifter i en viss databas eller i vissa dokument.

Utlämnande genom direktåtkomst till en domstol

De tydligaste och mest aktuella behoven av direktåtkomst finns domstolarna emellan. Partsuppgifter och annan strukturerad information bör kunna återanvändas av en överrätt när ett mål eller ärende överklagas så att uppgifterna inte behöver matas in manuellt i datorsystemen flera gånger. Effektiv återanvändning av uppgifter förutsätter att det finns möjlighet till direktåtkomst mellan domstolsinstanserna. När ett mål överklagas behöver överrätten vidare kunna ta del av ljud- och bildupptagningar som lagras elektroniskt i underrättens datorsystem via direktåtkomst. Utan denna möjlighet skulle ljud- och bildfilerna behöva lagras parallellt i flera domstolar.

En domstol bör, inom de begränsade ramar som föreslås i avsnitt 11.4, ha möjlighet att söka bland avgörandena från en annan domstol i syfte att främja en enhetlig rättstillämpning och effektiv handläggning. En förutsättning för att detta ska vara möjligt är att direktåtkomst kan etableras mellan dessa domstolar. Sådan direktåtkomst förekommer i viss utsträckning redan i dag. Direktåtkomsten kan exempelvis behöva avse domar och de ärendemeningar som registreras i varje mål.

En domstol kan vidare ha nytta av att via direktåtkomst få tillgång till uppgifter hos andra domstolar för att identifiera mål som har samband med ett mål vid den egna domstolen. Det kan vara önskvärt att mål som inlets i olika domstolar kan identifieras och sammanföras om det processrättsliga regelverket medger det.

Direktåtkomst till andra domstolars uppgifter kan också behövas för delgivningsändamål. Att parter och ombud kan delges handlingar är avgörande för att domstolarna över huvud taget ska kunna handlägga mål och ärenden. Dessvärre har domstolarna alltför ofta 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 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.

Det finns således ett antal fall där möjligheten till direktåtkomst mellan domstolarna är viktig för att främja att domstolarna ska kunna bedriva sitt arbete rättssäkert och effektivt. Detta är något som också i stort har bekräftats av remissinstanserna.

Domstolarnas behov måste dock vägas mot de integritetsrisker som kan vara förknippade med direktåtkomst. En sådan risk är att fler personuppgifter blir tillgängliga vid flera domstolar samtidigt genom direktåtkomsten. *Sveriges advokatsamfund* anser att det saknas tillräckliga skäl för att motivera direktåtkomst mellan domstolarna. En viktig utgångspunkt för regleringen är dock att den direktåtkomst som kan bli aktuell att tillåta i domstolsdatalagen inte bör vara mer omfattande än vad som är motiverat, vilket också *Hovrätten över Skåne och Blekinge* och *Förvaltningsrätten i Malmö* uppmärksammar från olika utgångspunkter. Direktåtkomsten bör alltså anpassas efter de olika behov som föreligger i domstolarnas verksamhet och som kan försvaras ur ett integritetsperspektiv. *Justitiekanslern* anser att domstolarnas ansvar för personuppgifterna genom direktåtkomsten riskerar att bli otydligare och bedömningar gällande tillåtligheten att behandla personuppgifter kan bli svårare att genomföra, eftersom den domstol som medger direktåtkomst förlorar kontrollen över vilka uppgifter mottagaren vid ett visst söktillfälle tar del av. Enligt regeringen bör detta inte bli något problem i praktiken eftersom både avsändaren och mottagaren omfattas av domstolsdatalagen. Det innebär att samma skydd kommer att gälla i alla led hos båda de inblandade domstolarna. Det ankommer på den personuppgiftsansvarige att avgöra vilka behandlingar som får utföras. I avsnitt 7.1 föreslår regeringen en bestämmelse som tydligt pekar ut vem som är personuppgiftsansvarig för vilka behandlingar.

Det finns således flera verksamhetsmässiga fördelar med en möjlighet till utlämnande genom direktåtkomst mellan domstolar. Domstolsdatalagen bör därför inte förhindra sådant utlämnande. Däremot måste de integritetsrisker som kan vara förknippade med utlämnande genom direktåtkomst bemästras. Regeringen anser därför, i linje med vad bl.a. *Hovrätten över Skåne och Blekinge* anför, att direktåtkomstens omfattning noggrant bör anpassas efter behoven och begränsas både beträffande för vilka kategorier av uppgifter som direktåtkomst ska kunna medges och vilka domstolar som ska kunna ha direktåtkomst till dessa kategorier av uppgifter. Av integritetsskyddsskäl bör den närmare

omfattningen av direktåtkomsten dessutom regleras så preciserat som möjligt med avseende på vilka domstolar som kan tillåtas ha direktåtkomst till vilka personuppgifter. Behoven ser olika ut beroende på om det är fråga om exempelvis åtkomst till domar eller åtkomst till uppgifter för delgivningsändamål. Behoven varierar över tiden och är bl.a. beroende av hur domstolarnas inre och yttre organisation utformas, arbetsrutiner, målsammansättningen i domstolarna och forumregler. Den närmare regleringen om vilka domstolar som ska kunna få direktåtkomst och till vilka uppgifter bör därför meddelas av regeringen i förordning. För att åstadkomma en restriktiv ram för direktåtkomsten bör huvudregeln enligt förordningsbestämmelserna vara att direktåtkomst är förbjuden utom i de fall som specificeras i förordning.

Sekretess vid utlämnande till en domstol genom direktåtkomst

De uppgifter som blir tillgängliga genom direktåtkomst anses utlämnade i offentlighets- och sekretesslagens mening. Det betyder att de tekniska systemen för direktåtkomst måste konstrueras så att de inte kommer i konflikt med offentlighets- och sekretesslagens bestämmelser. Den reglering som föreslås avseende direktåtkomst medför således inte i sig att uppgifter som omfattas av sekretess får lämnas ut.

Att säkerställa att datorsystemen och arbetsrutinerna vid domstolarna får en sådan utformning att direktåtkomsten inte kan komma i konflikt med sekretessregleringen är en viktig uppgift för domstolarna och Domstolsverket. Av 11 kap. 4 § OSL följer att den sekretess som gäller hos den utlämnande domstolen automatiskt överförs till den mottagande domstolen. Såsom *Hovrätten för Västra Sverige* påpekar blir den överförda sekretessen enligt 11 kap. 8 § OSL i vissa fall inte lika stark hos den mottagande domstolen.

Flera remissinstanser, däribland *Borås tingsrätt*, uppmärksammar att sådana uppgifter som en domstol har tillgång till via direktåtkomst till en annan domstol ofta kommer att betraktas som en allmän handling hos den mottagande domstolen. Det innebär att enskilda kan ha rätt att ta del av uppgifterna med stöd av offentlighetsprincipen hos den mottagande domstolen. Detta gäller också sådana uppgifter som den mottagande domstolen tekniskt har möjlighet att komma åt, även om uppgifterna i det enskilda fallet faktiskt inte har överförts till mottagande domstolen (överskottsinformation). Några remissinstanser, bl.a. *Göteborgs tingsrätt*, uppmärksammar att den mottagande domstolen således kan behöva sekretesspröva och lämna ut uppgifter som härrör från en annan domstol. Sekretessprövning av handlingar som härrör från en annan domstol är emellertid något som domstolarna redan i dag kan behöva hantera. Det gäller både uppgifter som har mottagits från en annan domstol genom direktåtkomst och uppgifter som överlämnats från en annan domstol i pappersform. Mot bakgrund av att direktåtkomst endast är tänkt att vara möjlig i mer begränsad omfattning bör konsekvenserna i detta avseende inte bli så omfattande som remissinstanserna befarar.

Vad särskilt gäller frågan om överskottsinformation vid direktåtkomst kan avslutningsvis nämnas att Informationshanteringsutredningen har haft i uppdrag att överväga en inskränkning i handlingsoffentligheten såvitt gäller just sådan information. Utredningen har stannat för att inte

föreslå någon annan förändring än ett förstärkt sekretesskydd för sådan information, se utredningens delbetänkande Överskottsinformation vid direktåtkomst (SOU 2012:92 s. 164 f.). Betänkandet bereds för närvarande i Regeringskansliet.

Skyldighet att medge direktåtkomst regleras inte

Några remissinstanser, bl.a. *Attunda tingsrätt och Kammarrätten i Göteborg*, efterlyser en reglering som inte bara innebär att domstolarna har en möjlighet att bevilja direktåtkomst, utan som också innebär en skyldighet för dem att ge varandra direktåtkomst. Genom domstolsdatalagen regleras emellertid på vilket sätt och under vilka förutsättningar som domstolarna får behandla personuppgifter – inte vilken skyldighet de ska ha att behandla personuppgifter. Enligt regeringen finns det för närvarande inget behov av att föreslå regler om domstolarnas skyldighet att medge varandra direktåtkomst.

Göta hovrätt, Hovrätten för Västra Sverige, Borås tingsrätt och Kammarrätten i Sundsvall ifrågasätter om de tekniska systemen kommer att medge att varje domstol individuellt kan styra över vem som får direktåtkomst. Regeringen konstaterar att domstolarna i praktiken kommer att vara beroende av de tekniska system som Domstolsverket utvecklar. Ytterst är det dock varje domstol som är ansvarig för de behandlingar som domstolen utför (se avsnitt 7.1), vilket Domstolsverket naturligtvis måste beakta vid utformningen av systemen. Samtidigt blir det genom RIF-samarbetet och övrig teknisk integrering allt viktigare att den elektroniska kommunikationen mellan domstolarna kan fungera enligt de standarder som tas fram. Regeringen följer denna utveckling.

Inga processrättsliga konsekvenser av regeringens förslag

Göteborgs tingsrätt undrar om möjligheterna till direktåtkomst påverkar domstolarnas skyldighet att utföra kontroller avseende om en fråga redan är anhängiggjord vid en domstol (lis pendens) eller rättskraftigt avgjord (res judicata). Regeringen konstaterar att domstolarnas utrednings-skyldighet beträffande denna typ av frågor styrs av de processuella regelverken och att bestämmelserna om direktåtkomst inte i sig påverkar domstolarnas skyldigheter i dessa avseenden. *Domstolsverket* anser att det behöver belysas ytterligare under vilka förutsättningar en domstol är skyldig att till mål och ärenden föra de uppgifter som domstolen har tagit del av via direktåtkomsten. *Ekobrottsmyndigheten* anser att domstolarnas och åklagarnas tillgång till överskottsinformation i samband med direktåtkomst kan leda till att det blir otydligt för en tilltalad vilka uppgifter domstolen och åklagaren faktiskt tagit del av. Regeringen kan med anledning av dessa påpekanden konstatera att domstolarna och åklagarna måste uppfylla processrättens krav i fråga om vilka uppgifter som ska fogas till ett mål eller ärende, vilka uppgifter som ska kommuniceras med parterna liksom övriga processrättsliga bestämmelser som syftar till att skapa insyn och klarhet. Detta gäller för alla uppgifter som finns tillgängliga för domstolen eller åklagaren, oavsett om det är via direktåtkomst, e-post eller på något annat sätt.

Utlämnande genom direktåtkomst till parter

En viktig processrättslig princip är att en part ska ha insyn i sitt mål. Ett sätt att förbättra insynen för parter vore att ordna system så att en part t.ex. från sin hemdator kan följa hur handläggningen av hans eller hennes mål fortskrider. Detta förutsätter bl.a. att det finns lagliga möjligheter att medge parten direktåtkomst till vissa personuppgifter i det egna målet, exempelvis de uppgifter som registreras i den s.k. dagboken i målhanteringssystemet. Dessutom förutsätter detta i praktiskt hänseende att nödvändiga tekniska lösningar finns tillgängliga så att direktåtkomsten kan avgränsas till personuppgifter som är lämpliga att göras tillgängliga på detta sätt och att inga sekretesskyddade uppgifter lämnas ut. Vidare måste det säkerställas att uppgifterna kan överföras säkert och att t.ex. identifierings- och inloggningsfunktioner fungerar tillförlitligt.

Domstolsverket är positivt inställt till att det skapas möjlighet för parter att i framtiden få direktåtkomst till personuppgifter i sitt eget mål eller ärende och framhåller att det är ett effektivt sätt för parter att få tillgång till uppgifter i de egna målen och kan leda till en ökad insyn i domstolarnas verksamhet. Enligt verket krävs det omfattande utvecklingsarbete och komplicerade analyser av autenticitet och säkerhet för att få fram en fungerande teknisk lösning för en sådan direktåtkomst. Flera andra remissinstanser är också positiva till att domstolsdatalagen ger en rättslig möjlighet för att utveckla direktåtkomst för parter. *Migrationsverket* framhåller att möjligheten till direktåtkomst till de egna målen kan underlätta och påskynda verkets ärendehandläggning och *Försäkringskassan* pekar på effektivitetsvinster för sin verksamhet. *Förvaltningsrätten i Härnösand* anser att direktåtkomst för parter kan underlätta arbetet, men menar att det finns omfattande tekniska och säkerhetsmässiga svårigheter, särskilt rörande sekretesskyddade uppgifter. *Kammarrätten i Sundsvall* menar att parter skulle uppskatta att få direktåtkomst som motsvarar funktionen ”allmänhetens PC”.

Med hänsyn till att domstolarnas handläggning i allt större utsträckning bygger på elektronisk akthantering och elektronisk kommunikation mellan instanserna anser regeringen att domstolsdatalagen inte bör utesluta möjligheten att ge parterna möjlighet att på elektronisk väg kunna följa vad som händer i det egna målet under handläggningen. Som framgår i avsnitt 6.1 är det ramarna för domstolarnas personuppgiftsbehandling som ska slås fast i domstolsdatalagen. Regeringen förslår därför att det enligt domstolsdatalagen ska vara möjligt för en domstol att lämna ut uppgifter genom direktåtkomst till en part och partens ombud, biträde eller försvarare. Möjligheten till direktåtkomst i dessa fall bör dock begränsas till personuppgifter i det egna målet eller ärendet.

Det bör också säkerställas att det inte blir tillåtet att lämna ut personuppgifter genom direktåtkomst till parter, ombud, biträden och försvarare förrän det står klart att de tekniska systemen och domstolarnas rutiner är tillräckligt utvecklade. Det bör exempelvis finnas system och rutiner för att garantera att personuppgifter genom direktåtkomsten inte blir åtkomliga för andra än rätt mottagare, att sekretesskyddade uppgifter inte lämnas ut och att inloggningsfunktionerna är pålitliga. På samma sätt

som när det gäller direktåtkomst för domstolar bör omfattningen av direktåtkomsten regleras så precist som möjligt för att på så sätt bemästra integritetsriskerna. Denna närmare reglering bör föreskrivas av regeringen i förordning. Regeringen har för avsikt att i avvaktan på den ovan beskrivna utvecklingen föreskriva att utlämnande genom direktåtkomst till parter, ombud, biträden och försvarare inte är tillåtet.

När det så småningom kan bli aktuellt att genom föreskrifter börja tillåta domstolarna att lämna ut personuppgifter genom direktåtkomst till sådana mottagare bör det ske inom noggrant avgränsade ramar. Det kan exempelvis röra sig om att tillåta direktåtkomst till uppgifter om inkommande och utgående handlingar i målet, förelägganden eller svarsfrister. Som framgår ovan är det endast aktuellt att medge direktåtkomst för parter till uppgifter som är såväl offentliga som av harmlös karaktär. De risker som ofta förknippas med direktåtkomst är mindre påtagliga när direktåtkomsten begränsas till denna typ av uppgifter. Det är fråga om uppgifter som parterna i många fall ändå får tillgång till under handläggningen oavsett direktåtkomsten och som domstolen ofta torde vara oförhindrad lämna ut även i elektronisk form till parten med stöd av den föreslagna bestämmelsen om utlämnande på medium för automatiserad behandling. Det är dock av integritetsskyddskäl lämpligt att parter som har många mål i en domstol endast kan bereda sig tillgång till uppgifterna i ett mål i taget. Med sådana begränsningar minimeras de risker som *Datainspektionen* pekar på. *Justitiekanslern* lyfter fram frågan hur domstolarna ska hantera sekretesskyddade uppgifter i förhållande till parterna och framhåller att sådana uppgifter inte bör kunna lämnas genom direktåtkomsten. Regeringen delar denna bedömning och föreslår därför ingen sekretessbrytande bestämmelse. Det innebär att det inte kommer att vara tillåtet för en domstol att bereda en part direktåtkomst till sekretesskyddade uppgifter. Det ankommer på Domstolsverket och domstolarna att säkerställa att så inte bli fallet.

Attunda tingsrätt efterfrågar ett klargörande avseende termen biträde. Enligt regeringen ska begreppet ges en vid tolkning och det bör i princip kunna omfatta såväl offentliga biträden, rättegångsbiträden och målsägandebiträden som gode män.

Annat utlämnande genom direktåtkomst

I promemorian görs bedömningen att utlämnande genom direktåtkomst inte ska få ske till andra mottagare än de som avses ovan (domstolar respektive parter och deras ombud, biträde eller försvarare). *Domstolsverket* anser att det bör övervägas om domstolarnas expedieringsskyldighet ska ersättas med en möjlighet för andra myndigheter att ha direktåtkomst. Ingen annan remissinstans har lämnat någon liknande synpunkt. En sådan reform rymmer många frågor som rör annat än personuppgiftshantering. Regeringen har inte i nuläget några planer på en sådan reform.

Ytterligare bestämmelser i förordning och myndighetsföreskrifter

För att säkerställa ett så fullgott integritetsskydd som möjligt bör omfattningen av direktåtkomsten, såsom framgår ovan, avgränsas mer

precist genom bestämmelser i förordning. Regeringen har också möjlighet att i förordning meddela särskilda bestämmelser om behörighet och säkerhet vid direktåtkomst. Dessa bestämmelser kan komma att behöva kompletteras med mer detaljerade bestämmelser i myndighetsföreskrifter. Sådana föreskrifter kan justeras efter hand som domstolarna omorganiserar, nya måltyper tillkommer, RIF-samarbetet går framåt och den tekniska infrastrukturen utvecklas. Regeringen föreslår därför en bestämmelse som upplyser om att regeringen eller den myndighet som regeringen bestämmer kan meddela ytterligare föreskrifter om begränsningar av direktåtkomsten samt om behörighet och säkerhet vid sådan åtkomst.

12.2 Utlämnande på medium för automatiserad behandling

Regeringens förslag: Personuppgifter får lämnas ut på medium för automatiserad behandling om det inte är olämpligt.

I lagen upplyses det om att regeringen eller den myndighet som regeringen bestämmer kan meddela ytterligare föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter på medium för automatiserad behandling.

Promemorians förslag överensstämmer inte med regeringens. I promemorian föreslås att personuppgifter får lämnas ut till myndigheter och parter, i egna mål och ärenden, utan något uttryckligt krav på lämplighetsprövning. Till andra mottagare får endast enstaka personuppgifter lämnas ut på medium för automatiserad behandling.

Remissinstanserna: Nästintill samtliga domstolar, liksom *Domstolsverket* och *Ekobrottsmyndigheten*, är kritiska till att begränsa utlämnademöjligheterna till enstaka personuppgifter. Många av dessa varnar för att det skulle ta mycket stora resurser i anspråk om domstolarna inte längre skulle kunna hantera utlämnande av större mängder personuppgifter elektroniskt. *Umeå tingsrätt* upplyser om att domstolen nästan inte har några papperskopior i brottmålen längre. Det framhålls av många remissinstanser att domstolarna kan tvingas skriva ut omfattande handlingar, som i övrigt hanteras elektroniskt, bara för att kunna lämna ut dem. Domstolsverket pekar på de omfattande resurser som läggs på att digitalisera informationshanteringen i brottmålen i syfte att eliminera paperhanteringen och anser att förslaget går stick i stäv med dessa strävanden. Flera remissinstanser, däribland *Lunds tingsrätt* och *Förvaltningsrätten i Malmö*, anser att det är oklart vad som menas med ”enstaka personuppgifter”. *Ekobrottsmyndigheten* ifrågasätter om det överhuvudtaget behövs någon begränsning avseende mängden uppgifter som kan lämnas ut med hänsyn till de bestämmelser angående säkerheten vid elektronisk överföring som ändå ska gälla enligt domstolsdatalagen och med hänsyn till att det enligt 21 kap. 7 § offentlighets- och sekretesslagen (2009:400, OSL) gäller sekretess för personuppgift om det kan antas att ett utlämnande skulle medföra att uppgifterna behandlas i strid med personuppgiftslagen (1998:204, PUL).

Västmanlands tingsrätt menar att det ur ett miljöperspektiv framstår som slöseri med att skicka papper i stället för att expediera domar och andra handlingar i digital form.

Om elektroniskt utlämnande efter s.k. massbeställningar helt skulle förhindras finns det enligt *Attunda tingsrätt* en risk för att medieföretagen i stället skulle begära ut kopior av avgörandena i pappersform. Med tanke på att antalet massbeställningar från medieföretagen ökar och de resurser det skulle kräva för att leverera deras beställningar i pappersform bör det enligt *Förvaltningsrätten i Malmö* även i fortsättningen ankomma på domstolarna själva att avgöra i vilken form utlämnande ska få ske. *Svea hovrätt* framhåller, liksom flera andra remissinstanser, att uppgifter som lämnas ut på papper ändå med allmänt tillgänglig teknik, såsom skanning, enkelt kan överföras till elektronisk format av mottagaren. Bland andra *Domstolsverket* ifrågasätter om det är rimligt att domstolarna under sådana förhållanden ska lägga resurser på att skriva ut elektroniska handlingar för att lämna ut dem i pappersformat. *Attunda tingsrätt* varnar för att begränsningen till enstaka personuppgifter kan tolkas på så sätt att den inte förhindrar att ett totalt sett stort antal personuppgifter lämnas ut elektroniskt genom att mottagaren gör flera på varandra följande beställningar. Tingsrätten framhåller att ett sådant förfarande skulle skapa stort merarbete. *Göteborgs tingsrätt* menar att en begränsning till enstaka uppgifter blir ihålig när medieföretag med utgivningsbevis kan göra liknande sammanställningar som domstolarna och sedan sprida dem. I likhet med *Förvaltningsrätten i Malmö* anser tingsrätten att åtgärder mot integritetsriskerna som är förknippade med kommersiella massuttag bör utredas.

Lunds tingsrätt föreslår att begränsningen till enstaka personuppgifter ska ersättas med en föreskrift om att domstolen vid utskick ska agera med försiktighet och med respekt för berördas integritet. Även *Svenska journalistförbundet* anser att begränsningen till enstaka personuppgifter bör ersättas med en bestämmelse om att domstolarna i det enskilda fallet ska göra en lämplighetsprövning. *Attunda tingsrätt* föreslår i stället en begränsning till personuppgifter i enstaka mål eller ärenden.

Datainspektionen, som avstyrker promemorians förslag, anser att regleringen i domstolsdatalagen bör vara så uttömmande som möjligt och undantag i förordning som utvidgar möjligheterna till utlämnande endast ska få föreskrivas i de fall som preciseras i lagen. För att säkerställa ett i alla avseenden fullgott integritetsskydd anser inspektionen vidare att behovet av mer detaljerade villkor för utlämnande bör övervägas och att det förslagsvis kan ske genom att regeringen eller den myndighet som regeringen bestämmer bemyndigas att meddela föreskrifter om begränsning av utlämnande på medium för automatiserad behandling och säkerhet vid sådant utlämnande.

Sundsvalls tingsrätt instämmer i promemorians bedömning att "allmänhetens PC" inte är att hänföra till direktåtkomst, men anser inte att det utesluter att avgränsningen av de uppgifter som tillhandahålls tydliggörs på lämpligt sätt. *Datainspektionen* föreslår att bestämmelser om innehållet och sökbegränsningar för "allmänhetens PC" övervägs i det fortsatta lagstiftningsarbetet.

Skälen för regeringens förslag

För annat elektroniskt utlämnande än genom direktåtkomst brukar begreppet ”utlämnande på medium för automatiserad behandling” användas i personuppgiftssammanhang. Sådant utlämnande kan exempelvis innebära att elektronisk information överförs via e-post, genom utlämnande av uppgifter på ett flyttbart lagringsmedium – t.ex. flashminne (s.k. usb-minne) – eller genom direkt överföring från ett datorsystem till ett annat. Varken dataskyddsdirektivet eller personuppgiftslagen innehåller några särskilda bestämmelser som begränsar möjligheterna till utlämnande på medium för automatiserad behandling. Samma sak gäller enligt Vera-förordningarna som för närvarande, vid sidan om personuppgiftslagen, reglerar domstolarnas personuppgiftsbehandling.

Ska möjligheterna till utlämnande begränsas?

Regeringen ansluter sig till bedömningen i promemorian att domstolarna även i fortsättningen ska kunna använda medium för automatiserad behandling för att skicka personuppgifter till en annan domstol eller myndighet. Sådan elektronisk kommunikation är en förutsättning för att domstolarna ska kunna använda elektroniska akter, för att RIF-samarbetet ska kunna fungera och för att verksamheten i övrigt ska kunna bedrivas effektivt och rättssäkert.

Av i huvudsak samma skäl behöver domstolarna kunna skicka personuppgifter i ett mål eller ärende till parterna och deras ombud, biträden eller försvarare. Att domstolarna kan skicka uppgifter elektroniskt till dessa mottagare är också viktigt för att rätten till partsinsyn ska få ett reellt innehåll. Ett ytterligare skäl för att tillåta sådan kommunikation är att den behövs för att enskilda och offentliga parter ska kunna vara likställda i domstolsprocesserna (equality of arms) eftersom alltfler uppgifter hanteras elektroniskt i rättskedjan. Åklagare, Skatteverket, Migrationsverket och andra offentliga parter har numera som regel tillgång till stora delar av processmaterialet i elektroniskt format. För att enskilda parter ska kunna vara likställda med en myndighet som är part bör domstolarna kunna skicka handlingar elektroniskt även till en enskild som är part. Ingen remissinstans har riktat någon invändning mot promemorians överväganden i dessa delar.

Vad gäller andra mottagare än myndigheter och parter anser regeringen att utgångspunkten ska vara att utlämnande i elektroniskt format bör vara möjligt även till dessa. Utvecklingen går mot att domstolarnas akter mer eller mindre uteslutande kommer att bestå av elektroniskt lagrade handlingar. E-post är både hos domstolarna och i omvärlden numera ett av de vanligaste kommunikationssätten. I vilken utsträckning som domstolarna kan lämna ut personuppgifter i elektronisk form begränsas av sekretessbestämmelsen i 21 kap. 7 § OSL som förhindrar utlämnande i de fall det kan antas att utlämnandet skulle medföra att uppgifterna behandlas i strid med personuppgiftslagen. Det är enligt regeringen inte lämpligt att därutöver slå fast alltför detaljerade villkor för i vilka fall elektronisk kommunikation ska få användas vid utlämnande av personuppgifter. Däremot bör det övervägas om det bör införas en mer allmänt

formulerad bestämmelse som tar sikte på de särskilda förhållanden som råder för utlämnande i domstolarna.

I promemorian övervägs två sätt att åstadkomma en begränsande reglering i domstolsdatalagen som tar sikte på utlämnande på medium för automatiserad behandling till andra mottagare än myndigheter och parter. Ett sätt är enligt promemorian att begränsa det elektroniska utlämnandet till enstaka personuppgifter och samtidigt ge regeringen möjlighet att meddela föreskrifter om undantag från begränsningen. Ett alternativt sätt, som också redovisas i promemorian, är att ta in en bestämmelse i domstolsdatalagen om att domstolarna i det enskilda fallet ska pröva om ett utlämnande är lämpligt med hänsyn till exempelvis personuppgifternas art, struktur och antal. I promemorian gjordes bedömningen att det var lämpligast att välja det första alternativet i avvaktan på Informationshanteringsutredningens (Ju 2011:11) översyn av gällande registerförfattningar, eftersom det alternativet överensstämde med vad som gäller enligt polisdatalagen (2010:361) och kustbevakningsdatalagen (2012:145). Informationshanteringsutredningen har sedan dess redovisat slutbetänkandet Myndighetsdatalag (SOU 2015:39). I betänkandet gör utredningen bedömningen att det inte behöver införas någon bestämmelse som generellt begränsar myndigheters möjlighet att lämna ut personuppgifter till andra myndigheter i elektronisk form. När det gäller utlämnanden till enskilda föreslås en bestämmelse som föreskriver att om en personuppgift får lämnas ut, kan det ske i elektronisk form om det inte är olämpligt med hänsyn till skyddet för personuppgiften. Betänkandet bereds för närvarande inom Regeringskansliet.

Regeringens förslag till domstolsdatalag innebär att domstolarna får skicka personuppgifter elektroniskt endast om säkerheten är tillräckligt god med hänsyn till bl.a. känsligheten hos de uppgifter som skickas (se avsnitt 9.1). Det får därför förutsättas att själva den elektroniska överföringen i sig inte kommer att orsaka några beaktansvärda risker. De övriga integritetsrisker som är förknippade med elektroniskt utlämnande har inte direkt med domstolarnas verksamhet att göra, utan hänför sig i allt väsentligt till de åtgärder som mottagaren kan tänkas vidta med de utlämnade uppgifterna. Om mottagaren har tillgång till uppgifterna elektroniskt kan det i viss mån bli lättare för honom eller henne att sprida uppgifterna. Samtidigt är det numera, såsom bl.a. *Svea hovrätt* påpekar, mycket enkelt och billigt för en mottagare av uppgifter på papper att genom skanning överföra uppgifterna till elektroniskt format, varför skillnaderna i nu aktuellt avseende av om uppgifterna lämnas ut på papper eller i elektroniskt format i praktiken är små.

Frågan om utlämnande på medium för automatiserad behandling har reglerats på olika sätt i registerförfattningar. En inte ovanlig lösning har varit just att ange att utlämnande får ske av enstaka personuppgifter, varvid brukar understrykas att termen enstaka ska anses ha en vidare innebörd än vad ordet från språklig utgångspunkt kan ge intryck av, se t.ex. prop. 2009/10:85, s. 333. Domstolarnas verksamhet skiljer sig dock från verksamheten vid t.ex. Polismyndigheten, Kustbevakningen och andra brottsbekämpande myndigheter. Domstolarna utmärker sig bl.a. genom att de flesta uppgifter som behandlas i deras verksamhet är offentliga både under handläggningen och när målet har avgjorts. Intresset av insyn och transparens väger särskilt tungt när det gäller den

dömande makt som domstolarna har, medan sekretess i många fall är huvudregeln i de brottsbekämpande myndigheternas operativa verksamhet. Inte minst ur demokratisk synvinkel är det av grundläggande betydelse att domstolarnas verksamhet kan granskas av allmänheten och av media. Möjligheten att få tillgång till domstolshandlingar i elektroniskt format är väsentlig för hur transparent verksamheten blir i praktiken och hur effektiv granskningen kan vara.

Promemorians förslag om att begränsa elektroniskt utlämnande till enstaka personuppgifter får omfattande och hård kritik av en majoritet av remissinstanserna. Det står klart att det skulle ta mycket stora resurser i anspråk hos domstolarna om de skulle förlora möjligheten att lämna ut bl.a. domar och andra offentliga dokument med e-post i de fall en begäran avser mer än enstaka personuppgifter. Samtidigt pekar flera remissinstanser på att promemorians förslag endast skulle ha en begränsad effekt i integritetsskyddshänseende. Det beror på att den som mottar uppgifter på papper ändå enkelt kan omvandla dem till digitalt format, t.ex. med hjälp av skanning. Detta gäller även om stora mängder pappersdokument begärs ut. Den som önskar få stora mängder personuppgifter direkt i elektroniskt format skulle också, som framgår ovan, kunna uppnå det genom att skicka in flera beställningar efter varandra till en domstol. De integritetsrisker som är förenade med att t.ex. en privat aktör, med stöd av offentlighetsprincipen, begär ut ett stort antal domar i brottmål och gör dem sökbara i en egen databas kan således inte begränsas genom den i promemorian föreslagna regleringen. Tvärtom kan konsekvenserna av en sådan reglering riskera att inskränkas till försämrade insyns- och granskningsmöjligheter av den dömande verksamheten och en ökad resursåtgång i domstolarna med att kopiera och expediera pappershandlingar som begärs utlämnade utan att några vinster görs i integritetshänseende.

Mot denna bakgrund går regeringen inte vidare med promemorians förslag att inom domstolsdatalagens tillämpningsområde begränsa utlämnande på medium för automatiserad behandling till enstaka personuppgifter. En annan, och bättre ordning, är i stället att låta utlämnandefrågan avgöras av om det i det enskilda fallet är lämpligt eller inte att lämna ut de efterfrågade uppgifterna i elektroniskt format. Detta ligger i linje med promemorians alternativa överväganden. En sådan typ av begränsning bör i princip gälla oavsett till vem uppgifterna lämnas ut, även om lämplighetsprövningen naturligtvis ser olika ut beroende på om det exempelvis är en myndighet eller en enskild person som är mottagare.

Bestämmelsen bör formuleras så att en domstol får lämna ut personuppgifter på medium för automatiserad behandling om det inte är olämpligt. Denna lösning förespråkas av *Svenska journalistförbundet* och stämmer också överens med *Lunds tingsrätts* förslag att domstolen vid utlämnande ska agera med försiktighet och med respekt för berördas integritet.

Några remissinstanser pekar på behovet av att utreda vilka åtgärder som kan vidtas för att stävja de integritetsrisker som är förknippade med att medieföretag med utgivningsbevis gör s.k. massuttag av personuppgifter från domstolarna och använder uppgifterna kommersiellt. Sedan promemorian remitterades har regeringen tillsatt en kommitté på

det tryck- och yttrandefrihetsrättsliga området med uppdrag att bl.a. analysera om skyddet för den personliga integriteten i databaser med utgivningsbevis är tillräckligt (dir. 2014:97). Utredningen ska redovisa sina överväganden och förslag senast den 1 september 2016.

Ytterligare begränsningar i förordning och myndighetsföreskrifter

Datainspektionen framhåller behovet av att det slås fast mer detaljerade villkor för utlämnande på medium för automatiserad behandling och föreslår att detta görs i förordning eller genom myndighetsföreskrifter. Regeringen delar bedömningen att det kan vara lämpligt att regeringen eller den myndighet regeringen bestämmer meddelar föreskrifter som begränsar möjligheterna att lämna ut uppgifter på medium för automatiserad behandling. Sådana föreskrifter kan bidra till att stärka integritetsskyddet och att främja en enhetlig tillämpning. Genom föreskrifterna kan också de närmare villkoren för ”allmänhetens PC” regleras, vilket *Sundsvalls tingsrätt* och *Datainspektionen* efterfrågar. I lagen bör det således upplysas om att regeringen eller den myndighet som regeringen bestämmer kan meddela ytterligare föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter på medium för automatiserad behandling.

12.3 Överföring till tredjeland

Regeringens förslag: Personuppgiftslagens bestämmelser om överföring av personuppgifter till tredjeland gäller i domstolarnas rättskipande och rättsvårdande verksamhet.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanserna tillstyrker promemorians förslag eller har ingen invändning mot det. *Attunda tingsrätt*, *Förvaltningsrätten i Göteborg* och *Domstolsverket* anser att det bör klargöras vilka möjligheter som finns till undantag från förbudet mot överföring till tredjeland exempelvis då en part som befinner sig i tredjeland ska delges handlingar. Förvaltningsrätten anser vidare att behovet av att överföra uppgifter vid handläggningen av mål är särskilt framträdande i viserings- och anknytningsmål men att behovet också finns i andra måltyper, t.ex. då en vårdnadshavare i ett LVU-mål befinner sig i tredjeland. *Attunda tingsrätt* anser även att det bör klargöras om en domstol i enlighet med 8 § PUL kan med stöd av offentlighetsprincipen lämna ut en allmän handling till en person som befinner sig i tredjeland.

Skälen för regeringens förslag: Enligt 33 § PUL är det förbjudet att överföra personuppgifter till tredjeland, dvs. en stat som inte är medlem av EU eller är ansluten till Europeiska ekonomiska samarbetsområdet, om landet inte har en adekvat nivå för skyddet av personuppgifter. Från förbudet finns vissa undantag och regeringen har också möjlighet att meddela föreskrifter om ytterligare undantag från förbudet (34 och 35 §§ PUL, se även 12–14 §§ personuppgiftsförordningen [1998:1191]). Dessa bestämmelser är redan i dag tillämpliga i domstolarnas verksamhet. En domstol kan alltså trots förbudet mot överföring av personuppgifter till

tredjeland med stöd av exempelvis 34 § PUL föra över personuppgifter per e-post till en part som befinner sig utomlands och som samtyckt till att kommunikationen med domstolen ska ske på detta sätt. Detta förutsätter dock att överföringen endast avser uppgifter om parten själv. Om inget samtycke har lämnats eller om uppgifterna avser någon annan än parten själv kan överföring ske om överföringen är nödvändig med hänsyn till vissa uppräknade syften i 34 § första stycket PUL, exempelvis om överföringen är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras. Enligt regeringen är bestämmelserna i 33–35 §§ PUL väl anpassade för en effektiv verksamhet i domstolarna. En hänvisning till dessa bestämmelser bör således tas in i domstolsdatalagen. Det bör dock understrykas att till följd av hänvisningen i domstolsdatalagen till lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen kan i vissa fall särskilda regler gälla för överföring till medlemsstater inom EU och till vissa andra stater (se avsnitt 6.7).

Attunda tingsrätt anser att det bör klargöras om personuppgifter kan föras över till tredjeland vid utlämnande av en allmän handling till en person som befinner sig i utlandet. Enligt 8 § första stycket PUL ska personuppgiftslagen inte tillämpas i den utsträckning det skulle inskränka en myndighets skyldighet att lämna ut personuppgifter enligt offentlighetsprincipen, såsom den kommer till uttryck i 2 kap. tryckfrihetsförordningen. I avsnitt 6.5 föreslås att 8 § första stycket PUL ska vara tillämplig i domstolarnas verksamhet. Offentlighetsprincipen innebär dock inte någon rätt för allmänheten att få ta del av personuppgifter på elektronisk väg. Vid bedömningen om en domstol kan föra över personuppgifter i en allmän handling i elektroniskt format till en person som befinner sig i tredjeland ska därför bestämmelserna i 33–35 §§ PUL beaktas.

13 Bevarande av personuppgifter

Regeringens förslag: Personuppgifter i allmänna handlingar får, på samma sätt som enligt personuppgiftslagen, bevaras elektroniskt i domstolarna för att tillgodose arkivändamål. Personuppgifter som inte är allmänna handlingar får, också på samma sätt som enligt personuppgiftslagen, bevaras elektroniskt endast så länge det är nödvändigt med hänsyn till ändamålen med behandlingen eller under längre tid om bevarandet sker för historiska, statistiska eller vetenskapliga ändamål.

I lagen upplyses det om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om ytterligare begränsningar för behandling av personuppgifter som hänför sig till ett mål eller ärende som har avgjorts genom en dom eller ett beslut som har fått laga kraft.

Promemorians förslag överensstämmer i huvudsak med regeringens. I promemorian föreslås en annan lagteknisk lösning.

Remissinstanserna: De flesta remissinstanserna tillstyrker promemorians förslag eller har ingen invändning mot det. *Kammarrätten i Stockholm* anser att det bör övervägas om domstolsdatalagen ska innehålla bestämmelser om bevarande och gallring på motsvarande sätt som bl.a. polisdatalagen (2010:361). En liknande synpunkt framförs av *Sundsvalls tingsrätt* som även anser att det kan vara lämpligt att närmare överväga under hur lång tid vissa mer integritetskänsliga söktermer ska få användas för sökning i det elektroniska arkivet. Vidare anser tingsrätten att det kan vara lämpligt att överväga frågan om ansvaret och formerna för utlämnande av allmänna handlingar ur elektroniska arkiv och om det är lämpligt att ansvaret ska ligga på den enskilda domstolen, särskilt om en central myndighet får ansvar för lagringen. *Uppsala universitet* efterfrågar en utförligare analys av frågan om elektronisk arkivering bl.a. utifrån ett rättssäkerhetsperspektiv. Vid en sådan analys bör beaktas bl.a. det starka rättssäkerhetsintresset av möjlighet till resning i brottmål även efter lång tid. *Kammarrätten i Sundsvall* anser att domstolarna framöver kommer att ha behov av direktåtkomst till uppgifter i ett elektroniskt arkiv under en längre tid än ett begränsat antal år med hänsyn till utvecklingen mot elektroniska arkiv. Enligt *Förvaltningsrätten i Malmö* bör det elektroniska arkivet erbjuda samma sökmöjligheter på namn och person- eller organisationsnummer som förvaltningsdomstolens manuella arkiv. *Domstolsverket* anser att det på ett tydligare sätt bör framgå att de särskilda föreskrifterna som ska få meddelas ska gälla vilket sätt uppgifter får användas efter det att avgörandet har fått laga kraft. *Kammarrätten i Göteborg* anser att de särskilda föreskrifterna inte bör få begränsa sökmöjligheterna i alltför stor utsträckning. *Attunda tingsrätt* anser att det förstärkta integritetsskyddet för elektroniskt bevarade uppgifter som redovisas i promemorian riskerar att urholkas genom att medieföretag bygger upp egna sökbara databaser med domstolarnas samtliga avgöranden. För dessa databaser finns inget integritetsskydd beträffande hur länge

uppgifter får lagras och vilka uppgifter som kan sökas fram i databaserna.

Skälen för regeringens förslag

Personuppgifter ska kunna bevaras i e-arkiv

Domstolarna är i likhet med andra myndigheter skyldiga att bevara allmänna handlingar för arkivändamål. 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 och 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. tryckfrihetsförordningen (TF) – minnesanteckningar, utkast och koncept – ska tas om hand för arkivering. Det framgår också av samma bestämmelse att varje anteckning i diariéer 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 allmänna handlingar ska bevaras. I fråga om domstolarnas rättskipande och rättsvårdande verksamhet har Riksarkivet meddelat föreskrifter som innebär undantag från huvudregeln att allmänna handlingar ska bevaras (10 § arkivlagen och 14 § arkivförordningen). I dessa föreskrifter anges hur länge olika allmänna handlingar i olika måltypen måste bevaras innan de får gallras.

Enligt personuppgiftslagen (1998:204, PUL) får personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till de ursprungliga ändamålen med behandlingen, om det inte behövs för historiska, statistiska eller vetenskapliga ändamål (9 § första stycket i och tredje stycket). Personuppgiftslagens bestämmelser hindrar dock inte att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet (8 § andra stycket). Personuppgiftslagens reglering innebär alltså i den meningen en prioritering av intresset att bevara allmänna handlingar framför integritetsskyddsintresset.

Det är viktigt att de arkivrättsliga ändamålen i 3 § arkivlagen får genomslag i domstolarnas verksamhet eftersom offentligheten har en särskilt stor betydelse där. Det är också viktigt att behovet av tillgång till information om tidigare mål och ärenden i domstolarnas rättskipande och rättsvårdande verksamhet kan tillgodoses. Arkivlagstiftningen är teknikneutral och ställer inte några krav på att handlingar ska sparas i t.ex. pappersform. Regeringens utgångspunkt är, i likhet med promemorians, att domstolarna ska ha möjlighet att på elektronisk väg fullgöra sin skyldighet att bevara allmänna handlingar i arkiv och att frågan om bevarande ska styras av det arkivrättsliga regelverket. En ordning där domstolarna i och för sig kan hantera aktbilagor och andra handlingar elektroniskt så länge handläggningen pågår, men sedan måste skriva ut handlingarna på papper när handläggningen avslutats, med det enda syftet att kunna arkivera handlingarna, vore otidsenlig och ineffektiv. För att möjliggöra en elektronisk hantering av uppgifter i mål och ärenden

genom det arkivrättsliga regelverket bör, på sätt som föreslås i promemorian, en hänvisning till 8 § andra stycket PUL tas in i domstolsdatalagen. På så sätt möjliggörs att domstolar på elektronisk väg arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet.

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 kan emellertid finnas behov av elektroniskt bevarande av vissa personuppgifter som inte finns i allmänna handlingar (t.ex. personuppgifter i en föredragningspromemoria). För att åstadkomma en heltäckande bevarandereglering bör det i domstolsdatalagen också finnas regler om bevarande av personuppgifter som inte utgör allmänna handlingar. Beträffande sådana personuppgifter bör domstolsdatalagen hänvisa till bestämmelserna i 9 § första stycket i och tredje stycket PUL. Det innebär att bevarande kan ske elektroniskt så länge det är nödvändigt med hänsyn till ändamålen med behandlingen eller om bevarandet sker för historiska, statistiska eller vetenskapliga ändamål. De flesta remissinstanser har inga invändningar i dessa avseenden. *Sundsvalls tingsrätt* och *Kammarrätten i Stockholm* anser att det bör övervägas om domstolsdatalagen ska innehålla bestämmelser om bevarande och gallring på motsvarande sätt som i bl.a. polisdatalagen. Regeringen konstaterar att bestämmelserna om bevarande och gallring i polisdatalagen är särskilt anpassade efter de förhållanden som råder i polisens brottsbekämpande verksamhet. Dessa bestämmelser bör därför inte utgöra en förebild för bevaranderegleringen i fråga om domstolarnas rättskipande och rättsvårdande verksamhet.

Sundsvalls tingsrätt anser vidare att det kan vara lämpligt att närmare överväga ansvaret och formerna för utlämnande av allmänna handlingar ur de elektroniska arkiven. Tingsrätten ifrågasätter om detta ansvar ska ligga på varje domstol, särskilt om ansvaret för lagringen läggs på en central myndighet. I avsnitt 7.1 föreslås att varje domstol ska vara personuppgiftsansvarig för den egna personuppgiftsbehandlingen. Det är således den personuppgiftsansvariga domstolen som i enlighet med huvudregeln i 4 § arkivlagen ska svara för vården av sitt arkiv. Denna lösning tillgodoser bäst och smidigast allmänhetens rätt att ta del av allmänna handlingar samt rättskipningens och förvaltningens behov av information. Att Domstolsverket utformar domstolarnas verksamhets-system eller anlitas som personuppgiftsbiträde åt domstolarna innebär inte att ansvaret för domstolarnas arkiv i stället bör ligga på verket. Så länge en domstols arkiv inte har övertagits av en arkivmyndighet är det alltså den personuppgiftsansvariga domstolen som ska pröva frågor om utlämnande av allmänna handlingar ur arkivet. Detta gäller oavsett om det är fråga om utlämnande av uppgifter ur manuella eller elektroniska arkiv. Någon särskild reglering för utlämnande av uppgifter ur elektroniska arkiv behövs enligt regeringen inte.

Ett särskilt integritetsskydd för uppgifter i avgjorda mål och ärenden

Ett elektroniskt bevarande av personuppgifter i mål och ärenden ska alltså styras av det arkivrättsliga regelverket. Dessa regler är dock inte

utformade med någon särskild hänsyn till de integritetsrisker som är förknippade med elektroniskt bevarande. Sådana risker kan uppstå framför allt om uppgifterna blir åtkomliga för automatiserade sökningar och sammanställningar. Möjligheterna till direktåtkomst och annan spridning av uppgifterna kan också utgöra 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 §). Med hänsyn till integritetsskyddet är det dock rimligt att begränsa domstolarnas och allmänhetens åtkomst till uppgifter i mål och ärenden när handläggningen avslutats genom ett lagakraftvunnet avgörande. Det bör därför inte sedan handläggningen av ett mål eller ärende har avslutats och domen eller beslutet har fått laga kraft vara möjligt för domstolarna att fortsätta hantera elektroniska personuppgifter på samma sätt som då handläggningen pågick.

I domstolsdatalagen bör det därför tas in en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela ytterligare föreskrifter om begränsningar för behandling av personuppgifter som hänför sig till ett mål eller ärende som har avgjorts genom en dom eller ett beslut som har fått laga kraft. Exempelvis kan det behövas begränsningar avseende sökning, direktåtkomst eller intern åtkomst vid domstolarna. Det är fråga om bestämmelser som bör vara relativt detaljerade och som bör kunna justeras ganska ofta, exempelvis när domstolarnas arbetssätt utvecklas eller då nya måltyper tillkommer i verksamheterna. En mer detaljerad reglering ger också bättre förutsättningar för att optimera den avvägning som ska göras mellan integritets- och effektivitetsintressena. Det är viktigt att domstolarna har möjlighet att i den utsträckning det är motiverat utnyttja de möjligheter till ökad effektivitet, rättssäkerhet och insyn som erbjuds tack vare övergången till elektroniskt bevarande. I linje med vad *Förvaltningsrätten i Malmö* anför finns det berättigade skäl för domstolarna att exempelvis på elektronisk väg göra sökningar på namn och person- eller organisationsnummer. Det bör också beaktas att domstolarna kan ha behov av att ha direktåtkomst till arkiverade uppgifter i viss utsträckning, såsom *Kammarrätten i Sundsvall* framhåller. Av rättsäkerhetsskäl kan det också vara viktigt med åtkomst till uppgifter i avslutade mål och ärenden vid exempelvis ansökan om resning, vilket *Uppsala universitet* anför. Av integritetsskyddsskäl kan det dock finnas behov av att införa tidsfrister beträffande möjligheterna till både sökningar och direktåtkomst så att regleringen kan göras mer restriktiv ju längre tid som har förflutit sedan det aktuella målet eller ärendet avgjordes.

14 Insyn och tillsyn

14.1 Enskildas insyn i personuppgiftsbehandlingen

Regeringens förslag: Den som är personuppgiftsombud ska föra en särskild förteckning över den personuppgiftsbehandling som sker med stöd av domstolsdatalagen. Den personuppgiftsansvarige är, på samma sätt som enligt personuppgiftslagen, skyldig att på begäran lämna sådan information till enskilda.

I lagen upplyses det om att regeringen eller den myndighet som regeringen bestämmer kan meddela närmare föreskrifter om vilka uppgifter som den aktuella förteckningen ska innehålla.

Promemorians förslag överensstämmer i huvudsak med regeringens. I promemorian föreslås dock att den personuppgiftsansvarige ska vara skyldig att föra förteckningen i stället för den som är utsedd till personuppgiftsombud.

Remissinstanserna: Flertalet remissinstanser tillstyrker promemorians förslag eller har ingen invändning mot det. *Kammarrätten i Stockholm* konstaterar att en skyldighet att upprätta och löpande föra en förteckning sannolikt kommer att medföra ett betydande merarbete för domstolarna och att förteckningen därför inte torde kunna bli annat än mycket allmänt hållen. *Hovrätten över Skåne och Blekinge* anser att det bör eftersträvas att alla domstolar ska ha samma utformning av de förteckningar som förs. *Göta hovrätt* anser att förslaget torde medföra en betungande informationsskyldighet för domstolarna. Vidare anser hovrätten att en hänvisning till en paragraf i personuppgiftslagen (1998:204, PUL) bör förtydligas.

Skälen för regeringens förslag

Enskildas rätt till insyn i domstolsprocessen

Enskildas insyn i domstolarnas personuppgiftsbehandling är en viktig aspekt av personuppgiftsskyddet eftersom insynen möjliggör för enskilda att försäkra sig om att domstolarnas personuppgiftsbehandling sker i enlighet med gällande regler, t.ex. att uppgifterna ska vara riktiga och behandlas för tillåtna ändamål.

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, de processuella regelverken, framför allt rättegångsbalken och förvaltningsprocesslagen (1971:291). 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 och att den enskilde som är part har en mycket långtgående rätt till insyn och dessutom själv bidrar med många av de uppgifter som tillförs målet.

Årlig information

Enligt nuvarande ordning är reglerna i personuppgiftslagen, om den personuppgiftsansvariges skyldighet att lämna besked till en enskild om att han eller hon är föremål för personuppgiftsbehandling, tillämpliga i domstolarnas verksamhet. Sådan information ska lämnas utan kostnad en gång per kalenderår till var och en som ansöker om det. Om uppgifter behandlas ska information också 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. Under förutsättning att uppgifterna inte har lämnats ut till tredje man behöver information dock inte lämnas om personuppgifter i löpande text som inte har fått sin ursprungliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. (26 § PUL)

Enligt regeringen bör en sådan informationsskyldighet även gälla enligt domstolsdatalagen. Det bidrar till öppenhet och transparens kring vilka personuppgiftsbehandlingar som domstolarna utför. Även ur integritetssynpunkt är det viktigt med regler som ger den registrerade rätt till information av den personuppgiftsansvarige om vilka uppgifter som är föremål för behandling. Genom en sådan reglering får den enskilde möjlighet att kontrollera om han eller hon är registrerad och, om så är fallet, att de registrerade personuppgifterna är riktiga vilket bidrar till den enskildes skydd mot felaktig personuppgiftsbehandling. Såvitt framkommit har denna informationsskyldighet, som alltså finns redan i dag, inte medfört några problem eller någon betungande administration i domstolarnas verksamhet. Mot den bakgrunden bör enligt regeringen en hänvisning till 26 § PUL tas in i domstolsdatalagen. En hänvisning bör även göras till 27 § PUL som innebär att rätten till information inte gäller 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. Information ska därmed inte lämnas om sådana förhållanden för vilka det gäller sekretess.

En förteckning över personuppgiftsbehandlingar

Enligt 36 § första stycket PUL ska automatiserade behandlingar av personuppgifter anmälas till tillsynsmyndigheten (Datainspektionen). Domstolarna omfattas dock inte av någon sådan anmälningskyldighet. Detta hänger samman med att anmälningskyldigheten enligt personuppgiftslagen inte gäller för behandlingar som regleras genom särskilda föreskrifter i lag eller förordning såsom i Vera-förordningarna eller den föreslagna domstolsdatalagen. Någon hänvisning till 36 § första stycket PUL behövs därför inte (3 § personuppgiftsförordningen [1998:1191]). Enligt regeringen finns det dock anledning att överväga om domstolarna bör vara skyldiga att sammanställa och göra tillgänglig den information som en sådan anmälan skulle ha innehållit. Det skulle exempelvis röra sig om uppgifter om ändamålet med behandlingen och en beskrivning av den eller de kategorier av registrerade som berörs av behandlingen. 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 med mer preciserad 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 uppräknings av vilka personuppgiftsbehandlingar som ska vara tillåtna (avsnitt 6.1).

Om domstolarna åläggs en skyldighet att föra en förteckning över sina personuppgiftsbehandlingar innebär det ett visst merarbete och kostnader för att inledningsvis upprätta förteckningen och att fortlöpande uppdatera den. Till skillnad från *Kammarrätten i Stockholm* anser regeringen dock att det inte kommer att medföra något betydande merarbete för domstolarna att upprätta och löpande föra en sådan förteckning. Såsom konstateras i promemorian kan detta arbete effektiviseras genom att Domstolsverket hjälper domstolarna att ta fram relevanta förteckningar.

Mot denna bakgrund anser regeringen att en generell skyldighet för domstolarna att föra en förteckning över sina personuppgiftsbehandlingar bör gälla enligt domstolsdatalagen. Enligt promemorians förslag är det den personuppgiftsansvarige som ska anges som ansvarig för att föra förteckningen. I likhet med vad som gäller enligt 2 kap. 2 § polisdatalagen (2010:361) anser regeringen emellertid att det bör vara personuppgiftsombudet eller personuppgiftsombuden som har ansvaret för att föra förteckningen. *Hovrätten över Skåne och Blekinge* anser att det bör eftersträvas att alla domstolar ska ha samma utformning av de förteckningar som förs. Såsom anförs i promemorian bör det dock finnas utrymme att anpassa förteckningarna till de rådande förhållandena hos varje enskild domstol. Det kan även finnas situationer då det framstår som motiverat att utforma förteckningarna på olika sätt för exempelvis olika domstolsslag. Detta talar enligt regeringen för att förteckningarna inte nödvändigtvis bör utformas på samma sätt för alla domstolar. De närmare kraven på innehållet i förteckningarna kan 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. Av 42 § PUL följer en skyldighet för den personuppgiftsansvarige att till var och en som begär det skyndsamt och på lämpligt sätt lämna upplysningar om sina behandlingar av personuppgifter. Vidare framgår att upplysningarna ska omfatta i princip samma information som ska framgå av den förteckning som domstolarna föreslås bli skyldiga att föra. Enligt regeringen bör en motsvarande skyldighet 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 insyn i domstolarnas personuppgiftsbehandling är att införa en skyldighet för den personuppgiftsansvarige att under vissa förutsättningar lämna information till den registrerade. Sådana bestämmelser finns i 23–25 §§ PUL. Bestämmelserna är enligt nuvarande ordning tillämpliga i domstolarnas rättskipande och rättsvårdande verksamhet.

Enligt 23 § PUL ska den personuppgiftsansvarige i samband med att personuppgifter samlas in självant lämna den registrerade information om behandlingen av uppgifterna. Av 25 § 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. Information behöver dock inte lämnas om sådant som den registrerade redan känner till. Regeringen anser, i likhet med vad som anförs i promemorian, att de registrerade som skickar in uppgifter till domstolarna (exempelvis parterna) i de flesta fall torde känna till vilka uppgifter som kommer att behandlas vid domstolarna eftersom detta framgår direkt av domstolsdatalagen, av den förteckning som domstolarna föreslås vara skyldig att sammanställa och av de processuella regelverken som styr domstolarnas verksamhet. Detta innebär att domstolarna i praktiken sällan torde behöva lämna särskild information till den registrerade även om 23 och 25 §§ PUL görs tillämpliga för domstolarna. *Göta hovrätt* anser att promemorians förslag om att göra 23 § PUL tillämplig enligt domstolsdatalagen innebär att domstolarna kommer att vara skyldiga att underrätta t.ex. parter och vittnen om att deras personuppgifter kommer att behandlas och att en strikt tillämpning av denna paragraf torde innebära en betungande informationsskyldighet för domstolarna. Det bör dock poängteras att promemorians förslag om att införa en hänvisning till 23 och 25 §§ PUL i domstolsdatalagen inte innebär någon ändring av gällande rätt. Såvitt framkommit har domstolarnas tillämpning av 23 och 25 §§ PUL inte medfört några problem eller betungande administration i domstolarnas verksamhet.

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 anser regeringen, i likhet med vad som anförs i promemorian, att dessa bestämmelser även fortsättningsvis bör vara tillämpliga i domstolarnas rättskipande och rättsvårdande verksamhet. Det bör därför i domstolsdatalagen tas in en hänvisning till bestämmelserna i 23 och 25 §§ PUL.

Informationsskyldigheten enligt 23 § PUL gäller i de fall uppgifter om en person samlas in från personen själv. I 24 § PUL föreskrivs en skyldighet för den personuppgiftsansvarige att självant 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 i domstolsdatalagen, rättegångsbalken, förvaltningsprocesslagen och övrig lagstiftning som styr domstolarnas verksamhet. Enligt regeringen bör det därför inte tas in någon hänvisning till 24 § PUL i domstolsdatalagen. Såsom *Göta hovrätt* uppmärksammar hänvisar 25 § PUL till både 23 och 24 §§ samma lag. Till skillnad mot hovrätten anser regeringen dock att det inte behövs något förtydligande i domstolsdatalagen om att 25 § PUL endast gäller i förhållande till 23 § PUL. Någon risk för tillämpningssvårigheter kan inte förutses. Förslaget i denna del är för övrigt identiskt med motsvarande reglering i 2 kap. 2 § första stycket polisdatalagen.

14.2 Tillsynsmyndighet

Regeringens förslag: I domstolarnas rättskipande och rättsvårdande verksamhet har tillsynsmyndigheten samma befogenheter att utöva tillsyn som enligt personuppgiftslagen, med undantag för möjligheten att utfärda vitesföreläggande.

Regeringen har, på samma sätt som enligt personuppgiftslagen, möjlighet att föreskriva att vissa särskilt känsliga behandlingar ska anmälas till tillsynsmyndigheten för förhandskontroll.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: Endast ett fåtal remissinstanser kommenterar förslaget. *Riksdagens ombudsmän (JO)* anser att Datainspektionen inte bör ha möjlighet att under vissa förutsättningar meddela förbud för domstolarna att behandla personuppgifter på annat sätt än genom att lagra dem. *Förvaltningsrätten i Göteborg* anser att det mot bakgrund av de allvarliga konsekvenser som ett förbud om att domstolarna inte får behandla personuppgifter på annat sätt än genom att lagra dem skulle medföra för rättssäkerheten, tilltron till rättsväsendet och för enskildas möjlighet att ta tillvara sin rätt bör övervägas om det i lagstiftningen bör uttryckas att tillsynsmyndigheten i det längsta ska undvika att tillgripa denna åtgärd. Alternativt bör det, enligt förvaltningsrätten, övervägas om det finns något annat, mindre ingripande påtryckningsmedel. *Göta hovrätt* ifrågasätter om det är lämpligt att tillsynsmyndigheten ska kunna ansöka hos förvaltningsrätten om att personuppgifter som har behandlats på ett olagligt sätt ska utplånas och att förvaltningsrätten ges befogenhet att fatta beslut i denna fråga. Förvaltningsrätten i Göteborg konstaterar att forumregeln i personuppgiftslagen innebär att en ansökan om att personuppgifter som har behandlats på ett olagligt sätt ska utplånas ska prövas av Förvaltningsrätten i Stockholm och anser att det framstår som oklart vilken domstol som ska pröva en ansökan avseende Förvaltningsrätten i Stockholm. Övriga remissinstanser tillstyrker eller har inte något att invända mot promemorians förslag.

Skälen för regeringens förslag: 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 ska behandlas (se avsnitt 9.1). Vidare framgår av 43 § PUL att tillsynsmyndigheten har möjlighet att på begäran få tillgång till de personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen och säkerheten vid denna och tillträde till lokaler. De redovisade bestämmelserna är enligt nuvarande ordning tillämpliga i domstolarnas rättskipande och rättsvårdande verksamhet. Regeringen anser, i likhet med promemorian, att tillsynsmyndigheten även i fortsättningen bör ha samma befogenheter som enligt den nuvarande ordningen. En hänvisning till de aktuella paragraferna bör därför tas in i domstolsdatalagen.

Datainspektionen har, enligt 44 § PUL, möjlighet att vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än genom att lagra dem, om myndigheten inte efter begäran enligt 43 § PUL kan få tillräckligt underlag för att konstatera att behandlingen av personuppgifter är laglig. Ett sådant förbud får även meddelas enligt 45 § PUL om det inte går att få till stånd rättelse genom påpekanden eller liknande förfaranden mot felaktig personuppgiftsbehandling, eller om saken är brådskande. Även ett sådant förbud kan förenas med vite.

Frågan är om Datainspektionen bör ha rätt att meddela förbud av nu aktuellt slag. Som *JO* och *Förvaltningsrätten i Göteborg* konstaterar kan ett förbud för en domstol att behandla personuppgifter på något annat sätt än genom att lagra dem i många fall innebära att verksamheten blockeras, vilket kan ha allvarliga följder för rätts säkerheten, tilltron till rättsväsendet och för enskildas möjligheter att ta tillvara sin rätt. *JO* anser därför att Datainspektionen inte bör ha möjlighet att meddela denna typ av förbud. Regeringen konstaterar dock att 44 och 45 §§ PUL enligt den nuvarande ordningen är tillämpliga i domstolarnas rättskipande och rättsvårdande verksamhet. Det följer av de aktuella bestämmelserna att Datainspektionens möjligheter att besluta om förbud är begränsade. Enligt regeringen bör Datainspektionen även fortsättningsvis ha den principiella möjligheten att förbjuda viss behandling. Genom de redovisade bestämmelserna får Datainspektionen också goda möjligheter att stödja domstolarna i deras arbete med att säkerställa integritetsskyddet i verksamheten. Förvaltningsrätten i Göteborg anser att det bör övervägas om det på något sätt ska komma till uttryck i lagstiftningen att Datainspektionen i det längsta ska undvika att meddela sådana förbud. Enligt regeringen behövs det dock inte någon uttrycklig reglering om detta i domstolsdatalagen. Det får anses tillräckligt att på samma sätt som polisdatalagen hänvisa till de aktuella paragraferna i personuppgiftslagen.

En ytterligare fråga är om det bör vara möjligt för Datainspektionen att förena ett förbud av nu aktuellt slag med vite. I polisdatalagen och flera andra 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, se prop. 2004/05:164 s. 54, propositionen Person-

uppgiftsbehandling hos Försvarmakten och Försvarets radioanstalt (prop. 2006/07:46 s. 105) och prop. 2009/10:85 s. 90. Samma skäl gör sig i högsta grad gällande i förhållande till domstolarna. Domstolsdatalagen bör alltså 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. Bestämmelsen har sin grund i dataskyddsdirektivet (artikel 28.3). Där anges att varje nationell tillsynsmyndighet ska ha befogenhet 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. Regeringen anser, i likhet med promemorian, att Datainspektionen för att tillgodose direktivets krav bör ha möjlighet att ansöka om utplåning av uppgifter i domstolarnas rättskipande och rättsvårdande verksamhet. Detta åstadkoms genom en hänvisning till 47 § PUL. 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.

Såsom *Förvaltningsrätten i Göteborg* konstaterar ska en ansökan om utplåning enligt 47 § PUL prövas av förvaltningsrätten inom vars domkrets tillsynsmyndigheten är belägen. Eftersom Datainspektionen är belägen i Stockholm ska denna fråga, enligt nuvarande forumregler, alltså prövas av Förvaltningsrätten i Stockholm. Förvaltningsrätten i Göteborg ställer frågan vilken domstol som ska pröva en ansökan som innefattar påståenden att personuppgifter har behandlats på ett olagligt sätt av Förvaltningsrätten i Stockholm. Regeringen konstaterar att forumregeln i 47 § PUL redan nu gäller i domstolarnas verksamhet och att det inte framkommit några problem med den nuvarande ordningen. Det förekommer även på andra områden att en domstol kan vara part i ett mål eller ärende som handläggs vid samma domstol. Någon särskild forumregel för det nu aktuella fallet behövs därför inte.

Enligt nuvarande ordning gäller även regeringens möjlighet att, med stöd av 41 § PUL, föreskriva att vissa särskilt känsliga behandlingar ska anmälas till Datainspektionen för förhandskontroll i domstolarnas verksamhet. 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 anges i 41 § PUL såvitt gäller domstolarnas verksamhet, saknas det skäl att inte behålla denna möjlighet. En hänvisning till nämnda bestämmelse bör därför, precis som i polisdatalagen, införas i domstolsdatalagen.

14.3 Personuppgiftsombud

Regeringens förslag: Den personuppgiftsansvarige ska utse ett eller flera personuppgiftsombud. Den personuppgiftsansvarige ska anmäla till Datainspektionen när ett personuppgiftsombud utses eller entledigas. Personuppgiftslagens bestämmelser om personuppgiftsombudets uppgifter gäller i domstolarnas verksamhet.

Promemorians förslag överensstämmer med regeringen.

Remissinstanserna: Samtliga remissinstanser tillstyrker promemorians förslag eller har ingen invändning mot det.

Skälen för regeringens förslag: I personuppgiftslagen föreskrivs en möjlighet för den personuppgiftsansvarige att utse ett personuppgiftsombud. 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. I första hand ska personuppgiftsombudet påpeka brister i uppgiftsbehandlingen för den personuppgiftsansvarige, men om den ansvarige inte rättar till bristerna är ombudet skyldigt att anmäla förhållandena 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 en valfrihet för den personuppgiftsansvarige att själv bestämma om ett sådant ombud ska utses. Det obligatoriska kravet för polisen på att utse personuppgiftsombud har enligt förarbetena till polisdatalagen motiverats med 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). I 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 utförs obefogade integritetskänsliga behandlingar avseende personuppgifter får därför anses vara mindre än inom polisen.

Enligt regeringen finns det dock flera fördelar med att göra det obligatoriskt för domstolarna att utse ett personuppgiftsombud. 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 enligt regeringen vara obligatoriskt för domstolarna att utse ett eller flera personuppgiftsombud. Regeringen lämnar därför, i likhet med promemorian, ett förslag om att domstolarna ska vara skyldiga att utse

personuppgiftsombud. Av 36 § andra stycket PUL framgår att den personuppgiftsansvarige ska anmäla till Datainspektionen när ett personuppgiftsombud utses och entledigas. Detta bör även gälla enligt domstolsdatalagen. Skyldigheten att utse personuppgiftsombud och anmäla dessa till Datainspektionen bör framgå direkt av domstolsdatalagen.

Det finns enligt regeringen 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.

15 Rättsmedel

15.1 Åtgärder vid felaktig personuppgiftsbehandling

Regeringens förslag: Den personuppgiftsansvarige är, på samma sätt som enligt personuppgiftslagen, skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna personuppgifter som har behandlats felaktigt i domstolarnas verksamhet. Den personuppgiftsansvarige har även samma skyldighet som enligt personuppgiftslagen att underrätta tredje man om sådana åtgärder.

Den registrerade har samma rätt som enligt personuppgiftslagen att få skadestånd vid skada eller kränkning som uppstår när personuppgifter behandlas på ett felaktigt sätt.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: Samtliga remissinstanser tillstyrker promemorians förslag eller har ingen invändning mot det.

Skälen för regeringens förslag

Skyldigheten att rätta felaktigt behandlade uppgifter

Enligt 9 § första stycket i personuppgiftslagen (1998:204, PUL), till vilken domstolsdatalagen ska hänvisa (se avsnitt 8.1), 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 snarast 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 under rättelse 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 i 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, enligt regeringen, 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.

Rätt till skadestånd

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.

Personuppgiftslagens bestämmelser om skadestånd är enligt gällande rätt tillämpliga i domstolarnas rättskipande och rättsvårdande verksamhet. Om personuppgifter skulle behandlas i strid med domstolsdatalagen är det principiellt viktigt att den som drabbas av skada eller kränkning även fortsättningsvis på ett rimligt sätt kan kompenseras genom skadestånd. En hänvisning till 48 § PUL bör därför tas in i domstolsdatalagen.

15.2 Överklagande

Regeringens förslag: Beslut av domstol om upplysningar till allmänheten, om information och om rättelse och underrättelse till tredje man får överklagas. Högsta domstolens och Högsta förvaltningsdomstolens beslut får dock inte överklagas.

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

Beslut av en hyres- eller arrendenämnd överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs i dessa fall vid överklagande till kammarrätten.

Datainspektionens beslut får, på samma sätt som enligt personuppgiftslagen, överklagas till allmän förvaltningsdomstol. Datainspektionens möjlighet att enligt personuppgiftslagen bestämma att dess beslut ska gälla även om det överklagas gäller dock inte i domstolarnas verksamhet.

Promemorians förslag överensstämmer i huvudsak med regeringens. I promemorian föreslås en annan lagteknisk lösning.

Remissinstanserna: De flesta remissinstanserna tillstyrker promemorians förslag eller har ingen invändning mot det. *Förvaltningsrätten i Göteborg* ställer frågan vilken domstol som ska pröva ett överklagande av Datainspektionens beslut som riktar sig mot exempelvis Högsta förvaltningsdomstolen eller Förvaltningsrätten i Stockholm. Förvaltningsrätten i Göteborg anser att det bör övervägas att

utförligt och samlat i domstolsdatalagen ange samtliga de beslut som avses kunna överklagas. Liknande synpunkter framförs av *Förvaltningsrätten i Malmö*.

Skälen för regeringens förslag

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 hos allmän förvaltningsdomstol (förvaltningsrätt).

Frågan är inledningsvis vilka beslut enligt domstolsdatalagen som ska kunna överklagas. 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 propositionen Översyn av personuppgiftslagen (prop. 2005/06:173 s. 52). Beslut enligt 26 och 28 §§ PUL, till vilka domstolsdatalagen ska hänvisa, bör mot denna bakgrund kunna överklagas. Även beslut om upplysningar till allmänheten, som enligt vad regeringen föreslår i avsnitt 14.1 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.

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 förvaltningsrätts beslut överklagas till kammarrätt, kammarrätts beslut till Högsta förvaltningsdomstolen och att tingsrätts och hovrätts beslut överklagas till kammarrätt. Det är också vad som gäller för beslut om utlämnande av handling i domstolarnas administrativa verksamhet enligt offentlighets- och sekretesslagen (6 kap. 8 § offentlighets- och sekretesslagen [2009:400]). Den nu redovisade instansordningen framstår som ändamålsenlig och bör gälla även vid överklagande av beslut enligt domstolsdatalagen.

De beslut som är överklagbara utgör administrativa beslut i respektive domstol. Kammarrätten 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 kammarrätt.

Högsta domstolen är högsta allmänna domstol och Högsta förvaltningsdomstolen är högsta förvaltningsdomstol (11 kap. 1 § regeringsformen). Av detta följer att dessa domstolars avgöranden inte kan överklagas. Högsta domstolens och Högsta förvaltningsdomstolens egna 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- eller 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 och att prövningstillstånd krävs vid överklagande till kammarrätt.

Beslut av tillsynsmyndigheten

I avsnitt 14.2 föreslås att Datainspektionen ska kunna besluta om säkerhetsåtgärder enligt 32 § PUL och förbud enligt 44 eller 45 § PUL. I likhet med vad som gäller enligt personuppgiftslagen bör sådana beslut kunna överklagas till allmän förvaltningsdomstol och prövningstillstånd bör krävas vid överklagande till kammarrätten (51 § första stycket och 53 § andra stycket PUL). Denna överklagandebestämmelse bör utformas på samma sätt som i personuppgiftslagen.

Såsom *Förvaltningsrätten i Göteborg* konstaterar kan Datainspektionen fatta beslut som riktar sig mot en personuppgiftsansvarig domstol. Eftersom Datainspektionen är belägen i Stockholm är det Förvaltningsrätten i Stockholm som är behörig att pröva ett överklagande från en domstol vilket avser ett sådant beslut. Detta följer av den allmänna forumregeln i 14 § andra stycket lagen (1971:289) om allmänna förvaltningsdomstolar. Förvaltningsrätten i Göteborg ställer frågan vilken domstol som ska pröva ett överklagande om tillsynsmyndighetens beslut riktar sig mot t.ex. Högsta förvaltningsdomstolen eller Förvaltningsrätten i Stockholm. Innebörden av regeringens förslag är att ett sådant beslut överklagas till Förvaltningsrätten i Stockholm. Det förekommer redan på andra områden att en domstol kan vara part i ett mål eller ärende som handläggs vid samma domstol eller i en annan instans. Forumregeln i 14 § andra stycket lagen om allmänna förvaltningsdomstolar gäller redan nu vid överklaganden av beslut som Datainspektionen har rätt att meddela gentemot en personuppgiftsansvarig domstol med stöd av personuppgiftslagen. Det har inte framkommit att den nuvarande ordningen innebär några problem. Det behövs därför enligt regeringen inte någon särskild forumregel beträffande sådana beslut av Datainspektionen som riktar sig mot Högsta förvaltningsdomstolen eller Förvaltningsrätten i Stockholm i egenskap av personuppgiftsansvariga.

Enligt 51 § andra stycket PUL får Datainspektionen i egenskap av tillsynsmyndighet bestämma att dess beslut ska gälla även om det överklagas. Regeringen delar promemorians bedömning att det inte finns något praktiskt behov av att ge Datainspektionen en sådan möjlighet och lämnar därför inte något sådant förslag, jfr propositionen Kustbevakningsdatalag (prop. 2011/12:45 s. 87) angående motsvarande bedömning för Kustbevakningen.

Övriga frågor

I avsnitt 14.2 föreslås att Förvaltningsrätten i Stockholm, efter ansökan av Datainspektionen, ska kunna besluta att sådana personuppgifter som har behandlats på ett olagligt sätt ska utplånas. Såsom *Förvaltningsrätten i Göteborg* uppmärksammar bör naturligtvis förvaltningsrättens dom i ett sådant mål kunna överklagas enligt förvaltningsprocesslagen (1971:291) på samma sätt som gäller för förvaltningsrättens domar i allmänhet. I personuppgiftslagen har detta förtydligats i 53 §. Av denna bestämmelse

följer även att prövningstillstånd krävs vid överklagande till kammarrätten i dessa fall. En motsvarande bestämmelse bör tas in i domstolsdatalagen.

I promemorian föreslås att domstolsdatalagen ska hänvisa till personuppgiftslagens överklagandebestämmelser och att kompletterande överklagandebestämmelser ska tas in i domstolsdatalagen. Denna lösning kan visserligen sägas vara i linje med hur domstolsdatalagen är uppbyggd i övrigt. I fråga om överklagandebestämmelserna anser dock regeringen, i likhet med *Förvaltningsrätten i Göteborg* och *Förvaltningsrätten i Malmö*, att denna lagtekniska lösning leder till en alltför oöverskådlig reglering. Det bör därför anges direkt i domstolsdatalagen vad som gäller i fråga om överklagande av Datainspektionens beslut och av domstolarnas beslut och domar.

16 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag och bedömning: Domstolsdatalagen träder i kraft den 1 januari 2016. Några särskilda övergångsbestämmelser behövs inte.

Promemorians förslag och bedömning överensstämmer delvis med regeringens. I promemorian föreslås ett tidigare ikraftträdande.

Remissinstanserna: De flesta remissinstanser tillstyrker promemorians förslag och bedömning eller har ingen invändning mot dem. *Domstolsverket* ifrågasätter om promemorians förslag om ikraftträdande är realistiskt. Verket förutser behov av stora systemändringar i domstolarnas datorsystem som tar tid att genomföra och kräver stora resurser. *Kammarrätten i Sundsvall* anser att de praktiska problem som följer av begränsningen av tillgången till personuppgifter till vad domstolens personal behöver för att fullgöra sina arbetsuppgifter måste beaktas i fråga om tiden för ikraftträdandet.

Skälen för regeringens förslag och bedömning: Den nya lagstiftningen om behandling av personuppgifter i domstolarnas rättskipande och rättsvårdande verksamhet bör träda i kraft den 1 januari 2016. Regeringen gör i avsnitt 17 bedömningen att det inte kommer att krävas några omfattande anpassningar av datorsystemen för att uppfylla domstolsdatalagens krav. De anpassningar som kan behövas av befintliga datorsystem bör kunna genomföras före lagens ikraftträdande.

Det behövs inga särskilda övergångsbestämmelser.

Regeringens bedömning: Genom förslagen skapas ett förstärkt integritetsskydd som är bättre anpassat till de risker som är förknippade med användningen av modern teknik. Samtidigt skapar förslagen 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. Vidare innebär förslagen att domstolarna kan ge både parter och allmänheten bättre service, insyn i domstolsprocesserna och tillgång till information.

De kostnader som inledningsvis kan uppkomma hos domstolarna ryms inom domstolarnas befintliga ekonomiska ramar. Förslagen bedöms inte heller leda till några ökade kostnader för andra myndigheter eller för enskilda.

Promemorians bedömning överensstämmer med regeringens.

Remissinstanserna: Remissutfallet är blandat. Många remissinstanser anser att förslagen medför behov av ökade resurser till domstolarna. Bland andra *Attunda tingsrätt*, *Kammarrätten i Jönköping* och *Domstolsverket* anser att promemorians förslag om direktåtkomst mellan domstolarna, i kombination med möjligheten att söka efter personuppgifter hos en annan domstol, kommer att leda till en ökning av antalet beställningar från medieföretag och allmänhet av domar och beslut. *Förvaltningsrätten i Göteborg* bedömer att förslaget om att tillåta sökningar efter mer detaljerade sökbegrepp och känsliga personuppgifter kan innebära att fler sekretessprövningar kan bli nödvändiga jämfört med i dag. För att kunna hantera detta krävs att domstolarna tillförs ytterligare resurser. *Attunda tingsrätt* för ett liknande resonemang. Några domstolar anser att konsekvenserna av förslaget om att begränsa tillgången till personuppgifter till vad domstolens personal behöver för att fullgöra sina arbetsuppgifter inte är tillräckligt belysta i promemorian. *Kammarrätten i Jönköping* påpekar att den föreslagna regleringen kan leda till att domstolarnas verksamhetsstöd Vera kan behöva byggas om vilket kräver resurser. Liknande synpunkter framförs av *Kammarrätten i Sundsvall* som anser att en sådan reglering kommer att kräva en mängd nya funktioner i Vera och att det är svåröverskådligt hur denna avgränsning ska ske i praktiken. De praktiska problem som detta innebär måste enligt kammarrätten beaktas vid bedömningen av kostnaden för genomförandet av förslaget. *Borås tingsrätt* ifrågasätter om Domstolsverket kommer att ha ekonomiska förutsättningar att utveckla de tekniska lösningar som regeln förutsätter. *Domstolsverket* ifrågasätter promemorians bedömning att lagförslaget inte kommer att förutsätta några mer omfattande anpassningar av verksamheten eller datorsystemen och att kostnaderna för att anpassa systemen ryms inom befintliga anslag. Enligt verket uppfyller de befintliga systemen inte lagens krav på begränsningen av tillgången till personuppgifter och systemen behöver därför byggas om. Även förslaget till nya sökmöjligheter kräver enligt verket en väsentlig

ombyggnad av Veras sökfunktioner. Vidare anser verket att det kommer att krävas extra resurser för att kunna införa ett förslag som innebär att varje enskild domstol självständigt ska kunna avgöra om direktåtkomst ska medges en annan domstol eller inte. Ett förslag som bygger på en skyldighet för domstolarna att göra detta vore mindre resurskrävande. Om Domstolsverket anvisar ett system som inte möjliggör direktåtkomst inom lagens ramar kan detta dessutom uppfattas som en indirekt styrning från verkets sida. Domstolsverket pekar dessutom på behovet av utbildning av personalen för att genomföra förslaget och att rutiner, instruktioner och informationsmaterial behöver tas fram vilket kräver resurser.

Skälen för regeringens bedömning

Sveriges Domstolar

Regeringens förslag innebär att det införs en ny lag, domstolsdatalagen, som syftar till att ge domstolarna möjlighet att behandla personuppgifter på ett effektivt och ändamålsenligt sätt och att skydda människor mot att deras personliga integritet kränks vid sådan behandling. Förslagen innebär en lagstiftning som är teknikneutral och möjliggör härigenom att nya datorsystem i framtiden kan tas i bruk utan att det blir nödvändigt att ändra regelverket. Förslagen medför också flexibilitet i fråga om möjligheterna för domstolarna att söka efter och få direktåtkomst till varandras personuppgifter. Detta främjar domstolarnas effektivitet och bidrar till en enhetlig rättstillämpning.

Många remissinstanser, bl.a. *Attunda tingsrätt*, *Kammarrätten i Jönköping* och *Domstolsverket*, anser att domstolens möjligheter att göra sökningar i handlingar från andra domstolar på begäran av allmänheten kommer att leda till en ökad arbetsbörda för domstolarna. Förslagen innebär emellertid inte någon skyldighet för domstolarna att inrätta sökfunktioner eller direktåtkomst. Frågan om direktåtkomst bör införas i domstolarna får i stället avgöras utifrån en bedömning av om det finns tillräckliga resurser och tekniska möjligheter för detta. Förslagen kan således inte i sig anses leda till några kostnader.

Genom att domstolarna kan ge bättre och snabbare tillgång till information kan de även ge bättre service till såväl parter som allmänheten. Förslagen innebär vidare att det skapas förutsättningar för domstolarna att 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. Risken för att förhandlingar behöver ställas in kan därmed minska vilket kan ha en kostnadsdämpande effekt på anslaget för Sveriges Domstolar.

Genom förslagen genomförs vidare 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 minskas.

Även om förslagen på olika sätt leder till effektiviseringar och andra förbättringar kan förslagen inledningsvis komma att orsaka vissa begränsade merkostnader för Sveriges Domstolar på grund av tekniska anpassningar. De krav som regleringen ställer bör dock kunna uppfyllas genom en anpassning av de befintliga systemen och genom utbildning, information och instruktioner till personalen. Förslagen är teknikneutrala och ställer således inte upp några krav beträffande vilka tekniska åtgärder som bör vidtas i fråga om exempelvis inrättandet av sökfunktioner eller begränsningen av tillgången till personuppgifter. Frågan om vilken anpassning som bör ske av de tekniska systemen är vidare en fråga som får bedömas fortlöpande utifrån domstolarnas olika förutsättningar och behov och med beaktande bl.a. av vad det skulle kosta att genomföra åtgärderna (jfr 31 § PUL). Några särskilda kostnader utöver vad som uppstår inom ramen för ordinarie utvecklingsarbete bör inte uppstå.

Ett annat förslag som kan antas medföra vissa begränsade merkostnader för domstolarna är domstolarnas skyldighet att upprätta en förteckning över de personuppgiftsbehandlingsprocesser som utförs med stöd av domstolsdatalagen. Regeringen bedömer dock att dessa insatser inte är mer omfattande än att de får anses utgöra en del av det ordinarie utvecklingsarbetet och de bör därför också rymmas inom befintliga anslag.

Några remissinstanser, bl.a. *Attunda tingsrätt* och *Kammarrätten i Jönköping*, anför att promemorians förslag till sökningar och direktåtkomst innebär att en domstol på grund av offentlighetsprincipen kan vara tvungen att på begäran göra en sökning på integritetskänsliga uppgifter vid den egna domstolen eller hos en annan domstol. Detta bedöms kunna öka arbetsbelastningen för domstolarna. Till skillnad mot promemorian föreslår regeringen dock att begränsningarna avseende möjligheterna att söka bör utformas så att de inte enbart gäller för domstolspersonalens användning av datorsystemen utan även skyddar mot de integritetsrisker som är förknippade med allmänhetens rätt att begära att sökningar utförs med stöd av offentlighetsprincipen. Detta innebär att en domstol efter förfrågan från allmänheten inte kommer att kunna utföra sökningar på integritetskänsliga uppgifter vid den egna domstolen eller hos en annan domstol om personalen är förhindrad att utföra sökningarna för att tillgodose domstolens verksamhetsbehov. De förslag som nu lämnas bedöms inte medföra någon betydande ökning av resursåtgången i domstolarna.

Effekter för andra myndigheter och för enskilda

Förslagen innebär att myndigheter och enskilda med partsställning ska kunna ges direktåtkomst till personuppgifter i sina mål och ärenden. Parter och ombud kommer därigenom på sikt att kunna få möjlighet att föra sina processer mer effektivt. Detta kan underlätta och påskynda myndigheternas handläggning. Förslagen medför samtidigt att enskildas insyn i domstolsprocessen förbättras ytterligare.

Förutom möjligheten till direktåtkomst för enskilda parter leder förslagen till en rätt för den enskilde att ta del av domstolarnas förteckning över de personuppgiftsbehandlingsprocesser som utförs av domstolarna.

Bedömningar och avvägningar som har gjorts avseende förslagets konsekvenser för enskildas personliga integritet har redovisats under skälen för respektive förslag.

Förslagen innebär vidare att det skapas en grund för ett elektroniskt informationsutbyte mellan domstolarna och övriga deltagande myndigheter i RIF-arbetet.

Förslagen ger även ett tydligt rättsligt stöd för allmänheten att få ta del av uppgifter på elektronisk väg.

Några merkostnader för myndigheter med partsställning och andra deltagande myndigheter inom RIF förutses inte.

Förslagen bedöms inte ha några ekonomiska konsekvenser för övriga myndigheter, kommuner och landsting.

Den nya lagstiftningen bedöms inte ha någon påverkan på jämställdheten mellan män och kvinnor eller möjligheterna att nå de integrationspolitiska målen.

18 Författningskommentar

Lagens syfte

1 § Syftet med denna lag är att ge de allmänna domstolarna, de allmänna förvaltningsdomstolarna och 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 6.3.

I paragrafen anges att syftet med lagen är att ge domstolarna och nämnderna möjlighet att behandla personuppgifter på ett ändamålsenligt sätt och att skydda den personliga integriteten vid sådan behandling. Bestämmelsen har utformats med förebild i 1 kap. 1 § polisdatalagen (2010:361).

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas och hyres- och arrendenämndernas rättskipande och rättsvårdande verksamhet. Lagen gäller också när personuppgifterna vidarebehandlas i den administrativa verksamheten för att lämnas ut efter begäran.

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

Paragrafen anger tillämpningsområdet för domstolsdatalagen. Övervägandena finns i avsnitt 6.2.

I *första stycket* anges inledningsvis att lagen gäller vid behandling av personuppgifter. Med begreppet personuppgifter avses detsamma som i 3 § personuppgiftslagen (1998:204, PUL), dvs. all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet (jfr 5 § första stycket 1 nedan). 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, lagring, bearbetning och spridning. Lagen gäller för de allmänna domstolarna, de allmänna förvaltningsdomstolarna och hyres- och arrendenämnderna i deras rättskipande och rättsvårdande verksamhet. Till denna verksamhet räknas den handläggning som sker inom ramen för de processuella regelverken i exempelvis rättegångsbalken, förvaltningsprocesslagen (1971:291) och lagen (1996:242) om domstolsärenden. Även de särskilda domstolarna vid de allmänna domstolarna och de allmänna förvaltningsdomstolarna, dvs. mark- och miljödomstolarna respektive migrationsdomstolarna, omfattas av domstolsdatalagens tillämpningsområde.

Vidare är lagen tillämplig när en domstol eller nämnd vidarebehandlar personuppgifter från den rättskipande och rättsvårdande verksamheten i den administrativa verksamheten för att lämna ut uppgifterna på begäran. Detta innebär att när exempelvis en enskild eller en myndighet begär att få ta del av en dom, en partsinlaga eller någon annan handling från den rättskipande och rättsvårdande verksamheten ska domstolsdatalagen tillämpas även beträffande den vidarebehandling av personuppgifterna som sker i den administrativa verksamheten. Utanför lagens tillämpningsområde faller däremot behandling av personuppgifter i samband med de interna och administrativa åtgärder som kan förekomma i domstolarnas och nämndernas verksamhet, t.ex. i ett personal- och löneregister. När det gäller nämndemän behandlar domstolarna personuppgifter både i den rättskipande och rättsvårdande verksamheten och i den administrativa verksamheten. Den behandling som sker i direkt anslutning till hanteringen av mål och ärenden vid t.ex. upprättande av domar sker i den rättskipande och rättsvårdande verksamheten. När det däremot gäller exempelvis utbetalning av ersättning till nämndemän för deras medverkan i handläggningen av mål och ärenden sker behandlingen i den administrativa verksamheten.

I *andra stycket* anges att lagen är tillämplig endast 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 därmed helt manuell behandling av personuppgifter som inte ingår i någon sådan samling.

3 § Om det i lagen (2013:329) med vissa bestämmelser 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 lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen. Övervägandena finns i avsnitt 6.7.

I paragrafen anges att om det i den nämnda 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.

Förhållandet till personuppgiftslagen

4 § Om inte något annat anges i 5 §, gäller denna lag i stället för personuppgiftslagen (1998:204).

I paragrafen regleras förhållandet till personuppgiftslagen (1998:204). Övervägandena finns i avsnitt 6.4.

Bestämmelsen innebär att domstolsdatalagen inom sitt tillämpningsområde helt ersätter personuppgiftslagen, utom i de fall som uttryckligen anges i 5 §. Vid sådan personuppgiftsbehandling som omfattas av lagen ska alltså bestämmelser i personuppgiftslagen tillämpas endast om det finns en hänvisning till dem i 5 §. Polisdatalagen (2010:361) bygger på samma lagtekniska lösning.

5 § 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. 22 § om behandling av personnummer,
 5. 23 och 25–27 §§ om information till den registrerade,
 6. 28 § om rättelse,
 7. 30 och 31 §§ samt 32 § första stycket om säkerheten vid behandling,
 8. 33–35 §§ om överföring av personuppgifter till tredjeland,
 9. 38, 40 och 41 §§ om personuppgiftsombud m.m.,
 10. 43 och 44 §§, 45 § första stycket och 47 § om tillsynsmyndighetens befogenheter, och
 11. 48 § om skadestånd.
- Förbud enligt 44 eller 45 § personuppgiftslagen får inte förenas med vite.

Paragrafen innehåller hänvisningar till tillämpliga bestämmelser i personuppgiftslagen (1998:204, PUL). Övervägandena finns i avsnitt 6.5, 6.6, 7.2, 8.1, 9.1, 10.2, 12.3, 13, 14.1–14.3 och 15.1.

I *första stycket* anges vilka bestämmelser i personuppgiftslagen som ska gälla vid tillämpningen av domstolsdatalagen. Enligt 3 § gäller domstolsdatalagen i stället för personuppgiftslagen, varför bestämmelserna i personuppgiftslagen inte ska tillämpas vid sådan behandling av personuppgifter som omfattas av domstolsdatalagen. Vissa utpekade paragrafer i personuppgiftslagen ska dock tillämpas. Uppräkningen är uttömmande.

Enligt *första stycket 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 bl.a. begreppen personuppgifter, behandling, personuppgiftsansvarig, personuppgiftsombud och personuppgiftsbiträde. I 9 § finns dock en särskild bestämmelse om personuppgiftsansvar för den behandling som domstolen respektive nämnden utför.

I *första stycket 2* hänvisas till 8 § PUL, där det i första stycket anges att bestämmelserna i personuppgiftslagen inte ska tillämpas i den utsträckning det skulle inskränka en myndighets skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut handlingar. Genom domstolsdatalagens hänvisning till denna upplysningsbestämmelse 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 en myndighet arkiverar eller bevarar allmänna handlingar 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 första stycket 3 nedan). Regeringen eller den myndighet som regeringen bestämmer kan meddela särskilda föreskrifter om bevarande av uppgifter som hänför sig till ett mål eller ett ärende som avslutats genom ett lagakraftvunnet avgörande (se författningskommentaren till 17 §).

I *första stycket 3* hänvisas till 9 § PUL. Hänvisningen innebär bl.a. att den personuppgiftsansvarige (se 9 §) ska se till att uppgifterna behandlas enbart om det är lagligt och att de behandlas på ett korrekt sätt.

Den personuppgiftsansvarige ska också se till att de behandlade personuppgifterna är adekvata och relevanta i förhållande till ändamålen med behandlingen och att inte fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen (9 § första stycket e och f PUL). Vidare ska den personuppgiftsansvarige se till 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 g och 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. 195). 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 personuppgiftsbehandlingen, se propositionen *Behandling av personuppgifter inom skatt, tull och exekution* (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 och nämnderna att behandla personuppgifterna 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. 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 (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 utför 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 rättegångsbalken, förvaltningsprocesslagen (1971:291) och andra handläggnings- och förfaranderegler. Av dessa regelverk framgår bl.a. vilka uppgifter som ska fogas till ett mål eller ärende och vilka uppgifter som ska kommuniceras med parterna. 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. Genom att ange vissa primära och sekundära ändamål i 6 och 7 §§ har ställningstagandet gjorts att vidarebehandling för dessa ändamål är förenlig med finalitetsprincipen, och dessa bestämmelser utgör en uttömmande reglering av vilka ändamål personuppgifter får behandlas för i domstolarnas och nämndernas rättskipande och rättsvårdande verksamhet. Bestämmelsen i 9 § första stycket d PUL har därför ingen självständig funktion inom domstolsdatalagens tillämpningsområde men bestämmelsen kan ge ledning om det exempelvis i ett enskilt fall framstår som tveksamt om vidarebehandling för utlämnande enligt 7 § är tillåten. Hänvisningen till 9 § andra stycket PUL innebär att vidarebehandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål inte ska anses som oförenliga med de ändamål för vilka uppgifterna samlades in. Vid behandling för historiska, statistiska eller 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).

Vidare hänvisas i *första stycket 4* till 22 § PUL. Bestämmelsen innebär att uppgifter som personnummer eller samordningsnummer får behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Genom hänvisningen i *första stycket 5* 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 till vara 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 är skyldiga att sammanställa och av de processuella regelverk som styr domstolarnas verksamhet. Följden blir att domstolarna i praktiken sällan torde behöva lämna särskild information till den registrerade. Samma sak gäller hyres- och arrendenämnderna.

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. Informationsplikten gäller inte heller i den utsträckning det råder sekretess eller tystnadsplikt för informationen. Bestämmelserna innebär inga skyldigheter för domstolarna och nämnderna 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 (se prop. 1997/98:44 s. 81 f.).

Enligt hänvisningen i *första stycket 6* 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 till vilka lagen hänvisar – eller föreskrifter som har utfärdats i anslutning till lagen. Rättelse ska dock inte göras enbart därför att uppgifter som framstod som riktiga eller rimliga när de samlades in

senare har visat sig vara oriktiga. Vad gäller frågan om när uppgifter är att betrakta som oriktiga, se första stycket 3.

I *första stycket 7* 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 bitrådets eller den personuppgiftsansvariges ledning behandla personuppgifter enbart i enlighet med instruktioner från den personuppgiftsansvarige. Om det i lag eller annan författning finns särskilda bestämmelser om behandlingen av personuppgifter i det allmännas verksamhet, gäller dock – enligt 30 § tredje stycket – dessa i stället. Den sistnämnda bestämmelsen syftar särskilt på bestämmelser om tystnadsplikt och sekretess (se prop. 1997/98:44 s. 136). Enligt 30 § andra stycket PUL ska det i fråga om personuppgiftsbiträden finnas ett skriftligt avtal om bitrådets behandling för den personuppgiftsansvariges räkning. Det ska i avtalet särskilt föreskrivas att bitradet får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige och att bitradet 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. Om exempelvis Domstolsverket utför personuppgiftsbehandlingar för en domstols räkning behöver alltså domstolen och verket 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 § första stycket PUL får tillsynsmyndigheten i enskilda fall besluta om vilka åtgärder som den personuppgiftsansvarige ska vidta enligt 31 § samma lag. Med tillsynsmyndigheten avses här tillsynsmyndigheten enligt personuppgiftslagen, dvs. Datainspektionen, se 2 § personuppgiftsförordningen (1998:1191).

En hänvisning görs i *första stycket 8* till 33–35 §§ PUL. Enligt 33 § PUL är det förbjudet att överföra personuppgifter till tredjeland 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 tredjeland. 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 syften. Det är också enligt den paragrafen tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit sig till dataskyddskonventionen. Av 35 § PUL framgår att regeringen, och för vissa fall även den myndighet som regeringen bestämmer, kan meddela föreskrifter om undantag från förbudet i 33 § PUL. Det framgår av 3 § att det i annan lagstiftning finns särskilda bestämmelser om överföring till bl.a. medlemsstater i Europeiska unionen som har företrädare framför bestämmelserna i domstolsdatalagen.

I *första stycket 9* görs en hänvisning till 38 och 40 §§ PUL, där det framgår vilka närmare uppgifter ett personuppgiftsombud har. Domstolarna och nämnderna är enligt 10 § skyldiga att utse ett eller flera

personuppgiftsombud. Den som är personuppgiftsombud 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 första stycket 9 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 *första stycket 10* 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 Datainspektionen vidare förbjuda den personuppgiftsansvarige att fortsätta att behandla personuppgifterna på något annat sätt än genom att lagra dem. 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 *första stycket 11* 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.

Förbud enligt 44 eller 45 § PUL får normalt förenas med vite. Av *andra stycket* följer dock att förbud som meddelas i samband med tillsyn enligt domstolsdatalagen inte får förenas med vite.

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 8.2.

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 ta emot partsinlagor, föra protokoll vid förhandlingar eller göra tjänsteanteckningar. I 7 § regleras de s.k. sekundära ändamålen.

Under den nu aktuella ändamålsbestämmelsen faller alla åtgärder som behöver vidtas i ett mål eller ärende. Inom ändamålsbestämmelsens tillämpningsområde faller exempelvis mottagande av uppgifter, diarieföring, kommunicering, protokollföring, sökning efter relevant praxis, upprättande av dom och expediering. Det förutsätts emellertid inte att en behandling är nödvändig för handläggningen av ett specifikt mål eller ärende utan behandling kan ske även för planering, uppföljning och utvärdering av verksamheten vid domstolarna eller nämnderna. Planering, uppföljning och utvärdering anses vara en integrerad del av själva verksamheten (se prop. 2004/05:164 s. 66 f. och prop. 2009/10:85 s. 116) och omfattas alltså av den nu aktuella ändamålsbestämmelsen. Därigenom kan sökningar efter relevant praxis och hantering av sådana uppgifter ske, oavsett om åtgärderna sker i syfte att underlätta domskrivningsarbete, praxisdiskussioner eller annat kompetensutvecklingsarbete.

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 8.2.

Enligt bestämmelsen får personuppgifter som samlats in eller på annat sätt behandlas för handläggningen av mål och ärenden 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 §. Behandling av personuppgifter enligt 7 § förutsätter alltså att uppgifterna redan är föremål för behandling enligt 6 §. Oavsett om uppgiftslämnandet sker muntligt, genom utskrift på ett papper som lämnas ut eller genom t.ex. e-post är bestämmelsen tillämplig.

Genom domstolsdatalagens hänvisning till 8 § första stycket personuppgiftslagen (1998:204, PUL), se 5 § första stycket 2, tydliggörs att det alltid är tillåtet att utföra sådana behandlingar som är nödvändiga för att fullgöra skyldigheten enligt 2 kap. tryckfrihetsförordningen 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 Polismyndigheten och Kriminalvården eller om domar i upphandlingsmål till Konkurrensverket. De utlämnanden som behöver göras från domstolarna t.ex. för att genomföra RIF-samarbetet, för att framställa rättsstatistik eller för att tillgodose polisens behov av återkoppling sker i överensstämmelse med lag eller förordning. Det kan också vara fråga om uppgiftslämnande som domstolen är skyldig att utföra enligt en EU-förordning. En domstol eller nämnd har också enligt 6 kap. 5 § offentlighets- och sekretesslagen (2009:400), en skyldighet att på begäran av en annan myndighet lämna uppgift som domstolen eller nämnden förfogar över, om uppgiften inte är sekretessbelagd eller det skulle hindra arbetets behöriga gång. 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 (1986:223)

Tillgången till personuppgifter

8 § Tillgången till personuppgifter ska begränsas till det som varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om tillgången till personuppgifter.

Paragrafen, som är utformad efter mönster av 2 kap. 11 § polisdatalagen (2010:361), reglerar den interna tillgången till personuppgifter för domstolens eller nämndens personal. Övervägandena finns i avsnitt 9.2.

I *första stycket* slås det fast att tillgången till personuppgifter i domstolarna och nämnderna ska begränsas till det som varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Beroende på hur en domstol eller nämnd är organiserad kan skilda personalkategorier vid olika tidpunkter behöva vidta åtgärder i ett mål eller ärende och därför också ha behov av tillgång till relevanta personuppgifter. Utöver den personal som deltar i den dömande verksamheten eller i målens och ärendenas beredning kan exempelvis en växeltelefonist behöva ha tillgång till en inlaga i ett mål för att besvara en fråga från en part eller allmänheten. Uttrycket ”varje tjänsteman” omfattar såväl fast anställd personal som t.ex. pensionerade domare som tillfälligt anlitas för att avgöra enstaka mål.

I *andra stycket* finns en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela närmare föreskrifter om förutsättningarna för tillgången till personuppgifter. Detaljbestämmelser kan således utformas så att tillgången till personuppgifter begränsas till vad som är nödvändigt för att bedriva verksamheten.

Personuppgiftsansvar

9 § En allmän domstol, en allmän förvaltningsdomstol eller en 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 7.1.

Enligt 3 § personuppgiftslagen (1998:204, PUL) är det den personuppgiftsansvarige som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Domstolsdatalagen hänvisar i 5 § första stycket 1 till denna definition. I den nu aktuella paragrafen förtydligas att varje enskild domstol eller nämnd ska vara personuppgiftsansvarig för den behandling som den domstolen eller nämnden utför. Genom ett sådant tydligt utpekad ansvar kan en enskild som vill framföra ett klagomål lätt identifiera vem som är personuppgiftsansvarig för en viss behandling. Flera bestämmelser i personuppgiftslagen, till vilka domstolsdatalagen hänvisar, innebär särskilda skyldigheter för den personuppgiftsansvarige. Det är t.ex. enligt 9 § första stycket e och f PUL den personuppgiftsansvariges skyldighet att se till att de behandlade uppgifterna är adekvata och relevanta i förhållande till ändamålen för behandlingen och att inte fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det ankommer också på den personuppgiftsansvarige att se till att information lämnas till den registrerade (23, 25 och 26 §§ PUL). Enligt domstolsdatalagen gäller vidare att den personuppgiftsansvarige ska utse ett eller flera personuppgiftsombud (10 §).

Personuppgiftsombud

10 § Den personuppgiftsansvarige ska utse ett eller flera personuppgiftsombud.

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

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

Enligt *första stycket* är den personuppgiftsansvarige skyldig att utse personuppgiftsombud. Hänvisningen i 5 § första stycket 9 till 38 och 40 §§ personuppgiftslagen (1998:204) innebär att personuppgiftslagens bestämmelser om personuppgiftsombudets uppgifter är tillämpliga vid domstolarna och nämnderna.

Enligt *andra stycket* ska den personuppgiftsansvarige anmäla till den myndighet som är tillsynsmyndighet enligt personuppgiftslagen, dvs. Datainspektionen, när ett personuppgiftsombud utses eller entledigas. En motsvarande bestämmelse om personuppgiftsombud finns i 2 kap. 5 § polisdatalagen (2010:361).

Förteckning över personuppgiftsbehandlingar

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

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om vilka uppgifter en sådan förteckning ska innehålla.

I paragrafen regleras den personuppgiftsansvariges skyldighet att föra en förteckning över personuppgiftsbehandlingar. Övervägandena finns i avsnitt 14.1.

I *första stycket* föreskrivs att den som är utsedd till personuppgiftsombud ska föra en förteckning över de personuppgiftsbehandlingar som utförs med stöd av domstolsdatalagen.

En utgångspunkt är att förteckningen bör innehålla samma kategorier av uppgifter som en anmälan enligt 36 § personuppgiftslagen (1998:204) ska innehålla. 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.

I *andra stycket* finns en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela närmare föreskrifter om vilka uppgifter förteckningen ska innehålla.

Upplysningar till allmänheten

12 § Den personuppgiftsansvarige ska skyndsamt och på lämpligt sätt lämna upplysningar om de behandlingar som utförs med stöd av denna lag till var och en som begär det. 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 14.1.

Enligt paragrafen har var och en, oavsett om vederbörande själv är registrerad, rätt att få information om vilka personuppgiftsbehandlingar som en domstol eller nämnd utför. Av andra meningens framgår att upplysningarna ska omfatta de uppgifter som en förteckning enligt 11 § ska innehålla. Bestämmelsen motsvarar vad som gäller enligt 42 § personuppgiftslagen (1998:204, 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 5 § första stycket 5 är tillämplig, har därutöver den som ansöker om det rätt att en gång per kalenderår gratis få information från den personuppgiftsansvarige om huruvida personuppgifter som rör honom eller henne behandlas.

Behandling av 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 bestämmelse om behandling av känsliga personuppgifter. Övervägandena finns i avsnitt 10.1.

I paragrafen ställs det upp 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). Bestämmelsen hindrar inte att domstolarna och nämnderna behandlar känsliga personuppgifter om det finns en annan konkret grund för behandlingen – såsom att underlätta den enhetliga rättstillämpningen och tillgodose likabehandlingsprincipen. Det kan t.ex. handla om att sammanställa socialförsäkringsdomar som rör en viss sjukdomsdiagnos. Sjukdomsdiagnosen utgör i sådana fall inte den enda grunden för behandlingen. En förutsättning för tillåtligheten är att den konkreta grunden för behandlingen är godtagbar utifrån ändamålsbestämmelserna.

Sökbegränsningar

14 § Vid sökning i personuppgifter är det förbjudet att som sökbegrepp använda uppgifter som avslöjar

1. ras eller etniskt ursprung,
2. politiska åsikter,
3. religiös eller filosofisk övertygelse,
4. medlemskap i fackförening,
5. hälsa,
6. sexualliv,
7. nationell anknytning, eller
8. brott eller misstanke om brott.

Användning av särskilda beteckningar för identifiering av en viss mål- eller ärendetyp som sökbegrepp omfattas inte av förbudet i första stycket.

Paragrafen innehåller bestämmelser som förbjuder användningen av integritetskänsliga sökbegrepp. Övervägandena finns i avsnitt 11.4.

I *första stycket* anges att vissa typer av uppgifter inte får användas som sökbegrepp. Förbudet gäller för de första uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa eller sexualliv (jfr bestämmelsen om behandling av känsliga personuppgifter i 13 §). Begreppen har samma innebörd som enligt personuppgiftslagen (1998:204). För det andra avser förbudet uppgifter som avslöjar nationell anknytning. Med sådana uppgifter avses bl.a. uppgifter om medborgarskap, om födelseort eller om utlandsfödda föräldrar. Varje form av nationell anknytning omfattas dock inte av bestämmelsen utan det krävs att uppgifterna visar på en anknytning till ett visst land som 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 som omfattas av sökförbudet. Normalt torde uppgifter om språkkunskaper eller om behov av tolk inte heller vara att anse som en uppgift om nationell anknytning.

För det tredje avser förbudet uppgifter som avslöjar brott eller misstanke om brott som sökbegrepp. Det innebär att det även är förbjudet att som sökbegrepp använda uppgifter om frihetsberövande på grund av brott, liksom uppgifter om brottspåföljder.

I *andra stycket* anges att användningen av särskilda beteckningar för identifiering av en viss mål- eller ärendetyp som sökbegrepp inte omfattas av förbudet i första stycket. Denna bestämmelse tar sikte på så kallade målgrupps- och måltypskoder.

15 § Förbudet i 14 § första stycket gäller inte användning

1. i allmän domstol av sökbegrepp som avslöjar brott eller misstanke om brott, och

2. i allmän förvaltningsdomstol av sökbegrepp som avslöjar hälsa, brott eller misstanke om brott.

Förbudet i 14 § första stycket gäller inte heller vid sökning i en viss handling eller i ett visst mål eller ärende.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om begränsningar av möjligheten att använda de sökbegrepp som anges i första stycket.

Paragrafen innehåller bestämmelser om undantag från sökförbudet i 14 §. Övervägandena finns i avsnitt 11.4.

I *första stycket 1* finns ett undantag som avser användning i de allmänna domstolarnas verksamhet av uppgifter som avslöjar brott eller misstanke om brott som sökbegrepp. Bestämmelsen innebär t.ex. att det finns möjlighet att använda brottsrubriceringar som sökbegrepp i allmän domstol. Detta gäller även om en viss brottsrubricering samtidigt också kan avslöja exempelvis sexualliv. I *första stycket 2* finns ett undantag som avser användning i de allmänna förvaltningsdomstolarnas verksamhet av uppgifter som avslöjar hälsa, brott eller misstanke om brott.

I *andra stycket* föreskrivs att sökbegränsningarna i 14 § första stycket inte gäller i fråga om sökningar som sker enbart bland uppgifter i en viss handling eller i ett visst mål eller ärende. I dessa fall kommer sökning endast att ske i begränsade informationsmängder.

I *tredje stycket* finns en bestämmelse om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om begränsningar av möjligheten att använda de sökbegrepp som anges i första stycket.

Elektroniskt utlämnande av personuppgifter

16 § Personuppgifter får lämnas ut på medium för automatiserad behandling om det inte är olämpligt.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar av möjligheterna att lämna ut personuppgifter på medium för automatiserad behandling.

Paragrafen reglerar i vilka fall personuppgifter får lämnas ut på medium för automatiserad behandling. Övervägandena finns i avsnitt 12.2.

I *första stycket* anges att personuppgifter får lämnas ut på medium för automatiserad behandling om det inte är olämpligt. Med utlämnande på medium för automatiserad behandling avses bl.a. utlämnande på ett usb-minne, genom e-post, eller annan elektronisk överföring. Lämplighetsprövningen ska ske i varje enskilt fall. Det har vid lämplighetsprövningen betydelse vem mottagaren är. I fråga om utlämnande till en annan domstol eller en myndighet torde utlämnande på medium för automatiserad behandling som utgångspunkt vara tillåtet enligt bestämmelsen. I fråga om utlämnande av processmaterial till en part eller partens ombud, biträde eller försvarare måste kravet på en rättvis rättegång och andra processrättsliga principer beaktas. Exempelvis bör en part som regel få ta del av processmaterialet i elektronisk form om det behövs för att säkerställa att parterna i en process är likställda (equality of arms).

Lämplighetsprövningen blir särskilt viktig när utlämnandet ska ske till enskild och det på grund av personuppgifternas art, struktur, antal eller någon annan särskild omständighet finns anledning att befara att utlämnandet i förlängningen kan leda till integritetsrisker. Försiktighet är exempelvis påkallad om det är fråga om fotografier eller ljudupptagningar. Samma sak gäller om de uppgifter som den enskildes begäran avser är sammanställda utifrån en sökning som framstår som integritetskänslig. För att uppgifterna ska kunna lämnas ut på elektronisk väg måste det även finnas rutiner för datasäkerhet. Även särskilda säkerhetsåtgärder kan behöva vidtas exempelvis när personuppgifterna överförs genom e-post för att minska säkerhetsriskerna vid sådan överföring. Bestämmelserna om säkerheten vid behandlingen i 31 § personuppgiftslagen (1998:204, PUL), som genom 5 § första stycket 7 är tillämpliga i domstolarnas och nämndernas verksamhet, får därmed betydelse vid lämplighetsprövningen.

I *andra stycket* finns en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om ytterligare begränsningar av möjligheterna att lämna ut personuppgifter på medium för automatiserad behandling.

17 § Direktåtkomst får endast medges

1. en allmän domstol,
2. en allmän förvaltningsdomstol,
3. en hyres- och arrendenämnd, eller
4. en part eller partens ombud, biträde eller försvarare.

Direktåtkomst enligt första stycket 4 får endast avse personuppgifter i partens mål eller ärende.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar av direktåtkomst enligt första stycket och om behörighet och säkerhet vid sådan åtkomst.

Paragrafen innehåller bestämmelser om direktåtkomst. Övervägandena finns i avsnitt 12.1. Med direktåtkomst avses att någon har direkt tillgång till register, databaser eller andra samlingar av uppgifter som behandlas automatiserat eller på egen hand kan söka efter information, dock utan att kunna påverka innehållet i uppgiftssamlingen. I begreppet direktåtkomst ligger också att den som är ansvarig för uppgiftssamlingen inte har någon

kontroll över vilka uppgifter som mottagaren vid ett visst tillfälle tar del av.

Enligt *första stycket* begränsas möjligheterna för en domstol eller en nämnd att medge direktåtkomst till vissa mottagare, nämligen dels myndigheter som omfattas av domstolsdatalagens tillämpningsområde, dels parter och parter ombud, biträde eller försvarare. Bestämmelsen ger en domstol eller nämnd möjlighet att medge direktåtkomst, men innebär inte någon rätt för mottagarna att få sådan åtkomst. Det är den domstol eller nämnd som innehar uppgifterna som bestämmer om direktåtkomst ska beviljas eller inte. Direktåtkomst får beviljas endast om det i det enskilda fallet bedöms lämpligt. Paragrafen, liksom övriga bestämmelser i domstolsdatalagen om elektroniskt utlämnande, saknar sekretessbrytande verkan. För att en domstol eller nämnd 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 (2009:400, OSL) med säkerhet skulle ha rätt att ta del av uppgifterna. I 11 kap. 4 och 8 §§ OSL finns särskilda bestämmelser om överföring av sekretess vid direktåtkomst.

Av *andra stycket* följer att direktåtkomsten för en part eller partens ombud, biträde eller försvarare endast får avse personuppgifter i partens eget mål eller ärende.

I *tredje stycket* finns en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter som ytterligare begränsar möjligheterna att medge direktåtkomst till personuppgifter. Det kan t.ex. röra sig om att begränsa direktåtkomstmöjligheten till domstolar inom samma domstolsslag i vissa fall. Genom sådana föreskrifter kan det också preciseras vilka uppgifter som direktåtkomsten får avse. I paragrafen finns också en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om behörighets- och säkerhetsfrågor såvitt avser direktåtkomst.

Personuppgifter i avgjorda mål och ärenden

18 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om begränsningar för behandling av personuppgifter som hänför sig till ett mål eller ärende som har avgjorts genom en dom eller ett beslut som har fått laga kraft.

I paragrafen informeras om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela ytterligare föreskrifter om begränsningar för behandling av personuppgifter som hänför sig till ett mål eller ärende som har avgjorts genom en dom eller ett beslut som har fått laga kraft. Övervägandena finns i avsnitt 13.

I domstolsdatalagen finns flera bestämmelser som informerar om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter som ytterligare begränsar behandlingen av personuppgifter utöver vad som följer av domstolsdatalagen, se t.ex. 17 § tredje stycket. Sådana begränsningar kan avse behandling av personuppgifter både

under handläggningen av ett mål eller ärende och efter det att handläggningen har avslutats och avgörandet har fått laga kraft. I den nu aktuella paragrafen finns en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela ytterligare föreskrifter om begränsningar för behandlingen av personuppgifter efter tidpunkten för laga kraft. Det kan t.ex. röra sig om att begränsa möjligheterna att söka efter personnummer och namn i avgöranden som har fått laga kraft.

Överklagande

19 § Tillsynsmyndighetens beslut enligt denna lag eller enligt de bestämmelser i personuppgiftslagen (1998:204) som anges i 5 § om annat än föreskrifter får överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen innehåller bestämmelser om överklagande av Datainspektionens beslut enligt domstolsdatalagen. Övervägandena finns i avsnitt 15.2.

Hänvisningen i 5 § första stycket 7 och 10 till 31, 32, 44 och 45 §§ personuppgiftslagen (1998:204) innebär att personuppgiftslagens bestämmelser om Datainspektionens befogenheter blir tillämpliga i domstolarnas och nämndernas verksamhet. Dessa bestämmelser innebär att Datainspektionen under vissa förutsättningar kan fatta beslut om säkerhetsåtgärder och om förbud. I den nu aktuella bestämmelsen anges att Datainspektionens beslut i sådana frågor får överklagas till allmän förvaltningsdomstol och att prövningstillstånd krävs vid överklagande till kammarrätten. Paragrafen har utformats på motsvarande sätt som i personuppgiftslagen (51 § första stycket).

20 § En hovrätts, tingsrätts eller förvaltningsrätts beslut om upplysningar enligt 12 § eller om information till den registrerade enligt 26 § personuppgiftslagen (1998:204) och 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 frågor som avses i första stycket får inte överklagas.

Paragrafen innehåller bestämmelser om överklagande av beslut som har meddelats av en personuppgiftsansvarig domstol. Övervägandena finns i avsnitt 15.2.

I *första stycket* första meningen anges vilka beslut av en personuppgiftsansvarig domstol som får överklagas. Det är beslut om upplysningar till allmänheten enligt 12 § och beslut om information enligt 26 § personuppgiftslagen (1998:204, PUL) och om rättelse och underrättelse till tredje man enligt 28 § PUL, vilka enligt 5 § första stycket 5 och 6 är tillämpliga vid personuppgiftsbehandling i domstolarnas och nämndernas rättskipande och rättsvärdande verksamhet. Av bestämmelsen framgår att de nämnda besluten av en personuppgiftsansvarig hovrätt, tingsrätt eller förvaltningsrätt får överklagas till kammarrätt. Det krävs inte prövningstillstånd i kammarrätten

vid ett sådant överklagande. I sista meningen sägs att ett beslut som meddelats av en kammarrätt i egenskap av personuppgiftsansvarig får överklagas till Högsta förvaltningsdomstolen.

Enligt *andra stycket* får Högsta domstolens och Högsta förvaltningsdomstolens beslut som dessa domstolar meddelat i egenskap av personuppgiftsansvariga inte överklagas.

21 § En hyres- och arrendenämnds beslut i frågor som avses i 20 § första stycket får överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen innehåller bestämmelser om överklagande av beslut som har meddelats av en personuppgiftsansvarig hyres- och arrendenämnd. Övervägandena finns i avsnitt 15.2.

Enligt paragrafen får beslut i frågor som avses i 20 § första stycket första meningen av en personuppgiftsansvarig hyres- och arrendenämnd överklagas till allmän förvaltningsdomstol. Enligt den vanliga ordningen för överklagande av förvaltningsbeslut krävs enligt paragrafen prövningstillstånd vid överklagande till kammarrätten.

22 § Andra beslut än sådana som avses i 19–21 §§ eller i 47 § personuppgiftslagen (1998:204) får inte överklagas.

Vid överklagande av förvaltningsrättens beslut i frågor som avses i 47 § personuppgiftslagen krävs prövningstillstånd vid överklagande till kammarrätten.

Paragrafen, som är utformad efter mönster av 53 § personuppgiftslagen (1998:204, PUL), innehåller bestämmelser om överklagandeförbud och prövningstillstånd vid överklagande till kammarrätten. Övervägandena finns i avsnitt 15.2.

Enligt *första stycket* får andra beslut än sådana som avses i 19–21 §§ eller 47 § PUL inte överklagas. Bestämmelsen i 47 § PUL, som enligt 5 § första stycket 10 är tillämplig vid personuppgiftsbehandling i domstolarnas och nämndernas rättskipande och rättsvårdande verksamhet, innebär att Datainspektionen hos förvaltningsrätten får ansöka om utplåning av personuppgifter som påstås ha behandlats på ett olagligt sätt.

I *andra stycket* anges att det krävs prövningstillstånd vid överklagande av förvaltningsrättens beslut i frågor som avses i 47 § PUL.

Sammanfattning av promemorian Domstolsdatalag (Ds 2013:10)

Promemorian innehåller förslag till en lag om behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas och 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 författningssenligt 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.

Domstolsdatalagen föreslås träda i kraft den 1 april 2014.

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.

Efter remiss har yttranden över promemorian Domstolsdatalag (Ds 2013:10) lämnats av Riksdagens ombudsmän, Svea hovrätt, Göta hovrätt, Hovrätten över Skåne och Blekinge, Hovrätten för Västra Sverige, Attunda tingsrätt, Stockholms tingsrätt, Nyköpings tingsrätt, Västmanlands tingsrätt, Lunds tingsrätt, Göteborgs tingsrätt, Borås tingsrätt, Sundsvalls tingsrätt, Umeå tingsrätt, Kammarrätten i Stockholm, Kammarrätten i Göteborg, Kammarrätten i Sundsvall, Kammarrätten i Jönköping, Förvaltningsrätten i Stockholm, Förvaltningsrätten i Malmö, Förvaltningsrätten i Göteborg, Förvaltningsrätten i Härnösand, Förvaltningsrätten i Jönköping, Justitiekanslern, Hyresnämnden i Stockholm, Hyresnämnden i Malmö, Domstolsverket, Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, Kriminalvården, Brottsförebyggande rådet, Migrationsverket, Datainspektionen, Kustbevakningen, Försäkringskassan, Socialstyrelsen, Tullverket, Skatteverket, Kronofogdemyndigheten, Stockholms universitet, Uppsala universitet, Diskrimineringsombudsmannen, Riksarkivet, Sveriges advokatsamfund och Svenska Journalistförbundet.

Arbetsdomstolen, E-delegationen och Sveriges Kommuner och Landsting har avstått från att yttra sig. Sveriges Radio AB har inte hörts av.