Stockholms stad

Bilaga 1e

GDPR årsrapport

År 2025

Exploateringsnämnden

Innehållsförteckning

GDPR årsrapport
Januari 2026

Dnr: E2026-00097
Utgivningsdatum: 2026-01-15
Kontaktperson: Patrik Stensson

Sammanfattning

GDPR, eller dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten. Ett dataskyddsombud (DSO) har i uppdrag att oberoende granska verksamhetens efterlevnad av dataskyddsförordningen. I denna rapport redovisar DSO årets granskning av Exploateringsnämnden dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

Inledning

GDPR, eller dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. Dataskyddsreglerna (*kallas GDPR fortsättningsvis*) sätter tydliga ramar för hur personuppgifter får behandlas för att minimera risken för skada och säkerställa att hanteringen sker ansvarsfullt och rättvist. GDPR har sin grund i de mänskliga rättigheterna, där varje individ har rätt till respekt för sitt privat- och familjeliv samt skydd av sina personuppgifter.

I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten.

Dataskyddsombudets (DSO) uppgift

Varje personuppgiftsansvarig (nämnd eller styrelse) ska utse en DSO. DSO:s uppgifter framgår direkt av lagstiftningen. Ombudets roll är att kontrollera att GDPR följs inom organisationen. Det innebär bland annat att ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. DSO har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs. DSO ska rapportera direkt till högsta förvaltnings-/bolagsnivå. I Stockholms stad innebär det att DSO rapporterar till nämnder och styrelser.

DSO lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och styrelse. Genom rapporten kan nämnd och styrelse ta emot de råd och rekommendationer som DSO lämnar. Årsrapporten syftar till att nämnd/styrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Årsrapporten är ett medel för nämnds/styrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Granskning av dataskyddsarbetet

Kontroll av obligatoriska områden

DSO har granskat verksamhetens dataskyddsarbete utifrån sex obligatoriska områden. De sex områdena har identifierats genom en analys av kraven i GDPR om hur verksamheter bör arbeta systematiskt med dataskydd. Varje område innehåller ett antal kontrollfrågor som ger en bild av verksamhetens dataskyddsarbete. Dessa områden överensstämmer med de delar som enligt Integritetsskyddsmyndigheten (IMY) utgör grunden för en verksamhets systematiska och rättssäkra hantering av personuppgifter.

I rapporten används en riskmodell med fyra nivåer av risk. Modellen hjälper DSO att visa vilken bedömning hen gör av verksamhetens dataskyddsrisker utifrån de iakttagelser som gjorts i granskningen.

Risknivå	Beskrivning
Hög risk 	Iakttagelsen avser en brist som kan leda till betydande risker för de registrerades rättigheter och friheter. Bristen kräver omgående åtgärd och korrigering.
Medelhög risk 	Iakttagelsen avser en brist som kan leda till risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas skyndsamt, men kräver inte omedelbar korrigering.
Låg risk 	Iakttagelsen avser en brist som kan leda till mindre risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas, men kräver inte omedelbar korrigering.
Inget att anmärka 	Dataskyddsombudet har inga brister att rapportera avseende denna del.

Notera att risken för att tilldelas en sanktion vid tillsyn är större desto högre risken är.

Resultatsammanställning och centrala iakttagelser inom dataskyddsarbetet

I detta avsnitt presenteras en sammanställning av den bedömda risknivån för verksamhetens dataskyddsarbete, grundat på kontrollfrågorna inom de sex obligatoriska områdena. Vidare redovisas DSO centrala iakttagelser, inklusive områden där verksamheten uppvisar goda resultat och bör upprätthålla sitt arbete, samt identifierade brister som kan utgöra dataskyddsrisker. Avsnittet innehåller även DSO rekommenderade åtgärder för att hantera dessa risker och stärka dataskyddsarbetet.

Register över personuppgiftsbehandlingar

Sammanfattning

Personuppgiftsbehandlingsregistret förs i en excelfil. Registret vårdas av IT-strateg. Registret kommer att läggas på en samarbetsyta i Sharepoint. Registret utgår inte renodlat från processer utan från både system/applikationer och vissa processer. Registret uppdateras framförallt vid informationsklassningar.

Bedömning av risknivå och rekommendationer från DSO

Fråga/kontroll	Risk	Rekommendationer/kommentarer
Antal behandlingar som är registrerade: 200		Exploateringskontoret genomför fortsatt registrering av personuppgiftsbehandlingar som ändras eller tillkommer.
Verksamheten har ändamålsenliga rutiner för att registrera nya/förändrade behandlingar: **DELVIS**		Rutinen för att uppdatera är att det görs vid informationsklassning.
Behandlingar registreras eller uppdateras i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför. **DELVIS**		Registret i stort sett komplett, men kontinuerlig uppdatering krävs.
Registret innehåller de uppgifter som är obligatoriska enligt artikel 30. **JA**		Ingen rekommendation/kommentar

Säkerhet i samband med behandlingen

Sammanfattning

Informationsklassningar görs kontinuerligt på exploateringskontoret både vid upphandling, driftsättning och förändring av system/applikationer.

Bedömning av risknivå och rekommendationer från DSO

Fråga/kontroll	Risk	Rekommendationer/kommentarer
DSO bedömer att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter. **JA**		De informationsklassningar som görs är av god kvalitet. Återstår arbete att följa upp informationsklassningar och handlingsplaner. Riskanalyser bör göras vid de klassningar vars objekt kräver det. Fortsatt klassning av system/applikationer/informationsmängder i prioritetsordning.
DSO bedömer att det finns tillräckligt mycket reglerat och tillräckligt stöd avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt). **JA**		Styrande dokument finns såsom lokal anvisning för informationssäkerhet på exploateringskontoret samt riktlinjer för personuppgiftsbehandling på exploateringskontoret. Incidentrapporteringsrutin samt lednings genomgång är framtagen. Lokala anvisningar ska tas fram.
DSO bedömer att de skriftligt styrande dokument och rutiner som finns är tillräckligt implementerade och kända. **DELVIS**		Utbildningsinsatser behövs för att göra styrande dokumentation och rutiner kända. Samarbetsyta för informationssäkerhet på gång. Peka på att alla gör den obligatoriska utbildning.

Konsekvensbedömning avseende dataskydd

Sammanfattning

Exploateringskontoret har inte behövt göra några konsekvensbedömningar detta år.

Bedömning av risknivå och rekommendationer från DSO

Fråga/kontroll	Risk	Rekommendationer/kommentarer
Det finns ändamålsenliga rutiner för att genomföra tröskelanalys vid nya/förändrade personuppgiftsbehandlingar. JA		Tröskelanalys görs vid informationsklassning.
Tröskelanalyser görs vid nya/förändrade personuppgiftsbehandlingar. JA		Tröskelanalys görs vid informationsklassning
Det finns en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd. JA		Exploateringskontoret använder stadens mall.
Konsekvensbedömning avseende dataskydd genomförs i de fall det krävs. JA		Konsekvensbedömningar
Personuppgiftsansvarig har identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta. JA		Samtliga behandlingar som kräver konsekvensbedömningar har identifierats.

Den registrerades rättigheter

Sammanfattning

Exploateringskontoret har en ingen tydlig rutin för begäran om registerutdrag. Men det ska tas fram.

Bedömning av risknivå och rekommendationer från DSO

Fråga/kontroll	Risk	Rekommendationer/kommentarer
Det finns ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade. **DELVIS**		Mall ska tas fram för att ta vara på de registrerades begäran på ett enhetligt sätt.
Antal begäranden (om registerutdrag, begränsning, radering etc.) från de registrerade under året. **0**		*Ingen rekommendation*
Antal begärandena som har besvarats av verksamheten inom en månad. **N/A**		*Inga rekommendationer*
Svaren till de registrerade uppfyller lagkraven. **N/A**		*Inga rekommendationer*

Personuppgiftsincidenter

Sammanfattning

Exploateringskontoret har rutinen att rapportera i IA.

Merparten incidenter är inte så allvarliga att de har rapporterats till IMY och de incidenter som rapporterats till IMY har inte föranlett några åtgärder från deras sida.

Bedömning av risknivå och rekommendationer från DSO

Fråga/kontroll	Risk	Rekommendationer/kommentarer
Det säkerställs att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident. **DELVIS**		Tydliggörande av roller och utbildning krävs för hela förvaltningen.
Ändamålsenliga rutiner finns för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter. **DELVIS**		En framtagen rutin finns men den behöver tydliggöras särskilt för större incidenter.
Antal personuppgiftsincidenter som har dokumenterats under året. **1**		En incident omfattade samtliga medarbetare på exploateringskontoret. Utmaningen i det fallet var framförallt information och kommunikation, då exploateringskontoret inte direkt hade mandat att åtgärda säkerhetsbristerna.
Antal personuppgiftsincidenter som har anmälts till IMY under året. **1**		Incidenten omfattade samtliga anställda på exploateringskontoret, även integritetskänsliga uppgifter förekom. Ingen åtgärd vidtogs gentemot exploateringskontoret. Exploateringskontoret hade ingen rådighet över incidenten och de säkerhetsåtgärder som krävdes.

Överföring till tredje land

Sammanfattning

Exploateringskontoret har inga tredjelandsöverföringar.

Fråga/kontroll	Risk	Rekommendationer/kommentarer
Personuppgiftsansvarig har identifierat de tredjelandsöverföringar som utförs. **JA**		Tredjelandsöverföring förekommer inte.
Personuppgiftsansvarig har gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar. **JA**		N/A

Kamerabevakning

Sammanfattning

Användningen av kameror och olika slags sensorer på exploateringskontoret är inte helt systematiserad. Under 2026 kommer exploateringskontoret att titta på frågan.

Bedömning av risknivå och rekommendationer från DSO

Fråga/kontroll	Risk	Rekommendationer/kommentarer
En övergripande organisation finns för att bevaka kamerafrågan på exploateringskontoret NEJ		Exploateringskontoret ska inventera och registrera eventuell kamerabevakning inom verksamheten under 2026