Stockholms stad

GDPR Årsrapport

2021

Kulturnämnden

GDPR årsrapport
Januari 2022

Dnr: YYYY
Utgivningsdatum: 2022-01
Kontaktperson: Sara Hällströmer

1 Bakgrund

Dataskyddsförordningen (GDPR) trädde i kraft den 25 maj 2018. Syftet med förordningen är att skapa enhetliga dataskyddsregler inom EU med respekt för privatlivet och rätten till skydd av personuppgifter. GDPR har även till syfte att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt stadens reglemente för nämnderna är respektive nämnd ansvarig för att verksamheten följer GDPR vid hantering av sina personuppgifter. Det innebär att kulturnämnden som myndighet är personuppgiftsansvarig för all verksamhet. Kulturnämnden behöver därför få information för att kunna styra och följa upp dataskyddsarbetet på myndigheten.

Kulturnämnden har utsett ett Dataskyddsombud (ibland används förkortningen DSO) som har till uppgift att övervaka att myndigheten följer GDPR. Dataskyddsombudet ska vara självständig och oberoende i förhållande till myndigheten och ge rekommendationer.

I årsrapporten ger Dataskyddsombudet råd och rekommendationer till kulturnämnden som är personuppgiftsansvarig enligt GDPR. Årsrapporten redovisar därmed hur myndigheten efterlever lagstiftningen.

Innehåll

2 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

Årsrapporten innehåller sex obligatoriska rapporteringsområden samt förslag till råd och rekommendationer för kulturnämnden. Därtill innehåller rapporten planerade fokusområden för Dataskyddsombudets granskningar 2022.

3 Sex rapporteringsområden

Denna årsrapport innehåller sex obligatoriska rapporteringsområden som kulturnämnden i egenskap av personuppgiftsansvarig ska få information om.

Dessa områden är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter.

Jag redovisar nedan min bedömning av hur dataskyddsarbetet ser ut inom respektive rapporteringsområde. I slutet av varje avsnitt redovisar jag mina rekommendationer.

3.1 Registerförteckning

3.1.1 Bakgrund till rapporteringsområdet

Registerförteckningen är kulturnämndens främsta verktyg för att få en tydlig lägesbild över hur myndigheten behandlar sina personuppgifter.

Kulturnämnden ska dokumentera alla personuppgiftsbehandlingar i en registerförteckning. Registerförteckningen är central för myndighetens dataskyddsarbete. I förteckning säkerställs att myndigheten har laglig grund för all personuppgiftsbehandling

Kulturnämnden får i årsrapporten information om hur komplett myndighetens registerförteckning är. Myndigheten får även upplysningar om hur väl dess verksamheter har lyckats inventera och ange en laglig grund för sin behandling av personuppgifter.

3.1.2 Resultat

Jag kommer nedan att beskriva resultatet av min granskning avseende kulturnämndens registerförteckning.

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	176
Har nödvändiga uppdateringar gjorts?	Ja, kulturnämnden har under året arbetat med att uppdatera registerförteckningen och har fört in alla behandlingar i DraftIT.
Bedöms registerförteckningen vara fullständig?	Ja, med några få undantag. Förteckningen behöver uppdateras när det uppstår nya personuppgiftsbehandlingar.
Har verksamheten lämpliga rutiner för registerföring?	Ja, men förvaltningen behöver bättre rutiner för att identifiera nya personuppgiftsbehandlingar.

Min bedömning är att det behövs ett kontinuerligt arbete med att identifiera och registrera personuppgiftsbehandlingar. Registerförteckningen är inte fullständig, eftersom vissa behandlingar saknas och vissa registrerade behandlingar saknar fullständiga uppgifter.

Det är viktigt att registerförteckningen fortsatt hålls aktuell.

3.1.3 Bedömning av bristerna

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.1.4 Råd och rekommendationer

Under året behöver kulturnämnden följa upp och komplettera registerförteckningen med de uppgifter som saknas.

3.2 Styrdokument

3.2.1 Bakgrund till rapporteringsområdet

Styrdokument för dataskydd ska ge kulturnämnden och alla medarbetare möjlighet att bedriva ett systematiskt dataskyddsarbete. Enligt bestämmelserna i GDPR är det viktigt att myndighetens arbetssätt och rutiner är väl dokumenterat.

Dataskyddsombudet ska i detta rapporteringsområde kontrollera om myndigheten har antagit styrdokument och bedöma om styrdokumenten är lämpliga, uppdaterade och aktuella.

3.2.2 Resultat

Jag kommer nedan att beskriva resultatet av min granskning av kulturnämndens styrdokument.

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Ja, men den behöver kompletteras.
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja, men de behöver hållas uppdaterade.
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Nej
Är dokumenten uppdaterade?	Ja.
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja, men det behöver kompletteras.

Kulturförvaltningen har under året uppdaterat Intranätet med information om GDPR, rutiner och styrdokument. Där finns bland annat rutiner för registerutdrag, rättelse och radering. Vidare finns rutiner för hur personuppgiftsincidenter ska rapporteras samt en beskrivning av roller och ansvar inom dataskyddsarbetet. Det finns även mallar för samtyckesavtal.

Det är viktigt att alla styrdokument hålls uppdaterade och uppdateras vid behov. Vissa dokument kan även behöva förenklas för att underlätta för myndighetens verksamheter.

3.2.3 Bedömning av bristerna

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.2.4 Råd och rekommendationer

Under året bör en genomgång göras av alla styrdokument. Utgångspunkten bör vara att uppdatera och se över de styrdokument som behövs för kulturnämnden.

3.3 Informationsklassning av personuppgiftsbehandlingar

3.3.1 Bakgrund till rapporteringsområdet

Enligt Stadens riktlinjer för informationssäkerhet ska alla informationstillgångar klassas med stöd av Sveriges Kommuners och Regioners (SKR) verktyg KLASSA. Kulturnämnden ska klassa och skydda sin information och behöver välja rätt åtgärder för att skydda sin information.

Dataskyddsombudet ska kontrollera om myndigheten har en informationsägare eller en informationsägarrepresentant med ansvar för klassning. I Dataskyddsombudets årsrapport är endast sådan informationsklassning som avser behandling av personuppgifter eller system som omfattar *personuppgifter* av intresse.

3.3.2 Resultat

Dataskyddsombudet ska kontrollera om myndighetens verksamheter har genomfört en informationsklassning avseende alla personuppgiftsbehandlingar. Kontrollen ska också avse om informationsklassningen är aktuell.

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	Omkring 25
Är klassade personuppgiftsbehandlingar aktuella?	Omkring 20 från och med 2018-01-01

Det är informationssäkerhetssamordnaren som ansvarar för att klassa information. Den tidigare informationssäkerhetssamordnaren har slutat sin anställning i december 2021. Uppdraget sköts tillfälligt av säkerhetschefen.

3.3.3 Bedömning av bristerna

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.3.4 Råd och rekommendationer

Kulturnämndens arbete för informationsklassning är viktigt. Myndighetens medarbetare behöver få ytterligare utbildning kring betydelsen av att informationsklassa personuppgiftsbehandlingar. Dataskyddsombudet bör tillsammans med avdelningscheferna ansvara för att ta fram ett utbildningsprogram avseende hur information bör klassas på kulturnämnden. Det bör också göras en inventering av vilka klassningar som genomförts och vilka som saknas.

3.4 Konsekvensbedömningar

3.4.1 Bakgrund till rapporteringsområdet

Kulturnämndens konsekvensbedömningar är ett viktigt verktyg för myndighetens dataskyddsarbete. Enligt GDPR ska kulturnämnden genomföra konsekvensbedömningar för personuppgiftsbehandlingar

som sannolikt leder till en hög risk för personers rättigheter och friheter.

Myndigheten ska vid alla konsekvensbedömningar identifiera och dokumentera eventuella risker med en viss personuppgiftsbehandling.

3.4.2 Resultat

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Nej. Anledningen är att de personuppgiftsbehandlingar som registrerats i DraftIT saknar uppgift om risknivå.
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Nej
Är alla genomförda bedömningarna aktuella?	Nej

3.4.3 Bedömning av bristerna

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
X	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.4.4 Råd och rekommendationer

Dataskyddsombudet rekommenderar att kulturnämnden gör riskanalyser av samtliga personuppgiftsbehandlingar i DraftIT, och därefter genomför konsekvensbedömningar för de behandlingar som bedömts ha hög risk. Enligt gällande delegationsordning är det avdelningschefen som ansvarar för konsekvensbedömningen. Detta är ett arbete som bör prioriteras under 2022.

3.5 Registrerades rättigheter

3.5.1 Bakgrund till rapporteringsområdet

Registrerade personer har rätt att få ett registerutdrag och begära rättelse av vissa personuppgifter. Radering, eller ”rätten att bli glömd”, är sällan aktuell inom stadens verksamheter eftersom de lyder under offentlighetsprincipen. Verksamheten ska svara på begäran inom 30 dagar.

Dataskyddombudet ska kontrollera om myndigheten har lämpliga rutiner för att tillgodose registrerade personers rättigheter. Om kulturnämnden saknar rutiner för att hantera en begäran från en registrerad person kan Integritetsskyddsmyndigheten inleda ett granskningsärende mot kulturnämnden.

Dataskyddombudet ska i detta rapporteringsområde kontrollera om myndigheten har lämpliga rutiner för att tillgodose registrerade personers rättigheter.

3.5.2 Resultat

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	0
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	-

Kulturnämnden har inte tagit emot någon begäran om registerutdrag, rättelse eller radering under 2021.

Myndigheten har en skriftlig rutin och mallar för att utlämna registerutdrag vid begäran. Dataskyddsombudet bedömer att kulturnämnden har god beredskap för att hantera en begäran om inom 30 dagar. Det kan finnas risk för att alla personuppgiftsbehandlingar inte tas med vid ett registerutdrag. Anledningen är att kulturnämndens registerförteckning behöver uppdateras.

Kulturnämndens hantering av registerutdrag är en manuell process, och det finns risk att alla behandlingar inte tas med vid ett utdrag.

För flera av myndighetens datasystem saknas idag möjligheter till fritextsökning av personuppgifter. Det kan också leda till att myndighetens registerutdrag inte blir komplett.

3.5.3 Bedömning av bristerna

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.5.4 Råd och rekommendationer

Dataskyddsombudet bedömer att kulturnämnden har lämpliga rutiner för att hantera en begäran om registerutdrag inom angiven tidsfrist. Det är viktigt att de automatiserade system som kulturnämnden använder har en funktion som gör det enkelt att ta fram ett registerutdrag.

3.6 Personuppgiftsincidenter

3.6.1 Bakgrund till rapporteringsområdet

Med personuppgiftsincident avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter.

Myndighetens incidenthantering består av två delar, att dokumentera och att rapportera. Dataskyddsombudet kontrollerar i detta rapporteringsområde kulturnämndens dokumentation av personuppgiftsincidenter.

För det fall kulturnämnden inte rapporterar personuppgiftsincidenter inom en viss tid kan Integritetsmyndigheten inleda ett granskningsärende mot kulturnämnden.

Enligt GDPR ska alla personuppgiftsincidenter dokumenteras. Även de incidenter som inte ska rapporteras till Integritetsmyndigheten omfattas av kravet på dokumentation.

3.6.2 Resultat

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Incidenter upptäcks på olika sätt, t.ex. genom information från medarbetare, leverantörer eller användare. Den inom kulturförvaltningen som upptäcker incidenten anmäler den i stadens incidentrapporteringssystem, IA.
Hur många personuppgiftsincidenter har dokumenterats?	2
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	0
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	-

Kulturnämnden har rapporterat två incidenter i IA-systemet under året. Ingen av incidenterna har bedömts behöva rapporteras till Integritetsskyddsmyndigheten.

Myndigheten har en rutin för hantering av personuppgiftsincidenter som finns tillgänglig för alla medarbetare på intranätet.

3.6.3 Bedömning av bristerna

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Dataskyddsombudet bedömer att de personuppgiftsincidenter som har rapporterats har hanterats korrekt och enligt myndighetens rutin. Samtliga incidenter har varit harmlösa och har inte bidragit till att personuppgifter har riskerats.

Det låga antalet rapporterade incidenter indikerar dock att alla incidenter inte har identifierats och anmälts i IA. Dataskyddsombudets bedömning är att det verkliga antalet incidenter troligtvis är högre.

3.6.4 Råd och rekommendationer

Dataskyddsombudet bör tillsammans med avdelningscheferna genomföra en utbildnings- och informationsinsats för att höja kunskapen om rutinen för hantering av personuppgiftsincidenter. Det är viktigt att alla personuppgiftsincidenter identifieras och anmäls i IA.

4 Dataskyddsombudets fokusområden 2021

4.1 Bakgrund till fokusområdena

Dataskyddsombudet ska övervaka att kulturnämnden följer GDPR. En central del av det arbetet är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar vilka dataskyddsåtgärder som myndigheten bör besluta om. Kulturnämnden ska i årsrapporten få information om vilka granskningar som Dataskyddsombudet har genomfört under året.

Dataskyddsombudet har 2021 arbetat med följande fokusområden.

4.1 Iakttagelser från fokusområden

Fokusområde 1 – Implementering av ny organisation

Implementeringen av nämndens nya organisation för dataskyddsarbetet har påbörjats men behöver fortsätta under 2022. Exempelvis saknas det kontaktpersoner på några av avdelningarna.

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Fokusområde 2 – Genomförda dataskyddsutbildningar

Dataskyddsombudet har genomfört en kontroll av hur många medarbetare som gått grundutbildningen i GDPR. Vid årets slut hade 487 personer påbörjat eller gått färdigt e-utbildningen Grundkurs i dataskydd.

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder

X	Brister identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Fokusområde 3 – Genomförda stickprover

Dataskyddombudet har genom stickprov kontrollerat om verksamheterna använder PUB-avtal med tillhörande instruktioner. I de flesta fall där kulturnämnden köper tjänster som omfattar personuppgiftsbehandlingar finns PUB-avtal. Däremot saknas det ofta instruktioner. Dataskyddsombudet har kunnat identifiera nio instruktioner bland de omkring 30 PUB-avtal som nämnden har tecknat.

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Fokusområde 4 – Dataskyddsombudets oberoende ställning

Det har inletts en diskussion om Dataskyddsombudet är tillräckligt oberoende och självständig. Kulturnämndens tidigare Dataskyddsombud arbetade både som informationssäkerhetssamordnare och Dataskyddsombud. Nuvarande Dataskyddsombud arbetar både som myndighetens jurist och Dataskyddsombud.

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
X	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men inte bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

4.1.1 Råd och rekommendationer

Jag ger utifrån fokusområdena följande råd och rekommendationer.

Implementering av ny organisation

Kulturnämnden rekommenderas att fortsätta sitt arbete med att implementera en ny organisation för myndighetens dataskyddsarbete. Exempelvis bör samtliga avdelningar utse kontaktpersoner för dataskyddsarbetet.

Genomförda dataskyddsutbildningar

Dataskyddsombudet bör tillsammans med avdelningscheferna arbeta för att samtliga medarbetare går den grundläggande dataskyddsutbildningen 2022.

Genomförda stickprover

Kulturnämnden rekommenderas komplettera samtliga PUB-avtal med instruktioner i de fall där det saknas.

Dataskyddsombudets oberoende ställning

Kulturnämnden bör överväga att anlita ett externt Dataskyddsombud. Nuvarande Dataskyddsombud är anställd av myndigheten. Kulturnämndens dataskyddsarbete skulle bli mer oberoende om det sköttes av en extern uppdragstagare.

5 Planerade fokusområden 2022

Dataskyddsombudet har valt ut tre fokusområden som ska kontrolleras särskilt 2022. Dessa fokusområden kommer att återrapporteras i nästa årsrapport.

Fokusområde 1 - Fokus på Schrems II

Under året ska Dataskyddsombudet tillse att det finns ännu tydligare information om dataskyddsarbetet och Schrems II tillgängligt för myndighetens medarbetare.

Fokusområde 2 – Genomföra stickprover

Dataskyddsombudet ska regelbundet genomföra stickprov av genomförda riskanalyser, konsekvensbedömningar och användandet av PUB-avtal och PUB-instruktioner.

Fokusområde 3 – Externt Dataskyddsombud

Dataskyddsombudet ska tillsammans med förvaltningens ledningsgrupp fortsätta diskussionen om möjligheterna att anlita ett externt och mer oberoende Dataskyddsombud.