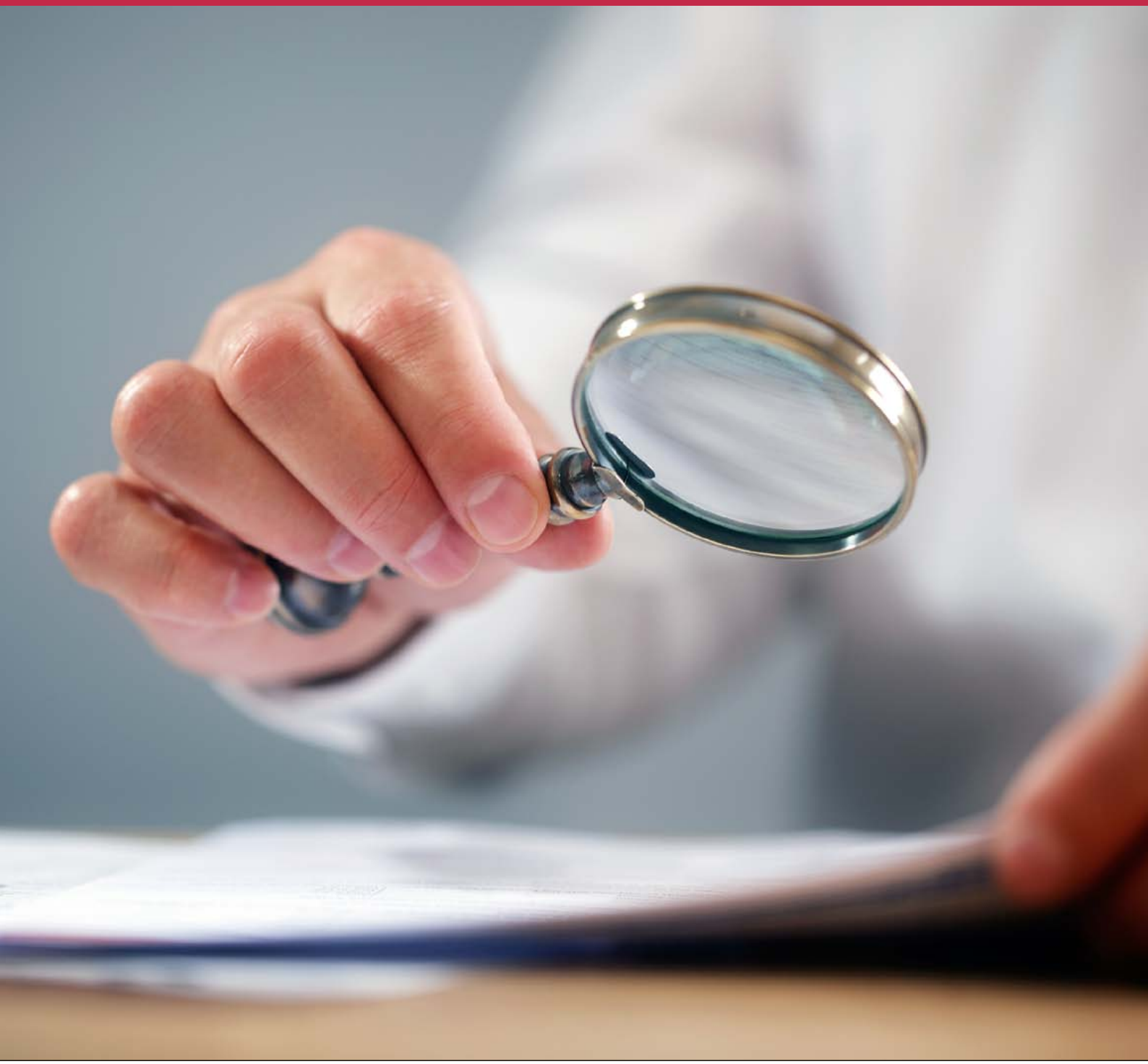

Vägledning för integritetsanalys

En vägledning från Datainspektionen för att bedöma integritetsriskerna med ny eller ändrad lagstiftning

Datainspektionen

Vägledning för integritetsanalys
September 2016
Synpunkter på utformningen av och förslag till förbättringar av denna vägledning tas tacksamt emot av Datainspektionen. Skicka synpunkter till datainspektionen@datainspektionen.se. Kontaktperson: Martin Brinnen.

Innehåll

Inledning

Syftet med vägledningen

Var och en har rätt till skydd för sitt privatliv och skydd av de personuppgifter som rör honom eller henne. Det följer av Europakonventionen, Europarådets dataskyddskonvention, EU:s stadga om de grundläggande rättigheterna, dataskyddsdirektivet och regeringsformen. Det följer också av EU:s dataskyddsförordning[1] som antogs den 14 april 2016 och som ska börja tillämpas den 25 maj 2018. Varje utredning måste därför reflektera över om föreslagna författningar innebär någon form av personuppgiftsbehandling och i så fall göra en bedömning av det rättsliga stödet för personuppgiftsbehandlingen och de integritetsrisker som följer av förslagen.

Syftet med denna vägledning är att underlätta arbetet med att analysera konsekvenserna för den personliga integriteten vid personuppgiftsbehandling (integritetsanalys) när förslag till nya lagar och andra föreskrifter tas fram. Bakgrunden är bland annat att Datainspektionen i remissyttranden över lagförslag många gånger tvingas konstatera att underlaget i betänkanden inte är tillräckligt utförligt för att inspektionen ska kunna ta ställning till integritetsriskerna med lagförslagen.

I vägledningen redogörs för ett antal viktiga faktorer som behöver belysas i en integritetsanalys. Den utgör dock inget komplett verktyg utan behöver kompletteras med fördjupade analyser i det enskilda fallet.

En väl genomförd integritetsanalys ska – utifrån ett fullgott beslutsunderlag – svara på frågan om förslaget är förenligt med reglerna om skydd för den personliga integriteten i grundlagarna och EU-rätten. Den ska också särskilt svara på frågan om konsekvenserna för den personliga integriteten som en föreslagen personuppgiftsbehandling medför, är proportionerliga i förhållande till det man avser att uppnå med behandlingen. I detta ingår att bedöma om behandlingen av personuppgifter är nödvändig utifrån de avsedda ändamålen med behandlingen och om det finns alternativ som är mindre integritetskänsliga. En förutsättning för en sådan analys är en noggrann kartläggning och beskrivning av den föreslagna personuppgiftsbehandlingen och en analys av vilka konsekvenser för den personliga integriteten behandlingen medför eller kan medföra.

1 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om de fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) härefter kallad dataskyddsförordningen

För en snabb ingång i arbetet med integritetsanalys se följande checklista.

Checklista

Tänk redan från början på vilka konsekvenser som utredningens uppdrag och tänkbara förslag kan komma att få för skyddet för den personliga integriteten i samband med behandling av personuppgifter.

Kartläggning

- Vilket behov av att behandla personuppgifter hos myndigheter, företag, organisationer och privatpersoner kan uppkomma med anledning av utredningens uppdrag och förslag ?
- För vilka ändamål ska personuppgifter behandlas?
- Med vilket rättsligt stöd ska personuppgifterna behandlas?
- Vem ska utföra personuppgiftsbehandlingen och vem ansvarar för den?
- Vilka personuppgifter kommer att behöva samlas in och i övrigt behandlas?
- Hur många personer kommer att beröras av personuppgiftsbehandlingen och hur många uppgifter om varje person kommer att behöva samlas in?
- Varifrån ska personuppgifterna samlas in?
- Vilka kommer att ha åtkomst till personuppgifterna och vilken spridning kan uppgifterna i övrigt komma att få?
- Finns det behov av nya sekretessbestämmelser och sekretessbrytande bestämmelser?
- Vilka sök- och sammanställningsmöjligheter är nödvändiga för ändamålet och hur kan de begränsas?
- Hur länge behöver personuppgifter bevaras?
- Vilket inflytande kommer de registrerade att ha över personuppgiftsbehandlingen?
- Vilken information om behandlingen av personuppgifter kommer de registrerade att få?
- Vilka (befintliga eller nya) regler kommer att gälla till skydd för de registrerades personliga integritet vid den föreslagna personuppgiftsbehandlingen?

Analys och proportionalitetsbedömning

- Finns det några mindre integritetsingripande alternativ för att uppnå det avsedda ändamålet än den föreslagna personuppgifts-behandlingen?
- Hur förhåller sig förslagen till rätten till skydd för privatlivet och rätten till skydd för personuppgifter enligt regeringsformen, Europakonventionen och EU:s rättighetsstadga?
- Vad regleras i dataskyddsförordningen och vad får respektive måste varje land reglera i nationell rätt?
- Innebär förslagen sådana integritetsrisker att det krävs särskild reglering i lag?
- Står integritetsintrånget som behandlingen medför i rimlig proportion till den nytta som behandlingen innebär för de avsedda ändamålen?

Integritetsanalys – varför, när och hur?

Varför måste utredningen göra en integritetsanalys?

Möjligheterna att få igenom ett författningsförslag ökar väsentligt om utredningen har gjort en noggrann kartläggning av eventuella integritetsrisker och en analys av vilka konsekvenser förslaget kan få för skyddet för enskildas personliga integritet. Var och en har nämligen rätt till skydd för sitt privatliv och skydd av de personuppgifter som rör honom eller henne. Det följer av artikel 8 i Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen), Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter, nr 108 (Europarådets dataskyddskonvention) och artikel 7 och 8 i EU:s stadga om de grundläggande rättigheterna (2010/C 83/02). Skyddet för den personliga integriteten i samband med behandling av personuppgifter inom EU regleras i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet).

I april 2016 antogs ett nytt regelverk för behandlingen av personuppgifter av EU-parlamentet och EU-rådet efter drygt fyra års förhandlingar. Syftet med det nya regelverket är att modernisera och ersätta reglerna i dataskyddsdirektivet från 1995 och få till stånd en mer enhetlig tillämpning inom EU. Det nya regelverket innehåller dels en generell dataskyddsförordning, dels ett särskilt dataskyddsdirektiv för brottsbekämpande myndigheter (det så kallade polisdirektivet). Den nya dataskyddsförordningen ska börja tillämpas den 25 maj 2018 och kommer då att ersätta personuppgiftslagen. Dataskyddsförordningen kommer också gälla för de verksamheter som har så kallade registerförfattningar, men det finns möjlighet att i vissa fall komplettera förordningen. Närmare om dataskyddsförordningen, se nedan.

Ett skydd för den personliga integriteten vid behandling av personuppgifter ges även i regeringsformen. Enligt 2 kap. 6 § andra stycket regeringsformen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Skyddet enligt denna bestämmelse kan begränsas endast enligt den särskilda ordning som föreskrivs i 2 kap. 20–22 §§ regeringsformen.

Skyddet för privatlivet är inte absolut och kan under vissa förutsättningar inskränkas med hänsyn till andra motstående intressen. Sådana

inskränkningar måste emellertid stå i rimlig proportion till de fördelar som personuppgiftsbehandlingen bidrar med till det motstående intresset. Den intresseavvägning som i sådana fall måste göras sker inom ramen för en så kallad proportionalitetsbedömning (se nedan) vilken även omfattar en bedömning av om personuppgiftsbehandlingen är nödvändig för uppnåendet av det avsedda ändamålet och om det finns alternativ som är mindre integritetskänsliga.

Lagstiftaren har således en skyldighet att särskilt motivera inskränkningar i skyddet för den personliga integriteten och se till att sådana inskränkningar står i rimlig proportion till ändamålet med behandlingen.

Ett integritetsskydd som är väl avvägt mot motstående intressen inger dessutom förtroende hos de vars personuppgifter ska behandlas och hos de som ska följa reglerna. Det ligger därför i lagstiftarens intresse att författningsförslag som innebär integritetsrisker bygger på en omsorgsfull kartläggning av dessa risker och en analys av konsekvenserna för integritetsskyddet.

Utredningen måste i princip alltid göra en integritetsanalys

Utredningen måste kartlägga vilken personuppgiftsbehandling som förslagen kan innebära och även bedöma integritetsriskerna med lagförslagen.

Behandlingen av personuppgifter i samhället är i dag omfattande vilket innebär att lagstiftningsarbete ofta rör frågor innehållande behandling av personuppgifter. I många fall handlar det om behandling av ett begränsat antal personuppgifter av inte särskilt integritetskänslig karaktär. I andra fall kan det handla om omfattande kartläggning av en stor del av befolkningen. En svårighet är att integritetsriskerna inte alltid framgår klart till exempel när det handlar om indirekta personuppgifter som, om de kombineras med redan befintliga uppgifter, avslöjar känsliga uppgifter om enskilda. En annan svårighet är att bedöma integritetsriskerna när författningsförslag innebär att uppgifter som har samlats in för ett ändamål ska användas för andra ändamål.

Det går inte att bedöma integritetsriskerna innan den personuppgiftsbehandling som förslaget kan innebära har kartlagts. En bedömning av integritetsriskerna ska därför göras inom varje utredningsuppdrag och för varje förslag som utredningen lägger fram. Omfattningen av arbetet med en integritetsanalys avgörs utifrån en preliminär bedömning av riskerna för integritetsintrång och sannolikheten för att riskerna förverkligas. Om denna preliminära bedömning visar att utredningens kommande förslag inte kommer att medföra behandling av personuppgifter kan arbetet förstås begränsas väsentligt.

När bör integritetsanalysen göras?

Det är viktigt att utredningen har med integritetsfrågorna i sitt arbete under hela utredningstiden.

Integritetsriskerna med utredningens uppdrag och tänkbara förslag bör kartläggas och bedömas redan i inledningsskedet av utredningsarbetet för att arbetet med integritetsanalysen ska kunna tas med i arbetsplaneringen. Omfattningen av det fortsatta arbetet med integritetsrisker måste även här avgöras utifrån de risker för integritetsintrång som har framkommit vid den inledande bedömningen.

Det kan vara lämpligt att regelbundet under utredningsarbetet analysera integritetsriskerna utifrån utkast till förslag och överväganden i andra frågor som bearbetas inom utredningen. Slutgiltiga förslag till författningstext bör analyseras särskilt noggrant. I slutskedet av arbetet bör dessutom de sammanlagda konsekvenserna för integritetsskyddet av utredningens samtliga förslag utvärderas.

Redovisa fakta och överväganden tydligt

Det är viktigt att utredningen noga beskriver den personuppgiftsbehandling som kan bli följden av utredningens förslag och öppet redovisar de överväganden avseende integritetsrisker som har gjorts. Det är inte tillräckligt att göra svepande slutsatser som ”vid en samlad bedömning anser utredningen att fördelarna med förslaget överväger integritetsriskerna”.

Det kan många gånger vara lämpligt att beskriva integritetsriskerna genom att redovisa exempel på faktiskt inträffade händelser och händelser som kan tänkas inträffa om utredningens förslag genomförs.

Metoder för integritetsanalysen

Integritetsrisker som har uppmärksammats vid liknande behandling av personuppgifter kan framgå av tidigare förarbeten, rättspraxis och Datainspektionens tillsynsbeslut och remissyttranden. Ledning kan också sökas i den så kallade Artikel 29-gruppens yttranden i olika integritetsfrågor.[2]

EU:s dataskyddsförordning

EU:s generella dataskyddsförordning ska börja tillämpas från och med den 25 maj 2018. Den kommer att ersätta dataskyddsdirektivet från 1995 och svenska personuppgiftslagen. Detta innebär att författningsförslag redan nu måste anpassas till förordningens innehåll. Behandling av personuppgifter som sker inom den brottsbekämpande verksamheten omfattas inte förordningen. I stället kommer den verksamheten att omfattas av det så kallade polisdirektivet.

Dataskyddsförordningen innehåller många bestämmelser som är hämtade från dataskyddsdirektivet men även flera ändringar och nyheter till exempel rätten att bli glömd, dataportabilitet, skyldighet att anmäla personuppgiftsincident och skylighet för den personuppgiftsansvarige att göra en konsekvensbedömning avseende dataskydd innan en riskfylld behandling påbörjas. Därutöver medför förordningen en skyldighet för dataskyddsmyndigheterna inom EU att samarbeta med varandra. Vid fall av så kallade gränsöverskridande behandling ska dessutom Europeiska dataskyddsstyrelsen kunna ta beslut som är bindande för de nationella dataskyddsmyndigheterna.

2 Artikel 29-gruppen är en rådgivande och oberoende arbetsgrupp med representanter för de olika dataskyddsmyndigheterna som ska se till att dataskyddsdirektivet tillämpas enhetligt i medlemsstaterna. Se vidare: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm
När förordningen ska börja tillämpas ersätts artikel 29-gruppen av den europeiska dataskyddsbyrån, EDPB.

Förordningsformen innebär att bestämmelserna inte får ersättas med svenska bestämmelser, förutom i de fall då förordningen ger uttryckligt stöd för detta. Vid författningsarbete måste således utredas om författningsförslagen – men även befintliga författningar – står i överensstämmelse med förordningens bestämmelser.

Det pågår för närvarande flera olika utredningar med uppdrag att analysera förordningens tillämpning i Sverige till exempel Dataskyddsutredningen. Därtill pågår inom de olika sakdepartementen en översyn av olika registerförfattningar. Det kan därför vara nödvändigt att samråda med dessa utredningar i frågor som rör dataskydd.

Konsekvensbedömningen i artikel 35 i förordningen kan genomföras som ett led i lagstiftningsarbetet. Om detta har skett är den personuppgiftsansvarige befriad från kravet att genomföra en konsekvensbedömning innan behandling påbörjas.[3] Detta kommer främst att gälla myndigheter eftersom det är dessa som tillämpar registerförfattningar i sin verksamhet. Det är därför viktigt att om lagstiftaren har för avsikt att genomföra en sådan konsekvensbedömning i lagstiftningsarbetet så ska den görs på ett sätt som uppfyller förordningens krav. Denna vägledning kan användas som ett hjälpmedel vid genomförandet av konsekvensanalysen.

Datainspektionen har påbörjat förberedelserna för införandet av dataskyddsförordningen och informerar fortlöpande om detta på myndighetens webbplats www.datainspektionen.se/dataskydd.

3 Se dataskyddsförordningen artikel 35.10

Grundläggande krav för behandling av personuppgifter

Vägledningen utgår i stora delar från de grundläggande kraven för behandling av personuppgifter som finns angivna i 9 § personuppgiftslagen. Motsvarande krav återfinns i artikel 5 i dataskyddsförordningen och dessa grundläggande krav har sitt ursprung i Europarådets dataskyddskonvention. De grundläggande kraven kan därför ses som mer allmängiltiga principer som är vägledande för all behandling av personuppgifter. Principerna kan förklaras på följande sätt.

1. Personuppgifter får behandlas bara om det är lagligt.

2. Personuppgifter ska alltid behandlas på ett korrekt sätt och i enlighet med god sed.[4] Uppgifterna ska enligt förordningen behandlas på ett öppet sätt i förhållande till den registrerade.

3. Personuppgifter får samlas in endast för särskilda, uttryckligt angivna och berättigade ändamål.

4. Personuppgifter får inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in.

5. Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen.

6. Personuppgifter får behandlas endast om det är nödvändigt med hänsyn till ändamålen med behandlingen, det vill säga fler uppgifter än vad som är nödvändigt får inte behandlas.

7. Personuppgifter som behandlas ska vara riktiga och, om nödvändigt, aktuella.

8. Personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen ska rättas, blockeras eller utplånas.

9. Personuppgifter får inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

För närmare beskrivning av innebörden av de grundläggande kraven enligt personuppgiftslagen hänvisas till Datainspektionens webbplats. Vad gäller motsvarande principer i dataskyddsdirektivet hänvisas till

4 Detta begrepp försvinner med dataskyddsförordningen.

Handbook on European data protection law, European Union agency for fundamental rights, 2014.[5]

I dataskyddsförordningen finns motsvarande bestämmelser i artikel 5 om principer för behandling av personuppgifter som talar om laglighet, korrekthet och öppenhet, ändamålsbegränsning, uppgiftsminimering, korrekthet, lagringsminimering, integritet och konfidentialitet samt ansvarsskydighet[6]. I tillhörande skäl 39 anges bland annat att öppenhetsprincipen kräver att all information och kommunikation i samband med behandlingen av personuppgifter är lättillgänglig och lättbegriplig samt att ett klart och tydligt språk används.

5 http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law

6 I den svenska versionen av dataskyddsförordningen har de engelska begreppen fairness och accuracy båda översatts till korrekthet.

Vägledning

Vägledningen är uppbyggd kring vissa centrala frågor som har betydelse för bedömningen av integritetsrisker vid behandling av personuppgifter. Under varje rubrik finns en kort bakgrund till ämnet, ett antal exempel på frågor som kan behöva besvaras och redovisas samt förslag på åtgärder som kan vidtas för att minska integritetsriskerna.

Vägledningen är inte uttömmande och innehåller endast kortfattade beskrivningar och frågeställningar. Den som arbetar med att ta fram lagförslag som inbegriper behandling av personuppgifter behöver således komplettera analysen med annat material för en fullständig analys av integritetsriskerna. Rekommendationer om viss ytterligare läsning finns sist i vägledningen.

Automatiserad behandling av personuppgifter

Skyddet mot de särskilda integritetsrisker som uppkommer vid automatiserad behandling av personuppgifter är en del av den grundläggande fri- och rättigheten om skydd för den enskildes privatliv. Skyddet mot integritetskränkningar vid automatiserad behandling av personuppgifter har därutöver ansetts kräva särskild reglering såsom i EU:s dataskyddsdirektiv, personuppgiftslagen och ett stort antal registerförfattningar.

En förutsättning för att dessa särskilda regleringar ska aktualiseras är att personuppgifter kommer att behandlas. Definitionen i personuppgiftslagen av vad som utgör personuppgifter är mycket vid och omfattar all information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

En andra förutsättning är att personuppgifter behandlas automatiserat, helt eller delvis. Observera även att olika förstadier till en automatiserad behandling av personuppgifter, såsom manuell insamling på papper som sker i syfte att senare registreras i ett it-system, omfattas av skyddet för personuppgifter. Detsamma gäller olika former av manuell efterbehandling, till exempel utlämnande av personuppgifter från ett it-system.

I vissa fall kan även manuell registerhantering omfattas (jämför 5 § andra stycket personuppgiftslagen och artikel 2 punkt 1 dataskyddsförordningen).

Frågor som kan behöva besvaras och redovisas

1) Innebär utredningens förslag att personuppgifter kommer att behandlas, antingen som en direkt följd eller som en indirekt konsekvens av förslagen? Med personuppgift avses enligt 3 § personuppgiftslagen

och artikel 4 punkt 1 dataskyddsförordningen all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

2) Är behandlingen av personuppgifter helt eller delvis automatiserad (jämför 5 § personuppgiftslagen och artikel 2 punkt 1 dataskyddsförordningen)?

3) Omfattar behandlingen av personuppgifter manuell behandling före eller efter en automatiserad behandling?

4) Kommer personuppgifter att behandlas i manuella register (jämför 5 § andra stycket personuppgiftslagen och artikel 2 punkt 1 dataskyddsförordningen)?

Åtgärder för att minska integritetsrisker

- Undvik att lämna förslag som medför behandling av personuppgifter om det är möjligt att uppnå det avsedda ändamålet utan sådan behandling.
- Om personuppgiftsbehandling behöver behandlas, utforma förslag som innebär så begränsad personuppgiftsbehandling som möjligt med hänsyn till ändamålen (jämför grundläggande krav för behandling av personuppgifter).
- Om personuppgifter kommer att behöva samlas in ska uppgifterna raderas eller anonymiseras när de inte längre behövs för de avsedda ändamålen och de inte heller ingår i allmänna handlingar som ska arkiveras enligt arkivlagen.
- Om personuppgiftsbehandling inte går att undvika, överväg att införa krav på pseudoanonymisering, det vill säga identifiering av de registrerade är inte möjligt utan särskild information (nyckel) som hålls avskild och som kombineras med ett förbud mot återidentifiering.

Ändamålet med personuppgiftsbehandlingen

För att det ska vara möjligt att bedöma om en viss personuppgiftsbehandling är tillåten är det nödvändigt att noga beskriva och specificera ändamålet med behandlingen, det vill säga varför behandlingen ska utföras, och på vilket sätt personuppgiftsbehandlingen bidrar till dessa ändamål. De fördelar som den föreslagna personuppgiftsbehandlingen bidrar med till det angivna ändamålet måste kunna vägas mot de integritetsrisker som förslaget medför.

Det måste också alltid finnas ett rättsligt stöd för behandlingen av personuppgifterna, se vidare sidan 31.

Frågor som kan behöva besvaras och redovisas

5) Vilket är det övergripande målet till vilket personuppgiftsbehandlingen ska bidra, till exempel brottsbekämpning, effektivisering.

- Beskriv omfattningen av det problem som ska lösas och vilka konsekvenser det får om behandlingen av personuppgifter inte tillåts.

6) För vilket eller vilka konkreta ändamål ska behandling av personuppgifterna ske?

- Ändamålsbeskrivningen ska vara så utförlig att det går att bedöma vilka personuppgifter som är nödvändiga att behandla.

7) På vilket sätt bidrar den föreslagna personuppgiftsbehandlingen till att uppfylla ändamålen med behandlingen?

8) Finns det mindre integritetskänsliga alternativ? Kan de på ett fullgott sätt bidra till att uppfylla det aktuella ändamålet?

Åtgärder för att minska integritetsrisker

- Överväg om ändamålet kan uppnås på ett sätt som inte innefattar behandling av personuppgifter.
- Begränsa behandlingen av personuppgifter till det som är nödvändigt för ändamålet.
- Ange ändamålet med behandlingen utförligt i författning.

Personuppgiftsansvarig

Vem som ansvarar för en viss behandling av personuppgifter kan ha betydelse för bedömning av vilka integritetsrisker som behandlingen kan medföra. Förutsättningarna för och riskerna med en viss personuppgiftsbehandling skiljer sig åt till exempel om det handlar om en myndighet eller ett företag som ska behandla personuppgifter.

Enligt personuppgiftslagen 3 paragrafen och dataskyddsförordningen artikel 4 punkt 7 är den som bär det rättsliga ansvaret för behandlingen av personuppgifter (personuppgiftsansvarig) den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Ansvaret kan också placeras på någon utpekad aktör genom lagstiftning.

När personuppgiftsbehandlingen ska ske till exempel inom en koncern eller i samarbete mellan flera kommuner och myndigheter kan det vara

svårt att bestämma vem eller vilka som ska ansvara för behandlingen. Det kan därför i vissa fall finnas anledning att författningsreglera personuppgiftsansvaret. Ansvaret för personuppgiftsbehandlingen bör i sådana situationer läggas på den som har faktisk möjlighet att påverka ändamålen och medlen för behandlingen. Den personuppgiftsansvarige måste kunna ta sitt ansvar.

Den som behandlar personuppgifter endast för någon annans räkning kallas enligt personuppgiftslagen och förordningen för personuppgiftsbiträde. Ett sådant biträde bär enligt personuppgiftslagen inget personuppgiftsansvar. Personuppgiftsbiträdets roll förändras dock 2018 med dataskyddsförordningen. Biträdet kommer att få nya skyldigheter och ett betydligt utökat eget ansvar för personuppgiftsbehandlingen.

Frågor som kan behöva besvaras och redovisas

9) Vem kommer att bestämma ändamålen med och medlen för behandlingen (jämför personuppgiftsansvarig enligt 3 § personuppgiftslagen och förordningen artikel 4 punkt 7)?

10) I vilken verksamhet ska behandlingen av personuppgifterna ske?

- Myndighet, företag, eller annan form av organisation?
- Beskriv verksamheten noggrant, särskilt de delar som är relevanta för personuppgiftsbehandlingen; hur den är organiserad, hur den bedrivs i dag och vilka eventuella förändringar som föreslås, i vilka situationer krävs att personuppgifter behandlas.
- Vilka regler styr verksamheten i dag? Finns det befintliga bestämmelser som gäller för personuppgiftsbehandlingen?

Åtgärder för att minska integritetsrisker

- Klargör vilken organisation som ska ha behörighet att besluta om personuppgiftsbehandlingen (ändamål) och hur den ska utföras (medel), i synnerhet om flera aktörer är inblandade eller då utomstående aktörer anlitas för drift och utveckling av systemet.
- Överväg om personuppgiftsansvaret ska fastställas genom författningsreglering.[7] Relevanta regler i dataskyddsförordningen måste då besktas.

7 Enligt förordningen är detta möjligt när behandlingen är nödvändig för att fullgöra en rättslig förpliktelse och när behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6).

Personuppgifternas karaktär

Personuppgifternas karaktär har stor betydelse för vilka integritetsrisker som en behandling av uppgifterna kan medföra. Behandling av personuppgifter som har nära anknytning till privatlivet och personliga egenskaper medför normalt större integritetsrisker än uppgifter som avser någons yrkesroll. Men även inom arbetslivsområdet finns det personuppgiftsbehandling av integritetskänslig karaktär till exempel i personalärenden. För att bedöma integritetsriskerna måste uppgifternas karaktär bedömas tillsammans med andra faktorer såsom i vilket sammanhang uppgifterna behandlas, för vilket syfte och vilken spridning som de får eller riskerar att få (se nedan).

Vissa uppgiftstyper har i dataskyddsdirektivet och personuppgiftslagen ansetts som särskilt känsliga och behandlingen av sådana uppgifter omfattas därför av särskilda begränsningar. Det gäller personuppgifter om etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa och sexualliv samt uppgifter om lagöverträdelser. Därutöver brukar även bland annat biometriska uppgifter – det vill säga uppgifter om fysiska, fysiologiska eller beteendemässiga egenskaper som kan hänföras till en person såsom ansiktsbilder och fingeravtryck – anses integritetskänsliga (jämför 13 § personuppgiftslagen och art. 8 dataskyddsdirektivet). Genetiska och biometriska uppgifter är enligt artikel 9 dataskyddsförordningen också känsliga personuppgifter. Även uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden behandlas i dataskyddsdirektivet och personuppgiftslagen som särskilt integritetskänsliga (jämför 21 § personuppgiftslagen, art. 8.5 dataskyddsdirektivet och art. 10 dataskyddsförordningen).

Det finns även andra personuppgifter som normalt anses vara integritetskänsliga. Vägledande för bedömning av vad som ska anses vara integritetskänsliga personuppgifter kan vara de överväganden som lagstiftaren har gjort vid bedömningen av vilka uppgifter som omfattas av sekretess till skydd för enskild enligt offentlighets- och sekretesslagen (2009:400). Det gäller i synnerhet uppgifter som omfattas av stark eller absolut sekretess. Även befintlig reglering av personuppgiftsbehandling kan tyda på att uppgifterna är integritetskänsliga, till exempel myndigheternas registerförfattningar. Uppgifter om privatpersoners personliga och ekonomiska förhållanden anses normalt som känsliga till exempel när de behandlas inom bank- och försäkringsväsendet samt i inkassoverksamhet. Sådan behandling är också särskilt reglerad i bland annat kreditupplysningslagen (1973:1173) och inkassolagen (1974:182). Behandling av personuppgifter som avser personer med skyddade personuppgifter

enligt beslut från Skatteverket innebär förstås särskilda integritetsrisker. Detsamma kan generellt sägas om personuppgifter som avser barn och ungdomar. Vidare kan noteras att personuppgiftslagen innehåller en särskild bestämmelse (22 §) för behandling av personnummer.

Frågor som kan behöva besvaras och redovisas

11) Vilka typer av personuppgifter kan komma att behöva behandlas med anledning av utredningens förslag? Innefattar behandlingen personuppgifter som kan anses vara särskilt integritetskänsliga? Det bör särskilt redovisas om behandlingen innefattar någon av följande typer av personuppgifter.

- Personuppgifter om ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa, sexualliv (jämför 13 § personuppgiftslagen) samt uppgifter om lagöverträdelser (jämför 21 § personuppgiftslagen). Behandlas biometriska och genetiska uppgifter (en särskild kategori av personuppgifter enligt artikel 9 i förordningen).
- Personuppgifter som omfattas av sekretess (särskilt vid stark eller absolut sekretess) eller tystnadsplikt.
- Andra personuppgifter som normalt uppfattas som integritetskänsliga, till exempel uppgifter om enskildas personliga och ekonomiska förhållanden såsom kreditupplysningar, uppgifter om barn eller om personer i utsatta situationer.
- Systematisk och omfattande kartläggning av enskildas liv vad gäller till exempel hälsa, vistelseort, personliga preferenser, pålitlighet, beteenden, ekonomiska förhållanden.
- Bilder eller ljud- och videoinspelningar.
- Detaljerade och overifierade personuppgifter, såsom värdeomdömen.

Åtgärder för att minska integritetsrisker

- Överväg om personuppgifter av integritetskänslig karaktär behöver samlas in och begränsa i så fall den nödvändiga behandlingen av dessa uppgifter till ett minimum.
- Klargör tydligt vilka personuppgifter som får samlas in och vilka som inte får samlas in.

- Föreslå särskilda skyddsåtgärder för behandling av integritetskänsliga personuppgifter.

Personuppgiftsbehandlingens omfattning

Antalet personer som berörs av en viss behandling av personuppgifter är en av de faktorer som påverkar bedömningen av integritetsriskerna med personuppgiftsbehandlingen. Det gäller särskilt personuppgiftsbehandling som den enskilde har ingen eller liten möjlighet att avstå ifrån såsom myndighetsregister och elbolagens behandling i samband med tillhandahållande av elnät. Integritetsriskerna kan vara stora även om det handlar om uppgifter som uppfattas som harmlösa om det finns risk för att uppgifterna sammanställs och används på ett sätt som inte är avsett och som inte heller kan förutses.

Antalet uppgifter om de registrerade personerna är en annan faktor som påverkar bedömningen av integritetsriskerna. Exempelvis kan uppgifter om samtliga kreditkortsköp som en person har genomfört under ett år avslöja mycket om bland annat personens vanor, intressen och var denne har befunnit sig. Men även hantering av ett fåtal uppgifter kan innebära ett betydande intrång i den personliga integriteten om uppgifterna är av känslig karaktär.

Frågor som kan behöva besvaras och redovisas

12) Hur många personer kan komma att beröras av behandlingen?

13) Hur många uppgifter om varje person kommer att behandlas och hur detaljerade är uppgifterna?

14) Vilka möjligheter finns att använda de insamlade personuppgifterna för att kartlägga en persons liv?

Åtgärder för att minska integritetsrisker

- Begränsa omfattning av den föreslagna personuppgiftsbehandlingen till det som är nödvändigt utifrån ändamålet, både vad gäller antalet personer och antal uppgifter om varje person.

Insamling av personuppgifterna

Personuppgifter som ska behandlas för ett visst ändamål kan samlas in på flera sätt till exempel från de registrerade, myndighetsregister, kreditupplysningsregister, medlems- och kundregister och internet. Det är också vanligt att personuppgifterna redan finns hos den personuppgifts-

ansvarige och att det handlar om att uppgifterna ska användas för ett nytt ändamål eller i en annan verksamhetsgren.

Frågor som kan behöva besvaras och redovisas

15) Varifrån ska uppgifterna samlas in?

16) Finns det behov av en författningsreglerad uppgiftsskyldighet när personuppgifterna ska hämtas från någon annan organisation?

17) Ska ett eventuellt elektroniskt informationsutbyte mellan myndigheter regleras, och i sådana fall, hur?

18) Vilken information får de registrerade om insamlingen av personuppgifterna?

Åtgärder för att minska integritetsriskerna

- Vid särskilt integritetskänslig behandling av personuppgifter kan det vara lämpligt att föreskriva från vilka källor personuppgifter får inhämtas.
- Elektroniskt informationsutbyte mellan myndigheter som innefattar personuppgifter bör författningsregleras särskilt.

Sök- och sammanställningsmöjligheter

De integritetsrisker som följer med användningen av ny informationsteknik är nära kopplade till informationsteknikens egenskaper att söka och sammanställa stora mängder av uppgifter. Sök- och sammanställningsmöjligheterna kan medföra att uppgifter lättare kan knytas till en fysisk person till exempel genom beteendemönster och att uppgifterna därför ska betraktas som personuppgifter. De kan även medföra att personuppgifter som annars uppfattas som relativt harmlösa får en mer integritetskänslig karaktär till exempel genom omfattande registrering som innebär kartläggning av en persons liv.

Den så kallade missbruksregeln som har gett möjlighet att undanta tillämpningen av vissa bestämmelser i personuppgiftslagen återfinns inte i dataskyddsförordningen. Någon sådan bestämmelse finns inte heller med i förslaget till myndighetsdatalag, se SOU 2015:39 s. 236 f.

Med ny informationsteknik är det inte endast uppgifter i text som är sökbara. Med teknik för till exempel ansiktsigenkänning kan personer identifieras från fotografier. Biometrisk data innebär ofta särskilda integritetsrisker.

Vidare har myndigheternas sökmöjligheter betydelse för vad som utgör allmän handling enligt 2 kap. 3 § andra stycket tryckfrihetsförordningen. För att minska integritetsriskerna kan det därför finnas anledning att i lag eller förordning begränsa myndighetens möjligheter att söka efter uppgifter som inte är nödvändiga att behandla i myndighetens verksamhet (se 2 kap. 3 § tredje stycket tryckfrihetsförordningen).

Frågor som kan behöva besvaras och redovisas

19) Vilket behov av sök- och sammanställningsmöjligheter av personuppgifter finns för den föreslagna personuppgiftsbehandlingen?

20) Vilka möjligheter till sökning efter och sammanställning av personuppgifter kommer att finnas för den föreslagna personuppgiftsbehandlingen?

21) Vilka sökbegrepp kan behöva användas i verksamheten?

22) Vilka sammanställningar av uppgifter kan en myndighet bli skyldig att ta fram och tillhandahålla på begäran av enskilda enligt 2 kap. tryckfrihetsförordningen?

Åtgärder för att minska integritetsrisker

- Inför bestämmelser som begränsar sök- och sammanställningsmöjligheter av de personuppgifter som ska behandlas till exempel genom att föreskriva tillåtna sökbegrepp.
- Inför författningsreglerade begränsningar i sök- och sammanställningsmöjligheter. De bör begränsas till de som är motiverade utifrån ändamålet med behandlingen.
- Sök- och sammanställning av känsliga personuppgifter bör endast tillåtas om det är särskilt motiverat utifrån ändamålet.
- Möjligheter att göra så kallad fulltextsökning bör begränsas och inte vara tillåten när det gäller behandling av integritetskänsliga personuppgifter.

Spridning av och åtkomst till personuppgifterna

Spridning av personuppgifter har av naturliga skäl stor betydelse för integritetsriskerna med behandlingen. Det följer inte bara av att människor ofta känner en allmän obehagskänsla av att andra människor har kännedom om deras personliga förhållanden. Ökad spridning

ger också ökad risk för att uppgifterna kommer att användas på ett otillbörligt och icke avsett sätt.

Utgångspunkten är att personuppgifter inte ska spridas till fler än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det saknar i princip betydelse hur många som faktiskt tar del av personuppgifterna. Integritetsriskerna är desamma i de fall spridningen innebär att mottagarna har möjlighet att ta del av dem, det vill säga har åtkomst till personuppgifterna.

Det är ofta inte tillräckligt att begränsa åtkomsten genom regler och instruktioner. Det kan vara nödvändigt att begränsa spridningen och åtkomsten genom tekniska åtgärder såsom behörighetsstyrning och andra säkerhetsåtgärder som skyddar uppgifterna mot obehörig åtkomst. Utredningen bör redogöra för vilken form av behörighetsstyrning som anses nödvändig i det aktuella fallet.

När det gäller myndigheternas insamling av personuppgifter måste man tänka på offentlighetsprincipen. För att upprätthålla ett tillräckligt integritetsskydd kan det vara nödvändigt att se över de sekretessbestämmelser som gäller till skydd för uppgifter om enskilda hos den insamlande myndigheten. Är avsikten att personuppgifterna ska vara tillgängliga för flera myndigheter kan det också finnas behov av sekretessbrytande bestämmelser.

Frågor som kan behöva besvaras och redovisas

23) Vilka kommer att ha åtkomst till uppgifterna och vad är det som motiverar deras åtkomst till uppgifterna?

24) Kommer ett behörighetsstyrningssystem användas så att åtkomsten begränsas till olika kategorier av personuppgifter utifrån användarens arbetsuppgifter?

25) Kommer personuppgifterna att spridas utanför den egna organisationen och, i sådana fall, för vilket syfte?

26) Innebär förslaget krav på ökat informationsutbyte mellan myndigheter eller mellan myndigheter och företag och andra organisationer?

27) Innebär behandlingen att personuppgifter kommer att spridas till, eller inhämtas från, andra länder inom EU eller till länder utanför EU?

28) Ska personuppgifterna publiceras på nätet och, i sådana fall, för vilket syfte?

Åtgärder för att minska integritetsrisker

- Reglera vilka personkategorier som ska ha åtkomst till behandlade personuppgifter. Begränsa åtkomsten till känsliga person-uppgifter.
- Reglera under vilka förutsättningar personuppgifterna ska få lämnas ut utanför organisationen, myndigheten, eller dylikt (särskilt vad gäller så kallad direktåtkomst, jämför HFD 2015 ref 61).

Arkivering och gallring samt användning av arkiverade uppgifter

Personuppgifter ska inte sparas längre än vad som krävs för ändamålet med behandlingen (9 § första stycket i personuppgiftslagen). I vissa fall ställs det krav i författningar om att personuppgifter måste sparas under en viss tid för andra ändamål än för de som uppgifterna ursprungligen samlades in, till exempel för bokföring och för att förhindra penningtvätt.

När uppgifter sparas för sådana sekundära ändamål är det viktigt att klargöra att uppgifterna under bevarandetiden inte får användas för andra ändamål. För kreditprövningsändamål får till exempel aktuella kreditupplysningar användas under en relativt kort period. Om de därefter sparas för bokföringsändamål får de inte återanvändas för framtida kreditprövningar. När det inte längre finns något ändamål som kräver att uppgifterna ska bevaras, ska de raderas. För forskning, statistiska och vetenskapliga ändamål kan uppgifter dock få bevaras under en längre tidsperiod (se 9 § tredje stycket personuppgiftslagen).

För myndigheter och andra organ som omfattas av bestämmelserna om allmänna handlingars offentlighet i 2 kap. tryckfrihetsförordningen gäller kravet på bevarande av allmänna handlingar enligt arkivlagen. Avvikelser kan dock göras i annan författning. Det är således inte ovanligt att registerförfattningar innehåller särskilda regler om gallring.

Ett sätt att skydda personuppgifter som behöver bevaras elektroniskt, till exempel för arkivändamål, men som inte behövs i den löpande verksamheten är att uppgifterna avskiljs så att de inte är direkt tillgängliga för sök- och sammanställning och kombineras med begränsad åtkomst. En annan åtgärd kan vara så kallad pseudonymi-sering som innebär att identifiering av de registrerade är möjlig endast med hjälp av annan information (nyckel) som hålls avskild.

Om ändamålet med bevarandet kan uppnås utan tillgång till de aktuella personuppgifterna bör man överväga införandet av rutiner för avidentifiering av personuppgifterna.

Frågor som kan behöva besvaras och redovisas

29) Hur länge behöver personuppgifterna sparas och för vilka syften?

30) Omfattas personuppgifterna av handlingsoffentligheten enligt 2 kap. tryckfrihetsförordningen och finns det i sådana fall särskilda gallringsbestämmelser eller bör sådana införas?

Åtgärder för att minska integritetsrisker

- Reglera hur länge personuppgifter ska bevaras.
- Överväg gallringsbestämmelser för personuppgifter som ingår i allmänna handlingar.
- Överväg att införa krav på att personuppgifter som inte används i den dagliga verksamheten avskiljs med begränsad åtkomst.

De registrerades inflytande och rättigheter

De registrerades inflytande över behandlingen av deras personuppgifter har betydelse för bedömningen av vilka integritetsrisker behandlingen medför. Behandling av personuppgifter som sker på initiativ av den registrerade själv efter att denne har fått utförlig information om behandlingen innebär normalt ett mindre integritetsintrång än den som sker utan att den registrerade har möjligheter att påverka eller ens känner till den.

Den registrerade har rättigheter då dennes personuppgifter behandlas av någon annan, till exempel rätt att få information om behandlingen, rätt att begära rättelse av felaktiga uppgifter och rätt att begära skadestånd vid felaktig behandling.

Frågor som kan behöva besvaras och redovisas

31) Vilken inställning kan de registrerade antas ha till personuppgiftsbehandlingen?

32) Vilka möjligheter har en enskild person att motsätta sig behandlingen?

33) Vad är konsekvenserna för en enskild person om denne motsätter sig behandlingen?

34) Kommer den enskilde att vara i beroendeställning till den som behandlar uppgifterna?

35) Har den registrerade möjlighet att begära rättelse av uppgifter som behandlas på ett felaktigt sätt (jämför 28 § personuppgiftslagen)?

36) Vilken information får de registrerade om behandlingen (jämför 23–27 §§ personuppgiftslagen)?

- Hur och när lämnas informationen?
- Vad innefattas i informationen?
- Om information inte lämnas direkt till de registrerade, kan de ändå antas känna till behandlingen?

Åtgärder för att minska integritetsrisker

- Om behandlingen ska kunna utföras mot den registrerades vilja bör det uttryckligen regleras (jämför till exempel 2 kap. 2 § patientdatalagen, 2008:355).
- Överväg krav på information till de registrerade även i de fall behandlingen av personuppgifter sker med stöd av författning och information inte behöver lämnas (24 § andra stycket personuppgiftslagen, jämför artikel 11.2 dataskyddsdirektivet och art. 13–15 dataskyddsförordningen).

Användning av ny teknik

Användning av ny teknik eller nya användningssätt av befintlig teknik leder ofta till integritetsrisker som är svåra att förutse. Det kan handla om nya sätt att samla in uppgifter från användarnas utrustning till exempel wifi-tracking eller nya elektroniska tjänster för försäljning eller inom den offentliga förvaltningen. För att kunna analysera integritetsriskerna i sådana situationer krävs vanligtvis en noggrann beskrivning av förfarandet.

Vid utvecklingen av ny teknik för personuppgiftsbehandling finns det ofta möjlighet att bygga in ett särskilt skydd för den personliga integriteten (så kallad inbyggd integritet eller privacy by design). Det kan till exempel handla om att begränsa mängden personuppgifter som ska registreras, tekniska begränsningar för tillgång till personuppgifter och att låta systemet styra hur personuppgifter registreras.

Frågor som kan behöva besvaras och redovisas

37) Kommer personuppgifter att behandlas med teknik som inte är vanligt förekommande eller kommer etablerad teknik att användas på nya sätt?

38) På vilket sätt skiljer sig den använda tekniken från tidigare etablerad teknik? På vilket sätt skiljer sig användningssättet från tidigare förfaranden?

Åtgärder för att minska integritetsrisker

- Överväg möjligheterna att ställa krav på integritetsvänlig utformning av den teknik som ska användas för behandling av personuppgifter (inbyggd integritet, privacy by design).

Risker för missbruk

Den som behandlar någon annans personuppgifter har en skyldighet att skydda personuppgifterna (jämför 30–31 §§ personuppgiftslagen och artikel 25, 32–36 dataskyddsförordningen). Skyddet kan bestå av olika åtgärder för att skydda personuppgifterna från yttre och inre hot, till exempel genom att ha tillräcklig hög teknisk och organisatorisk säkerhet så att ingen obehörig kommer åt uppgifterna eller att uppgifter av misstag förvanskas. Vad som utgör en lämplig säkerhetsnivå måste bedömas utifrån en risk- och sårbarhetsanalys. Generellt gäller att ju känsligare personuppgifterna är och ju fler personuppgifter som hanteras, desto mer omfattande bör säkerhetsåtgärderna vara.

Frågor som kan behöva besvaras och redovisas

39) Vilka risker finns för otillåten eller oavsiktlig användning av personuppgifter inom och utanför den egna organisationen och vilka åtgärder ska vidtas för att skydda personuppgifterna från sådan användning?

- Finns det risk för att felaktiga eller inaktuella uppgifter kommer att behandlas?
- Finns det risk för att uppgifter kommer att behandlas utan rättsligt stöd, på ett olagligt sätt eller i strid med god sed?
- Finns det risk för att personuppgifterna sprids på ett icke avsett sätt?

- Hur många personer riskerar att drabbas av sådana integritetsintrång?

Åtgärder för att minska integritetsrisker

- Utför en risk- och sårbarhetsanalys för den föreslagna personuppgiftsbehandlingen.
- Överväg att införa författningskrav på säkerhetsåtgärder vid behandling av integritetskänsliga personuppgifter, till exempel krav på kryptering och stark autentisering vid överföring i ett öppet nät.

Integritetsrisker vid utökad eller förändrad personuppgiftsbehandling

I vissa fall måste integritetsriskerna med en viss personuppgiftsbehandling bedömas i ett bredare perspektiv och till exempel vägas samman med riskerna med befintlig personuppgiftsbehandling. Det kan vara aktuellt vid en gradvis utökad personuppgiftsbehandling eller då en tidigare otillåten personuppgiftsbehandling tillåts. Det kan också finnas anledning att överväga vilka effekter förslaget får för en viss bransch, delar av samhället eller samhället i stort.

Frågor som kan behöva besvaras och redovisas

40) Kan förslaget få konsekvenser för integritetsskyddet även om det endast handlar om ändringar av redan befintlig och tillåten personuppgiftsbehandling?

41) Har det tidigare förekommit förslag om liknande behandling av personuppgifter? Hur har integritetsriskerna redovisats och bedömts i dessa fall? Hur bedömdes tidigare förslag av remissinstanserna? Vad motiverar en annan bedömning i detta fall?

42) Vad blir den sammantagna bedömningen av integritetsriskerna av förslaget om integritetsriskerna vägs samman med eventuella tidigare förändringar avseende samma eller liknande fråga?

Sammanfattande analys och proportionalitetsbedömning

Efter en noggrann kartläggning och beskrivning av den föreslagna personuppgiftsbehandlingen och analys av de integritetsrisker som behandlingen kan medföra, bör en sammanfattande proportionalitetsbedömning göras där hänsyn tas till eventuella åtgärder som vidtagits för

att minska integritetsriskerna. Kravet på en sådan proportionalitetsbedömning följer, som nämnts ovan i inledningen, av Europakonventionen, EU:s grundläggande stadga samt regeringsformen. Kravet på proportionalitet framgår också i anslutning till flera bestämmelser i dataskyddsförordningen, exempelvis vid inskränkningar av de registrerades rättigheter enligt artikel 23. Dataskyddsförordningen innehåller även bestämmelser om att den personuppgiftsansvarige ska göra en bedömning av den planerade behandlingens konsekvenser för skyddet för personuppgifter innan särskilt riskfyllda behandlingar påbörjas (så kallad konsekvensbedömning avseende dataskydd, artikel 35). Såsom anges ovan kan i vissa fall en sådan konsekvensbedömning genomföras i samband med lagstiftningsåtgärder.

En proportionalitetsbedömning innebär i korthet att integritetsriskerna med en viss personuppgiftsbehandling vägs mot de fördelar som behandlingen bidrar med till det ändamål som förslaget avser att uppfylla. För att behandlingen ska vara tillåten måste fördelarna stå i rimlig proportion till nackdelarna. I detta ingår att bedöma om behandlingen av personuppgifter är nödvändig utifrån det avsedda ändamålet med behandlingen och om det finns alternativ som är mindre integritetskänsliga.

Frågor som kan behöva besvaras och redovisas

43) Vilket eller vilka ändamål motiverar behandlingen av personuppgifter?

44) Finns det alternativa sätt att uppnå ändamålet som innebär mindre integritetsrisker?

45) Är behandlingen ändamålsbegränsad (jämför 9 § c–f och i personuppgiftslagen, artikel 5.1 b-c och e dataskyddsförordningen)?

- Kommer behandlingen att omfatta fler personuppgifter än vad som är motiverat med hänsyn till ändamålet?
- Kommer behandlingen att omfatta uppgifter som inte är adekvata och relevanta i förhållande till ändamålet med behandlingen (9 § e personuppgiftslagen)?
- Kommer personuppgifterna behandlas för ändamål som är oförenliga med det ändamål för vilka de samlades in för?
- Kommer personuppgifterna bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen?

46) Står integritetsintrånget som behandlingen medför i rimlig proportion till de fördelar som behandlingen innebär för de avsedda ändamålen (jämför med intresseavvägningen i 10 § f personuppgiftslagen)?

47) Om proportionalitetsbedömningen visar att integritetsintresset väger över intresset för att få utföra behandlingen kan en reglering om integritetsskyddande åtgärder övervägas för att ändå möjliggöra behandlingen. Detta kan ske genom till exempel reglering om

- begränsningar av antalet personuppgifter eller användning av anonymiserade uppgifter,
- begränsning av ändamålen för personuppgiftsbehandlingen,
- begränsning av sökmöjligheter,
- begränsning av spridningen av personuppgifterna genom tekniska åtgärder såsom behörighetssystem,
- krav på rutiner för kvalitetsgranskning av personuppgifterna om det finns risk för felaktiga eller missvisande uppgifter,
- bättre teknisk säkerhet för de behandlade uppgifterna såsom kryptering och stark autentisering vid inloggning.

Rättsligt stöd för personuppgiftsbehandling

En fråga som hör nära samman med bedömningen av integritetsriskerna med ett författningsförslag är med vilket rättsligt stöd som förslaget bör genomföras. Det gäller bland annat frågan om förslaget är förenligt med grundlagarna, dataskyddsdirektivet och övrig EU-rätt. Det innefattar även frågan om förslaget kräver särskild reglering av personuppgiftsbehandlingen eller om det är tillräckligt med befintlig lagstiftning i framförallt personuppgiftslagen.

När dataskyddsförordningen börjar tillämpas den 25 maj 2018 är det den som primärt reglerar hur personuppgifter får behandlas. Förordningen är överordnad svensk rätt, men ger ett visst utrymme för nationell lagstiftning. I vissa fall är det påbjudet att anta nationella regler, i andra fall finns det utrymme för nationella regler. Det är därför av stor vikt att noggrant överväga vilket utrymme för nationella regler som förordningen ger.

Frågor som kan behöva besvaras och redovisas

48) Är behandlingen av sådan art att en bedömning enligt 2 kap. 6 § andra stycket regeringsformen behöver göras?
Bestämmelsen i 2 kap. 6 § andra stycket regeringsformen innebär att sådana åtgärder som föreslås ska prövas mot grundlagen och regleras i lag. Det är endast tillåtet med lagar som inskränker integritetsskyddet om det intresse som ska tillgodoses är så starkt och integritetsskyddsintresset så förhållandevis svagt att inskränkningen framstår som proportionerlig. Bestämmelsen innebär också att lagstiftaren tydligt måste redovisa vilka avvägningar som gjorts vid proportionalitetsbedömningen.
En begränsning av rättigheterna i 2 kap. 6 § andra stycket regeringsformen ska för att vara tillåten stadgas i lag och får inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den, se 2 kap. 20 och 21 §§ regeringsformen. I ett konkret lagstiftningsärende innebär det att det intrång som sker i den enskildes personliga integritet måste vara befogat och inte större än nödvändigt. Intrånget ska mötas av integritetshöjande bestämmelser till förmån för den enskilde vars personuppgifter behandlas.

49) Hur förhåller sig den föreslagna personuppgiftsbehandlingen och eventuell reglering av denna till

- EU:s dataskyddsdirektiv

- EU:s dataskyddsförordning som börjar gälla den 25 maj 2018 (Är utredningens förslag förenliga med dataskyddsförordningen? Finns det utrymme för nationell reglering?)
- EU-rätten i övrigt
- artikel 8 i Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR) samt
- artikel 7, 8 och 52 i EU:s stadga om de grundläggande rättigheterna.

50) Hur förhåller sig den föreslagna personuppgiftsbehandlingen, och eventuell reglering av denna, till bestämmelserna i tryckfrihetsförordningen och yttrandefrihetsgrundlagen?

För lagstiftning som ska omfatta tiden innan dataskyddsförordningen ska börja tillämpas bör punkterna 51–54 beaktas. I punkt 55 anges istället vad som behöver beaktas från och med den 25 maj 2018.

51) Om det anses tillräckligt att behandlingen omfattas av personuppgiftslagen bör bland annat följande frågor besvaras?

- På vilken grund ska behandlingen utföras? Tillåten behandling enligt personuppgiftslagen, det vill säga samtycke eller om behandlingen är nödvändig för ett avtal med den registrerade, för att uppfylla en rättslig skyldighet för den personuppgiftsansvarige, för att skydda vitala intressen för den registrerade, en arbetsuppgift av allmänt intresse eller efter en intresseavvägning (10 § personuppgiftslagen). Jämför artikel 6 i dataskyddsförordningen.
- Hur uppfylls kraven på information till den registrerade (23–27 §§ personuppgiftslagen)? Jämför artikel 12-15 i dataskyddsförordningen.
- Hur uppfylls den registrerades rättigheter i övrigt till exempel rätten till rättelse (28 § personuppgiftslagen)? Jämför artikel 16-19 i dataskyddsförordningen.
- Vilka krav på säkerhetsåtgärder krävs för den aktuella personuppgiftsbehandlingen (30–31 §§ personuppgiftslagen)? Jämför artikel 24-25 och 32-36 i dataskyddsförordningen.

52) Krävs särskilt författningsstöd för den föreslagna personuppgiftsbehandlingen?

- Konstitutionsutskottet har i flera lagstiftningsärenden som rört myndigheters personuppgiftsbehandling framhållit att målsätt-

ningen bör vara att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll ska regleras särskilt i lag (se till exempel bet. 1990/91:KU11 s. 11, 1997/98:KU18 s. 43). Regeringen har vid åtskilliga tillfällen instämt i denna bedömning (se till exempel prop. 1997/98:44 s. 41, 1999/2000:39 s. 78 och 2009/10:80 s. 183). Regeringen har också uttalat att behovet av lagstiftning är särskilt stort om uppgifterna sprids externt i inte obetydlig omfattning (prop. 1990/91:60 s. 58).

53) Om det krävs särskilt författningsstöd för den föreslagna personuppgiftsbehandlingen, bör man bland annat tänka på följande.

- Den som ska vara personuppgiftsansvarig och ändamålet med behandlingen bör anges.
- Hur förhåller sig den särskilda regleringen till bestämmelserna i personuppgiftslagen (jämför 2 § personuppgiftslagen)?
- Observera att vissa bestämmelser i personuppgiftslagen, på grund av formuleringen ”denna lag”, inte genom hänvisning i annan författning kan göras tillämpliga utanför personuppgiftslagen (jämför bestämmelsen om rättelse i 28 § och skadestånd i 48 §).[8]
- Är ändamålen med behandlingen angivna exklusivt eller är det mening att behandling för andra ändamål inom samma verksamhet ska bedömas enligt personuppgiftslagen eller annan lagstiftning?
- Begrepp som används i författningen bör ha samma betydelse som i personuppgiftslagen och dataskyddsförordningen.
- Finns det anledning att föreskriva om särskilda säkerhetsåtgärder utöver de som följer av personuppgiftslagen?

54) Har samtliga delar av den föreslagna personuppgiftsbehandlingen stöd i personuppgiftslagen eller annan författning?

55) Bedömningar som måste göras när dataskyddsförordningen ska börja tillämpas:

- Vilket utrymme finns det för nationella regler (art 6.2)? Det är viktigt att den nationella regleringen enbart omfattar sådant som dataskyddsförordningen ger utrymme för.

8 Observera att i dataskyddsförordningen som ersätter personuppgiftslagen i maj 2018 finns ingen bestämmelse som motsvarar 5 a § personuppgiftslagen med.

- Krävs det nationella regler för den avsedda personuppgiftsbehandlingen (art 6.3 och art 9)?
- Rör den föreslagna lagstiftningen behandling av personuppgifter inom något av följande i förordningen särreglerade områden: yttrande- och informationsfrihet (art 85), tillgång till allmänna handlingar (art 86), anställningsförhållanden (art 88) eller forskning, statistik eller arkivering (art 89)?
- Uppfyller lagstiftningen ett mål av allmänt intresse och är den proportionell mot det legitima mål som eftersträvas (art 6.3)?
- Är reglerna tydliga, precisa och förutsägbara för de personer som omfattas av bestämmelserna (skäl 41 i förordningen)?
- Om förslagen innebär begränsningar i registrerades rättigheter, är då kraven på sådan lagstiftning uppfyllda (art 23 respektive art 89)?

Ytterligare läsning

Om Europakonventionen och Europarådets dataskyddskonvention

- Europarådets webbplats www.coe.int/t/dghl/standardsetting/DataProtection/default_en.asp
- Danelius, Hans (2012), Mänskliga rättigheter i europeisk praxis: en kommentar till Europakonventionen om de mänskliga rättigheterna

Om EU:s stadga om de grundläggande rättigheterna, dataskyddsdirektivet och dataskyddsförordningen

- Handbook on European data protection law, European Union Agency for fundamental rights, 2014.
- Handbok om den europeiska lagstiftningen om skydd av personuppgifter http://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-handbook-data-protection-sv.pdf
- 29-gruppens yttranden ec.europa.eu/justice/data-protection/article-29/index_en.htm

Om integritetsskyddet i regeringsformen

- Prop. 2009/10:80 En reformerad grundlag s. 171 f. och 249 f.

Om personuppgiftslagen m.m.

- Datainspektionens webbplats www.datainspektionen.se/lagar-och-regler/

Om Datainspektionens synpunkter på lagförslag m.m.

- Datainspektionens remissyttranden www.datainspektionen.se/ladda-ner-och-bestall/remisser/

Kontakta Datainspektionen

E-post: datainspektionen@datainspektionen.se Webb: www.datainspektionen.se
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm.

Datainspektionen