

Bilaga 2 Behandla personuppgifter i Primus och DigitaltMuseum

Datum 2023-05-29

Diarienummer AN-07382/22

Begrepp

Arkivbestånd och arkivsamling

Med begreppet arkiv avses både arkivinstitutioner, arkivlokaler, arkivbestånd och arkivsamlingar. Ett arkivbestånd växer fram som ett resultat av en arkivbildares verksamhet och ska begreppsmässigt skiljas från arkivsamling som är resultatet av en aktiv insamling i syfte att dokumentera eller synliggöra en viss del av samhället. Det som utmärker en samling är att den har brutits ut ur det arkiv den tillhört alternativt att det aldrig har tillhört ett arkiv. En arkivinstitution kan ha både arkivbestånd och arkivsamlingar i sina arkivlokaler. Objekt för att beskriva enskilda objekt/föremål i en samling.

Typordnad och objektsordnad förvaring

Typordnad förvaring utgår från handlingstypen (handlingens kategori), till exempel protokoll, avtal eller beslut. En del handlingar är dock svåra att sätta någon typ för eller det är mer naturligt att förvara dem utifrån vad de handlar om så kallad objektsordnad förvaring. Objekten kan vara fotografer/konstnärer, fastigheter, produkter, föremål, klienter, anställda, projekt eller ämnen. Ibland kan samlingarna vara en kombination typordnad och objektsordnad förvaring. Det kan röra sig om ritningar, fotografier, målningar, fanor, kartor och andra informationstyper som har en gemensam nämnare i att det behöver hanteras på objektsnivå.

Dataskydd

Dataskyddsförordningen gäller för behandling av personuppgifter. Ett av syftena med dataskyddsförordningen (GDPR) är att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.

Personuppgift

En personuppgift är information som direkt eller indirekt kan knytas till en fysisk person (som lever). Typiska personuppgifter är namn, adress och personnummer. Även bild- och ljudupptagningar kan räknas som personuppgifter även om inga namn nämns, om man kan se eller höra vem det rör.

- Vanliga personuppgifter är exempelvis namn, adressuppgifter och bild- och ljuduppgifter om en person
- Extra skyddsvärda personuppgifter är exempelvis personnummer, sekretessreglerade uppgifter och uppgifter som ligger nära den privata sfären
- Känsliga personuppgifter är exempelvis politiska åsikter, uppgifter om hälsa och genetiska uppgifter

Registrerad

Definitionen (av registrerad) är varje upplysning som avser en identifierad eller identifierbar fysisk person (som är i livet). Den registrerade är alltså den person vars personuppgifter vi behandlar. Den registrerade har ett antal rättigheter.

Personuppgiftsbehandling

Enligt definitionen i artikel 4 i GDPR är en behandling: *en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genomöverföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.*

Finalitetsprincipen

Finalitetsprincipen, eller principen om ändamålsbegränsning, innebär att om en tilltänkt behandling av redan insamlade personuppgifter inte omfattas av de ursprungliga ändamålen måste det göras en bedömning av om ändamålet med den senare behandlingen är förenligt med de ursprungliga ändamålen eller inte.

Arkivändamål av allmänt intresse

Behandling av personuppgifter för arkivändamål av allmänt intresse är en vidarebehandling (ytterligare behandling) av personuppgifter som ursprungligen samlats in för ett annat ändamål.

Arkivmyndigheter kan ha som sitt huvudsakliga ändamål att samla in personuppgifter för arkivändamål av allmänt intresse, till exempel när de tar emot arkiv.

Rättslig grund för behandling

Det finns sju rättsliga grunder i GDPR att stödja sig på för att få behandla personuppgifter. Myndigheter och andra inom offentlig verksamhet kan främst använda grunderna:

- Rättslig förpliktelse
- Uppgift av allmänt intresse
- Myndighetsutövning

Personuppgiftsansvarig

Personuppgiftsansvarig är den organisation som bestämmer för vilka ändamål personuppgifter ska behandlas och hur behandlingen ska gå till. När det handlar om myndigheter är det alltid nämnd eller styrelse som är personuppgiftsansvarig för de behandlingar som sker på förvaltningen. Det juridiska och yttersta ansvaret för att skapa följsamhet mot GDPR för Regionarkivets behandlingar ligger därmed hos Arkivnämnden. Den personuppgiftsansvariga ansvarar för att kunna visa att de grundläggande principerna om dataskydd efterlevs. Den som är ansvarig för behandlingen måste kunna visa hur och på vilket sätt man följer bestämmelserna i dataskyddsförordningen. Beslut måste motiveras och hur den personuppgiftsansvarige har tänkt och gjort måste dokumenteras.

Personuppgiftsbiträde

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Personuppgiftsbiträdet finns alltid utanför den personuppgiftsansvariges organisation och kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ. Biträdet uppträder osjälvständigt i förhållande till de registrerade, då biträdet endast får behandla personuppgifter enligt instruktion från den personuppgiftsansvarige.

Regionarkivets personuppgiftsbiträde KulturIT tillhandahåller den tekniska plattformen Primus samt den publika förmedlingsplattformen DigitaltMuseum.

Underbiträde

Amazon Web Services är en underleverantör till KulturIT. Amazon Web Services ("AWS") är en populär molntjänst som används av många företag, myndigheter och organisationer. Att använda AWS

innebär i många fall att personuppgifter behandlas och även överförs till tredjeländer som till exempel USA.

Dataskyddsombud

Enligt dataskyddsförordningen ska varje myndighet ha ett dataskyddsombud. Dataskyddsombudets huvuduppgifter är att säkerställa att organisationens behandling av personuppgifter sker i enlighet med dataskyddsförordningen. Dataskyddsombudet har inget eget ansvar för att organisationen följer dataskyddsförordningen. Det ansvaret ligger alltid hos den personuppgiftsansvariga nämnden.

Tredjelandsoverföring

Syftet med dataskyddsförordningen (GDPR) är att säkerställa rätten till privatliv och rätten till skydd för personuppgifter, samt möjliggöra personuppgifternas fria flöde inom EU/EES. För att dessa rättigheter inte ska urholkas krävs tydliga regler för överföring av personuppgifter till länder som inte ingår i EU/EES.

Med överföring till tredjeland menas i stort sett alla sammanhang då personuppgifter hamnar utanför EU eller blir tillgängliga utanför EU. Det räknas som en överföring även om mottagaren inte själv använder personuppgifterna i sin egna verksamhet utan bara lagrar dem åt andra i en molntjänst eller driftar och supportar ett system, exempelvis. Begreppet överföring kan även omfatta åtkomst till personuppgifterna från tredjeland, även om uppgifterna rent fysiskt lagras inom EU.

EU-domstolen har i Schrems II-målet konstaterat att överföringar som görs till USA innebär hög risk för intrång i den registrerades integritet. CLOUD Act innebär att amerikanska företag som tillhandahåller it-tjänster kan tvingas lämna ut sina kunders information till amerikanska myndigheter oavsett var informationen fysiskt är lagrad.

Tröskelanalys

När en personuppgiftsbehandling ska påbörjas eller förändras ska den personuppgiftsansvariga bedöma om behandlingen innebär en hög risk för de personer vars personuppgifter kommer behandlas, så kallade registrerade. Detta görs för att kunna avgöra om en konsekvensbedömning enligt GDPR ska göras. Denna bedömning kallas ibland för tröskelanalys.

Konsekvensbedömning

Av artikel 35.1 dataskyddsförordningen följer att den personuppgiftsansvariga ska utföra en konsekvensbedömning om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Enligt huvudregel ska den utföras innan en behandling påbörjas. Den personuppgiftsansvariga måste alltid göra en självständig bedömning av den planerade behandlingen för att avgöra om en konsekvensbedömning är nödvändig i det enskilda fallet.