Hammarö

Riktlinjer för dataskyddsarbetet i Hammarö kommun

Riktlinje

Dnr: KS 2023/61

Kommunfullmäktige, 2023-04-24, § 65

Dokumenttitel: Riktlinjer för dataskyddsarbetet i Hammarö kommun

Typ av styrdokument: Riktlinjer

Beslutad av: Kommunfullmäktige

Datum och beslutsparagraf: 2023-04-24 § 65

Diarienummer: KS 2023/61

Gäller för: Hammarö kommunkoncern

Giltighetstid: Från och med 2023-04-24 och tills vidare

Senast reviderad: -

Ersätter: Riktlinjer för hantering av personuppgifter, KS 2018/302

Dokumentansvar: Kommunstyrelsens förvaltning

Innehåll

1 Inledning

EU:s dataskyddsförordning (DSF) och den svenska dataskyddslagen (2018:218) ställer krav på Hammarö kommuns hantering av personuppgifter och systematiska dataskyddsarbete. Dessa riktlinjer beskriver övergripande de skyldigheter som åligger kommunens nämnder och bolag samt hur dataskyddsarbetet ska bedrivas.

1.1 Omfattning, syfte och mål

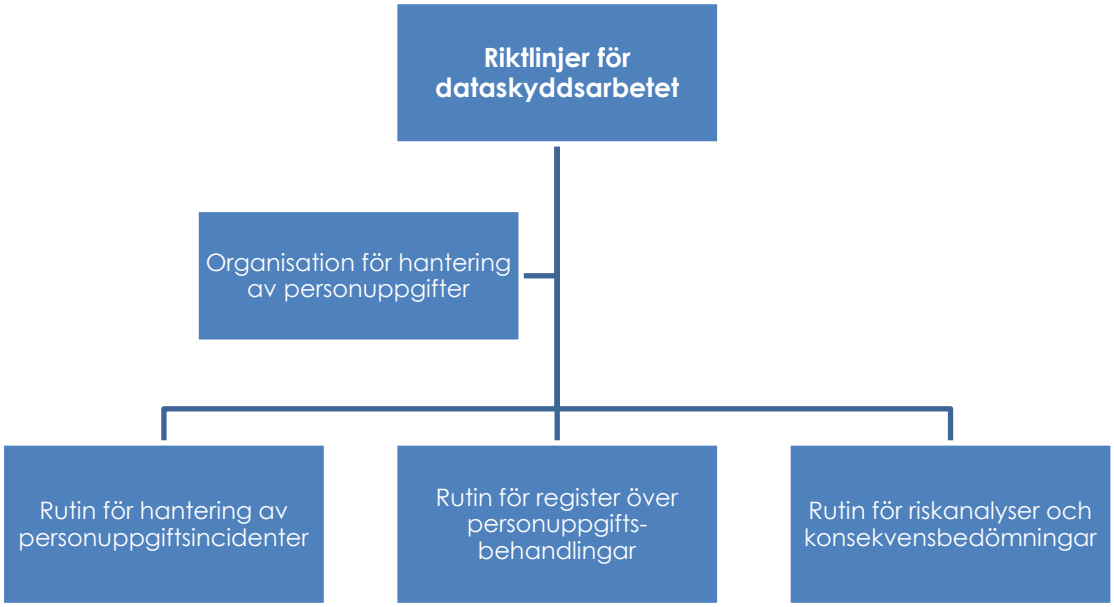
Dessa riktlinjer omfattar samtliga nämnder och bolag i Hammarö kommun. Syftet är att ge en överblick av de olika delarna av dataskyddsarbetet samt att sätta ramar för att möjliggöra planering och uppföljning av dataskyddsarbetet.

Hammarö kommuns mål för dataskyddsarbetet är att all behandling sker med hänsyn till den enskildes friheter och rättigheter. Innebörden i detta är att värna om den personliga integriteten genom att medborgare och anställda är trygga i att kommunen eftersträvar att alltid sätta en hög nivå av dataskydd.

1.1.1 Styrdokument

Dessa riktlinjer utgör ett paraplydokument som innehåller de övergripande ansvarsområdena som åligger de personuppgiftsansvariga myndigheter i Hammarö kommun. I riktlinjerna hänvisas till andra styrdokument som i närmre detalj styr och vägleder arbetet med de olika ansvarsområdena.

Figur 1. Illustration över styrdokument rörande dataskydd.



1.2 Organisation och ansvar

Varje nämnd/bolag i Hammarö kommun är ansvarig för information och personuppgifter inom de respektive verksamheterna. Kommunstyrelsen agerar i många fall som personuppgiftsbiträde till de övriga nämnderna/bolagen genom sitt ansvar för centrala processer såsom personal- och ekonomiadministration.

Dataskyddsombudet är en obligatorisk funktion vars roll i huvudsak är att kontinuerligt granska nämndernas efterlevnad av lagstiftningen och kommunens styrdokument inom dataskydd. Dataskyddsombudet är också en rådgivande funktion som kan ge vägledning och rekommendationer kring dataskyddsfrågor. Dataskyddsombudet är en funktion som delas med Kils kommun och Forshaga kommun och är gemensam för samtliga nämnder/bolag i Hammarö kommun.

Hur organisationen ska utformas och fungera regleras i närmre detalj genom styrdokumentet "Organisation för hantering av personuppgifter i Hammarö kommun".

1.2.1 Tillsynsmyndighet

Tillsynsmyndighet för dataskyddsfrågor är Integritetsskyddsmyndigheten (IMY)[1], utöver ansvaret för tillsyn och tillämpning av andra regler i enlighet med DSF är IMY också en rådgivande och vägledande myndighet.

2 Bakgrund

Dataskyddslagstiftningen syftar till att stärka den enskildes rätt till personlig integritet och kontroll över de egna personuppgifterna och utgörs främst av DSF och den underlydande svenska dataskyddslagen. Krav ställs bland annat på att den som behandlar personuppgifter ska ha laglig grund för behandlingen, att den enskilde har rätt till information om hur personuppgifter behandlas samt att register ska föras över personuppgiftsbehandlingar.

Dataskyddsförordningen kräver även att den som behandlar personuppgifter ska kunna visa att lagen efterlevs, det är därför av stor vikt att dataskyddsarbetet är transparent och väl dokumenterat.

[1] Myndigheten hette tidigare Datainspektionen.

2.1 Personuppgiftsansvarig, personuppgiftsbiträde och den registrerade

Personuppgiftsansvarig är den som på något sätt ansvarar för behandling av personuppgifter, för Hammarö kommuns del är respektive nämnd/styrelse personuppgiftsansvariga.

Personuppgiftsbiträde är den som behandlar uppgifter för den personuppgiftsansvariges räkning, exempelvis systemleverantörer eller andra företag/organisationer som anlitas och behandlar personuppgifter på uppdrag av den personuppgiftsansvariga. Notera att ett biträde även kan finnas inom kommunen då myndigheterna i vissa fall behandlar personuppgifter åt varandra.

Den registrerade avser den enskilda person vars personuppgifter behandlas och som har vissa rättigheter i enlighet med DSF. Även kommunens anställda och förtroendevalda betraktas som registrerade och bär rättigheter enligt DSF.

2.2 Vad är personuppgifter?

Med personuppgifter avses uppgifter som direkt eller indirekt kan knytas till en fysisk person. Direkta personuppgifter kan kopplas till en person utan att någon ytterligare information behövs. Exempel på direkta personuppgifter är:

- Namn
- Personnummer

Indirekta personuppgifter kan kopplas till en person i kombination med annan information. Exempel på indirekta personuppgifter är:

- Adress, telefonnummer eller andra kontaktuppgifter
- Födelsedatum
- Kundnummer
- Fastighetsbeteckning
- Registreringsnummer för fordon

2.2.1 Känsliga personuppgifter

Vissa typer av personuppgifter betraktas enligt artikel 9 i DSF som känsliga:

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Hälsa
- Sexualliv eller sexuell läggning

- Genetisk eller biometrisk information

Det är som huvudregel förbjudet att behandla känsliga personuppgifter, det finns dock flera undantag från detta (se kapitel 3.1 nedan).

2.2.2 Extra skyddsvärda personuppgifter

Vissa personuppgifter är inte att anse som känsliga men är ändå extra skyddsvärda:

- Barns personuppgifter
- Löneuppgifter
- Fullständigt personnummer
- Lagöverträdelser
- Värderande uppgifter
- Information som rör den privata sfären
- Uppgifter om sociala förhållanden

2.3 Vad är en personuppgiftsbehandling?

Alla former av åtgärder med personuppgifter är personuppgiftsbehandling. Som exempel kan nämnas insamling, registrering, organisering, strukturering, lagring, bearbetning, ändring, framtagning, utlämning, spridning eller att de tillhandahålls på annat sätt, sammanförande, begränsning eller förstöring av personuppgifter.

2.4 Grundläggande principer för dataskydd

Artikel 5 i DSF anger grundläggande principer som ska följas vid all hantering av personuppgifter, det gäller exempelvis även offentliga allmänna handlingar.

2.4.1 Laglighet, korrekthet och öppenhet

Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Detta innebär att den personuppgiftsansvariga behöver säkerställa att behandlingen sker enligt förordningens krav samt att den registrerade kan få information om vilka personuppgifter vi behandlar samt hur vi behandlar dem.

2.4.2 Ändamålsbegränsning

Ändamålsbegränsning innebär att den personuppgiftsansvariga bara får samla in personuppgifter för specifika, särskilt angiva och berättigade ändamål. I praktiken innebär detta att personuppgifter endast får samlas in och behandlas om det är nödvändigt för att kunna bedriva den avsedda verksamheten. Läs mer i kapitel 3.1 nedan om rättslig grund.

2.4.3 Uppgiftsminimering och lagringsminimering

En personuppgiftsansvarig får inte behandla fler personuppgifter än vad som är nödvändigt för det angiva ändamålet eller under längre tid än nödvändigt. Det innebär att den personuppgiftsansvariga behöver säkerställa att uppgifter inte samlas in och behandlas endast av praktiska skäl utan att de behövs för den faktiska handläggningen. Den personuppgiftsansvariga behöver även säkerställa att det finns rutiner för att gallra personuppgifter när de inte längre behövs. De krav som ställs på bevarande av allmänna handlingar har företräde i förhållande till kravet på lagringsminimering, det är därför viktigt att den personuppgiftsansvariga fattar erforderliga beslut om gallring[2].

2.4.4 Riktighet

Den personuppgiftsansvariga ska se till att personuppgifter som behandlas är riktiga och om nödvändigt uppdaterade. Det innebär att det ska säkerställas att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas, samt att uppgifter som är felaktiga till innehållet om möjligt rättas utan dröjsmål.

2.4.5 Integritet och konfidentialitet

Personuppgifter som behandlas ska skyddas så att obehöriga inte får tillgång till dem och så att de inte förloras eller förstörs. Detta innebär att den personuppgiftsansvariga ska säkerställa både tekniska och organisatoriska åtgärder för att skydda uppgifterna. Detta kan handla om att exempelvis ställa lämpliga krav på IT-säkerhet vid behandling av digital information eller att medarbetare genomför grundläggande åtgärder såsom att låsa datorer, mobiler och arbetsrum.

2.4.6 Ansvarsskyldighet

Dataskyddsförordningen kräver att den personuppgiftsansvariga – utöver att tillämpa dessa principer – ska kunna visa att principerna efterlevs. Det innebär att dataskyddsarbetet behöver dokumenteras och redovisas. Bland annat ska ett register föras över personuppgiftsbehandlingar och riskanalyser och konsekvensbedömningar ska genomföras och dokumenteras.

[2] Genom informationshanteringsplan eller särskilda gallringbeslut.

3 Behandling av personuppgifter

3.1 Rättslig grund

Alla personuppgiftsbehandlingar måste som tidigare nämnts ha stöd i dataskyddsförordningen. Det innebär att behandlingen måste stödjas på någon av de sex rättsliga grunderna som finns i artikel 6 i DSF. Innan en ny behandling påbörjas ska en bedömning alltid göras om det finns rättslig grund, om bedömningen görs att det finns rättslig grund för behandlingen ska det dokumenteras vilken rättslig grund som tillämpas i registret över personuppgiftsbehandlingar (se kapitel 4.2 nedan). De rättsliga grunderna är:

1. **Samtycke** - Den registrerade har frivilligt och uttryckligen samtyckt till personuppgiftsbehandlingen, ett samtycke bör vara skriftligt med hänsyn till att det är svårt att dokumentera/påvisa ett muntligt samtycke. Samtycke bör endast användas om ingen annan laglig grund finns, detta då samtycke inte är lämpligt om det råder en obalans mellan personuppgiftsansvarig och den registrerade. Ett samtycke kan dessutom alltid återkallas. Förutsättningar för att använda sig av samtycke regleras i artikel 7 DSF.

2. **Avtal** - Den registrerade har ingått eller ska ingå ett avtal med den personuppgiftsansvariga. Avtal kan användas som rättslig grund om personuppgiftsbehandlingen är nödvändig antingen för att kunna ingå eller för att kunna fullgöra avtalet med den registrerade. Tänk på att behandlingen ska vara en direkt följd av avtalet för att denna rättsliga grund ska kunna tillämpas.

3. **Intresseavvägning** – Denna rättsliga grund kan inte tillämpas av offentliga myndigheter.

4. **Rättslig förpliktelse** – Rättslig förpliktelse kan användas som rättslig grund om det finns lagar och regler som gör att den personuppgiftsansvariga specifikt måste behandla vissa personuppgifter i sin verksamhet. Exempel på detta är krav på journalföring inom vården som regleras i patientdatalagen (2008:355) eller krav på redovisning enligt bokföringslagen (1999:1078).

5. **Myndighetsutövning och allmänt intresse** – Myndighetsutövning som rättslig grund kan användas då personuppgifter måste behandlas för att utföra myndighetsutövning på uppdrag av staten.

Allmänt intresse kan användas som rättslig grund då personuppgifter måste behandlas för att uppfylla lagar eller andra författningar av allmänt intresse. Till skillnad från rättslig förpliktelse kan allmänt intresse användas som rättslig grund då behandlingen är nödvändig för att utföra en uppgift, även om den specifika uppgiften inte uttryckligen framgår av den aktuella författningen. Exempel på detta kan vara administration av utbildningar eller IT-stöd för personal.

6. **Grundläggande intresse** – Grundläggande intresse kan tillämpas då personuppgifter måste behandlas för att skydda en registrerad som inte kan lämna samtycke, till exempel om hen är medvetslös.

3.1.1 Hantering av känsliga och extra skyddsvärda personuppgifter

Det är som huvudregel förbjudet att behandla känsliga personuppgifter. För att behandling ska kunna ske krävs att det finns stöd i artikel 9.2 i DSF och dataskyddslagens 3 kapitel. Exempel på undantag från förbudet att behandla känsliga personuppgifter:

- Känsliga personuppgifter får behandlas om behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och inom områdena social trygghet och socialt skydd (artikel 9.2b).
- Uppgifter om förtroendevaldas politiska åsikter får behandlas då den förtroendevalda tydligt har offentliggjort uppgifter (artikel 9.2e).
- Känsliga personuppgifter får behandlas om behandlingen är nödvändig för arkivändamål av allmänt intresse (artikel 9.2j).

I praktiken innebär detta att den personuppgiftsansvariga behöver bedöma om den planerade behandlingen är skälig i förhållande till det intrång den innebär i den registrerades integritet samt säkerställa att det finns lagstöd innan känsliga personuppgifter behandlas.

Behandling av extra skyddsvärda personuppgifter kräver ingen särskild rättslig grund, det är däremot en faktor som behöver vägas in exempelvis i frågor om förvaring, personuppgiftsincidenter och konsekvensbedömningar.

3.2 Förvaring och åtkomst

Utifrån grundprinciperna om integritet och konfidentialitet samt lagringsminimering ska personuppgifter förvaras på ett säkert sätt, det gäller även harmlösa

personuppgifter. Det framgår i artikel 32 i DSF att lämpliga tekniska och organisatoriska åtgärder ska vidtas vid behandling av personuppgifter. Med organisatoriska åtgärder avses att det finns organisation, kompetens och styrning för att säkerställa en säker hantering. Tekniska åtgärder kan innebära flera olika saker, tänk bland annat på följande:

- Datorer och surfplattor ska alltid låsas då de lämnas, även om det bara är för en kortare stund.
- Fysiska handlingar ska förvaras brandsäkert och skyddat från obehörig åtkomst och bör därför förvaras i brandsäkra och behörighetsstyrda rum eller skåp.
- Information ska förvaras på ett sådant sätt att inte fler än nödvändigt får åtkomst. Det kan ske genom att tänka igenom var information är lämpligast att förvara och genom behörighetsstyrning i ett verksamhetssystem.
- Digital information ska skyddas från förstörelse och obehörig åtkomst med lämpliga tekniska åtgärder såsom tvåfaktorsinloggning, virusskydd och backup.

Vilken nivå av skydd som krävs är en bedömning som behöver göras för respektive behandling. För att kunna bedöma vilka krav som ska ställas kan en riskanalys och i vissa fall en konsekvensbedömning behöva genomföras. Se kapitel 4.1 nedan.

3.2.1 Förvaring av känsliga och extra skyddsvärda personuppgifter

Gemensamt för känsliga personuppgifter och extra skyddsvärda personuppgifter är att när sådana uppgifter behandlas kan högre krav behöva ställas på säkerheten vid hanteringen av uppgifternas. Exempelvis kan högre krav behöva ställas på säker förvaring och begränsning av åtkomst till informationen.

3.2.2 Anlitande av personuppgiftsbiträden

När personuppgiftsbiträden anlitas i någon form ska den personuppgiftsansvariga säkerställa att krav ställs på personuppgiftsbiträdet enligt ovan. Personuppgiftsbiträdet ska således förväntas uppfylla samma krav på tekniska och organisatoriska åtgärder enligt DSF som den personuppgiftsansvariga. Att biträden anlitas är vanligt vid inköp av nya IT-system men gäller även i andra sammanhang då någon behandlar personuppgifter för den personuppgiftsansvarigas räkning.

Detta innebär att det innan nya avtal tecknas behöver ställas erforderliga krav på säkerhetsåtgärder utifrån den/de aktuella behandlingarna som ska hanteras av

biträdet samt eventuella underbiträden. För att identifiera vilka krav som ska ställas ska en riskanalys och i vissa fall konsekvensbedömning genomföras innan nya avtal tecknas (se kapitel 4.1 nedan). För att reglera ansvaret för hanteringen och de krav som ställs ska alltid ett personuppgiftsbiträdesavtal tecknas vid anlitande av ett personuppgiftsbiträde (se kapitel 4.3 nedan).

3.2.3 Tredjeland

Artikel 44 i DSF reglerar möjligheten att överföra personuppgifter till tredjeland (länder utanför EU/EES). Överföring till tredjeland kan exempelvis vara:

- Att personuppgifter lagras i en molntjänst som är baserad i tredjeland. Personuppgifter görs därmed tekniskt tillgängliga för en tjänsteleverantör som kan bli skyldig att överlämna personuppgifterna till staten (exempel på detta är USA).
- Att personuppgifter lagras på exempelvis en server utanför EU/EES.
- Att via e-post, chatt, eller någon annan typ av elektronisk kommunikation skicka personuppgifter till USA.
- Att ge en person som befinner sig utanför EU/ESS elektronisk åtkomst till personuppgifter som lagras i EU/EES. Det är alltså inte enbart själva lagringsplatsen som är avgörande utan det räcker med att någon som befinner sig utanför EU/EES får tillgång exempelvis för service/underhåll/felsökning.

Överföring av personuppgifter till tredjeland får endast ske under vissa förutsättningar. Vissa länder har EU-kommissionen beslutat har en adekvat skyddsnivå, till dessa länder kan personuppgifter överföras på samma sätt som inom EU/EES. Utanför dessa länder kan överföring i vissa fall ske med stöd av standardavtalsklausuler som godkänts av EU-kommissionen eller genom bindande företagsbestämmelser[3].

Om överföring ska ske med stöd av standardavtalsklausuler eller bindande företagsbestämmelser behöver den personuppgiftsansvariga också säkerställa att den registrerade ges samma rättigheter i mottagarlandet som denne ges i ett medlemsland i EU/EES. Detta är en bedömning från fall till fall och kräver att den personuppgiftsansvariga utreder om det aktuella landets lagstiftning ger likvärdigt

[3] Mer information om vad detta innebär finns på IMY:s hemsida: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/.

skydd som dataskyddförordningen. Riskanalys och konsekvensbedömning behöver alltid göras innan nya systemavtal eller andra samarbeten ska ingås som kan innebära tredjelandsöverföring av personuppgifter.

3.4 Gallring och rensning

För att personuppgifter inte ska behandlas längre än nödvändigt krävs att det finns beslut om gallring samt rutiner för gallring eller rensning av information som innehåller personuppgifter och som inte behöver sparas.

Med gallring avses förstörelse av allmänna handlingar, för gallring krävs att beslut fattas om att gallra den specifika handlingstypen. Detta sker främst genom nämnders/styrelsers informationshanteringsplaner men kan även ske genom särskilda gallringsbeslut. Rensning innebär att information som *inte* är att betrakta som allmänna handlingar raderas. Det kan röra sig om kopior men kan också vara minnesanteckningar eller arbetsmaterial/utkast. Ett exempel på information som ofta innehåller personuppgifter men som inte alltid är allmänna handlingar är inkommande och utgående e-post (framför allt intern kommunikation). För rensning krävs inga särskilda beslut men det är viktigt att det finns tydliga rutiner så att rensning sker i tillräcklig utsträckning.

3.5 Den registrerades rättigheter

3.5.1 Rätt till registerutdrag

Den registrerade har enligt artikel 15 i DSF rätt att få bekräftelse på huruvida personuppgifter som rör hen håller på att behandlas eller inte genom ett registerutdrag. Behandlas personuppgifter så ska det av utdraget bland annat framgå vilka uppgifter om den registrerade som behandlas, varifrån dessa uppgifter kommer, vad som är ändamålet med behandlingen och till vilka mottagare eller kategorier av mottagare uppgifterna lämnas ut.

Processbeskrivning för hur ett registerutdrag ska hanteras finns på kommunens intranät. Informationen ska tillhandahållas den registrerade senast en månad efter inkommen begäran och är *inte* att betrakta som en begäran om allmän handling.

3.5.2 Rätt att begära flytt, rättning, begräsning eller radering av personuppgifter

Den registrerade har bland annat rätt att begära att få sina personuppgifter flyttade till en annan utförare, rättade, begränsade eller raderade. Rätten att inkomma med en sådan begäran innebär inte att den registrerade har rätt att få begäran beviljad, rätten gäller att få frågan prövad. Tänk på att beslut om att

avslå en begäran är ett beslut i kommunallagens mening. Vid en sådan begäran ska dataskyddsamordnare alltid kontaktas för stöd i den vidare hanteringen.

3.5.3 Rätt till information

Den registrerade har enligt artikel 12 och 13 i DSF rätt att få information om hur dennes personuppgifter behandlas då personuppgifter samlas in från den registrerade eller om den registrerade ber om det. Den registrerade har bland annat rätt att få veta:

- för vilka ändamål personuppgifter kommer att behandlas
- den rättsliga grunden för behandlingen
- hur länge personuppgifter kommer att lagras
- vem som kommer att ta del av personuppgifterna
- registrerades rättigheter enligt dataskyddsförordningen
- om personuppgifter kommer att överföras till ett så kallat tredjeland (land utanför EU/EES)
- att hen kan lämna in klagomål till IMY
- att den registrerade kan återkalla sitt samtycke, om hen har lämnat ett sådant
- kontaktuppgifterna till den personuppgiftsansvariga och till dess dataskyddsombud

Detta ska till exempel alltid beaktas då personuppgifter begärs in genom formulär eller blanketter. Information ska också lämnas i e-postsignaturen för samtliga e-postkonton inom kommunen, mer information om detta finns i Hammarö kommuns riktlinjer för e-posthantering. I de fall det inte lämpar sig att direkt förmedla samtliga delar av informationen kan hänvisning göras till kommunens hemsida eller intranät där fullständig information finns.

4 Dokumentation och rapportering

4.1 Riskanalys och konsekvensbedömning

Enligt artikel 35.1 i DSF ska en konsekvensbedömning genomföras om en personuppgiftsbehandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. För att identifiera behovet av en konsekvensbedömning ska först en riskanalys genomföras, om riskanalysen visar att vissa kriterier är uppfyllda ska den fullständiga konsekvensbedömningen göras. I tveksamma fall bör en konsekvensbedömning alltid göras.

Arbetet med riskanalyser och konsekvensbedömningar ska ses som ett löpande arbete. Riskanalys och eventuell konsekvensbedömning ska genomföras inför nya behandlingar såsom införande av nya system eller nya arbetssätt, men bör också ses över och omvärderas regelbundet utifrån att förutsättningarna kan förändras. Enligt artikel 35.2 i DSF ska dataskyddsombudet alltid rådfrågas vid genomförande av konsekvensbedömning, därför ska dataskyddsombudets kommentarer alltid dokumenteras i en konsekvensbedömning. Det är också viktigt att samtliga riskanalyser och konsekvensbedömningar dokumenteras skriftligt.

Mer information om när och hur riskanalyser och konsekvensbedömningar ska genomföras finns i rutinen för riskanalyser och konsekvensbedömningar.

4.2 Register över personuppgiftsbehandling (registerförteckning)

Enligt artikel 30 i DSF ska varje personuppgiftsansvarig föra ett register i elektronisk form över behandlingar som utförts under dess ansvar, registret ska vid begäran kunna göras tillgängligt för IMY. Förordningstexten innehåller också en detaljerad beskrivning över vilka uppgifter som ska ingå i registret. Arbetet med registret över personuppgiftsbehandlingar ska ses som ett löpande arbete där nya behandlingar ska föras in och befintliga ska ses över regelbundet.

Hammarö kommun använder ett webbaserat verktyg från JP infonet där samtliga nämnder och bolag ska föra sitt register över personuppgiftsbehandlingar. Den verksamhet som ska inleda ett nytt eller förändrat arbetssätt ansvarar för att säkerställa att registret uppdateras. Det är emellertid respektive dataskyddsamordnare som administrerar och godkänner nya behandlingar i registerverktyget. Dataskyddsombudet kan vid tillsyn eller kontroller komma att återkalla godkännandet för behandlingar i registret.

Mer information om hur registret över personuppgiftsbehandlingar ska hanteras finns i rutinen för register över personuppgiftsbehandlingar.

4.3 Personuppgiftsbiträdesavtal (PUB-avtal)

Den personuppgiftsansvariga får anlita någon annan att behandla personuppgifter, det kallas då att anlita ett personuppgiftsbiträde. Den personuppgiftsansvariga får enligt artikel 28 i DSF bara anlita ett biträde som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i DSF (se kapitel 3.2 ovan).

För att säkerställa detta ska det alltid tecknas ett särskilt avtal när ett biträde anlitas som är bindande både för den personuppgiftsansvariga och för personuppgiftsbiträdet (PUB-avtal). Ett PUB-avtal ska bland annat beskriva behandlingens ändamål, typen av personuppgifter och kategorier av registrerade samt den personuppgiftsansvariges skyldigheter och rättigheter. Det är också genom PUB-avtalet som den personuppgiftsansvariga ställer krav på biträdets säkerhet vid hanteringen av personuppgifterna. Det är viktigt att biträdet redovisar eventuella underbiträden i avtalet, även underbiträden omfattas exempelvis av bestämmelserna rörande tredjeland (se 3.2 ovan).

Vid tecknande ska Hammarö kommuns mall för PUB-avtal med tillhörande bilagor användas, i mallen finns instruktioner för hur PUB-avtal ska tecknas.

4.4 Rapportering av personuppgiftsincidenter

En personuppgiftsincident har uppstått när de personuppgifter vi behandlar:

- medvetet, omedvetet eller olagligt förstörs, förvanskas, förloras eller felaktigt ändras
- när någon som inte har behörig tillgång till personuppgifterna får tillgång/åtkomst till dessa
- när personuppgifterna på ett obehörigt sätt röjs (obehörigt röjande)

Det kan alltså röra sig om oavsiktliga handlingar såsom en borttappad mobil eller dator, eller att uppgifter råkas skickas till fel mottagare. Det kan också vara konsekvenser av avsiktliga handlingar såsom dataintrång. Personuppgiftsincidenter ska alltid rapporteras i kommunens e-tjänst när medarbetare eller personuppgiftsbiträde (leverantör):

- vet att det inträffat en incident

- misstänker att det har inträffat en incident
- ser en risk för att det kan inträffa en incident

Alla personuppgiftsincidenter ska rapporteras så snart som möjligt efter upptäckt. Det gäller även om incidenten hunnit bli åtgärdad. Artikel 33 i DSF reglerar den personansvarigas ansvar att rapportera personuppgiftsincidenter till IMY. Om det är sannolikt att personuppgiftsincidenten kommer att medföra en risk för de registrerade så måste händelsen anmälas till IMY inom 72 timmar från det att incidenten upptäcktes. Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska även den registrerade utan onödigt dröjsmål informeras om incidenten. Risker för den enskilde kan exempelvis vara:

- ekonomisk skada
- diskriminering
- identitetsstöld och bedrägeri
- skadlig ryktesspridning

Med tanke på kravet att en anmälan till IMY ska ske inom 72 timmar är det viktigt att det finns kunskap och tydliga rutiner i organisationen för att kunna hantera personuppgiftsincidenter omgående.

Mer information om hur personuppgiftsincidenter ska bedömas hanteras finns i rutinen för hantering av personuppgiftsincidenter.