IMY. Integritetsskydds myndigheten

Vägledning för integritetsanalys i lagstiftningsarbete

Diarienr:
IMY-2022-10835

Innehåll

Inledning ... 4
Syftet med vägledningen ... 4
Integritetsfrågorna måste beaktas redan när lagstiftningsarbetet inleds ... 4
Hur regleras skyddet av den personliga integriteten? ... 5
STEG 1: Kartlägg personuppgiftsbehandlingen och bedöm vilket regelverk som är tillämpligt ... 6
Exempel på frågor att ta ställning till: ... 7
STEG 2: Kartlägg och bedöm integritetsriskerna med personuppgiftsbehandlingen ... 7
Vilka typer av personuppgifter ska behandlas? ... 8
Exempel på frågor att ta ställning till: ... 9
Hur omfattande är personuppgiftsbehandlingen? ... 9
Exempel på frågor att ta ställning till: ... 9
Vilka aktörer ska behandla personuppgifter och vilka roller har de? ... 9
Exempel på frågor att ta ställning till: ... 10
Vilket inflytande kommer de registrerades att ha över behandlingen och hur ser förhållandet ut till den personuppgiftsansvarige? ... 10
Exempel på frågor att ta ställning till: ... 10
Vilka är de övergripande ändamålen med personuppgiftsbehandlingen? ... 11
Exempel på frågor att ta ställning till: ... 11
Vilken spridning kommer personuppgifterna att få? ... 11
Exempel på frågor att ta ställning till: ... 12
STEG 3: Kartlägg befintlig reglering ... 12
Dataskyddsförordningens krav på laglighet och rättslig grund ... 12
Kartläggning av befintlig reglering och rättsliga grunder ... 13
STEG 4: Behovet av ny reglering ... 14
Finns det rättslig grund enligt artikel 6 i dataskyddsförordningen för personuppgiftsbehandlingen? ... 14
Finns det stöd i artikel 9 för behandling av känsliga personuppgifter? ... 15
Finns det stöd för behandling av personuppgifter som rör lagöverträdelser? ... 16
Finns det behov av stöd för vidarebehandling av personuppgifter (artiklarna 5.1 b och 6.4)? ... 17
Behövs det undantag enligt artikel 23 i dataskyddsförordningen? ... 18
Bedömning av om det finns stöd för personuppgiftsbehandlingen ... 19
STEG 5: 2 kap. 6 § andra stycket regeringsformen ... 19
Exempel på frågor att ta ställning till: ... 20
STEG 6: Utformningen av ny reglering ... 20
Allmänna utgångspunkter för regleringen ... 20
Normgivningsnivå ... 21

Hur ska den rättsliga grunden enligt artikel 6.3 regleras? ... 21
Särskilda typer av bestämmelser som kan behövas för att uppfylla kraven i dataskyddsförordningen ... 22
Bestämmelser om personuppgiftsansvar ... 22
Bestämmelser om vilka personuppgifter som får behandlas ... 22
Bestämmelser om känsliga personuppgifter ... 22
Bestämmelser som ger stöd för behandling av uppgifter om lagöverträdelser ... 23
Bestämmelser om tillåtna ändamål ... 23
Reglering av andra integritetshöjande åtgärder i syfte att minska integritetsrisker ... 23
STEG 7: Slutlig proportionalitets- och nödvändighetsbedömning ... 24
Integritetsanalys i lagstiftningsarbete – checklista ... 26
STEG 1: Kartlägg personuppgiftsbehandlingen och bedöm vilket regelverk som är tillämpligt ... 26
STEG 2: Kartlägg och bedöm integritetsriskerna med personuppgiftsbehandlingen ... 26
STEG 3: Kartlägg befintlig reglering ... 26
STEG 4: Behovet av ny reglering ... 27
STEG 5: 2 kap. 6 § andra stycket regeringsformen ... 27
STEG 6: Utformningen av ny reglering ... 27
STEG 7: Slutlig proportionalitets- och nödvändighetsbedömning ... 28

Inledning

Syftet med vägledningen

Denna vägledning riktar sig främst till den som tar fram författningsförslag som medför behandling av personuppgifter, till exempel inom Regeringskansliet, offentliga utredningar eller myndigheter. Den ger också stöd till den som skriver kommittédirektiv eller andra typer av uppdragsbeskrivningar som omfattar författningsändringar eller framtagande av ny reglering.

Vägledningen tillhandahåller en metod för att göra en integritetsanalys. Med integritetsanalys avses här en analys av om ett förslag är förenligt med bestämmelserna om skyddet för den personliga integriteten vid behandling av personuppgifter. En viktig del i denna analys är bedömningen av om konsekvenserna för den personliga integriteten som personuppgiftsbehandlingen medför är nödvändiga och proportionerliga i förhållande till det man avser att uppnå med behandlingen. En förutsättning för att kunna göra en sådan bedömning är att det sker en kartläggning av såväl behoven som integritetsriskerna med personuppgiftsbehandlingen.

Vägledningen tar framför allt sikte på sådan personuppgiftsbehandling som omfattas av dataskyddsförordningen[1], men kan även ge vägledning för sådan behandling av personuppgifter som omfattas av brottsdatalagen[2] eller annan dataskyddslagstiftning som faller utanför EU-rättens tillämpningsområde.

För att ge en översiktlig och användbar metod har vägledningen fokuserats på centrala och vanligt förekommande frågeställningar. Vägledningen innehåller således inte en uttömmande beskrivning av alla dataskyddsfrågor som kan uppkomma i lagstiftningsarbetet.

Vägledningen är uppbyggd i sju steg och innehåller exempel på frågor som kan behöva besvaras och redovisas samt förslag på bestämmelser om skyddsåtgärder som kan vidtas för att minska integritetsriskerna. När bedömningen görs att befintlig reglering, tillsammans med föreslagen verksamhetsreglering, ger tillräckligt stöd är det möjligt att avsluta integritetsanalysen efter steg 4.

Integritetsfrågorna måste beaktas redan när lagstiftningsarbetet inleds

Det är viktigt att integritetsfrågorna identifieras i ett tidigt skede i lagstiftningsprocessen, det vill säga redan i samband med framtagandet av kommittédirektiv, regeringsuppdrag till en myndighet eller liknande. Det behöver i det skedet bedömas om det i direktiven eller uppdragsbeskrivningen bör ges ett uppdrag att genomföra en integritetsanalys. När det kan förutses att förslagen kommer att medföra integritetsrisker som inte är obetydliga bör utredningen ges i uppdrag att utföra en integritetsanalys. Steg 1 och 2 i vägledningen kan användas som stöd för att bedöma den frågan. Steg 3, 4 och 6 i vägledningen kan användas för att bedöma om utredningen behöver ges i uppdrag att överväga om det finns behov av särskilda typer av bestämmelser om behandlingen av personuppgifter.

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[2] Brottsdatalagen (2018:1177).

Om det förutses att grundlagsskyddet i 2 kap. 6 § andra stycket regeringsformen kan bli tillämpligt bör utredningen ges i uppdrag att utreda om förslagen innebär en begränsning av grundlagsskyddet och, i så fall, att bedöma om förslagen är förenliga med 2 kap. 20 och 21 §§ regeringsformen. Steg 5 kan ge stöd i bedömningen av om ett sådant uppdrag behövs.

Hur regleras skyddet av den personliga integriteten?

I detta avsnitt görs en översiktlig genomgång av regleringen om den personliga integriteten.

Var och en har rätt till skydd för sitt privatliv enligt artikel 8 i Europakonventionen[3] och artikel 7 i EU:s stadga om de grundläggande rättigheterna[4]. I artikel 8 i stadgan anges även att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

Ett skydd för den personliga integriteten 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.

Det allmänna skyddet för den personliga integriteten i samband med behandling av personuppgifter regleras i dataskyddsförordningen. Dataskyddsförordningen är direkt tillämplig i varje medlemsstat, men både förutsätter och tillåter att det i vissa fall finns nationella bestämmelser som kompletterar eller utgör undantag från förordningens regler. Europeiska dataskyddsstyrelsen (EDPB), har till uppgift att utfärda bland annat riktlinjer och rekommendationer för att se till att dataskyddsförordningen tillämpas enhetligt (se artikel 70 i dataskyddsförordningen). Sådana dokument ger viktig vägledning även i lagstiftningsarbetet.

I Sverige finns generella bestämmelser som kompletterar dataskyddsförordningen i dataskyddslagen[5] och kompletteringsförordningen[6]. Det finns även andra författningar som kompletterar dataskyddsförordningen inom olika områden. Det finns till exempel så kallade registerförfattningar som innehåller särskilda regler om personuppgiftsbehandling för framför allt myndigheter. Det är dock viktigt att komma ihåg att dataskyddsförordningen är direkt tillämplig. Det innebär att kompletterande nationell reglering behöver vara förenlig med förordningen och tillämpas tillsammans med den.

I brottsdatadirektivet[7] finns särskild reglering för den personuppgiftsbehandling som utförs av behöriga myndigheter i syfte att bland annat förebygga, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Brottsdatadirektivet har genomförts i svensk rätt genom brottsdatalagen och brottsdataförordningen[8]. Dessutom har varje brottsbekämpande myndighet en egen lag som kompletterar brottsdatalagen, till

[3] Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.
[4] EU:s stadga om de grundläggande rättigheterna (2010/C83/02).
[5] Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.
[6] Förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.
[7] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.
[8] Brottsdataförordningen (2018:1202).

exempel lagen om polisens behandling av personuppgifter inom brottsdatalagens område[9].

Vidare har Sverige tillträtt Europarådets dataskyddskonvention[10] som framför allt har betydelse inom det område som inte omfattas av EU-rätten, till exempel försvar och nationell säkerhet.[11] Inom det området gäller varken dataskyddsförordningen eller brottsdatadirektivet. På det här området finns det idag nationell lagstiftning som till exempel styr Försvarsmaktens[12] och Försvarets radioanstalts behandling av personuppgifter[13].

Bestämmelser om sekretess och tystnadsplikt kan också vara en del av skyddet för personuppgifter. Det finns således en samverkan mellan sådana bestämmelser och dataskyddsbestämmelserna.

STEG 1: Kartlägg personuppgiftsbehandlingen och bedöm vilket regelverk som är tillämpligt

Det första steget i integritetsanalysen är att så detaljerat som möjligt kartlägga och beskriva den behandling av personuppgifter som förslaget medför eller förutsätter. Ofta är det flera aktörer som kommer att behandla personuppgifter. Det är viktigt att tidigt skapa sig en helhetsbild av den personuppgiftsbehandling som kommer att aktualiseras genom förslaget.

En förutsättning för att dataskyddsförordningen ska vara tillämplig är att *personuppgifter* behandlas. Definitionen av personuppgifter är mycket vid. Med personuppgifter avses varje upplysning som avser en identifierad eller identifierbar fysisk person som är i livet. Avgörande är om den personuppgiftsansvarige eller någon annan kan knyta den aktuella uppgiften, ensamt eller i kombination med andra uppgifter, till en individ (se artikel 4.1 i dataskyddsförordningen samt skäl 26 och 27 till dataskyddsförordningen). Den person som personuppgifterna rör kallas i dataskyddsförordningen för *den registrerade*.

Om en uppgift varken direkt eller indirekt kan knytas till en fysisk person är det inte en personuppgift. Utanför dataskyddsförordningens tillämpningsområde faller uppgifter som anonymiserats så att de inte längre kan kopplas till en fysisk person. Man bör dock vara uppmärksam på att det kan vara mycket svårt att helt och hållet anonymisera uppgifter. Genom att behandla flera uppgifter om en fysisk person, som var för sig inte kan knytas till den personen, är det ibland möjligt att identifiera denne genom så kallad bakvägsidentifiering.

För att dataskyddsförordningen ska vara tillämplig krävs vidare att personuppgifterna *behandlas*. Behandling är ett vidsträckt begrepp och omfattar exempelvis insamling, registrering, lagring, bearbetning, utlämnande genom överföring, spridning eller radering (se artikel 4.2 i dataskyddsförordningen).

[9] Lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område.
[10] Europarådets konvention 108 av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter.
[11] Det bör dock noteras att genom 1 kap. 2 § dataskyddslagen har dataskyddsförordningens tillämpningsområde i Sverige utsträckts till att omfatta bland annat området utanför EU-rätten.
[12] Lagen (2021:1171) om behandling av personuppgifter vid Försvarsmakten.
[13] Lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt.

Dataskyddsförordningen omfattar personuppgiftsbehandling som *helt eller delvis är automatiserad* (se artikel 2.1). Automatiserad behandling omfattar till exempel behandling som sker med hjälp av datorer, smartphones och digitalkameror. Att delvis automatiserad behandling omfattas innebär till exempel att förordningen är tillämplig när uppgifter som behandlas automatiskt skrivs ut eller lämnas ut i pappersform. Även *manuell behandling* av personuppgifter – till exempel renodlad pappershantering – omfattas om personuppgifterna ingår eller kommer att ingå i ett register (se artiklarna 2.1 och 4.6).

Dataskyddsförordningen är inte tillämplig inom brottsdatalagens tillämpningsområde och inte heller utanför EU-rättens tillämpningsområde. Det är viktigt att tidigt avgöra om förslaget kommer att omfatta områden där dataskyddsförordningen inte är tillämplig. Tänk på att en och samma behandling kan omfattas av olika regelverk. Ett exempel på detta är förslag som innebär att uppgifter som behandlas av Försäkringskassan (dataskyddsförordningen) lämnas ut till Polismyndigheten för användning i den myndighetens brottsbekämpande verksamhet (brottsdatalagen).

Exempel på frågor att ta ställning till:

- Innebär förslaget att personuppgifter kommer att behandlas, antingen som en direkt följd eller som en indirekt konsekvens av förslaget? Även en utökad personuppgiftsbehandling kräver en analys vilket är särskilt viktigt när den tidigare bedömningen är gjord i tiden före dataskyddsförordningens ikraftträdande.
- Är behandlingen av personuppgifter helt eller delvis automatiserad eller kommer uppgifterna att behandlas i ett så kallat manuellt register?[14]
- Kartlägg personuppgiftsbehandlingen. Beskriv så tydligt som möjligt vilka personuppgifter som kommer att behandlas, på vilket sätt personuppgifterna kommer att behandlas och av vilka aktörer. Ofta är flera aktörer inblandade – beskriv då hela flödet, till exempel vilka aktörer som samlar in, lämnar ut, tar emot och vidarebehandlar uppgifterna.
- Kommer personuppgiftsbehandlingen att ske utanför det område som regleras av dataskyddsförordningen, till exempel inom tillämpningsområdet för brottsdatadirektivet[15]? Tänk på att ett förslag kan omfatta behandling inom flera områden, till exempel vid informationslämnande mellan brottsbekämpande myndigheter och myndigheter som lyder under dataskyddsförordningen.

STEG 2: Kartlägg och bedöm integritets-riskerna med personuppgiftsbehandlingen

Nästa steg är att göra en kartläggning och bedömning av integritetsriskerna med personuppgiftsbehandlingen. En svårighet är att integritetsriskerna inte alltid framgår klart från början. Till exempel kan en föreslagen behandling av personuppgifter innebära risker för intrång i den enskildes personliga integritet om de kopplas samman med personuppgifter som redan behandlas. Ibland kan flera mindre omfattande författningsförslag, som var för sig kan anses ha rättsligt stöd enligt dataskyddsregleringen, sammantaget innebära ett avsevärt intrång i den enskildes personliga integritet.

[14] Se artikel 2.1 i dataskyddsförordningen.
[15] Se artikel 2.2 d i dataskyddsförordningen.

Kartläggningen och bedömningen bör omfatta alla aktörer och personuppgiftsbehandlingar som omfattas av förslaget. Nedan anges frågor som är centrala för att bedöma integritetsriskerna.

Vilka typer av personuppgifter ska behandlas?

Personuppgifternas karaktär har stor betydelse för vilka integritetsrisker som en behandling av uppgifterna kan medföra. Av regleringen i dataskyddsförordningen framgår att vissa typer av personuppgifter kräver ett särskilt skydd.

- *Känsliga personuppgifter*. Det är som huvudregel förbjudet att behandla känsliga personuppgifter, det vill säga personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.[16] Se nedan under avsnittet Finns det stöd i artikel 9 för behandling av känsliga personuppgifter?, sid. 15 f.
- *Personuppgifter som rör lagöverträdelser*. Personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott eller därmed sammanhängande säkerhetsåtgärder ges ett särskilt skydd i förordningen.[17] Se nedan under avsnittet Finns det stöd för behandling av personuppgifter som rör lagöverträdelser?, sid. 16 f.
- *Personnummer och samordningsnummer*. Dessa uppgifter har ett särskilt skydd genom bestämmelserna i 3 kap. 10 och 11 §§ dataskyddslagen (se också artikel 87 i dataskyddsförordningen).

Även behandling av andra personuppgifter än de som anges ovan kan medföra särskilda integritetsrisker. Allmänt kan sägas att behandling av personuppgifter som rör den registrerade som privatperson, till exempel uppgifter om personliga egenskaper, sociala förhållanden och privata ekonomiska skulder innebär större integritetsrisker än behandling av personuppgifter som avser den registrerades yrkesliv. Men även inom arbetslivsområdet förekommer det behandling av personuppgifter av integritetskänslig karaktär, exempelvis i personalärenden.

Att personuppgifter omfattas av sekretess eller tystnadsplikt som syftar till att skydda enskildas personliga eller ekonomiska förhållanden är något som talar för att det finns särskilda integritetsrisker. Det gäller också behandling av personuppgifter som avser personer med skyddade personuppgifter enligt beslut från Skatteverket.

För att bedöma integritetsriskerna måste uppgifternas karaktär bedömas tillsammans med andra faktorer, till exempel i vilket sammanhang som uppgifterna behandlas, för vilket ändamål och vilka som kan få åtkomst till uppgifterna.

Vissa kategorier av registrerade kan även generellt sett anses vara i behov av särskilt skydd då de kan ha svårare att tillvarata sina rättigheter. Barn anses enligt dataskyddsförordningen vara en särskilt skyddsvärd grupp (se skäl 38 till dataskyddsförordningen).

[16] Se artikel 9 i dataskyddsförordningen och 3 kap. dataskyddslagen.
[17] Se artikel 10 i dataskyddsförordningen, 3 kap. 8 och 9 §§ dataskyddslagen, 5-7 §§ kompletteringsförordningen och IMY:s föreskrifter om behandling av personuppgifter som rör lagöverträdelser (DIFS 2018:2).

Exempel på frågor att ta ställning till:

- Behandlas känsliga personuppgifter?
- Behandlas personuppgifter om lagöverträdelser?
- Behandlas personnummer eller samordningsnummer?
- Behandlas andra uppgifter som innebär särskilda integritetsrisker? Det gäller till exempel personuppgifter som rör enskilda som privatpersoner, personuppgifter som omfattas av sekretess till skydd för enskildas personliga eller ekonomiska förhållanden eller uppgifter om särskilda skyddsvärda kategorier av registrerade, till exempel barn.

Hur omfattande är personuppgiftsbehandlingen?

Antalet personer som omfattas av personuppgiftsbehandlingen är en av de faktorer som påverkar bedömningen av integritetsriskerna. Även antalet uppgifter om varje registrerad är en faktor som påverkar integritetsriskerna eftersom det innebär en större möjlighet att kartlägga personen. Detta gäller både om det är fråga om en större mängd uppgifter av samma typ eller om det är fråga om många olika typer av uppgifter. Exempelvis kan uppgifter om samtliga kortköp 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.

Sök- och sammanställningsmöjligheter kan medföra att personuppgifter som annars uppfattas som relativt harmlösa får en mer integritetskänslig karaktär. Sökningar som tar sikte på känsliga personuppgifter och personuppgifter om lagöverträdelser är av naturliga skäl förknippade med större risker i integritetshänseende.

I vissa fall måste integritetsriskerna med en viss personuppgiftsbehandling bedömas i ett bredare perspektiv och till exempel vägas samman med riskerna med redan befintlig personuppgiftsbehandling. Det kan särskilt bli aktuellt vid personuppgiftsbehandling som gradvis utökas på ett särskilt område. Det kan också finnas anledning att överväga vilka effekter förslaget får för en viss bransch, delar av samhället eller samhället i stort.

Exempel på frågor att ta ställning till:

- Hur många personer kan komma att omfattas av personuppgiftsbehandlingen?
- Vilka kategorier av personuppgifter kommer att behandlas för varje registrerad?
- Hur många personuppgifter kommer att behandlas i varje kategori och hur detaljerade är uppgifterna?
- Vilka möjligheter finns det att använda personuppgifterna för att kartlägga en persons liv?
- Vilket behov av och vilka möjligheter till sökning och sammanställning av personuppgifter kommer att finnas för personuppgiftsbehandlingen?

Vilka aktörer ska behandla personuppgifter och vilka roller har de?

Hur rollfördelningen ser ut vid personuppgiftsbehandling påverkar både förutsättningarna för behandlingen och vilka integritetsrisker som behandlingen kan medföra.

Personuppgiftsansvarig är den eller de som bestämmer för vilket eller vilka ändamål som personuppgifterna ska behandlas (varför) och medlen för behandlingen (hur), se artikel 4.7 i dataskyddsförordningen. Om flera aktörer tillsammans bestämmer ändamål och medel för personuppgiftsbehandlingen kan de anses vara *gemensamt personuppgiftsansvariga* (se artikel 26). Personuppgiftsansvaret bestäms normalt utifrån de faktiska omständigheterna i varje enskilt fall. Det är också möjligt att fastställa vem som är personuppgiftsansvarig i unionsrätt eller i nationell rätt (se artikel 4.7).

Ett *personuppgiftsbiträde* är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning (se artikel 4.8). När uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal eller en rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet (se artikel 28.3).

EDPB har beslutat om riktlinjer som ger vägledning för tolkningen av ovan nämnda bestämmelser.[18]

Exempel på frågor att ta ställning till:

- Vem kommer att bestämma ändamål och medlen för personuppgiftsbehandlingen?
- Finns det flera aktörer som är gemensamt personuppgiftsansvariga?
- Kommer ett personuppgiftsbiträde att behandla personuppgifter för någon annans räkning?

Vilket inflytande kommer de registrerades att ha över behandlingen och hur ser förhållandet ut till den personuppgiftsansvarige?

De registrerades inflytande över behandlingen av deras personuppgifter har betydelse för bedömningen av vilka integritetsrisker som behandlingen medför. Personuppgiftsbehandling som sker på den registrerades initiativ efter att denne har fått information om behandlingen innebär normalt ett mindre integritetsintrång. Behandling som den registrerade inte har någon möjlighet att motsätta sig är typiskt sett mer integritetskänslig. Om den registrerade inte får information om behandlingen innebär den normalt ett ännu större integritetsintrång.

Vidare har förhållandet mellan den personuppgiftsansvarige och den registrerade betydelse för hur integritetskänslig behandlingen är. Om den registrerade står i beroendeförhållande till den personuppgiftsansvarige eller om den registrerade befinner sig i en utsatt position ökar integritetsriskerna. Exempel på sådana situationer kan vara förhållandet mellan arbetsgivare-arbetstagare, myndighet-enskild, vårdgivare-patient eller skola-elev.

Exempel på frågor att ta ställning till:

- Kommer de registrerade att ges information om behandlingen (artiklarna 12-15) eller kommer det att krävas undantag?
- Kommer det att krävas undantag från de registrerades rättigheter i övrigt (artiklarna 16-22)?

[18] EDPB:s riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_sv.pdf

- Kommer de registrerade att vara i beroendeförhållande eller i en utsatt position i förhållande till den som behandlar personuppgifterna?

Vilka är de övergripande ändamålen med personuppgiftsbehandlingen?

En grundläggande princip är att personuppgifter endast får samlas in för särskilda, uttryckligt angivna och berättigade ändamål och att de inte senare får behandlas på ett sätt som är oförenligt med dessa ändamål (artikel 5.1 b, principen om ändamålsbegränsning). I registerförfattningar, det vill säga författningar som innehåller särskild reglering om framför allt myndigheters personuppgiftsbehandling, finns det ofta en reglering av tillåtna ändamål för behandlingen av personuppgifter.

Det är inte alltid möjligt att i lagstiftningsarbetet fastställa de närmare ändamålen för behandlingen. Det är dock viktigt att man, som ett led i integritetsanalysen, beskriver de tänkta ändamålen så utförligt som möjligt. En beskrivning av ändamålen är en förutsättning för att kunna bedöma om behovet av personuppgiftsbehandlingen överväger de integritetsrisker som behandlingen kommer att medföra och om behandlingen således är tillåten.

Typen av ändamål påverkar riskerna med behandlingen. Behandling som syftar till att övervaka eller kartlägga enskilda innebär stora integritetsrisker. Vidare är större integritetsrisker förknippade med behandling som syftar till att vidta åtgärder med negativa konsekvenser för den registrerade. Även behandling av personuppgifter med positiva konsekvenser för den enskilde kan emellertid innebära stora integritetsrisker, till exempel inom hälso- och sjukvård och social omsorg.

Exempel på frågor att ta ställning till:

- För vilket eller vilka ändamål ska behandlingen av personuppgifterna ske, det vill säga varför ska behandlingen utföras?
- Finns det särskilda risker att det kan ske en ändamålsglidning, det vill säga att uppgifter som samlas in för ett ändamål senare behandlas för ett annat?
- Är syftet eller effekten med behandlingen kartläggning eller övervakning av den enskilde?
- Är syftet med behandlingen att vidta åtgärder med negativa konsekvenser för den enskilde?

Vilken spridning kommer personuppgifterna att få?

Normalt ökar integritetsriskerna med en större spridning av personuppgifterna. I steg 1 har de aktörer som kommer att behandla personuppgifter kartlagts. Av den kartläggningen kan vissa slutsatser dras om spridningen.

Vidare är bestämmelser om sekretess och tystnadsplikt ofta avgörande för vilken spridning som personuppgifterna kommer att få. Det bör därför kartläggas om de aktuella uppgifterna omfattas av sekretess eller inte för att bedöma spridningsriskerna.

Vid informationsutbyte mellan myndigheter och andra aktörer kan det ibland bli aktuellt med direktåtkomst. Det som vanligtvis avses med direktåtkomst är att någon har direkt tillgång till någon annans register eller databas, och på egen hand kan söka efter information, men utan att kunna påverka innehållet i registret eller databasen.[19] Sådan

[19] Jfr HFD 2015 ref. 61 och Myndighetsdatalag, SOU 2015:39.

åtkomst anses medföra särskilda integritetsrisker och brukar normalt bli föremål för särskild reglering.

En särskild form av spridning är överföring av personuppgifter till tredjeland, det vill säga utanför EU- och EES-området. Sådana överföringar kan innebära särskilda integritetsrisker och regleras särskilt i kapitel V i dataskyddsförordningen. Om förslaget medför att sådana överföringar ska ske krävs det särskilda överväganden för att säkerställa att överföringen är förenlig med dataskyddsförordningen. En vanlig fråga är om det finns ett tillämpligt undantag enligt artikel 49 i dataskyddsförordningen.[20]

Exempel på frågor att ta ställning till:

- Vilka aktörer kommer att få tillgång till personuppgifterna?
- På vilket sätt kommer olika aktörer att få tillgången till uppgifterna? Kommer exempelvis direktåtkomst vara nödvändig?
- Omfattas uppgifterna av sekretess eller lagreglerad tystnadsplikt?
- Ska personuppgifterna publiceras på internet? En sådan personuppgiftsbehandling medför ofta särskilda integritetsrisker.
- Innebär behandlingen att personuppgifter kommer att föras över till andra länder utanför EU och EES?[21]

STEG 3: Kartlägg befintlig reglering

I detta steg kartläggs befintlig reglering som kan ge stöd för personuppgiftsbehandlingen. Det är viktigt att kartlägga både reglering som styr själva verksamheten, till exempel hälso- och sjukvårdslagen[22], och eventuell dataskyddsreglering, exempelvis patientdatalagen[23].

Inledningsvis redogörs för de krav som dataskyddsförordningen ställer på laglighet och rättslig grund.

Dataskyddsförordningens krav på laglighet och rättslig grund

Laglighetsprincipen i artikel 5.1 a i dataskyddsförordningen innebär bland annat att varje personuppgiftsbehandling måste ha stöd i minst ett av de villkor som räknas upp i artikel 6.1 i dataskyddsförordningen. Man brukar säga att det ska finnas en rättslig grund för behandlingen. Flera rättsliga grunder i artikel 6.1 kan vara tillämpliga avseende en och samma behandling.

Merparten av *myndigheternas personuppgiftsbehandling* sker med stöd av artikel 6.1 c (rättslig förpliktelse) och 6.1 e (uppgift av allmänt intresse eller myndighetsutövning). För sådan behandling finns det enligt artikel 6.2 ett generellt utrymme för nationell reglering som preciserar bestämmelserna i förordningen. Vidare finns det i artikel 6.3 ett krav på att den grund för behandlingen som avses i artikel 6.1 c och e ska fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. I svensk rätt kan den rättsliga grunden för

[20] Se EDPB:s riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_sv.pdf
[21] Se kap. V i dataskyddsförordningen. EDPB har antagit riktlinjerna 05/21 ”Guidelines on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR” som klargör vad som utgör en överföring av personuppgifter till tredjeland, https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf
[22] Hälso- och sjukvårdslagen (2017:30).
[23] Patientdatalagen (2008:355).

behandlingen fastställas i lag eller annan författning, i kollektivavtal eller beslut som har meddelats med stöd av lag eller annan författning.[24]

Den reglering som fastställs i nationell rätt för att ge stöd för behandlingen benämns i förordningen som ”rättslig grund”. Begreppet ”rättslig grund” används således i lagstiftningsarbetet i två betydelser; dels som en beteckning för de villkor för laglighet som anges i artikel 6.1 i dataskyddsförordningen, dels som en beteckning för den reglering i unionsrätt eller nationell rätt som fastställs enligt artikel 6.3 i förordningen. I den rättsliga grunden som fastställs enligt artikel 6.3, kan även mer specifika bestämmelser om personuppgiftsbehandlingen tas in.[25] Detta kan vara nödvändigt för att uppfylla förordningens krav på tydlighet, precision och proportionalitet (se vidare i steg 4 nedan).

Myndigheter kan inte använda intresseavvägning (artikel 6.1 f) som rättslig grund för sin personuppgiftsbehandling när de utför sina uppgifter.[26] Vidare har myndigheter begränsade möjligheter att använda samtycke (artikel 6.1 a) som rättslig grund eftersom obalansen i maktförhållandet mellan myndigheter och enskilda medför att det krav på frivillighet som gäller för samtycke oftast inte är uppfyllt.[27] Detsamma gäller i andra förhållanden där det råder en liknande obalans, till exempel i förhållandet mellan arbetsgivare och arbetstagare.

Även *andra än myndigheter* kan behandla uppgifter med stöd av artikel 6.1 c och e om det finns en fastställd rättslig grund enligt artikel 6.3. Detta är ofta fallet för den behandling som privata aktörer utför inom offentligfinansierad verksamhet, till exempel privata vårdgivare och friskolor. Ofta sker dock behandling som utförs inom den privata sektorn med stöd av andra rättsliga grunder, till exempel samtycke (artikel 6.1 a)[28], avtal (artikel 6.1 b) eller intresseavvägning (artikel 6.1 f). För sådan behandling finns det inte ett generellt utrymme för nationell preciserade reglering enligt artikel 6.2 och det finns inte heller ett krav på att den rättsliga grunden ska fastställas i nationell rätt enligt artikel 6.3.

Kartläggning av befintlig reglering och rättsliga grunder

När ett förslag medför en ny eller utökad behandling av personuppgifter bör det kartläggas vilka av de villkor för laglighet som anges i artikel 6.1 i dataskyddsförordningen som kan utgöra stöd för behandlingen. Kartläggningen behöver omfatta alla aktörer som kommer att behandla personuppgifter.

När det gäller behandling som sker med stöd av artikel 6.1 c och e i dataskyddsförordningen måste, som framgår ovan, grunden för behandlingen vara fastställd i unionsrätten eller nationell rätt enligt artikel 6.3.

[24] Se 2 kap. 1 och 2 §§ dataskyddslagen. Regeringen har tolkat dataskyddsförordningen som att det är den rättsliga förpliktelsen, uppgiften av allmänt intresse eller rätten att utöva myndighet som ska fastställas i den rättsliga grunden, och inte själva personuppgiftsbehandlingen, se regeringens proposition 2017/18:105 Ny dataskyddslag, s. 49.
[25] Se artikel 6.3 i dataskyddsförordningen där följande anges. Den rättsliga grunden kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning, bland annat: de allmänna villkor som ska gälla för den personuppgiftsansvariges behandling, vilken typ av uppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål, ändamålsbegränsningar, lagringstid samt typer av behandling och förfaranden för behandling, inbegripet åtgärder för att tillförsäkra en laglig och rättvis behandling, däribland för behandling i andra särskilda situationer enligt kapitel IX.
[26] Jfr artikel 6.1 andra stycket i dataskyddsförordningen.
[27] Se artikel 4.11 och skäl 43 till dataskyddsförordningen.
[28] EDPB:s riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/679, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_sv.pdf

Den rättsliga grunden enligt artikel 6.3 är ofta fastställd i till exempel myndigheters instruktioner eller i annan reglering som styr verksamheten, till exempel hälso- och sjukvårdslagen[29] och socialtjänstlagen[30]. På vissa områden kompletteras verksamhetsregleringen av en särskild författning som reglerar personuppgiftsbehandlingen, en så kallad registerförfattning[31]. Den rättsliga grunden som fastställs i nationell rätt enligt artikel 6.3 omfattar då både verksamhetsregleringen och registerförfattningen.

Vid informationsutbyte fastställs ofta den rättsliga grunden för utlämnandet genom bestämmelser som reglerar skyldighet eller möjlighet att lämna uppgifter. För myndigheter styrs informationsutbytet till stor del av regleringen om sekretess i offentlighets- och sekretesslagen och av bestämmelser som bryter sekretessen.[32]

Exempel på frågor att ta ställning till:

- Kartlägg vilka rättsliga grunder enligt artikel 6.1 i dataskyddsförordningen som kan ge stöd för den behandling som krävs enligt förslaget. Tänk på att göra denna bedömning för alla inblandade aktörer, det vill säga för alla som ska behandla personuppgifter till följd av förslaget.
- Vilken verksamhetsreglering och personuppgiftsreglering finns för de inblandade aktörerna?
- Vilken reglering kan ge stöd för informationsutbyte mellan de inblandade aktörerna?

STEG 4: Behovet av ny reglering

När personuppgiftsbehandlingen och befintlig reglering är kartlagd är nästa steg att bedöma om den befintliga regleringen är tillräcklig eller om det krävs kompletterande reglering.

Finns det rättslig grund enligt artikel 6 i dataskyddsförordningen för personuppgiftsbehandlingen?

Som framgår av steg 3 måste all personuppgiftsbehandling uppfylla minst ett av de villkor som anges i artikel 6.1 i dataskyddsförordningen. Viss behandling kommer att stödja sig på någon av de rättsliga grunder som inte förutsätter ytterligare reglering, till exempel samtycke (artikel 6.1 a), avtal (artikel 6.1 b) och intresseavvägning (artikel 6.1 f). Bedömningen av om det finns stöd för behandlingen i dessa rättsliga grunder sker med beaktande av bland annat praxis från svenska domstolar, EU-domstolen och EDPB:s riktlinjer.

När det gäller rättslig förpliktelse (artikel 6.1 c) och uppgift av allmänt intresse och myndighetsutövning (artikel 6.1 e) krävs kompletterande reglering i unionsrätten eller nationell rätt enligt artikel 6.3.

När det ska bedömas om den befintliga regleringen som kartlagts i steg 3 är tillräcklig för att ge stöd för personuppgiftsbehandlingen är utgångspunkten dataskyddsförordningens krav på proportionalitet (artikel 6.3) samt tydlighet, precision

[29] Hälso- och sjukvårdslagen (2017:30).
[30] Socialtjänstlagen (2001:453).
[31] Se exempelvis patientdatalagen (2008:355) och lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet.
[32] Se till exempel 6 kap. 5 § offentlighets- och sekretesslagen (2009:400).

och förutsebarhet för de registrerade (skäl 41). Vid denna bedömning är kartläggningen av integritetsriskerna i steg 2 av avgörande betydelse. Ett mer kännbart intrång kräver en mer preciserad rättslig grund som gör intrånget förutsebart, medan personuppgiftsbehandling med lägre integritetsrisker kan ske med stöd av en mer allmänt hållen rättslig grund enligt artikel 6.3.[33] För att kravet på proportionalitet ska vara uppfyllt kan krävas att bestämmelser med kompletterande skyddsåtgärder också behöver införas. Sammantaget ska analysen säkerställa att integritetsintrånget inte blir större än nödvändigt utifrån vad man vill uppnå med förslaget.

Exempel på frågor att ta ställning till:

- Om behandlingen är tänkt att grunda sig på artikel 6.1 a, b, d eller f – kommer behandlingen att kunna utföras med stöd av de grunderna enligt bland annat EU-domstolens praxis och EDPB:s riktlinjer?
- Finns det utrymme för nationella regler, det vill säga baseras behandlingen på de rättsliga grunderna i artikel 6.1 c och e (artikel 6.2 och 6.3)?
- Om behandlingen baseras på någon av de rättsliga grunderna i artikel 6.1 c och e, är dessa fastställda enligt kraven i artikel 6.3?
- Är bestämmelserna i förslaget tydliga, precisa och förutsägbara för de personer som omfattas av dem, det vill säga de registrerade (skäl 41)?
- Är kravet på proportionalitet i artikel 6.3 uppfyllt? Om behandlingen inte kan anses proportionerlig kan det innebära att ytterligare reglering av till exempel tillåtna ändamål och skyddsåtgärder behöver införas (se steg 6).

Finns det stöd i artikel 9 för behandling av känsliga personuppgifter?

Som framgår av steg 2 är behandling av känsliga personuppgifter enligt artikel 9.1 i dataskyddsförordningen som utgångspunkt förbjuden. Förbudet gäller dock inte om något av de undantag som beskrivs i artikel 9.2 a–j kan tillämpas. Dessa undantag är uttömmande och det finns således inte något utrymme för medlemsstaterna att föreskriva ytterligare undantag. Medlemsstaterna får dock införa mer specifika bestämmelser i fråga om behandling som sker med stöd av artikel 6.1 c (rättslig förpliktelse) och 6.1 e (allmänt intresse och myndighetsutövning), även när det gäller känsliga personuppgifter (artikel 6.2).

Vissa av undantagen i artikel 9.2 innehåller också uttryckliga hänvisningar till och krav på innehållet i unionsrätten och medlemsstaternas nationella rätt avseende proportionalitet och åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen. Det kan medföra krav på kompletterande nationell reglering avseende en viss behandling av känsliga personuppgifter. Detta gäller bestämmelserna i artikel 9.2 b (arbetsrätt med mera), g (viktigt allmänt intresse), h (hälso- och sjukvård med mera), i (folkhälsa) och j (arkiv, forskning och statistik).

Generell kompletterande reglering avseende känsliga personuppgifter finns i 3 kap. dataskyddslagen för myndigheter och vissa andra organ. Den regleringen kan i många fall vara tillräcklig för att ge stöd för myndigheternas personuppgiftsbehandling. För mer omfattande behandling av känsliga personuppgifter i myndigheters kärnverksamhet kan det dock behövas särskilda bestämmelser om behandlingen för att skapa en tillräckligt tydlig och förutsebar rättslig grund som också uppfyller kravet på proportionalitet.[34] Vid sådan personuppgiftsbehandling kan det alltså vara

[33] Se prop. 2017/18:105 s. 51.
[34] Jfr prop. 2017/18:105 s. 91.

nödvändigt att mer precist reglera vilka personuppgifter som ska få behandlas och villkoren för behandlingen, till exempel i en registerförfattning eller genom särskilda dataskyddsbestämmelser i verksamhetsregleringen.

Exempel på frågor att ta ställning till:

- Kommer känsliga personuppgifter att behandlas?
- Är något av undantagen i artikel 9.2 tillämpligt? Om ja, är kraven i undantagsbestämmelsen, till exempel kravet på bestämmelser om skyddsåtgärder, uppfyllt?
- Finns det stöd för den behandlingen, till exempel i en registerförfattning eller i den allmänna regleringen i dataskyddslagen?

Finns det stöd för behandling av personuppgifter som rör lagöverträdelser?

Artikel 10 i dataskyddsförordningen innehåller särskilda bestämmelser för personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder (personuppgifter som rör lagöverträdelser). IMY har tagit fram ett rättsligt ställningstagande om tolkningen av detta begrepp.[35]

Utöver de villkor som gäller vid all behandling av personuppgifter gäller att personuppgifter som rör lagöverträdelser endast får behandlas under kontroll av en myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet.

Att en myndighet får behandla uppgifter om lagöverträdelser framgår direkt av artikel 10 i dataskyddsförordningen och det har även tydliggjorts genom 3 kap. 8 § dataskyddslagen. Även om myndigheter inte behöver något särskilt rättsligt stöd för att behandla uppgifter om lagöverträdelser är behandling av sådana personuppgifter integritetskänslig.

Enligt 5 § kompletteringsförordningen får personuppgifter som rör lagöverträdelser behandlas av andra än myndigheter om behandlingen är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras, eller för att en rättslig förpliktelse enligt lag eller förordning ska kunna fullgöras. IMY har meddelat föreskrifter om att personuppgifter som rör lagöverträdelser får behandlas av andra än myndigheter i vissa situationer.[36]

Enligt 3 kap. 8 § andra stycket dataskyddslagen får även andra än myndigheter behandla personuppgifter som rör lagöverträdelser, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv. Enligt 7 § kompletteringsförordningen får Riksarkivet meddela föreskrifter och beslut om att andra än myndigheter får behandla personuppgifter som rör lagöverträdelser för arkivändamål av allmänt intresse.

[35] IMYRS 2021:1, https://www.imy.se/globalassets/dokument/rattsligt-stallningstagande/imyrs-2021-1-lagovertradelser.pdf
[36] DIFS 2018:2, https://www.imy.se/globalassets/dokument/foreskrifter/difs-2018-2.pdf

IMY kan också, med stöd av 3 kap. 9 § andra stycket dataskyddslagen och 6 § andra stycket kompletteringsförordningen, i enskilda fall ge tillstånd till att behandla personuppgifter som rör lagöverträdelser.

Exempel på frågor att ta ställning till:

- Kommer personuppgifter som rör lagöverträdelser att behandlas av andra än myndigheter?
- Finns det stöd för den behandlingen i befintlig reglering, till exempel 5 § kompletteringsförordningen eller DIFS 2018:2?

Finns det behov av stöd för vidarebehandling av personuppgifter (artiklarna 5.1 b och 6.4)?

Principen om ändamålsbegränsning innebär att personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (artikel 5.1 b).[37] Kravet på att senare behandling (så kallad vidarebehandling) inte får ske för ändamål som är oförenliga med insamlingsändamålen brukar kallas för finalitetsprincipen. All behandling som sker efter den ursprungliga behandlingen utgör en vidarebehandling av uppgifterna, oberoende av ändamålet med den senare behandlingen.[38] Frågan om vidarebehandlingen är förenlig med de ursprungliga ändamålen uppkommer dock endast om de nya ändamålen inte är identiska med de ursprungliga.[39]

Det är den personuppgiftsansvarige som enligt artikel 5.2 i dataskyddsförordningen ska säkerställa och kunna visa att behandlingen är förenlig med finalitetsprincipen. Ofta är dock möjligheten till vidarebehandling av personuppgifter en central förutsättning för att ett författningsförslag ska fungera som det är avsett. Därför kan lagstiftaren behöva göra en bedömning av om en tänkt vidarebehandling är tillåten. Vid bedömningen av om vidarebehandlingen är förenlig med insamlingsändamålen ska följande faktorer som anges i artikel 6.4 i dataskyddsförordningen beaktas:

- Kopplingar mellan de ändamål för vilka personuppgifterna har samlats in och ändamålen med den avsedda ytterligare behandlingen.
- Det sammanhang inom vilket personuppgifterna har samlats in, särskilt förhållandet mellan de registrerade och den personuppgiftsansvarige.
- Personuppgifternas art, särskilt om känsliga personuppgifter eller personuppgifter om lagöverträdelser behandlas.
- Eventuella konsekvenser för registrerade av den planerade fortsatta behandlingen.
- Förekomsten av lämpliga skyddsåtgärder, vilket kan inbegripa kryptering eller pseudonymisering.

Ibland kan det vara tydligt att en viss vidarebehandling är förenlig med finalitetsprincipen. Men ofta är det svårt att göra den bedömningen i ett lagstiftningsärende, bland annat eftersom förutsättningarna för bedömningen i artikel 6.4 inte är klara. Det är dock möjligt för lagstiftaren att införa reglering som ger stöd för

[37] Av artikel 5.1 b framgår också att ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 inte ska anses vara oförenlig med de ursprungliga ändamålen.
[38] EU-domstolens dom den 20 oktober 2022, Digi, C-77/21, EU:C:2022:805, p. 31.
[39] A. dom p. 34.

sådan vidarebehandling som är oförenlig med den ursprungliga behandlingen (se artikel 6.4 och skäl 50 andra stycket).

Sådan lagstiftning måste enligt artikel 6.4 vara en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda de mål som avses i artikel 23.1. Om det i lagstiftningen ges stöd för en viss vidarebehandling behöver någon förenlighetsbedömning inte göras av den personuppgiftsansvarige. Enligt IMY kan den grund som fastställs för vidarebehandlingen även omfatta behandling som är förenlig med finalitetsprincipen. Enligt skäl 41 till dataskyddsförordningen måste grunden vara tydlig och precis och förutsägbar för personer som omfattas av den.

Exempel på frågor att ta ställning till:

- Innebär förslagen att personuppgifter kommer att behandlas av någon av aktörerna för andra ändamål än insamlingsändamålen (vidarebehandling)? Tänk på att vidarebehandling kan ske både inom en organisation och vid utlämnande till en annan organisation.
- Är vidarebehandlingen förenlig med finalitetsprincipen (artiklarna 5.1 b och 6.4)? Om det är osäkert om vidarebehandlingen är förenlig med finalitetsprincipen bör det övervägas om det går att införa reglering enligt artikel 6.4 som ger stöd för vidarebehandlingen (se steg 6).

Behövs det undantag enligt artikel 23 i dataskyddsförordningen?

Ibland kan det i lagstiftningsarbetet finnas behov av att göra undantag från de rättigheter som dataskyddsförordningen ger registrerade. Enligt artikel 23.1 i dataskyddsförordningen är det möjligt att i en medlemsstats nationella rätt, införa en lagstiftningsåtgärd som begränsar tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs i artiklarna 12–22 och 34, samt artikel 5 i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som fastställs i artiklarna 12–22. En sådan begränsning måste ske med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgöra en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa ett antal olika mål som anges i artikel 23.1 a–j. Enligt artikel 23.2 i dataskyddsförordningen ska en lagstiftningsåtgärd som begränsar rättigheter och skyldigheter som följer av dataskyddsförordningen innehålla specifika bestämmelser åtminstone, när så är relevant, avseende bland annat ändamålen med behandlingen eller kategorierna av behandling, kategorierna av personuppgifter, skyddsåtgärder för att förhindra missbruk eller olaglig tillgång eller överföring och lagringstiden. EDPB har beslutat om riktlinjer som ger vägledning för tolkningen av artikel 23.[40]

I dataskyddsförordningen finns också särskilda undantagsmöjligheter med hänsyn till yttrande- och informationsfriheten (artikel 85) samt för sådan personuppgiftsbehandling som sker för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål (artikel 89).

I 5 kap. dataskyddslagen finns vissa generella undantag från rätten till information och rätten att få tillgång i artiklarna 13–15 i dataskyddsförordningen. Undantagen innebär bland annat att dessa rättigheter inte gäller sådana uppgifter som den personuppgiftsansvarige inte får lämna ut enligt lag eller annan författning eller enligt

[40] EDPB:s riktlinjer 10/2020 ”Restrictions under Article 23 GDPR”, https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf

beslut som har meddelats med stöd av författning. Därigenom undantas bland annat personuppgifter som omfattas av sekretess från rätten till information och tillgång i artiklarna 13–15.

Exempel på frågor att ta ställning till:

- Finns det ett behov av att göra undantag med stöd av artikel 23 från bestämmelserna i artiklarna 12–22?
- Rör den föreslagna lagstiftningen behandling av personuppgifter som sker för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål? Behövs det undantag enligt artikel 89?

Bedömning av om det finns stöd för personuppgiftsbehandlingen

Om det efter kartläggningen och bedömningen i steg 1-4 står klart att det kommer att krävas kompletterande reglering för att ge stöd för behandlingen av personuppgifter går man vidare till steg 5.

Om det i stället framgår att det finns stöd för behandlingen i befintlig dataskyddsreglering och den föreslagna verksamhetsregleringen, behöver det göras en samlad nödvändighets- och proportionalitetsanalys av förslagen (se artikel 6.3 i dataskyddsförordningen). I denna bedömning behöver även befintlig personuppgiftsbehandling beaktas. Analysen bör omfatta en bedömning av det samlade behovet av att personuppgifter behandlas samt om och i vilken utsträckning personuppgiftsbehandlingen är ägnad att tillgodose behovet. Vidare behöver det göras en bedömning av det intrång som den nya personuppgiftsbehandlingen, tillsammans med befintlig behandling, får för de registrerades personliga integritet. För att personuppgiftsbehandlingen ska vara tillåten behöver behoven stå i rimlig proportion till intrånget i den personliga integriteten. Om det finns alternativa sätt att uppnå ändamålet som innebär mindre integritetsrisker, men som på ett fullgott sätt kan bidra till att uppfylla det aktuella ändamålet med personuppgiftsbehandlingen, bör det övervägas.

Om det vid bedömningen konstateras att kraven i artikel 6.3 är uppfyllda kan integritetsanalysen avslutas. I annat fall behövs en fortsatt analys enligt steg 5–7.

STEG 5: 2 kap. 6 § andra stycket regeringsformen

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.

Avgörande för om en åtgärd ska anses innebära övervakning eller kartläggning är inte dess huvudsakliga syfte utan vilken effekt som åtgärden har. Vid bedömningen av vilka åtgärder som kan anses utgöra ett ”betydande intrång” ska både åtgärdens omfattning och arten av det intrång som åtgärden innebär beaktas. Grundlagsskyddet omfattar endast sådana intrång som på grund av åtgärdens intensitet eller omfattning,

eller av hänsyn till uppgifternas integritetskänsliga natur eller andra omständigheter, innebär ett betydande ingrepp i den enskildes privata sfär.[41]

Grundlagsskyddet får enligt 2 kap. 20 § första stycket regeringsformen endast begränsas genom lag. Det är således inte möjligt att begränsa skyddet genom förordning. Enligt 2 kap. 21 § regeringsformen ställs också krav på att begränsningar endast får göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningar får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen. Det betyder att en proportionalitetsbedömning ska göras. Av förarbetena framgår att grundlagsskyddet innebär att lagstiftaren tydligt måste redovisa vilka avvägningar som gjorts vid proportionalitetsbedömningen.[42] Proportionalitetsbedömningen enligt regeringsformen kan med fördel göras i samband med proportionalitetsbedömningen enligt dataskyddsförordningen (se steg 7).

Bestämmelserna i 2 kap. 20 och 21 §§ regeringsformen innebär att det krävs att behandlingen regleras på ett tydligt sätt i lag för att säkerställa att intrånget i den personliga integriteten är proportionerlig i förhållande till vad som ska uppnås med behandlingen. Det behöver dock inte innebära att lagen alltid måste innehålla detaljerade regler, men de skyddande ramarna behöver lagstiftaren ge för att säkerställa att den föreslagna behandlingen är proportionerlig.

Exempel på frågor att ta ställning till:

- Är 2 kap. 6 § andra stycket regeringsformen tillämplig? Denna fråga kan delas in i följande delfrågor:
    - Innebär personuppgiftsbehandlingen ett betydande intrång i den personliga integriteten?
    - Sker personuppgiftsbehandlingen utan samtycke?
    - Innebär personuppgiftsbehandlingen övervakning eller kartläggning av den enskildes personliga förhållanden?
    - Är personuppgiftsbehandlingen proportionerlig?

STEG 6: Utformningen av ny reglering

Om man i steg 4 konstaterat att det krävs kompletterande reglering behöver det bedömas hur regleringen ska utformas för att vara förenlig med dataskyddsförordningen och övrig dataskyddsreglering. Den regleringen som ska tas fram kan vara av många olika slag. Det kan till exempel vara fråga om att ta fram en ny författning som reglerar en myndighets personuppgiftsbehandling, en så kallad registerförfattning. Ett annat exempel är förslag som innebär ett utökat informationsutbyte mellan flera myndigheter. Olika frågor kan aktualiseras beroende på vilken reglering som föreslås. Nedan ges allmän vägledning kring utformningen av ny dataskyddsreglering. Vidare anges vissa exempel på bestämmelser som kan införas för att begränsa integritetsriskerna.

Allmänna utgångspunkter för regleringen

Den grundläggande principen om uppgiftsminimering innebär att personuppgifter inte får vara för omfattande i förhållande till de ändamål för vilka de behandlas (artikel 5.1 c i dataskyddsförordningen). Utgångspunkten bör därför vara att utforma regleringen på

[41] Se regeringen proposition 2009/10:80 En reformerad grundlag s. 250.
[42] A. prop. s. 177.

ett sådant sätt att personuppgiftsbehandlingen blir så begränsad som möjligt med hänsyn till ändamålet, till exempel vad gäller antalet personer och antal uppgifter om varje person. Det gäller särskilt behandling av känsliga personuppgifter och andra personuppgifter av integritetskänslig karaktär. Om det finns alternativa sätt att uppnå ändamålet som innebär mindre integritetsrisker, men som på ett fullgott sätt kan bidra till att uppfylla det aktuella ändamålet, behöver det övervägas.

Trots att dataskyddsförordningen är direkt tillämplig finns det utrymme att införliva delar av förordningen i nationell rätt i den utsträckning det krävs för att göra de nationella bestämmelserna begripliga för de personer som de tillämpas på (se skäl 8 till dataskyddsförordningen).

En annan utgångspunkt är att de begrepp som förekommer i dataskyddsförordningen bör användas även i nationell rätt. Det kan i annat fall uppstå tolknings- och tillämpningssvårigheter.

Normgivningsnivå

Dataskyddsförordningen ställer inte krav på att reglering i nationell rätt, till exempel av en rättslig grund, införs på en viss normhierarkisk nivå.[43] Utifrån dataskyddsförordningens perspektiv kan således nationell reglering införas även i förordning.

Om det i steg 5 konstaterats att grundlagsskyddet i 2 kap. 6 § andra stycket regeringsformen är tillämpligt krävs dock reglering i lag. I övrigt styrs normgivningsnivån i svensk rätt av reglerna om normgivningsmakten i 8 kap. regeringsformen. Vid mer omfattande personuppgiftsbehandling görs dock ofta bedömningen att den grundläggande regleringen bör införas i lag, även om det inte krävs enligt 8 kap. regeringsformen. Detta eftersom det kan vara lämpligt att riksdagen får ta ställning till om de integritetsrisker som förslaget medför är motiverade. Bestämmelser på detaljnivå kan ofta placeras i förordning. En fördel med detta är att bestämmelserna lättare kan ändras när det behövs.

Hur ska den rättsliga grunden enligt artikel 6.3 regleras?

En central fråga är hur den rättsliga grunden enligt artikel 6.3 ska regleras. Dataskyddsförordningen ställer krav på tydlighet, precision, förutsebarhet och proportionalitet (artikel 6.3 och skäl 41). Kravet på förutsebarhet ska ses från den registrerades – och inte den personuppgiftsansvariges – perspektiv (skäl 41). EU-domstolen har i sin praxis ställt höga krav på utformningen av de rättsliga grunder som ska ligga till grund för personuppgiftsbehandling.[44]

Det måste alltid göras en bedömning av personuppgiftsbehandlingens och verksamhetens karaktär för att avgöra hur stor grad av tydlighet och precision som

[43] Se skäl 41 till dataskyddsförordningen.

[44] EU-domstolens dom den 24 februari 2022, Valsts ieņēmumu dienests, C-175/20, EU:C:2022:124, punkt 83, där EU-domstolen uttalar följande: ”I detta sammanhang ska det dock erinras om att för att uppfylla det proportionalitetskrav som föreskrivs i artikel 5.1 c i förordning 2016/679 (se för ett liknande resonemang, dom av den 22 juni 2021, Latvijas Republikas Saeima (Prickning), C-439/19, EU:C:2021:504, punkt 98 och där angiven rättspraxis), måste de föreskrifter som ligger till grund för behandlingen innehålla tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt ange minimikrav, så att de personer vars personuppgifter lämnas ut ges tillräckliga garantier för att uppgifterna på ett effektivt sätt är skyddade mot riskerna för missbruk. Dessa föreskrifter måste även vara rättsligt bindande enligt nationell rätt och i synnerhet ange under vilka omständigheter och på vilka villkor en åtgärd för behandling av sådana uppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strikt nödvändigt (dom av den 6 oktober 2020, Privacy International, C-623/17, EU:C:2020:790, punkt 68 och där angiven rättspraxis).”

krävs. Ett mer kännbart intrång kräver en mer preciserad rättslig grund, medan personuppgiftsbehandling med lägre integritetsrisker kan ske med stöd av en mer allmänt hållen rättslig grund.[45]

Det är viktigt att göra en helhetsbedömning av den rättsliga grunden och se samspelet med verksamhetsregleringen när behovet av kompletterande dataskyddsreglering bedöms. En tydlig verksamhetsreglering kan medföra att behovet av särskilda dataskyddsbestämmelser, för att avgränsa och förtydliga den rättsliga grunden, kan minska. En mer allmänt hållen verksamhetsreglering kan däremot kräva en mer preciserad reglering av personuppgiftsbehandlingen, till exempel genom reglering av ändamålsbegränsningar. De särskilda typer av bestämmelser som beskrivs nedan kan tas in i den rättsliga grunden enligt artikel 6.3 för att uppnå kraven på tydlighet, precision, förutsebarhet och proportionalitet.

Särskilda typer av bestämmelser som kan behövas för att uppfylla kraven i dataskyddsförordningen

Bestämmelser om personuppgiftsansvar
Det är enligt artikel 4.7 i dataskyddsförordningen möjligt att i nationell rätt reglera vem som ska vara personuppgiftsansvarig. En fördel med detta är att det skapar tydlighet och förutsebarhet för både de som ska behandla personuppgifter och för de registrerade. Det gäller i synnerhet om flera aktörer är inblandade. Ansvaret ska läggas på den som har faktisk möjlighet att påverka ändamålen och medlen för behandlingen. Den personuppgiftsansvarige måste ha möjlighet att ta sitt ansvar. Om sådan reglering inte införs, kan det vara lämpligt att i förarbetena att klargöra vem eller vilka som ska vara personuppgiftsansvarig.

Bestämmelser om vilka personuppgifter som får behandlas
Det kan vara svårt att i förväg avgöra exakt vilka personuppgifter som bör kunna behandlas inom ramen för en verksamhet. En precisering av vilka uppgifter som får behandlas kan därför normalt ta sikte på kategorier eller typer av uppgifter (jfr artiklarna 6.3 och 23.2 b i dataskyddsförordningen). Behovet av reglering måste dock bedömas från fall till fall utifrån dataskyddsförordningens krav på tydlighet, precision, förutsebarhet och proportionalitet. Vid särskilt integritetskänslig behandling av personuppgifter kan det vara nödvändigt att mer precist reglera vilka personuppgifter som ska få behandlas.

Bestämmelser om känsliga personuppgifter
Vissa av undantagen i artikel 9.2 i dataskyddsförordningen beträffande känsliga personuppgifter innehåller uttryckliga hänvisningar till och krav på innehållet i unionsrätten och medlemsstaternas nationella rätt såsom krav på bestämmelser om så kallade skyddsåtgärder, se nedan under avsnittet Reglering av andra integritetshöjande åtgärder i syfte att minska integritetsrisker, sid. 23 f. Det kan medföra krav på kompletterande nationell reglering avseende en viss behandling av känsliga personuppgifter. Detta gäller bestämmelserna i artikel 9.2 b (arbetsrätt med mera), g (viktigt allmänt intresse), h (hälso- och sjukvård med mera), i (folkhälsa) och j (arkiv, forskning och statistik) samt artikel 9.3, se ovan under avsnittet Finns det stöd i artikel 9 för behandling av känsliga personuppgifter?, sid. 15 f.

I sådan kompletterande reglering av känsliga personuppgifter bör det tydligt framgå med vilket undantag i artikel 9.2 som behandlingen ska ske eftersom det är den

[45] Se prop. 2017/18:105 s. 51.

bestämmelsen som utgör det faktiska undantaget för behandlingen (jfr utformningen av 3 kap. 2-3 och 5-7 §§ dataskyddslagen). Detta så att det är tydligt med vilket rättsligt stöd som behandlingen utförs för att skapa tydlighet och förutsebarhet för de registrerade och för den personuppgiftsansvarige i frågan om den har rätt att behandla känsliga personuppgifter.

Bestämmelser som ger stöd för behandling av uppgifter om lagöverträdelser
I vissa fall kan det krävas särskild rättslig reglering för den personuppgiftsbehandling som utförs av personuppgiftsansvariga som inte är myndigheter vid behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder enligt artikel 6.1 (personuppgifter som rör lagöverträdelser, artikel 10 i dataskyddsförordningen), se ovan under avsnittet Finns det stöd för behandling av personuppgifter som rör lagöverträdelser?, sid. 16 f.

Bestämmelser om tillåtna ändamål
En vanlig typ av bestämmelser vid reglering av behandling av personuppgifter är ändamålsbestämmelser som syftar till att klargöra för vilka ändamål som myndigheten får behandla uppgifter i sin verksamhet. Sådana bestämmelser kan fylla flera funktioner. Den viktigaste funktionen är att begränsa integritetsintrånget genom att ange den yttersta ram inom vilken personuppgifter får behandlas. Ändamålsbestämmelser kan sägas anpassa tillämpningen av dataskyddsförordningen och säkerställa en laglig och rättvis behandling av personuppgifter. Under dataskyddsförordningen kan sådana bestämmelser vara avgörande för att en rättslig grund ska leva upp till förordningens krav på förutsebarhet och proportionalitet.

Reglering av andra integritetshöjande åtgärder i syfte att minska integritetsrisker
Andra bestämmelser som minskar integritetsrisker kan exempelvis vara följande.

- Bestämmelser om begränsningar i sök- och sammanställningsmöjligheter, till exempel tillåtna sökbegrepp. Detta är särskilt viktigt vid behandling av känsliga personuppgifter och uppgifter om lagöverträdelser.
- Bestämmelser om pseudonymisering (se artiklarna 4.5 och 32 i dataskyddsförordningen).
- Bestämmelser om begränsningar av möjligheter till utlämnande, till exempel begränsning av tillåtna mottagare eller tillåtna ändamål för utlämnande samt bestämmelser om sekretess eller tystnadsplikt.
- Bestämmelser om vilka som ska ha åtkomst till personuppgifterna.
- Bestämmelser om säkerhetsåtgärder, särskilt vid behandling av känsliga personuppgifter och andra personuppgifter av integritetskänslig karaktär. Det kan till exempel avse krav på kryptering och stark autentisering vid överföring eller bestämmelser om loggning för att möjliggöra kontroller av vem eller vilka som haft åtkomst till personuppgifterna (åtkomstkontroll), se artikel 32.
- Bestämmelser om elektroniskt utlämnande. Direktåtkomst är den mest integritetskänsliga formen för utlämnande. Om direktåtkomst ska förekomma bör det normalt regleras särskilt.
- Bestämmelser om hur länge personuppgifterna får bevaras eller, om det är fråga om allmänna handlingar, gallringsfrister. För att sådana bestämmelser ska ge ett mervärde från integritetsperspektiv behöver de vara mer konkreta än den grundläggande principen om lagringsminimering i artikel 5.1 d.
- Bestämmelser om krav på medgivande[46] från den registrerade för att behandlingen ska vara tillåten. Ett alternativ till detta kan vara att ge den

[46] Ett sådant medgivande är en integritetshöjande åtgärd och utgör inte rättslig grund för behandlingen. Det är således något annat än ett samtycke enligt artikel 6.1 a i dataskyddsförordningen.

registrerade en ovillkorlig rätt att motsätta sig behandlingen, en så kallad opt-out.

STEG 7: Slutlig proportionalitets- och nödvändighetsbedömning

När man gjort en bedömning av hur den kompletterande regleringen bör utformas behöver man göra en samlad proportionalitets- och nödvändighetsbedömning av förslagen. Vid denna bedömning kan det ofta finnas skäl att gå tillbaka till steg 6 för att ta ställning till vilken ytterligare reglering som behövs för att säkerställa att förslaget uppfyller kraven på nödvändighet och proportionalitet.

När det gäller begränsningar av enskildas rätt till skydd för sina personuppgifter följer det av artiklarna 8 och 52.1 i EU:s stadga om de grundläggande rättigheterna att sådana begränsningar endast får göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter. Kravet på nödvändighet innebär att om flera lämpliga åtgärder finns ska den minst betungande åtgärden väljas. Endast en åtgärd som visat sig vara nödvändig, bör bli föremål för en proportionalitetsbedömning.[47]

För att en behandling av personuppgifter ska vara tillåten enligt artikel 6.1 b–f i dataskyddsförordningen krävs att den är nödvändig i förhållande till den rättsliga grunden. Kravet på nödvändighet innebär dock inte att det ska vara omöjligt att utföra till exempel uppgiften av allmänt intresse utan att den specifika behandlingen genomförs.[48] Behandlingen kan anses nödvändig och därmed tillåten enligt artikel 6 om den leder till effektivitetsvinster.[49]

Av såväl EU:s stadga om de grundläggande rättigheterna som datasskyddsförordningen framgår att nationella lagstiftningsåtgärder som ger stöd för behandling av personuppgifter måste vara förenliga med proportionalitetsprincipen. För att uppfylla kravet på proportionalitet krävs att inskränkningarna i skyddet av personuppgifter begränsas till vad som är strikt nödvändigt. Lagstiftning som innebär ett ingrepp måste enligt EU-domstolens praxis innehålla tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden.[50]

En proportionalitetsbedömning omfattar en bedömning av vikten med det eftersträvade målet samt om och i vilken utsträckning den föreslagna åtgärden är ägnad att tillgodose målet. En bedömning behöver även göras av vilken påverkan som intrånget har på de grundläggande rättigheterna till privatliv och dataskydd. Åtgärden bör inte medföra en oproportionerlig börda för de personer som berörs av begränsningen i förhållandet till det eftersträvade målet. En proportionalitetsbedömning innebär att en bedömning ska göras av vilka skyddsåtgärder som behövs för att minska de risker som den planerade lagstiftningsåtgärden utgör för de grundläggande rättigheterna och friheterna för de individer som berörs till en proportionerlig nivå. Om slutsatsen blir att åtgärden inte är proportionerlig kan åtgärden inte föreslås alternativt behöver förslaget

[47] Se EU-domstolens dom den 8 april 2014, Digital Rights Ireland och Seitlinger m.fl., C-293/12 och C-594/12, ECLI:EU:C:2014:238, där EU-domstolen inte fortsatte att bedöma proportionaliteten efter att ha konstaterat att begränsningarna av rättigheterna i artiklarna 7 och 8 inte var strikt nödvändiga.
[48] Se prop. 2017/18:105 s. 46 f.
[49] Se prop. 2017/18:105 s. 189.
[50] Se till exempel EU-domstolens dom den 16 juli 2020, Schrems II, C-311/18, ECLI:EU:C:2020:559, p. 176 och dom den 22 juni 2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504, p. 105.

omarbetas. Införandet av skyddsåtgärder kan då behövas för att göra åtgärden proportionerlig.[51]

Exempel på frågor att ta ställning till:

- Motiveras förslagen av mål av allmänt samhällsintresse (artikel 52.1 i EU:s stadga om de grundläggande rättigheterna)?
- Finns det mindre ingripande sätt att nå dessa mål?
- Är behandlingen av personuppgifter ägnad att uppnå de uppställda målen av allmänt samhällsintresse?
- Står de behov som motiverar personuppgiftsbehandlingen i rimlig proportion till intrånget i den personliga integriteten?
- Behövs ytterligare reglering för att stärka skyddet för den personliga integriteten (se steg 6)?

[51] EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 December 2019.

Integritetsanalys i lagstiftningsarbete – checklista

STEG 1: Kartlägg personuppgiftsbehandlingen och bedöm vilket regelverk som är tillämpligt

Det första steget i en integritetsanalys är att så detaljerat som möjligt kartlägga och beskriva den behandling av personuppgifter som förslaget medför eller förutsätter, antingen som en direkt eller indirekt följd av förslaget. Tänk på att även en utökning av en befintlig behandling av personuppgifter kräver en analys.

- Vilka personuppgifter kommer att behandlas och på vilket sätt kommer det att ske?
- Vilka aktörer kommer att behandla personuppgifterna? Om det finns flera aktörer beskriv då hela flödet.
- Vilket regelverk är tillämpligt? Kommer personuppgiftsbehandlingen att ske utanför det område som regleras av dataskyddsförordningen, till exempel inom tillämpningsområdet för brottsdatadirektivet? Tänk på att ett förslag kan omfatta personuppgiftsbehandling inom flera regelverk.

STEG 2: Kartlägg och bedöm integritetsriskerna med personuppgiftsbehandlingen

Nästa steg är att göra en kartläggning och bedömning av integritetsriskerna med personuppgiftsbehandlingen. Det bör omfatta alla aktörer och personuppgiftsbehandlingar som omfattas av förslaget.

- Behandlas känsliga personuppgifter, uppgifter om lagöverträdelser eller person- eller samordningsnummer?
- Behandlas andra uppgifter som innebär särskilda integritetsrisker, till exempel personuppgifter som rör enskildas privatliv, sekretessbelagda personuppgifter eller personuppgifter om barn?
- Hur omfattande är personuppgiftsbehandlingen?
- Vem eller vilka kommer att bestämma ändamål och medel för behandlingen (personuppgiftsansvarig)?
- Vilket inflytande kommer de registrerade att ha över behandlingen och hur ser förhållandet ut till den personuppgiftsansvarige?
- Vilka är de övergripande ändamålen med personuppgiftsbehandlingen?
- Vilken spridning kommer personuppgifterna att få?

STEG 3: Kartlägg befintlig reglering

I detta steg kartläggs den befintliga reglering som kan ge rättsligt stöd för personuppgiftsbehandlingen.

- Kartlägg vilka rättsliga grunder enligt artikel 6.1 i dataskyddsförordningen som kan ge stöd för den behandling som krävs enligt förslaget. Tänk på att göra denna bedömning för alla inblandade aktörer, det vill säga för alla som ska behandla personuppgifter till följd av förslaget.
- Vilken verksamhetsreglering och personuppgiftsreglering finns för de inblandade aktörerna?
- Vilken reglering kan ge stöd för informationsutbyte mellan de inblandade aktörerna?

STEG 4: Behovet av ny reglering

När utredningen har kartlagt personuppgiftsbehandlingen, riskerna med denna och befintlig reglering är nästa steg att bedöma om det finns behov av ny kompletterande reglering. När det ska bedömas om den befintliga regleringen är tillräcklig för att ge stöd för personuppgiftsbehandlingen är utgångspunkten dataskyddsförordningens krav på proportionalitet (artikel 6.3) samt tydlighet, precision och förutsebarhet för de registrerade (skäl 41). Ett mer kännbart intrång kräver en mer preciserad rättslig grund som gör intrånget förutsebart, medan personuppgiftsbehandling med lägre integritetsrisker kan ske med stöd av en mer allmänt hållen rättslig grund enligt artikel 6.3.

- Finns det rättslig grund enligt artikel 6 i dataskyddsförordningen för personuppgiftsbehandlingen?
- Finns det stöd i artikel 9 för behandling av känsliga personuppgifter?
- Finns det stöd för behandling av personuppgifter som rör lagöverträdelser?
- Finns det behov av stöd för vidarebehandling av personuppgifter (artiklarna 5.1 b och 6.4 i dataskyddsförordningen)?
- Behövs det undantag enligt artikel 23 i dataskyddsförordningen?

Om det efter kartläggningen och bedömningen i steg 1–4 står klart att det kommer att krävas kompletterande reglering för att ge stöd för behandlingen av personuppgifter, går man vidare till steg 5.

Om det i stället framgår att det finns stöd för behandlingen i befintlig dataskyddsreglering och den föreslagna verksamhetsregleringen, behöver det göras en samlad nödvändighets- och proportionalitetsanalys av förslagen enligt bland annat artikel 6.3 i dataskyddsförordningen, se vidare steg 7.

Om det vid bedömningen konstateras att kraven i artikel 6.3 är uppfyllda kan integritetsanalysen avslutas. I annat fall behövs en fortsatt analys enligt steg 5–7.

STEG 5: 2 kap. 6 § andra stycket regeringsformen

Även i 2 kap. 6 § andra stycket regeringsformen ges skydd för den personliga integriteten vid behandling av personuppgifter. I steg 5 behöver det därför utredas om bestämmelsen är tillämplig. Den proportionalitetsbedömning som under vissa förutsättningar ska göras enligt regeringsformen, kan med fördel göras i samband med proportionalitetsbedömningen enligt dataskyddsförordningen (se steg 7).

- Innebär personuppgiftsbehandlingen ett betydande intrång i den personliga integriteten?
- Sker personuppgiftsbehandlingen utan samtycke?
- Innebär personuppgiftsbehandlingen övervakning eller kartläggning av den enskildes personliga förhållanden?
- Är personuppgiftsbehandlingen proportionerlig?

STEG 6: Utformningen av ny reglering

Om man i steg 4 konstaterat att det krävs kompletterande reglering behöver det bedömas hur regleringen ska utformas för att vara förenlig med dataskyddsförordningen och övrig dataskyddsreglering.

- Vilken normgivningsnivå är lämplig?
- Hur ska den rättsliga grunden regleras?
- Behöver det regleras vem eller vilka som ska vara personuppgiftsansvariga?
- Behöver det preciseras vilka personuppgifter som får behandlas?
- Behövs rättsligt stöd för behandling av känsliga personuppgifter eller uppgifter om lagöverträdelser?
- Behöver det regleras för vilka ändamål behandlingen får ske?
- Behövs andra bestämmelser för att minska integritetsriskerna, till exempel bestämmelser om sökbegränsningar, sekretess och tystnadsplikt, säkerhetsåtgärder eller bestämmelser som ställer krav på att den registrerade ska ge sitt medgivande till behandlingen?
- Om direktåtkomst ska förekomma bör det ofta regleras särskilt.

STEG 7: Slutlig proportionalitets- och nödvändighetsbedömning

När man gjort en bedömning av hur den kompletterande regleringen bör utformas behöver man göra en samlad proportionalitets- och nödvändighetsbedömning av förslagen enligt såväl EU:s stadga om de grundläggande rättigheterna som datasskyddsförordningen.

- Motiveras förslagen av mål av allmänt samhällsintresse (artikel 52.1 i EU:s stadga om de grundläggande rättigheterna)?
- Finns det mindre ingripande sätt att nå målen?
- Är behandlingen av personuppgifter ägnad att uppnå de uppställda målen av allmänt samhällsintresse?
- Står de behov som motiverar personuppgiftsbehandlingen i rimlig proportion till intrånget i den personliga integriteten?
- Behövs ytterligare reglering för att stärka skyddet för den personliga integriteten? Gå då tillbaka till steg 6.