Stadsarkivet
Ledningsstöd

Handläggare
Louise Högberg

Till
Kulturnämnden
2021-02-16

Årsrapport över Stadsarkivets arbete med skydd och behandling av personuppgifter 2020

Stadsarkivets förslag till beslut

Stadsarkivet föreslår att kulturnämnden beslutar:

1. Nämnden godkänner dataskyddsombudets årsrapport över kulturförvaltningens arbete med skydd och behandling av personuppgifter 2020.

Lennart Ploom
Stadsarkivarie

Sammanfattning

Denna rapport är sammanställd av dataskyddsombudet i syfte att ge personuppgiftsansvarig (PUA), i Stadsarkivets fall är det kulturnämnden, en redogörelse för hur arbetet med persondataskydd har genomförts på Stadsarkivet under 2020.

Dataskyddsombudets bedömning är att arbetet har bedrivits på ett mycket tillfredställande sätt utifrån dataskyddsförordningen. Medvetenheten och kunskapen om dataskyddsförordningen och den efterlevnad som krävs kopplat till denna på Stadsarkivet är hög. Genom löpande information, stöd, utbildningsinsatser och egenkontroll har förståelse och kunskap i verksamheten höjts ytterligare under det gångna året.

Utifrån genomlysning av efterlevnaden i verksamheten och egenkontroller kan ett antal rekommendationer till förbättringsåtgärder redovisas. Dessa återfinns under rubriken ”DSO ger råd och rekommendationer till PUA” i denna rapport.

Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnden behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett Dataskyddsombud (DSO). DSO:n har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnden att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar samt för att nämnden ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnden ska kunna visa att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna dokumenteringsskyldighet. Årsrapporten är även ett medel för nämndens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Ärendets beredning

Ärendet har beretts av Stadsarkivets dataskyddsombud Louise Högberg. De erfarenheter som löpande har samlats in av dataskyddsombudet under året ligger till grund för det utlåtande som lämnats.

Stadsarkivets dataskyddsarbete

Personuppgiftsregister

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför i klartext av dataskyddsförordningen alla personuppgifter som behandlas i verksamheten ska dokumenteras i ett personuppgiftsregister.

När registerförteckningen är upprättad skapar den en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Registerförteckningen är därför dataskyddsarbetets centrala utgångspunkt och bas samt säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling.

Inför införandet av dataskyddsförordningen i maj 2018 genomfördes ett grundligt arbete med att registrera verksamhetens personuppgiftsbehandlingar i förteckningen. Därefter har registret löpande uppdaterats när behov kommit till DSO:s kännedom.

Registret omfattar idag 140 stycken behandlingar. En del av dessa behandlingar sammanfattar flera enskilda behandlingar t ex ”Behandling av personuppgifter för att kunna hantera offerter och uppdragsöverenskommelser/avtal”

Registerförteckningen är fullständig utifrån vad DSO känner till, men verksamheten förändras löpande och behandlingarna med detta. I och med den nya organisationen from 1 september 2019 och att pandemin har förändrat våra arbetssätt, behöver dataskyddsarbetet under 2021 fokusera till stor del på att gå igenom och uppdatera registerförteckningen.

Styrdokument

Området syftar till att PUA genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna, när de hanterar personuppgifter. Att styrdokument

finns nedtecknade, beslutade och kommunicerade medför att medarbetaren får dataskyddsinformation och kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt. En röd tråd i dataskyddsförordningen är att viktiga arbetssätt och rutiner ska vara dokumenterade. Detta följer bland annat av kravet på att den personuppgiftsansvarige måste kunna *visa* att dataskyddsförordningens principer för behandling av personuppgifter efterlevs.

Stadsarkivet har samtliga styrande dokument på plats som dataskyddsförordningen föreskriver och som Stadsledningskontoret (SLK) uppmanar till.

I de flesta fall finns centrala dokument och mallar framtagna av SLK, dessa har anpassats till Stadsarkivets verksamhet. Våra styrdokument och mallar hålls uppdaterade av DSO finns samlade och tillgänglig för Stadsarkivets medarbetare i en gemensam katalog.

Under 2020 har Stadsarkivets dataskyddsorganisation fastställt och samlats i ett dokument beslutat av Förvaltningschefen. Detta dokument har publicerats på intranätet men bör göras ytterligare känt i organisationen, speciellt vad det innebär för de olika nyckelrollerna som t ex informationsansvarig (avdelningschef).

Informationsklassning

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd så ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av Sveriges Kommuner och Regioners (SKR) verktyg KLASSA. Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att PUA ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

Ansvaret för att informationsklassning genomförs ligger på den som är informationsägare. Genom det beslutade styrdokumentet för Stadsarkivets dataskyddsorganisation framgår vilka som är informationsägare i Stadsarkivet. Som nämnts under rubriken ovan behöver innebörden av informationsägaransvaret förankras hos dem som har rollen.

Enbart sådan informationsklassning som avser behandling eller system som omfattar personuppgifter är av intresse för DSO:s arbete och årsrapportering. Verksamheten har dock mycket att vinna på, att när man klassar sin information som innehåller personuppgifter, även klassa samtlig information inom området t ex personal. Eftersom informationsklassning är ett arbete som görs inom ramen för informationssäkerhetsarbetet, bör DSO samråda och planera uppföljningen tillsammans med informationssäkerhetssamordnare. Enligt stadens metodik klassas personuppgifter och övrig information i samma workshop, och slutsatserna kring klassningen dokumenteras i samma protokoll. För att detta ska var möjligt behöver ett samarbete mellan DSO och informationssäkerhetsansvarig etableras.

eDok infördes precis innan årsskiftet på Stadsarkivet och en klassning hanns inte med under 2020. Klassningen av information i systemstöd eDok är prioriterad och görs i januari 2021.

Under året har klassning av området ”personal” genomförts av DSO och personalansvarig på Stadsarkivet.

Vid den revision som stadens revisionskontor genomförde av dataskyddsarbete på Stadsarkivet juni 2019 anmärktes det på att systemstöden eDok och e-arkiv Stockholm inte hade eller behövde uppdatera sin klassning. Verksamheterna planerade in klassning under första delen av 2020 men klassningarna är ännu ej genomförda, vilket DSO påtalat för informationsägarna.

Stadsarkivets informationsklassning av sina personuppgifter behöver arbetas vidare med under året. Det är viktigt att systemstöden eDok och e-arkivet verkligen blir klassade under 2021. DSO rekommenderar även att området ekonomi klassas och att man ser över klassningen av informationen i eDok efter att halvår och återigen vid årets slut för att försäkra sig om att personuppgifter i systemet är klassade.

Flertalet av de klassningar som gjorts börjar bli ett par år gamla och behöver ses över. Vissa verksamhetsområden är inte kompletta vad gäller klassning. DSO föreslår att en inventering om vilka klassningar som behöver göras och var klassning saknas görs i samband med uppdateringen av personuppgiftsregistret.

Konsekvensbedömningar

Konsekvensbedömningen hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas i projekt eller linjeverksamhet. En konsekvensbedömning har till syfte att identifiera och dokumentera risker kopplade till en viss behandling, samt att bedöma sannolikheten och konsekvensen om riskscenariot skulle inträffa. Baserat på bedömningen kan/ska riskförebyggande åtgärder vidtas.

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning vara ett viktigt verktyg för verksamhetens dataskyddsarbete. Kravet på konsekvensbedömning är dessutom ett uttryckligt krav enligt dataskyddsförordningen och ska utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”.

DSO har under året informerat Stadsarkivet medarbetare i allmänhet och informationsägare och GDPR-samordnare i synnerhet om vikten av att konsekvensbedömningar görs. Mallar och instruktioner finns lätt tillgängliga i gemensam katalog och DSO finns som stöd vid genomförande. Trots detta har endast en konsekvensbedömning genomförts under 2020 på initiativ av verksamheten.

Bristerna på detta område är således stora och DSO rekommenderar att omtag görs på informationsinsats riktad till informationsägare och GDPR-samordnare. DSO föreslår vidare att en av DSO:s interna granskningar ägnas åt att identifiera prioriterade befintliga behandlingar som det behöver göras konsekvensanalys för. Detta arbete kan med fördel göras parallellt med uppdateringen av personuppgiftsregistret.

Individens rättigheter

Registrerade personer har enligt dataskyddsförordningen ett antal rättigheter som på olika sätt ska garantera att den registrerade personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att personuppgiftsansvarig tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, som exempelvis att lämna ut ett så kallat registerutdrag eller begära rättning av vissa uppgifter.

Verksamheten har enligt dataskyddsförordningen en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran.

Stadsarkivet har under året fått en begäran om registerutdrag. Denna begäran besvarades av DSO inom loppet av tre dagar. Denna begäran är den första som inkommit till förvaltningen sedan GDPR började gälla, alltså är detta inte något som är vanligt förekommande. Rutin finns för att hantera begäran och vi kan säkerställa att vi kan bevara förfrågan inom loppet av trettio dagar.

DSO lämnar inga vidare rekommendationer till åtgärder inom detta område.

Personuppgiftsincidenter

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

Enligt dataskyddsförordningen ska alla personuppgiftsincidenter dokumenteras, det vill säga även i de fall då incidenten inte ska rapporteras till Integritetsskyddsmyndigheten (IMY, tidigare Datainspektionen). Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden och bristande dokumentering är sanktionsgrundande.

Under året har ett tiotal incidenter kommit till dataskyddsombudets kännedom och noterats i personuppgiftsincidentregistret. Ingen av dessa har anmälts till IMY då ingen av incidenterna bidragit till större skada rörande personuppgifter.

Antalet incidenter som kommit till DSO:s kännedom är relativt få och troligen finns här ett antal incidenter som ej rapporterats in. DSO rekommenderar fortsatt kommunikation till medarbetarna om vikten att anmäla och dokumentera dessa i Stadsarkivets incidentregister för personuppgifter.

Genomförda granskningar under året

En av dataskyddsombudets viktigaste uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En central del av det arbetet är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder.

Under året utfördes, enligt plan, tre stycken granskningar av DSO. Granskningarna omfattade hela det område som GDPR omfattar som t ex klassning, incidenter, behandlingar i personuppgiftsregister och behörighet:

1. Personuppgifter inom personalområdet
2. Systemstöd eDok
3. E-arkiv Stockholm

Med anledning av en ökad frekvens i staden av sk it- och phishingattacker gjordes under juni en extra granskning av DSO på detta område. Syftet var att få kännedom om och i vilken utsträckning detta förekommer på Stadsarkivet samt höja medvetandet. Granskningen visade att en hel del bluffmail förekommer, men att dessa anmäls enligt fastställda rutiner. I det fall ett mer allvarligt it-angrepp hade inträffat vidtogs omgående åtgärder för att försvåra att detta sker igen.

Ytterligare en extra granskning gjordes av DSO under året mad anledning av det uppmärksammade Schrems II målet där avtalet Privacy Shield ogiltigförklarades. Ogiltigförklarandet innebär att Privacy Shield inte ger ett tillräckligt skydd för de personuppgifter som förs över till USA – en sådan överföring bryter nu mot dataskyddsförordningen.

För Stadsarkivets del får detta främst konsekvenser i vårt användande av vissa sociala media som t ex Facebook. Ansvariga på Stadsarkivet för vår kommunikation och publika arbete jobbar med frågan tillsammans med andra i stadens som är i samma situation.

Förvaltningen av e-arkiv Stockholm har svarat att deras leverantör inte har några kontakter med tredjepartsländer.

Inom eDok har man kartlagt eDoks leverantörer och tjänster samt skickat formella förfrågningar till de två av leverantörerna som inte täcks av stadens avtal. Efter en genomgång av deras inkomna svar så bekräftas att inga överföringar sker till tredjepartland.

Övrigt att rapportera

Kompetensutveckling hos medarbetare

Under året har det inte hållits någon större kompetensutvecklingsinsats inom området. Detta beror på att vi endast haft ett fåtal nyanställda, hemarbete p g a pandemin och att behovet inte har lyfts. Istället har DSO arbetat med att ge stöd och fördjupad kompetensöverföring vid speciella situationen och när behov uppstått. Två mindre utbildningstillfällen har hållits dels med ledningsgruppen och dels med GDPR-samordnarna.

Stadsarkivets medarbetare har uppmanats via utskick per mail att genomföra de e-utbildningar som staden tagit fram inom informationssäkerhetsområdet. Stor del av Stadsarkivets medarbetare har genomför e-utbildningarna.

Dataskyddsombudets arbete

Dataskyddsombudet har medverkat i stadens nätverk för dataskyddsombud. Nätverket är ett bra stöd för att utbyta erfarenheter samt få råd i dataskyddsfrågor.

Stadsarkivets DSO har under hösten ingått i en operativ referensgrupp med syftet att stödja och kvalitetssäkra SLKs arbete med att ta fram och utveckla mallar och instruktioner för dataskyddsarbetet i Stockholms stad.

Dataskyddsombudet har deltagit i det arbete som ämnat till att hitta nya samarbetsområden för Stadsarkivet och Kulturförvaltningen. Dataskyddsarbetet är en av dessa och föreslagna åtgärder för samarbetet finns dokumenterat i en separat rapport.

Extern granskning

I juni 2019 genomförde stadens revisionskontor en revision av Stadsarkivets arbete med skydd och behandling av personuppgifter. Granskningen fann att vi har rutiner på plats och god ordning. Revisorn anmärkte på att de två systemstöd som vi förvaltar behöver informationsklassas, respektive genomgå en uppdaterad klassning. En uppföljning av granskningen gjordes av revisionskontoret i november 2020. DSO rapporterade då att informationsklassningarna av eDok och e-arkivet ännu inte gjorts av respektive verksamhet.

Jämställdhetsanalys

Dataskyddsarbetet berör alla personer som kommer i kontakt med Stadsarkivet oavsett kön, men är neutralt ur ett jämställdhetsperspektiv.

Barnchecklista

Barn påverkas i viss mån indirekt av dataskyddsförordningen, men påverkan är neutral ur ett jämställdhetsperspektiv. Dataskyddsförordningen reglerar om och vilka uppgifter om barn som kan få behandlas. Dataskyddsförordningens artiklar 6.1f och artikel 8 berör särskilt behandling av barns personuppgifter.

Arbetet med skydd av personuppgifter främjar barns säkerhet och trygghet såtillvida att skyddet för barns personuppgifter stärks. På sikt har Stadsarkivets arbete med skydd av personuppgifter därför positiva konsekvenser för barn.

Gällande övriga frågor i stadens barnchecklista är ärendet neutralt.

DSO ger råd och rekommendationer till PUA

Dataskyddsombudets uppfattning är att Stadsarkivets medarbetare har god kännedom om dataskyddsarbetet och att man är ansvarstagande gentemot att följa dataskyddsförordningen på bästa sätt. Det är ett tacksamt och rolig uppdrag att vara DSO på Stadsarkivet.

Dataskyddsombudet planerar göra följande granskningar för 2021:

- personuppgifter inom området ekonomi
- identifiera prioriterade befintliga behandlingar som behöver göras konsekvensanalys av
- att personuppgiftsregistret är uppdaterat och samtliga behandlingar har en ägare och att ägarskapet är känt

Dataskyddsombudet rekommenderar följande åtgärder för 2021:

Åtgärd	Ansvarig
Uppdatering av personuppgiftsregister. En notering görs också för respektive behandling om den är informationsklassad. Arbetet görs med stöd av DSO.	Respektive informationsägare (tillika avdelningschef) i samarbete med GDPR-samordnare. Rapportera slutförd status till DSO.

Förankring av roller och ansvar inom dataskyddsområdet utifrån Stadsarkivets nyligen beslutade datasskyddsorganisation.	DSO
Etablera samarbete mellan dataskyddsombud och informationssäkerhetsansvarig.	DSO och Gabriel Marawgeh (chef för avdelningen där informations-säkerhetsansvaret finns).
Fortsatt kommunikation till medarbetarna om vikten att anmäla och dokumentera dessa i Stadsarkivets incidentregister för personuppgifter.	DSO i samarbete med informationsägare (tillika avdelningschef)
Informationsklassning av e-arkiv Stockholm. Kvarstår från 2020.	Informationsägare Jonas Egardt
Uppdatera informationsklassning av systemstöd eDok. Kvarstår från 2020.	Informationsägare Kane Neman
Få in obligatorisk e-utbildning i dataskydd och informationssäkerhet i introduktion till nyanställda Kvarstår från 2020.	HR-chef Rapportera slutförd status till DSO och informations-säkerhetsansvarig

Slutligen vill DSO tacka för nämndens förtroende att få vara Stadsarkivets dataskyddsombud under tre år. Louise Högberg lämnar sin anställning sista februari 2021 och ett nytt dataskyddsombud behöver därmed utses för förvaltningen.

Stadsarkivets synpunkter och förslag

Stadsarkivet föreslår att kulturnämnden beslutar att godkänna denna årsrapport över förvaltningen arbete med behandling och skydd av personuppgifter 2020.