Handläggare
Eija Bodbacka
Telefon: 08-508 31 218

Till
Kulturnämnden
2021-02-16

Årsrapport över kulturförvaltningens arbete med skydd och behandling av personuppgifter 2020

Kulturförvaltningens förslag till beslut

Kulturförvaltningen föreslår att kulturnämnden beslutar:

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

Robert Olsson
Kulturdirektör

Lena Nilsson
Administrativ chef

Sammanfattning

Årsrapporten är sammanställd av dataskyddsombudet i syfte att ge personuppgiftsansvarig (PUA), i kulturförvaltningens fall är det kulturnämnden, en redogörelse för hur arbetet med integritets- och dataskydd har genomförts på kulturförvaltningen under 2020.

Dataskyddsombudets uppfattning är att kulturförvaltningens medarbetare har kännedom om dataskyddsförordningen och att man är ansvarstagande för att följa dataskyddsförordningen på bästa sätt.

Medvetenheten och kunskapen om dataskyddsförordningen och den efterlevnad som krävs kopplat till denna behöver dock höjas genom löpande information, stöd, utbildningsinsatser och egenkontroll.

Struktur och arbetssätt i dataskyddsarbete med tydliga roller och ansvar behöver fastställas och beslutas för att förbättra och möjliggöra nämndens uppföljning och styrning av verksamhetetens systematiska integritets- och dataskyddsarbete.

Dataskyddsombudets bedömning är att dataskyddsarbetet har i sin helhet bedrivits på ett mindre tillfredsställande sätt utifrån dataskyddsförordningen.

Dataskyddsombud ger råd och rekommendationer till personuppgiftsansvarig i slutet av denna rapport under rubriken ”DSO ger råd och rekommendationer till PUA”.

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 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 kulturförvaltningens dataskyddsombud Eija Bodbacka. De erfarenheter som löpande har samlats in av dataskyddsombudet under det gångna året ligger till grund för det utlåtande som lämnats.

Kulturförvaltningens dataskyddsarbete

Registerförteckning

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför i klartext av dataskyddsförordningen att 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 inventera och registrera verksamhetens personuppgifter i förteckningen.

Det är den del av verksamheten som äger informationen i fråga som ansvarar för registerföring av personuppgiftsbehandlingar.

Under det gångna året har registret anpassats så att varje verksamhetsavdelning har varsin del av registerförteckningen.

Kulturförvaltningen har fortsatt att använda Excel för registrering av personuppgiftsbehandlingar. Arbetet att uppdatera och hålla dessa Excel-ark aktuella har varit svårhanterligt, inte minst på grund av otydligt ansvar och saknaden av en gemensam lagringsyta.

Vid verksamhetsårets utgång har 256 behandlingar registerförts.

Registerförteckningar bedöms inte vara fullständiga och uppdaterade. I slutet av det gånga året startade arbetet med att flytta samtliga personuppgiftsbehandlingar från Excel till stadens verktyg Draftit.

DSO rekommenderar att ett stort fokus i dataskyddsarbetet ska läggas på att få registerförteckningar fullständiga och att ta fram lämpliga rutiner för registerföring.

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.

DSO:s bedömning är att innehållet i de existerande dokument håller lämplig kvalitet och att de flesta styrande dokument som dataskyddsförordningen föreskriver finns på plats. Dock finns det anledning att se över att en lämplig uppsättning av grundläggande styrdokument och rutinbeskrivningar uppnår sitt syfte, dvs. att det ska vara ”lätt att göra rätt” för de medarbetare som kan ha behov av stöd från dokumenten. De ska också vara tillgängliga.

Samtliga styrdokument ska även ha en ägare utpekad så att uppdateringar kan bli gjorda vid behov. Det är viktigt att styrdokumenten är pedagogiska och ger ett tillräckligt stöd.

Under det gånga året har det tagits fram ett förslag till organisation för dataskyddsarbete och som också beskriver olika roller och ansvar inom integritet och dataskydd, speciellt vad det innebär för de olika nyckelrollerna som t.ex. avdelningschefer. Detta dokument är ännu inte fastställt eller beslutat.

DSO rekommenderar att översyn av samtliga styrdokument och mallar genomförs för att minimera risk för misstag eller fel som kan uppstå vid saknaden av dokumentation. Speciellt processen med samtycke behöver ses över.

Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

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 KLASSA, ett verktyg som Sveriges kommuner och regioner (SKR) tillhandahåller. KLASSA ger förslag på lämpliga tekniska och organisatoriska skyddsåtgärder i relation till informationens skyddsvärde. 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 säkerställa att informationen skyddas på avsett sätt och att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. På kulturförvaltningen ligger det ansvaret på avdelningschefen för sin verksamhet.

Enbart sådan informationsklassning som avser behandling eller system som omfattar personuppgifter är av intresse för DSO:s arbete och årsrapportering.

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.

Vid den revision som stadens revisionskontor genomförde av dataskyddsarbete på kulturförvaltningen år 2019 visade brister i informationsklassning av informationstillgångar.

Flertalet av de informationsklassningar som gjorts på kulturförvaltningen börjar bli gamla och behöver ses över.

DSO rekommenderar att en inventering om vilka klassningar som har utförts och var klassning saknas görs i samband med uppdateringen av registerförteckningen.

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”.

Mallar och instruktioner för konsekvensbedömning finns lätt tillgängliga på stadens intranät och DSO finns som stöd vid genomförande.

Under det gånga året har en (1) konsekvensbedömning genomförts på initiativ från verksamheten. I samband med detta uppdagades brist i delegationsordningen. Denna brist kommer att åtgärdas nästa gång delegationsordningen uppdateras.

DSO rekommenderar att dataskyddsarbetet fokuserar på att identifiera prioriterade befintliga behandlingar som behöver göras konsekvensbedömningar av. Detta arbete kan med fördel göras parallellt med uppdateringen av registerförteckningen.

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 att rätta vissa uppgifter. Verksamheten har enligt dataskyddsförordningen en skyldighet att vidta åtgärder inom 30 dagar efter att ha mottagit begäran.

Kulturförvaltningens registratur har under det gångna året fått fyra (4) begäran om registerutdrag. Samtliga begäranden hanterades av verksamheten inom 30 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 Datainspektion. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden och bristande dokumentering är sanktionsgrundande.

Under det gångna året har endast fyra (4) personuppgiftsincidenter inträffat och rapporterats i IA, stadens verktyg för incidenthantering. Samtliga incidenter har varit harmlösa och inte ansetts behöva rapporteras till IMY då ingen av incidenterna bidragit till större skada rörande personuppgifter.

Antalet personuppgiftsincidenter som kommit till DSO:s kännedom är väldigt få och troligen finns det ett antal incidenter som inte har rapporterats in.

DSO rekommenderar fortsatt information/kommunikation till medarbetarna om vikten att anmäla och dokumentera personuppgiftsincidenter i incidentrapporteringsverktyget IA.

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.

EU-domstolen meddelade i juli 2020 en dom i det så kallade Schrems II-målet om skydd av personuppgifter. Domen betyder bland annat att överföringsmekanismen Privacy Shield inte ger ett tillräckligt skydd vid överföring av personuppgifter till USA. Överföring sker vid användande av molntjänster, som Office365, sociala medier, som Facebook med flera.

Med anledning av Schrems II-målet har en omfattande kartläggning genomförts på förvaltningen för att identifiera eventuella tredjelandsöverföringar av personuppgifter.

Detta arbete har även medfört att personuppgiftsbiträdesavtalen (PUB-avtalen) med olika leverantörer och deras underleverantörer uppdaterats och kompletterats med instruktion där den geografiska platsen för behandlingen anges.

Utifrån rådande läge uppmanas verksamheterna att undvika att hantera personuppgifter i olika tjänster t.ex. i sociala medier som har ägare/support utanför EU/EES.

Övrigt att rapportera

Kompetensutveckling hos medarbetare

Under året har kulturförvaltningens medarbetare uppmanats via utskick per mejl och via intranätet att genomföra de e-utbildningar som staden tagit fram inom dataskydd.

Vid årets slut har sammanlagt 302 personer antingen påbörjat eller genomgått e-utbildningen, grundkurs i dataskydd.

Dataskyddsombudets arbete

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

Dataskyddsombudet har under hösten ingått i en operativ referensgrupp med syftet att stödja och kvalitetssäkra stadsledningskontorets 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 gemensamma samarbetsområden för kulturförvaltningen och Stadsarkivet. Dataskyddsarbetet är en av dessa föreslagna åtgärder för samarbete och finns dokumenterat i en separat rapport.

Extern granskning

År 2019 genomförde stadens revisionskontor en revision av kulturförvaltningens arbete med skydd och behandling av personuppgifter.

Granskningen visade på brister, varpå följande rekommendationer gavs:

- Revisionskontoret rekommenderar att nämnden utvecklar styrning och uppföljning av arbetet med att efterleva dataskyddsförordningen.
- Vidare rekommenderar revisionskontoret att nämnden informationsklassificerar sina informationstillgångar samt regelbundet och systematiskt inventera sina personuppgifts-behandlingar.

En uppföljning av granskningen gjordes av revisionskontoret i januari 2021 och är ännu inte färdig, den blir klar i samband med att årsrapporten färdigställs för kulturförvaltningen.

Jämställdhetsanalys

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

Barnchecklista

Barn påverkas i viss mån indirekt av dataskyddsförordningen. 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 kulturförvaltningens 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

Dataskyddsombudet rekommenderar följande åtgärder för 2021:

Åtgärd	**Ansvarig**
Uppdatering av registerförteckning över personuppgiftsbehandlingar i stadens verktyg Draftit. En notering görs för respektive behandling om den har informationsklassats	Respektive avdelningschef Rapportera slutförd status till DSO
Genomför en översyn av styrdokument och mallar, specifikt process för samtycke.	Administrativ chef Rapportera slutförd status till DSO
Fastställ och besluta om dataskyddsorganisation och förankra därefter roller och ansvar inom dataskyddsarbete	Administrativ chef Rapportera slutförd status till DSO
Information/kommunikation till medarbetarna om vikten att anmäla och dokumentera personuppgiftsincidenter i IA	Säkerhetsenheten i samarbete med DSO
Uppdatera och genomför informationsklassning av alla de behandlingar som rör personuppgifter	Respektive avdelningschef Rapportera slutförd status till DSO och informationssäkerhetsansvarig
Uppföljning av vidtagna tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar	Respektive avdelningschef Rapportera slutförd status till DSO och informationssäkerhetsansvarig
Få in obligatorisk e-utbildning i dataskydd och informationssäkerhet i introduktion till nyanställda	HR-chef Rapportera slutförd status till DSO och informationssäkerhetsansvarig

Kulturförvaltningens synpunkter och förslag

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