Stockholms stad

Bilaga 9

# GDPR årsrapport

År 2025

Trafiknämnden

**GDPR årsrapport**
**Januari 2025**

**Dnr: T2025-03978**
**Utgivningsdatum: 2026-01-13**
**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 Trafiknämndens dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

# Innehållsförteckning

# 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 ett 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 DSOet 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.

En fullständig redovisning av DSO underlag och resultat från granskningen av de sex obligatoriska områdena finns att läsa i bilaga 1. Bilagan innehåller även en beskrivning av syftet och bakgrunden för varje område.

### Register över personuppgiftsbehandlingar

Sammanfattning

Personuppgiftsbehandlingsregistret förs i en excelfil som är registrerad i Public 369 med diarienummer T2024-00989. Registret vårdas av DSO. Registret utgår inte renodlat från processer utan från både system/applikationer och vissa processer. DSO och informationssäkerhetssamordnare (ISAM) kommer gemensamt att arbeta om registret under 2026 och då utgå från processerna i Vintergatan. Registret uppdateras framförallt vid informationsklassningar.

Bedömning av risknivå och rekommendationer från DSO

| Fråga/kontroll | Risk | Rekommendationer/kommentarer |
|---|---|---|
| Antal behandlingar som är registrerade:<br><br>**128** | | TK genomför Fortsatt registrering av personuppgiftsbehandlingar som ändras eller tillkommer. |
| Verksamheten har ändamålsenliga rutiner för att registrera nya/förändrade behandlingar:<br><br>**DELVIS** | | Rutinen för att uppdatera är att det görs vid informationsklassning eller om det kommer till DSO:s kännedom att en ny/ändrad behandling sker. |
| Behandlingar registreras eller uppdateras i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför.<br><br>**DELVIS** | | Registret i stort sett komplett, men kontinuerlig uppdatering krävs. |

| | | |
|---|---|---|
| Registret innehåller de uppgifter som är obligatoriska enligt artikel 30.<br><br>**JA** | | Ingen rekommendation/kommentar |

## Säkerhet i samband med behandlingen

Sammanfattning

Informationsklassningar görs kontinuerligt på Trafikkontoret både vid upphandling, driftsättning och förändring av system/applikationer. DSO är med vid informationsklassningar. Trafikkontoret använder sig av en stor mängd system/applikationer, därför har prioriteringar gjorts i vilken omfattning informationsklassningar görs. För många äldre informationsklassningar saknas uppföljning av handlingsplan och säkerhetsåtgärder samt riskanalys. Det har gjorts stora förbättringar på området, men fortfarande återstår mycket arbete.

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.<br><br>**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).<br><br>**JA** | | Styrande dokument finns såsom lokal anvisning för informationssäkerhet på trafikkontoret samt riktlinjer för personuppgiftsbehandling på trafikkontoret. |
| DSO bedömer att de skriftligt styrande dokument och rutiner som finns är tillräckligt implementerade och kända.<br><br>**DELVIS** | | Utbildningsinsatser behövs för att göra styrande dokumentation och rutiner kända |

## Konsekvensbedömning avseende dataskydd

Sammanfattning

Trafikkontoret använder Stadens mall för konsekvensbedömningar men det finns ingen riktigt bra rutin för att genomföra konsekvensbedömningar på trafikkontoret. De bäst genomförda konsekvensbedömningarna är de som genomförts vid tillståndsansökningar för kamerabevakning. Det finns upphandlat konsultstöd att genomföra konsekvensbedömningar.

Bedömning av risknivå och rekommendationer från DSO

| Fråga/kontroll | Risk | Rekommendationer/kommentarer |
|---|---|---|
| Det finns ändamålsenliga rutiner för att genomföra tröskelanalys vid nya/förändrade personuppgiftsbehandlingar.<br><br>JA | | Tröskelanalys görs vid informationsklassning. |
| Tröskelanalyser görs vid nya/förändrade personuppgiftsbehandlingar.<br><br>JA | | Tröskelanalys görs vid informationsklassning |
| Det finns en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd.<br><br>DELVIS | | Trafikkontoret använder Stadens mall, men det finns däremot inga utarbetade rutiner för konsekvensbedömningar |
| Konsekvensbedömning avseende dataskydd genomförs i de fall det krävs.<br><br>DELVIS | | Konsekvensbedömningar genomförs och har genomförts, men de har letts av DSO, vilket inte är lämpligt. En ny rutin behöver upprättas. Det finns upphandlat konsultstöd för att genomföra konsekvensbedömningar. |
| Personuppgiftsansvarig har identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta. | | Samtliga behandlingar som kräver konsekvensbedömningar har identifierats men konsekvensbedömningarna har inte alltid följts upp. |

| | | |
|---|---|---|
| DELVIS | | |

## Den registrerades rättigheter

Sammanfattning

Trafikkontoret har en mall för svar till de registrerade samt en tydlig rutin för begäran om registerutdrag. Det som brister är att det inte finns tydliga, skriftliga rutiner för att tillmötesgå begäran om invändning, radering, begränsning och dataportabilitet. Verksamheten kan be DSO att stödja dem de få fall som förekommer.

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.<br><br>**DELVIS** | | Mall finns och kontaktuppgifter till objektspecialister för respektive system där personuppgifter behandlas för att kunna ge registerutdrag. Däremot är kunskapen bristfällig när det kommer till begränsning och invändning. Verksamheten får vända sig till DSO om begäran kommer in.. |
| Antal begäranden (om registerutdrag, begränsning, radering etc.) från de registrerade under året.<br><br>**2** | | *Ingen rekommendation* |
| Antal begärandena som har besvarats av verksamheten inom en månad.<br><br>**SAMTLIGA** | | *Inga rekommendationer* |
| Svaren till de registrerade uppfyller lagkraven.<br><br>**JA** | | *Inga rekommendationer* |

## Personuppgiftsincidenter

Sammanfattning

Trafikkontoret har rutinen att fylla i en egen rapportmall enligt en lokalt framtagen rutin*: Trafikkontorets rutin för hantering av informationssäkerhetsincidenter* med bilagor för personuppgiftsincidenter. Att rapportera i IA är inte tillfredsställande utan trafikkontoret använder den rapporten bara som bilaga till incidentrapporten som diarieförs.

Det finns brister när det gäller rapporteringskedjan från personuppgiftsbiträden eller förvaltningar inom staden som agerar biträde till trafikkontoret. Detta behöver förbättras med tydligare kontaktpunkter och rutiner.

Rutinen för större incidenter behöver stramas upp, särskilt när det gäller hur kommunikationen inom kontoret sker och vilka roller som ska involveras. Den behöver kommuniceras och förankras. Särskilt när det gäller att tydliggöra vilka i Objekten som ska vara incidentledare. Det gäller även vilka chefer som ska vara incidentledare om det sker en incident som ligger utanför Objekten.

Rutinen för när biträden inom staden behandlar personuppgifter för trafikkontorets räkning behöver stramas upp, DSO, ISAM och ansvarig chef/Objektledare ska involveras om det handlar om personuppgifter med hög risk och därmed en konsekvensbedömning behöver genomföras.

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.<br><br>**DELVIS** | | Tydliggörande av roller och utbildning krävs för varje Objekt och på chefsnivå. |
| Ändamålsenliga rutiner finns för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter.<br><br>**DELVIS** | | En framtagen rutin finns men den behöver skärpas och tydliggöras särskilt för större incidenter. |
| Antal personuppgiftsincidenter som har dokumenterats under året. | | Samtliga utom en (1) har varit mycket små incidenter. En incident omfattade samtliga medarbetare på trafikkontoret. Utmaningen i det fallet var framförallt information och |

| | | |
|---|---|---|
| **5** | | kommunikation, då trafikkontoret inte direkt hade mandat att åtgärda säkerhetsbristerna. |
| Antal personuppgiftsincidenter som har anmälts till IMY under året.<br><br>**1** | | Incidenten omfattade samtliga anställda på trafikkontoret, även integritetskänsliga uppgifter förekom. Ingen åtgärd vidtogs gentemot trafikkontoret. Trafikkontoret hade ingen rådighet över incidenten och de säkerhetsåtgärder som krävdes. |

## Överföring till tredje land

Sammanfattning

Tidigare har trafikkontoret utgått från förutsättningen att tredjelandsöverföring sker även när tjänsten har t.ex. amerikanska ägare, trots att själva behandlingen skett inom EU/EES. Men den nuvarande bedömningen är det i det fallet enbart föreligger risk för tredjelandsöverföring och att det kan stävjas med säkerhetsåtgärder. Däremot är trafikkontoret fortsatt försiktiga med att tillåta tredjelandsöverföring även till bolag som omfattas av EU-U.S. Data Privacy Framework (DPF) då det är osäkert om den kommer att gälla framöver.

Det är inte lätt att alltid försäkra sig om att tredjelandsöverföring sker, då vissa tjänster längre ner i kedjan möjligtvis nyttjar exempelvis Amazon Web Service, Microsoft Azure eller något Googleverktyg. Det är inte helt lätt att se flödet av personuppgifter i alla steg.

| Fråga/kontroll | Risk | Rekommendationer/kommentarer |
|---|---|---|
| Personuppgiftsansvarig har identifierat de tredjelandsöverföringar som utförs.<br><br>**DELVIS** | | Tredjelandsöverföring undviks i majoriteten av behandlingar, särskilt när det gäller högriskbehandlingar. Det är inte möjligt i vissa fall, men då minimeras risken med säkerhetsåtgärder. |
| Personuppgiftsansvarig har gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar.<br><br>**JA** | | TIA görs vid behov. Är en punkt vid informationsklassning. |

## Kamerabevakning

Sammanfattning

Användningen av kameror och olika slags sensorer på trafikkontoret är ganska stor. Trafikkontoret har under 2025 genomfört en stor kartläggning av användandet av kameror och utarbetat rutiner för registrering och intresseavvägningar för kameror.

Ett särskilt område är de trafikkameror som driftas av trafikkontoret med som nyttjas i samarbetet *Trafik Stockholm*, där Trafikverket och ett antal grannkommuner ingår. Där har ett s.k. *inbördes arrangemang*, ett avtal, tecknats med Trafikverket för att klargöra roller och ansvar för personuppgiftsbehandlingen inom samarbetet. Även sekretessfrågan har utretts.

Bedömning av risknivå och rekommendationer från DSO

| Fråga/kontroll | Risk | Rekommendationer/kommentarer |
|---|---|---|
| En övergripande organisation finns för att bevaka kamerafrågan på trafikkontoret<br><br>DELVIS | | Det är beslutat att kamerafrågor ska ligga på säkerhetsenheten, men projektet pågår fortfarande. |
| Ett register över kameror finns på trafikkontoret<br><br>DELVIS | | Register finns i excel men ska föras över till tekniska anläggningsregistret. |
| Rollerna inom Trafik Stockholm är klargjorda när det gäller personuppgiftsbehandling.<br><br>JA | | Trafikkontoret och Trafikverket har gemensamt personuppgiftsansvar och har tecknat ett avtal som reglerar detta. Bör följas upp. |

## AI

Sammanfattning

Användningen av AI-teknik på trafikkontoret är fortfarande begränsat. Det förekommer i vissa sensorer, som stöd för kommunikationsavdelningen, samt för maskning av bilder.

Trafikkontoret har en AI-samordnare.

En lokal riktlinje för AI finns inte på kontoret och bör tas fram. Kommunikation har tagit fram en egen rutin för generativ AI.

Bedömning av risknivå och rekommendationer från DSO

| Fråga/kontroll | Risk | Rekommendationer/kommentarer |
|---|---|---|
| Lokal riktlinje för AI finns för trafikkontoret<br><br>NEJ | | Riktlinje bör tas fram för hela trafikkontoret |
| En organisation finns på trafikkontoret för att bevaka AI-frågor. Roller och ansvar är tydliga.<br><br>DELVIS | | En AI-samordnare är utsedd. Det är oklart hur roller och ansvar fördelas mellan Objekt, linje och projekt. |