



Dataskyddspolicy

Beslutad den 4 juni 2024 av vikarierande riksantikvarien Susanne Thedéen.

Detta dokument beskriver Riksantikvarieämbetets dataskyddsarbete. Policyn gäller för alla medarbetare.

Innehållsförteckning

1	INLEDNING	2
2	GENERELLT OM PERSONUPPGIFTSBEHANDLING	2
2.1	Personuppgifter	2
2.1.1	Känsliga personuppgifter	3
2.1.2	Uppgifter om lagöverträdelser	3
2.1.3	Personnummer och samordningsnummer	3
2.1.4	Andra integritetskänsliga personuppgifter	4
2.2	Behandling av personuppgifter	4
2.3	Principer för personuppgiftsbehandling	4
2.3.1	Laglighet, korrekthet och öppenhet	4
2.3.2	Ändamålsbegränsning	5
2.3.3	Uppgiftsminimering	5
2.3.4	Riktighet	5
2.3.5	Lagringsminimering	5
2.3.6	Integritet och konfidentialitet	5
2.3.7	Ansvarsskyldighet	5
2.4	Rättsliga grunder för personuppgiftsbehandling	6
2.4.1	Samtycke	6
2.4.2	Fullgöra ett avtal	6
2.4.3	Rättslig förpliktelse	6
2.4.4	Skydda grundläggande intressen	6
2.4.5	Uppgift av allmänt intresse eller myndighetsutövning	7
2.4.6	Intresseavvägning	7

2.5	De registrerades rättigheter	7
1(13)		
2.5.1	Rätt till information om personuppgiftsbehandlingen	7
2.5.2	Rätt att få tillgång till sina personuppgifter	8
2.5.3	Rätt att få sina personuppgifter rättade	8
2.5.4	Rätt att få sina personuppgifter raderade	8
2.5.5	Rätt att få sina personuppgifter överförda (dataportabilitet)	8
2.5.6	Rätt till begränsning av behandlingen	8
2.5.7	Rätt att göra invändningar mot behandlingen	8
2.6	Säkerhetsåtgärder	9
2.7	Inbyggt dataskydd och dataskydd som standard	9
2.8	Överföring till tredje land och internationella organisationer	9
2.9	Personuppgiftsbiträden	10
2.10	Personuppgiftsincidenter	10
	DATASKYDDSORGANISATION	10
3.1	Personuppgiftsansvarig	10
3.2	Dataskyddsombud	10
3.3	Avdelningschefer	10
3.4	Anställda, konsulter och andra uppdragstagare	11
3.5	Juridiska enheten	11
3.6	Dataskyddskoordinatorer	11
3.7	Dataskyddsgruppen	12
3.8	Chefsavstämningar	12
4	INTERNA STYRANDE OCH STÖDJANDE DOKUMENT AV BETYDELSE FÖR VÅR PERSONUPPGIFTSBEHANDLING	12

1 Inledning

Riksantikvarieämbetet samordnar och stödjer arbetet med digitalisering, digitalt bevarande och digital förmedling inom kulturarvsområdet. Vi främjar kunskapsförsörjning och bedriver informations- och rådgivningsverksamhet samt förvaltar nationella databaser för kulturhistorisk information. Inom ramen för detta samt övriga uppgifter som åligger oss som förvaltningsmyndighet värnar vi om både medborgarnas och våra anställdas integritet.

Skyddet för enskildas integritet grundar sig i de mänskliga rättigheterna. Individens rätt till respekt för sitt privat- och familjeliv regleras i artikel 8 i den europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna som gäller som lag i Sverige.¹ I artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna framgår att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Skyddet för vår personliga integritet är även inskriven i vår grundlag. I 2 kap. 6 § andra stycket regeringsformen stadgas att ”var och en [är] 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.”

Bestämmelser om hur personuppgifter ska behandlas för att skydda enskildas integritet finns i 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) (nedan *dataskyddsförordningen* eller *DSF*). Den kompletteras i Sverige av lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (nedan *dataskyddslagen*) och förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Felaktig personuppgiftsbehandling kan leda till att enskildas integritet kränks. Det kan även leda till kostnader för Riksantikvarieämbetet i form av sanktionsavgifter och skadestånd samt ett minskat förtroende för oss.

För att kunna leva upp till dataskyddsförordningens krav behöver vi en organisation för dataskyddsarbetet och relevanta styrande och stödjande dokument för att hjälpa alla medarbetare att göra rätt.

Riksantikvarieämbetets dataskyddspolicy syftar till att ge en övergripande beskrivning av hur vårt dataskyddsarbete är organiserat och hur du som anställd ska agera för att behandla personuppgifter på ett ansvarsfullt sätt.

2 Generellt om personuppgiftsbehandling

2.1 Personuppgifter

Personuppgifter definieras i artikel 4.1 DSF och är enkelt uttryckt varje uppgift som direkt eller indirekt identifierar en fysisk levande person. Exempel på personuppgifter som vi behandlar på Riksantikvarieämbetet är:

¹ 1 § lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna

- personnummer, namn och adress, telefonnummer, e-postadress, användarnamn, befattning, diarienummer, meritförteckning,
- löneuppgifter,
- bilder och ljudupptagningar av personer (även om inga namn nämns),
- fastighetsbeteckningar och gårdsnamn, och
- IP-nummer och cookies, om de kan kopplas till en fysisk person.

2.1.1 Känsliga personuppgifter

I artikel 9 DSF finns en särskild reglering för särskilda kategorier av personuppgifter, som vi i Sverige benämner känsliga personuppgifter.² Uppräkningen är uttömmande, det vill säga formellt sett är det bara de kategorierna som utgör ”känsliga personuppgifter.” Känsliga personuppgifter är uppgifter som är kopplade till en person och rör

- etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- hälsa (t.ex. sjukfrånvaro, allergier, specialkost)
- en persons sexualliv eller sexuella läggning
- genetik
- biometriska uppgifter som används för att entydigt identifiera en person (till exempel fingeravtryck som används för att låsa upp en mobiltelefon).

Utgångspunkten är att det är förbjudet att behandla känsliga personuppgifter men i artikel 9.2 DSF finns ett antal undantag från förbudet uppräknade. I dataskyddslagens tredje kapitel finns bestämmelser om när en myndighet får behandla känsliga personuppgifter. Enligt 3 kap. 3 § dataskyddslagen får känsliga personuppgifter bland annat behandlas av en myndighet om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

2.1.2 Uppgifter om lagöverträdelser

Uppgifter om lagöverträdelser definieras i artikel 10 DSF som ”fällande domar i brottmål och lagöverträdelser som innefattar brott eller därmed sammanhängande säkerhetsåtgärder”. Det kan vara att någon är misstänkt för eller har dömts för ett visst brott men även om någon har friats i ett brottmål. Även uppgifter om att någon har häktats eller fått egendom beslagtagna omfattas av begreppet. Att vi får behandla sådana uppgifter framgår av 3 kap. 8 § dataskyddslagen. När vi åtalsanmäler t.ex. ett brott mot kulturmiljölagen innebär det att vi behandlar uppgifter om lagöverträdelser om vi anger en specifik person som misstänkt.

2.1.3 Personnummer och samordningsnummer

Dataskyddsförordningen ger medlemsstaterna möjlighet att bestämma på vilka villkor nationella identifikationsnummer får behandlas. Sådana bestämmelser finns i 3 kap. 10 § dataskyddslagen. Där

² 3 kap. 1 § dataskyddslagen

framgår att personnummer och samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Bestämmelser om att personnummer ska behandlas kan finnas i annan lagstiftning som vi som myndighet ska följa, t.ex. bestämmelserna om arbetsgivardeklaration som ska lämnas enligt skattelagstiftningen.

2.1.4 Andra integritetskänsliga personuppgifter

Det finns vissa personuppgifter som inte omfattas av de särskilda bestämmelserna i dataskyddsförordningen men ändå ses som mer integritetskänsliga. Sådana uppgifter kan vara lönespecifikationer och bankkontonummer, uppgifter från utvecklingssamtal eller uppgifter om en anställds sociala förhållanden. När vi behandlar sådana uppgifter kan vi behöva vidta extra säkerhetsåtgärder.

2.2 Behandling av personuppgifter

Det finns en definition av behandling i artikel 4.2 DSF. Behandling är en åtgärd eller en kombination av åtgärder avseende enskilda personuppgifter eller uppsättningar av sådana och oavsett om de sker automatiserat eller inte. I artikeln finns en icke uttömmande uppräkningslista av åtgärder som är behandlingar.

Enkelt uttryckt behandlar vi personuppgifter hela tiden i vårt arbete – t.ex. när vi skickar ett mejl eller chattar i Teams, handlägger en bidragsansökan eller svarar på en remiss, lägger ut en nyhet på vår hemsida eller ordnar ett webinarium. All vår behandling omfattas av och ska följa dataskyddsreglerna.

2.3 Principer för personuppgiftsbehandling

I dataskyddsförordningen finns sex viktiga principer som gäller för all vår behandling av personuppgifter.

2.3.1 Laglighet, korrekthet och öppenhet

Principen om att personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade finns i artikel 5.1 a DSF.

Kravet på *laglighet* innebär bland annat att det måste finnas en rättslig grund för behandlingen. Vilka rättsliga grunder som vi vanligtvis stödjer oss på framgår närmare nedan under rubriken ”Rättslig grund”. Om det inte finns någon rättslig grund som vi kan tillämpa på en viss behandling betyder det att vi inte får utföra behandlingen.

Med *korrekthet* avses att vår behandling ska vara rättvis och skälig samt proportionerlig i förhållande till den registrerades integritet och nytta för oss. Vår behandling ska inte gå utöver vad den registrerade kan förvänta sig av oss.

Innebörden av kravet på *öppenhet* är att den registrerade ska få tydlig information om bl.a. för vilka ändamål vi behandlar personuppgifterna och på vilket sätt. Vi ska även informera om vi kommer att lämna över personuppgifterna till andra, hur länge vi lagrar personuppgifterna och hur den registrerade kan komma i kontakt med Riksantikvarieämbetet som personuppgiftsansvarig. Det är därför viktigt att vi lämnar klar och tydlig information om vår behandling och gör det enkelt för de registrerade att hitta den, t.ex. genom tydliga rubriker på våra webbplatser eller genom länkar i autosvar och e-postsignaturer.

2.3.2 Ändamålsbegränsning

Principen om *ändamålsbegränsning* regleras i artikel 5.1 b DSF. Den innebär att vi bara får samla in personuppgifter för särskilda uttryckligt angivna och berättigade ändamål. Det betyder att vi redan innan vi börjar samla in personuppgifterna måste ha bestämt vilket vårt ändamål med behandlingen är. Huvudregeln är att vi därefter inte får behandla uppgifterna på ett sätt som är oförenligt med de ursprungliga ändamålen. De ändamål vi bestämt från början utgör ramarna för vår behandling. I vissa fall kan det vara tillåtet att använda personuppgifterna för ytterligare ändamål än de ursprungliga om det nya ändamålet är förenligt med det ursprungliga och vi informerar de registrerade om det nya ändamålet med behandlingen.

2.3.3 Uppgiftsminimering

Principen om *uppgiftsminimering* framgår av artikel 5.1 c DSF.

Det är inte tillåtet att samla in fler personuppgifter än de vi behöver för vårt fastställda ändamål. De personuppgifter som vi behandlar ska vara adekvata, relevanta och inte alltför omfattande i förhållande till ändamålet. Vi får till exempel inte samla in personuppgifter för att de kan vara bra att ha i framtiden. Det betyder att vi, innan vi påbörjar vår insamling, ska ha gjort en bedömning av vilka personuppgifter som är nödvändiga och att vi utformar våra blanketter och e-tjänster på ett sätt som säkerställer att vi bara får in just dessa.

2.3.4 Riktighet

Principen om *riktighet* i artikel 5.1 d DSF innebär att de personuppgifter som vi behandlar ska vara riktiga och om nödvändigt uppdaterade. Vi måste därför vidta alla rimliga åtgärder för att säkerställa att felaktiga uppgifter raderas eller rättas utan dröjsmål. Som ett led i vår uppfyllelse av principen försöker vi undvika att lagra kopior av personuppgifter i mer än ett system vilket ger oss möjlighet att undvika både felkällor och att ej uppdaterad information sparas.

2.3.5 Lagringsminimering

Principen om *lagringsminimering* återfinns i artikel 5.1 e DSF. Vi får inte spara personuppgifter under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Det är dock tillåtet att bevara personuppgifter för arkivändamål av allmänt intresse. Som statlig förvaltningsmyndighet ska Riksantikvarieämbetet följa bestämmelserna i arkivlagstiftningen vilket betyder att vi sparar personuppgifter i allmänna handlingar som ska bevaras. Det innebär att vi bevarar och gallrar uppgifter i allmänna handlingar enligt de bestämmelser som finns där och enligt särskilda gallringsrutiner. För personuppgifter som behandlas i handlingar som inte är allmänna säkerställer vi att rensning sker kontinuerligt. Vi säkerställer att personuppgifter inte hanteras på fler lagringsytor är nödvändigt.

2.3.6 Integritet och konfidentialitet

Principen om integritet och konfidentialitet finns i artikel 5.1 f DSF.

Som personuppgiftsansvarig måste Riksantikvarieämbetet skydda de personuppgifter vi behandlar mot bland annat obehörig eller otillåten behandling och mot förlust, förstörelse eller skada genom olyckshändelse. För att kunna göra det behöver vi vidta lämpliga tekniska och organisatoriska åtgärder, vilket utvecklas nedan under rubriken ”Säkerhetsåtgärder”.

2.3.7 Ansvarsskyldighet

Principen om *ansvarsskyldighet* finns i artikel 5.2 DSF. Den innebär att Riksantikvarieämbetet som personuppgiftsansvarig måste kunna visa att alla bestämmelser i dataskyddsförordningen efterlevs.

Även artikel 24 DSF beskriver den personuppgiftsansvariges ansvar. Enligt den ska Riksantikvarieämbetet, med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. I ansvaret ligger också att se över och uppdatera åtgärderna vid behov.

I artikel 30 DSF finns också ett krav på att vi ska föra ett register över den personuppgiftsbehandling som sker under Riksantikvarieämbetets ansvar. Den så kallade artikel 30förteckningen ska uppdateras med information vid nya och ändrade behandlingar.

2.4 Rättsliga grunder för personuppgiftsbehandling

I artikel 6 DSF finns en uppräkningslista över de rättsliga grunder som kan åberopas till stöd för behandling av personuppgifter. För att en behandling ska vara tillåten måste det finnas en rättslig grund som är tillämplig och det är viktigt att fastställa den innan en behandling påbörjas.

2.4.1 Samtycke

Enligt artikel 6.1 a DSF får personuppgifter behandlas om den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål. För att ett samtycke ska vara giltigt finns vissa krav som måste uppfyllas. Ett samtycke måste till exempel vara helt frivilligt. När förhållandet mellan den registrerade och den personuppgiftsansvarige är ojämnt, t.ex. medborgare i förhållande till myndighet eller anställd i förhållande till arbetsgivare, är det svårt att få till ett helt frivilligt samtycke. Samtycke är därför en rättslig grund som har en begränsad tillämpning för oss på Riksantikvarieämbetet.

2.4.2 Fullgöra ett avtal

När det är nödvändigt för att fullgöra ett avtal i vilket den registrerade är eller avser att bli part får personuppgifter behandlas enligt artikel 6.1 b DSF. Ett exempel är att Riksantikvarieämbetet vid anlitande av en konsult behandlar personuppgifter för att uppfylla villkoren i avtalet och till exempel betala ut ersättning eller administrera andra frågor kopplade till avtalet. För att kunna åberopa den här rättsliga grunden krävs att det är den registrerade som är part i avtalet och den kan därför inte åberopas när vi till exempel köper bilder på personer från ett företag eftersom det då är företaget som är part i avtalet.

2.4.3 Rättslig förpliktelse

Av artikel 6.1 c DSF framgår att det är tillåtet att behandla personuppgifter när det är nödvändigt för att uppfylla en rättslig förpliktelse. Förpliktelsen ska framgå av en författning eller kollektivavtal. När Riksantikvarieämbetet redovisar skatter och sociala avgifter för oss som anställda till Skatteverket sker det med stöd av en rättslig förpliktelse. Ett annat exempel är att man ska ange upphovsman i anslutning till ett upphovsrättsligt skyddat verk, till exempel ett foto eller en artikel.

2.4.4 Skydda grundläggande intressen

Den rättsliga grunden att skydda grundläggande intressen regleras i artikel 6.1 d DSF och har ett mycket begränsat tillämpningsområde, i första hand inom vården. Det handlar till exempel om tillfällen när personuppgifter måste behandlas för att rädda liv. Det är därför svårt att se en situation hos Riksantikvarieämbetet där detta är en rättslig grund som vi kan åberopa.

2.4.5 Uppgift av allmänt intresse eller myndighetsutövning

Den rättsliga grund som större delen av vår personuppgiftsbehandling grundar sig på är att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning, artikel 6.1 e DSF.

Ett krav är att uppgiften ska vara fastställd i EU-rätt eller svensk rätt vilket framgår av artikel 6.3 DSF. Av 2 kap. 1 § dataskyddslagen framgår att personuppgifter får behandlas med stöd av artikel 6.1 e DSF, om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning eller som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning.

För Riksantikvarieämbetet, precis som för andra svenska myndigheter, innebär detta att de arbetsuppgifter eller åtgärder vi vill vidta ska framgå av lag, förordning, regeringsuppdrag eller liknande. Utöver de uppgifter som framgår av vår instruktion³ finns bestämmelser i t.ex. förvaltningslagen och myndighetsförordningen som handlar om oss som myndighet på ett mer övergripande plan medan mer specifika uppgifter finns i t.ex. kulturmiljölagen.

Exempel på myndighetsutövning är när vi beslutar om bidrag enligt förordningen (2014:108) om statsbidrag till ideella organisationer inom kulturmiljöområdet.

Ett annat exempel på en arbetsuppgift för Riksantikvarieämbetet är att pröva ansökningar om att använda vissa kännetecken enligt lagen om skydd för kännetecken i den internationella humanitära rätten. Den arbetsuppgiften framgår av 20 a § totalförsvarets folkrättsförordning (1990:12).

Även åtgärder som t.ex. rekrytering är en uppgift av allmänt intresse och hur rekrytering ska genomföras i statlig förvaltning följer bl.a. av lagen (1994:260) om offentlig anställning.

Enligt 6 § myndighetsförordningen (2007:515) ska en myndighet tillhandahålla information om myndighetens verksamhet, vilket kan utgöra en laglig grund för till exempel extern kommunikation.

Riksantikvarieämbetet har även arbetsuppgifter som följer av EU-lagstiftning. Myndigheten har i uppgift att pröva ansökningar om importlicenser enligt Europaparlamentets och rådets förordning (EU) 2019/880 av den 17 april 2019 om införsel och import av kulturföremål.

2.4.6 Intresseavvägning

Den sjätte rättsliga grunden är att behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges berättigade intressen som väger tyngre än den registrerades intressen eller grundläggande rättigheter, artikel 6.1 f DSF. Vi kan inte tillämpa den här grunden när vi som myndighet utför våra uppgifter. Det är alltså inte en rättslig grund vi använder oss av här på Riksantikvarieämbetet.

2.5 De registrerades rättigheter

Dataskyddsförordningen ger alla registrerade ett antal rättigheter och som personuppgiftsansvarig måste Riksantikvarieämbetet säkerställa att de kan utövas.

2.5.1 Rätt till information om personuppgiftsbehandlingen

När personuppgifter samlas in ska vi lämna information om personuppgiftsbehandlingen till de registrerade, både när det är den registrerade själv som lämnar uppgifterna och när det är någon

³ Förordning (2014:1585) med instruktion för Riksantikvarieämbetet

annan som gör det, t.ex. när en organisation som ansöker om bidrag lämnar uppgifter om anställda eller medlemmar. Det framgår av artikel 13 och 14 DSF. Informationen ska finnas tillgänglig kostnadsfritt i en lättillgänglig, skriftlig form, vilket kan vara elektroniskt, och med ett tydligt och enkelt språk. Vi har information på vårt intranät och vår externa hemsida samt länkar till den i vår kommunikation, t.ex. i autosvar och e-postsignaturer.

2.5.2 Rätt att få tillgång till sina personuppgifter

Av artikel 15 DSF framgår att den registrerade har rätt att få veta om personuppgifter om denne behandlas, och i sådana fall få en kopia av personuppgifterna, det som brukar kallas registerutdrag, samt få information om till vilka mottagare vi har lämnat ut uppgifterna. Vi har en rutin för hur vi ska hantera en begäran om registerutdrag.

2.5.3 Rätt att få sina personuppgifter rättade

Rätten att få sina personuppgifter rättade regleras i artikel 16 DSF. Det är viktigt att komma ihåg att vi vid rättelser kan behöva beakta relevanta regler i arkivlagstiftningen när uppgifterna som ska rättas finns i en allmän handling. Den här rättigheten innebär också att den registrerade har rätt att komplettera med sådana personuppgifter som saknas och som är relevanta med hänsyn till ändamålet med vår personuppgiftsbehandling. Vi har en rutin för hantering av begäran om rättelse.

2.5.4 Rätt att få sina personuppgifter raderade

Artikel 17 DSF innehåller rätten att få sina uppgifter raderade, det som brukar kallas för rätten att bli bortglömd. Rätten till radering är dock begränsad när behandlingen är nödvändig för att tillgodose andra viktiga rättigheter, till exempel rätten till yttrande- och informationsfrihet, för att uppfylla en rättslig förpliktelse, utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövningen. Det betyder att den här rättigheten har en begränsad tillämpning på Riksantikvarieämbetet eftersom vi som statlig myndighet måste följa reglerna om allmänna handlingar och bevarande av sådana och i huvudsak grundar vår behandling på den rättsliga grunden uppgift av allmänt intresse eller myndighetsutövning. Vi har en rutin för hantering av begäran om radering.

2.5.5 Rätt att få sina personuppgifter överförda (dataportabilitet)

Rätten till dataportabilitet, artikel 20 DSF, innebär att den som har lämnat sina personuppgifter till en personuppgiftsansvarig i vissa fall har rätt att få ut och använda sina personuppgifter hos en annan personuppgiftsansvarig. I nuläget är det svårt att se att vi har sådan information som skulle kunna bli föremål för dataportabilitet på Riksantikvarieämbetet.

2.5.6 Rätt till begränsning av behandlingen

Rätten till begränsning enligt artikel 18 DSF innebär att uppgifterna markeras så att dessa i framtiden endast får behandlas för vissa avgränsade syften. Den här rättigheten kan åberopas bland annat när den registrerade har begärt rättelse enligt artikel 16 DSF vilket kan inkludera en begäran om att behandlingen av uppgifterna begränsas under tiden som den personuppgiftsansvarige utreder uppgifternas riktighet. Vi har en rutin för att hantera en begäran om begränsning.

2.5.7 Rätt att göra invändningar mot behandlingen

Artikel 21 DSF reglerar den registrerades rätt att invända mot en personuppgiftsbehandling.

Rättigheten gäller när vi behandlar personuppgifter för att utföra en uppgift av allmänt intresse eller myndighetsutövning. Vid en invändning får vi endast fortsätta att behandla uppgifterna om vi kan visa att det finns tvingande berättigade skäl till att uppgifterna måste behandlas och dessa skäl måste

väga tyngre än den enskildes intressen och rättigheter. En enskild har alltid rätt att invända mot att personuppgifter används för direkt marknadsföring. Vi har en rutin för att hantera invändningar.

2.6 Säkerhetsåtgärder

Riksantikvarieämbetet måste som personuppgiftsansvarig säkerställa att all personuppgiftsbehandling sker på ett sätt som säkerställer en lämplig säkerhet för personuppgifterna. Säkerhetsåtgärder kan vara både tekniska och organisatoriska. För att kunna avgöra vilka säkerhetsåtgärder som behövs och är lämpliga är det viktigt att först kartlägga vilka personuppgifter som behövs för att utföra en viss uppgift och vilka risker som de behöver skyddas från. Vissa personuppgifter, t.ex. känsliga personuppgifter, kräver högre säkerhet. Detsamma gäller för uppgifter om lagöverträdelse, personnummer och andra integritetskänsliga personuppgifter.

Genom vårt systematiska informationssäkerhetsarbete skapar vi bra underlag för våra bedömningar om lämpliga säkerhetsåtgärder. Informationsklassningar och riskbedömning kompletteras av en personuppgiftskartläggning som kan utgå från vår artikel 30-förteckning. Dessa underlag utgör grunden för att avgöra om behandlingen innebär sådana risker att det är obligatoriskt att göra en konsekvensbedömning enligt artikel 35 DSF. Innan en ny behandling påbörjas ska dessa underlag alltid tas fram. Detsamma gäller när åtgärder av något slag som berör en pågående behandling ska vidtas, t.ex. genom att ett nytt systemstöd ska anskaffas. Även i andra fall kan det finnas anledning att göra en personuppgiftskartläggning för en pågående behandling eftersom det utgör ett bra sätt att dokumentera att vi lever upp till kraven i dataskyddsförordningen och vidtar rätt säkerhetsåtgärder.

Tekniska åtgärder kan vara backup-rutiner och brandväggar, lösenordskyddade trådlösa nätverk, uppdaterat virusskydd, uppdaterad programvara, lösenordsskydd för till exempel mobiltelefoner och surfplattor, skydd mot obehörig åtkomst, lösenordskrav, kryptering vid behov, loggning av åtkomst till och användning av IT-system m.m.

Organisatoriska åtgärder kan vara att alla vi anställda men även konsulter får kontinuerlig utbildning i dataskyddsfrågor, att det finns styrande och stödjande dokument som vi kan använda i vårt dagliga arbete och att ledningen löpande följer upp arbetet.

2.7 Inbyggt dataskydd och dataskydd som standard

Kravet på inbyggt dataskydd och dataskydd som standard finns i artikel 25 DSF. Det innebär att vi ska beakta dataskyddsreglerna redan när vi utvecklar nya it-tjänster och arbetssätt. Genom att tidigt i utvecklingsarbetet fundera över t.ex. fritextfält eller behörighetsnivåer kan vi undvika onödig personuppgiftsbehandling. Detsamma gäller i vårt dagliga arbete genom att vi tänker igenom vem som behöver få ett mejl eller var vi lagrar information som innehåller personuppgifter. Genom att arbeta systematiskt och ta fram relevanta underlag med hjälp av de rutiner och mallar som tagits fram säkerställer vi att vi uppfyller dataskyddsreglerna.

2.8 Överföring till tredje land och internationella organisationer

Överföring till tredje land eller internationell organisation är som huvudregel förbjudet men kan ske under vissa förutsättningar som framgår av kapitel V i dataskyddsförordningen. Ett exempel på överföring till tredje land kan vara när vi använder en molntjänst. Vi har särskilda rutiner för att fatta beslut om användningen av sådana tjänster. Överföring sker även när vi t.ex. mejlar någon på en organisation eller myndighet i tredje land. Vi säkerställer att sådana överföringar sker korrekt och i enlighet med bestämmelserna i dataskyddsförordningen.

2.9 Personuppgiftsbiträden

Kravet i artikel 28.1 DSF är att den personuppgiftsansvarige endast ska anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder så att dataskyddsförordningens krav uppfylls och de registrerades rättigheter skyddas. För att säkerställa att kraven uppfylls gör vi ett noggrant förarbete och en utförlig kravställning inför anskaffningar. Detta gäller förstås även när vi överväger att börja använda olika grätistjänster. Vi utgår från att det är vårt förslag till personuppgiftsbiträdesavtal som ska gälla och går endast i undantagsfall med på att använda biträdets mall om det ger en lika god skyddsnivå som vårt.

2.10 Personuppgiftsincidenter

Personuppgiftsincident definieras i artikel 4.12 DSF som en säkerhetsincident som leder till oavsiktlig eller olaglig förstörelse, förlust, ändring eller obehörig åtkomst till personuppgifter. Den vanligaste personuppgiftsincidenten som rapporteras in till Integritetsskyddsmyndigheten är att personuppgifter röjs, genom till exempel felskick av e-post, och är orsakad av den mänskliga faktorn.

Riksantikvarieämbetet måste utreda och dokumentera alla personuppgiftsincidenter som inträffar och som huvudregel anmäla dem till Integritetsskyddsmyndigheten inom 72 timmar. Alla anställda ansvarar för att rapportera misstänkta personuppgiftsincidenter till dataskyddsombudet eller Servicedesk så snart som möjligt. Dataskyddsombudet har en delegation att rapportera till Integritetsskyddsmyndigheten.

3 Dataskyddsorganisation

3.1 Personuppgiftsansvarig

Riksantikvarieämbetet är personuppgiftsansvarig och som organisation ansvarig för all personuppgiftsbehandling som sker på myndigheten. Riksantikvarien är den som ytterst är ansvarig för att dataskyddsreglerna följs.

3.2 Dataskyddsombud

Riksantikvarieämbetet har ett dataskyddsombud. Dataskyddsombudets uppgifter regleras i artikel 39 DSF. Den viktigaste uppgiften för dataskyddsombudet är att övervaka att Riksantikvarieämbetet som personuppgiftsansvarig följer dataskyddsförordningen. Dataskyddsombudet ska även informera och ge råd om behandlingen av personuppgifter, delta i arbetet med konsekvensbedömningar och vara kontaktperson i förhållande till vår tillsynsmyndighet Integritetsskyddsmyndigheten.

Riksantikvarieämbetet stöder dataskyddsombudet vid utförandet av ovanstående uppgifter och säkerställer att det finns tillräckliga resurser för att fullgöra uppdraget som dataskyddsombud.

3.3 Avdelningschefer

Enligt arbetsordningen har varje avdelningschef ansvar för informations- och systemägarskapet för de informationsmängder och IT-system som avdelningen ansvarar för. Avdelningschefen är också ansvarig för att avdelningens verksamhet bedrivs i enlighet med gällande regler, vilket inkluderar dataskyddsreglerna. I ansvaret ligger att säkerställa att alla medarbetare har den kunskap och det stöd som behövs för en korrekt personuppgiftsbehandling i det dagliga arbetet, till exempel att efterfråga utbildning av personalen samt nya eller uppdaterade styrande eller stödjande dokument.

Avdelningscheferna ansvarar också för

- att funktionen dataskyddskoordinator är bemannad,
- att kartläggningar och riskanalyser samt konsekvensbedömningar genomförs vid behov
 - innan system eller tjänster köps in, utvecklas eller börjar användas för annan information än den ursprungliga, ○ innan analog information digitaliseras eller en process digitaliseras,
 - när myndigheten får ett nytt eller ändrat uppdrag genom regleringsbrev, särskilt regeringsuppdrag eller författningsändring,
- att information till de registrerade tas fram eller uppdateras,
- att underlag till artikel 30-förteckningen lämnas innan personuppgiftsbehandlingen påbörjas och att informationen i förteckningen ses över och uppdateras regelbundet, och
- att lämna underlag till dataskyddsombudets granskningar.

Avdelningschefen har det övergripande ansvaret för att säkerställa att personuppgiftsbiträdesavtal tecknas vid behov och att avtalet följs upp regelbundet i enlighet med framtagna rutiner.

Till sitt stöd har avdelningscheferna en eller flera utpekade dataskyddskoordinatorer, se närmare nedan.

3.4 Anställda, konsulter och andra uppdragstagare

Alla anställda samt konsulter och andra uppdragstagare som vi anlitar får behandla personuppgifter endast enligt de instruktioner som Riksantikvarieämbetet ger i egenskap av personuppgiftsansvarig. Utöver de instruktioner som framgår här i dataskyddspolicyn finns instruktioner i myndighetens övriga styrande och stödjande dokument.

För att säkerställa en korrekt personuppgiftsbehandling är det viktigt att vi alla tar ansvar för att bara behandla de personuppgifter som är nödvändiga för att utföra våra arbetsuppgifter och att följa styrande och stödjande dokument rörande ärendehantering och informationsförvaltning. Det är också viktigt att överväga vilka uppgifter som anges i beslut eller annan extern kommunikation, t.ex. bör känsliga personuppgifter undvikas om det inte är absolut nödvändigt att de finns med i ett beslut. Detsamma gäller för uppgifter om lagöverträdelser och personnummer.

3.5 Juridiska enheten

Juridiska enheten tar fram styrande och stödjande dokument, inklusive mallar av olika slag, som är nödvändiga för att Riksantikvarieämbetets personuppgiftsbehandling sker i enlighet med reglerna. Enheten arbetar även med att utbilda anställda, omvärldsbevaka på området samt ta fram intern information om praxis och ändringar i regelverken. Enheten stödjer dataskyddskoordinatorerna i deras arbete och lämnar rättsligt stöd och vägledning i dataskyddsregelverket, t.ex. om personuppgiftsbiträdesavtal behöver tecknas.

Juridiska enheten administrerar Riksantikvarieämbetets artikel 30-förteckning och uppdaterar den med den information som respektive avdelning lämnar som underlag på en mall som enheten tagit fram.

3.6 Dataskyddskoordinatorer

På varje avdelning finns funktionen dataskyddskoordinator som kan bemannas av en eller flera personer. En dataskyddskoordinators uppdrag är att vara kontaktperson för juridiska enheten i dataskyddsfrågor. Dataskyddskoordinatören ansvarar för att

- vidarefördela information från dataskyddsombudet och juridiska enheten till avdelningens ledningsgrupp och medarbetare,
- fördela underlag till artikel 30-förteckningen till Juridiska enheten,
- samt samordna arbetet med underlag inför inköp, utveckling eller nya användningsområden för system eller tjänster, digitisering av information eller digitalisering av en process samt vid nya eller ändrade uppdrag för Riksantikvarieämbetet.

3.7 Dataskyddsgruppen

På Riksantikvarieämbetet finns en dataskyddsgrupp. Den består av dataskyddsombudet, dataskyddskoordinatorerna och de verksjurister som arbetar med digitalisering. Vid behov kan även andra medarbetare delta. Dataskyddsgruppen har regelbundna möten för att stämma av det löpande dataskyddsarbetet på myndigheten. Juridiska enheten är sammankallande och ansvarar för att mötena dokumenteras på lämpligt sätt.

3.8 Chefsavstämningar

Minst två gånger per år, en gång på våren och en på hösten, har avdelningscheferna avstämning med dataskyddsombudet, chefsjuristen och representanter för dataskyddsgruppen. Syftet med mötet är att stämma av dataskyddsarbetet som bedrivs på respektive avdelning, gå igenom behov av utbildningar och nya eller uppdaterade styrande och stödjande dokument samt behov av åtgärder till följd av dataskyddsombudets granskningar. Dataskyddsombudet är sammankallande och ansvarar för att mötena dokumenteras på lämpligt sätt.

4 Interna styrande och stödjande dokument av betydelse för vår personuppgiftsbehandling

Det finns flera interna styrande och stödjande dokument som innehåller bestämmelser som är av betydelse för en korrekt personuppgiftsbehandling. Några av dessa är

- Arbetsordning och delegationsordning
- Informationssäkerhetspolicy
- Regler för IT-säkerhet
- IT-regler för medarbetare
- Regler för hantering av allmänna handlingar, diarieföring och arkivering
- Riksantikvarieämbetets strategi för bevarande av allmänna handlingar