Dataskyddsenheten

Göteborgs Stad

2023-02-14 Regionarkivet

# Dataskyddsombudets rekommendationer

Avseende tröskelanalys: Stöd för hantering av objekt och samlingar.

## När ska en konsekvensbedömning genomföras?

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.[1]

I artikel 35.3 anges vissa situationer när en konsekvensbedömning krävs. Därutöver ska tillsynsmyndigheten enligt artikel 35.4 upprätta och offentliggöra en förteckning över behandlingar som kräver en sådan bedömning. IMY (Integritetsskyddsmyndigheten) har, med ledning av riktlinjer från den Europeiska dataskyddsstyrelsen (EDPB) och de kriterier som gruppen tagit fram, antagit en förteckning över när en konsekvensbedömning ska göras.

### Behöver en konsekvensbedömning genomföras avseende behandlingen Stöd för hantering av objekt och samlingar?

Innan dataskyddsombudet går in på bedömningen av om en konsekvensbedömning behöver göras vill dataskyddsombudet lämna några generella synpunkter gällande ansatsen till tröskelanalysen.

GDPR säger inte något särskilt om det faktum att de personuppgifter som ni tar över sedan tidigare har organiserats på ett visst sätt; om de har organiserats i en ”samling”, utifrån ”objekt”, ”typ” eller utifrån hur den administrativa verkligheten har sett ut hos den arkivbildande verksamheten. Fokus enligt GDPR ligger i stället på *personuppgifterna* och de sammanhängande *personuppgiftsbehandlingarna.* Dataskyddsombudet bedömer därför att det troligen saknar betydelse för bedömningen av personuppgiftsbehandlingen om ni till exempel tar över och lagrar en samling, respektive tar över och lagrar ett ”vanligt” arkivbestånd som är organiserat utifrån den administrativa verksamheten. Bedömningen blir troligen den samma i båda fall. Det centrala när ni tar över personuppgifter är med andra ord inte den arkivmässiga organiseringen av personuppgifterna utan i stället vad det rör sig om för uppgifter och om personuppgiftsbehandlingen i sig uppfyller kraven enligt GDPR. Därmed inte sagt att organiseringen av personuppgifterna aldrig har betydelse (se mer i resonemanget vid punkten ”Upprättandet av egna samlingar”).

[1] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/forteckning-over-nar-en-konsekvensbedomning-ska-goras/

**Övertagandet och lagringen av arkiv och samlingar**

Utifrån den beskrivning som förvaltningen har lämnat framgår det att övertagandet av arkiv och samlingar i princip kan innefatta alla tänkbara kategorier av personuppgifter, även t.ex. känsliga personuppgifter. Om man ser till alla arkiv och samlingar som förvaltningen överhuvudtaget tar emot är det fråga om personuppgiftsbehandling i stor omfattning av särskilda kategorier av personuppgifter (känsliga personuppgifter) vilket innebär att det är en högriskbehandling som behöver utredas genom en konsekvensbedömning.[2] Sannolikt kommer det även förekomma personuppgifter om personer som tillhör sårbara kategorier av registrerade vilket är ytterligare en faktor som talar för behovet av konsekvensbedömning.[3]

Även om en behandling skulle visa sig ha stöd i en laglig grund och det finns ett berättigat ändamål så räcker inte detta, utan det finns ytterligare krav enligt GDPR. Ett exempel på ett sådant centralt krav enligt GDPR är att man ska vidta lämpliga skyddsåtgärder i relation till de risker som finns med behandlingen.[4] GDPR ställer även krav på att man ska kunna visa genom dokumentation att man följer GDPR. Behovet av konsekvensbedömningar ska förstås bl.a. mot bakgrund av dessa krav.

Som en del av konsekvensbedömningen behöver förvaltningen beskriva vilka informationsbärare som används d.v.s. vilka IT-system, lagringsytor m.m. som personuppgifterna behandlas i. Förvaltningen har inte klargjort för dataskyddsombudet om Primus och DigitaltMuseum bara hänger samman med tillgängliggörandet internt och externt eller om dessa IT-lösningar också används initialt i samband med att personuppgifterna tas över från någon annan. Detta behöver klargöras i synnerhet med tanke på att det förekommer känsliga personuppgifter i det initiala skedet. Kommer personuppgifterna från samlingarna bara behandlas i Primus och DigitaltMuseum eller även i andra informationsbärare? Även andra informationsbärare som aktualiseras i de aktuella personuppgifternas totala livscykel hos förvaltningen behöver beskrivas.

**Upprättandet av egna samlingar**

Förvaltningen har beskrivit att ändamålet med att upprätta samlingar är att underlätta för både Regionarkivet och allmänheten att söka fram och få tillgång till information.

Dataskyddsombudet bedömer att upprättandet av egna samlingar är en egen behandling som behöver utredas och motiveras särskilt. Förvaltningen behöver titta särskilt på hur upprättandet av egna samlingar förhåller sig till finalitetsprincipen/principen om ändamålsbegränsning och säkerställa att ni håller er inom ramarna för vad som är tillåtet. Eftersom man för samman personuppgifter från olika personuppgiftsbehandlingar behöver man ”tänka till” så att personuppgiftsbehandlingen inte blir något som avviker från vad den registrerade rimligen kan ha förväntat sig.[5] Här kommer ett exempel för att

[2] Artikel 35.3.b i GDPR.
[3] Integritetsskyddsmyndigheten (tidigare Datainspektionen). Förteckning enligt artikel 35.4 i Dataskyddsförordningen (se punkten 7). Tillgänglig: Förteckning enligt artikel 35.4 i Dataskyddsförordningen (imy.se).
[4] Se bl.a. artikel 24.1 och artikel 32 i GDPR.
[5] Integritetsskyddsmyndigheten (tidigare Datainspektionen). Förteckning enligt artikel 35.4 i Dataskyddsförordningen (se punkten 6). Tillgänglig: Förteckning enligt artikel 35.4 i

illustrera. En registrerad som har varit elev på en kommunal grundskola i Göteborgs stad kan rimligen förvänta sig att personuppgifter om hen kommer att förekomma i ett arkiv eftersom det följer av offentlighetsprincipen att allmänna handlingar ska bevaras. Det är dock inte lika självklart att den registrerade eleven rimligen kan förvänta sig att personuppgifterna kommer att förekomma i en samling som samlar fotografier av alla möjliga slag och som kommer från diverse olika sammanhang som publicerats öppet på webben och att man med enkla sökord kan få fram bilder på eleven där.

Förvaltningen rekommenderas att utreda särskilt om bedömningen av finalitetsprincipen/ändamålsbegränsning ser olika ut beroende på vem ni har tagit över personuppgifterna ifrån. Hur ser ramarna ut för vidarebehandling vad gäller personuppgifter som ni har tagit över från en förvaltning eller ett bolag som ni är arkivmyndighet för? Hur ser ramarna för vidarebehandling ut vad gäller personuppgifter som ni har tagit emot från en privat förening? Etc.

**Tillgängliggörandet**

Utifrån den beskrivning som förvaltningen har lämnat framgår ytterligare behandlingar som är att tillgängliggöra de övertagna arkiven och samlingarna internt och externt.

Eftersom det framkommit att Amazon webservices är en underleverantör till KulturIT som är personuppgiftsbiträde (KutlurIT tillhandahåller Primus och DigitaltMuseum) är detta en omständighet som behöver utredas närmare utifrån reglerna kring tredjelandsöverföringar.

Förvaltningen ska bara anlita biträden som bedöms kunna ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven enligt GDPR och säkerställer att den registrerades rättigheter skyddas.[6] Detta följer av den så kallade omsorgsplikten som personuppgiftsansvarig har enligt GDPR.

Amazon Webservices (AWS) omfattas av amerikansk säkerhetslagstiftning och även om uppgifterna i praktiken lagras inom EU/EES så finns det risk för tredjelandsöverföring bara genom det faktum att företaget omfattas av amerikansk lagstiftning och kan åläggas att lämna ut uppgifter till amerikanska säkerhetsorgan. USA säkerställer inte samma skydd för personuppgifter som det skydd som gäller inom EU/EES och det finns brister vad gäller möjligheten att få sin sak prövad i domstol.

Förvaltningen behöver vidta åtgärder för att säkerställa att personuppgifter inte olagligen överförs till tredjeland. Om förvaltningen lagligen ska kunna använda tjänsten behöver förvaltningen säkerställa att tillräckliga skyddsåtgärder vidtas för att uppnå ett effektivt skydd för personuppgifterna. Enligt Europeiska dataskyddsstyrelsen (EDPB) rekommendationer om kompletterande åtgärder i samband med tredjelandsöverföringar ställs det höga krav på att ni som personuppgiftsansvarig ska ha betydande rådighet över personuppgifterna.[7]

---

Dataskyddsförordningen (imy.se). Artikel 29-arbetsgruppen. Riktlinjer om öppenhet enligt förordning (EU)2016/679. Tillgänglig: xxxx/17/EN (imy.se).

[6] Artikel 28.1 i GDPR.

[7] Europeiska dataskyddsstyrelsen (European data protection board). Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med

Förvaltningen har förklarat att KulturIT använder sig av kryptering genom AWS Key Management Service. Eftersom krypteringstjänsen tillhandahålls av AWS har förvaltningen inte full kontroll över krypteringsnyckeln. Även om förvaltningen skulle välja en egen krypteringsnyckel så hanteras den momentant i klartext inuti AWS vid varje krypteringstillfälle.[8] Det finns således begränsningar i förvaltningens rådighet över personuppgifterna.

Utifrån den information som dataskyddsombudet har fått ta del av är dataskyddsombudets bedömning att förvaltningen inte har visat på ett tillfredsställande sätt att man följer reglerna om tredjelandsöverföringar i kapitel 5 i GDPR och förvaltningen kan anses brista i sin omsorgsplikt enlig artikel 28.1 i GDPR. Förvaltningen behöver utreda frågan närmare och säkerställa en tillräcklig skyddsnivå innan man går vidare med eventuell personuppgiftsbehandling i tjänsten.

Förvaltningen har förklarat att man aldrig publicerar ”bilder eller handlingar som visar människor i kränkande eller utsatta lägen utan endast vardagliga situationer i kommun, landsting/region, föreningsliv eller stadsmiljö/landsbygd. Vi överväger noga varje publicering ur ett etiskt perspektiv genom avstämning mellan kollegor utifrån syftet och nyttan.”. Vidare har man förklarat att bara för att man tar emot arkiv och samlingar som kan innehålla extra skyddsvärda och känsliga personuppgifter så innebär inte detta att man kommer upprätta egna samlingar eller tillgängliggöra befintliga samlingar som innehåller extra skyddsvärda eller känsliga personuppgifter. Dataskyddsombudet tycker att detta låter klokt, men även om just känsligare personuppgifter undantas från webbpublicering så uppfattar dataskyddsombudet det som att personuppgifter kommer publiceras på webben och att det därför kommer vara fråga om personuppgiftsbehandling. Webbpublicering av personuppgifter från arkiv är enligt dataskyddsombudets uppfattning en behandling som medför ökade risker (detta gäller alldeles oavsett om det är fråga om tredjelandsöverföring eller inte). Frågan om webbpublicering av personuppgifter behöver därför adresseras.

Dataskyddsombudet är medveten om att det finns en utveckling och politisk vilja i rörelse mot ökad digitalisering av arkiv och målsättningar om att arkiven ska bli mer tillgängliga.[9] I den statliga offentliga utredningen om en ny arkivlag SOU 2019:58 föreslås en särskild paragraf om att arkivmyndigheterna aktivt ska verka för att tillgängliggöra och främja användningen av arkiven.[10] Utredningen som är från 2020 har inte gått vidare till proposition och någon ny arkivlag har inte klubbats igenom. I dagsläget finns alltså inte någon motsvarande paragraf i arkivlagen som i klartext innebär ett utvidgat uppdrag att aktivt tillgängliggöra och främja användningen av arkiven (men offentlighetsprincipen gäller såklart fortfarande). Så länge det inte är reglerat i svensk rätt

EU-nivån för skydd av personuppgifter. Tillgänglig: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_sv.pdf.

[8] Jämför E-sams molngrupps analys i promemoria”Kompletterande svar angående Zoom X” där kryptering och AWS diskuteras, s. 3.

[9] Se t.ex. Härifrån till evigheten. En långsiktig arkivpolitik för förvaltning och kulturarv. SOU 2019:58. Tillgänglig: Härifrån till evigheten. En långsiktig arkivpolitik för förvaltning och kulturarv, SOU 2019:58 (regeringen.se).

[10] Härifrån till evigheten. En långsiktig arkivpolitik för förvaltning och kulturarv. SOU 2019:58. Se s. 640 (ny 7§). Tillgänglig: Härifrån till evigheten. En långsiktig arkivpolitik för förvaltning och kulturarv, SOU 2019:58 (regeringen.se).

att arkivmyndigheterna har ett sådant utvidgat uppdrag anser dataskyddsombudet att förvaltningen behöver iaktta försiktighet i avvägningen mellan tillgänglighet och personlig integritet. Förvaltningen behöver motivera och dokumentera de ställningstaganden som man gör.

European Archives Group[11] som är en av EU-kommissionens officiella expertgrupper har i en vägledning om dataskydd gällande arkiv berört frågan kring behovet av konsekvensbedömningar. I denna vägledning anges att det kan vara nödvändigt med en konsekvensbedömning när man har för avsikt att digitalisera eller skapa digitala sökhjälpmedel för personuppgifter för användning på plats eller online.[12] Även mot bakgrund av detta rekommenderar dataskyddsombudet att förvaltningen genomför en konsekvensbedömning.

### Sammanfattande rekommendation

- Genomför en konsekvensbedömning.
- Klargör användningen av olika informationstillgångar.
- Utred hur upprättandet av egna samlingar förhåller sig till finalitetsprincipen/principen om ändamålsbegränsning och säkerställ att ni håller er inom ramarna för vad som är tillåtet.
- Utred och säkerställ att personuppgifterna omfattas av effektivt skydd och att de inte olagligen överförs till tredjeland.
- Utred webbpubliceringen särskilt och iaktta försiktighet i avvägningen mellan tillgänglighet och personlig integritet.
- Motivera och dokumentera era ställningstaganden.

Astrid Helmstad
Dataskyddsombud

[11] European Commission, European archives group. Tillgänglig: https://commission.europa.eu/about-european-commission/service-standards-and-principles/transparency/access-documents/information-and-document-management/archival-policy/european-archives-group_en.
[12] European archives group. Guidance on data protection on the implementation of the general data protection regulation in the archive sector, s. 27. Tillgänglig: eag_draft_guidelines_1_11_0.pdf (europa.eu).