Stockholms stad

# GDPR Årsrapport

2024

**Bromma Stadsdelsförvaltning**

**GDPR årsrapport**
Januari 2025

**Dnr:** BRO 2025/31
**Utgivningsdatum:** 2025-01-08
**Kontaktperson:** Jessica Hillergård

# Sammanfattning

**I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.**

År 2024 började AI-verktygen implementeras i IT-tjänster där man minst kunnat ana det tidigare. Den nya lagen om AI, AI förordningen, antogs i EU under våren och kommer implementeras under de kommande åren i olika faser. Ur ett dataskyddsperspektiv blir frågorna än mer intressanta och komplexa i och med att AI:n skapar nya personuppgiftsbehandlingar. Det är också uppmärksammat att ett antal incidenter har skett i staden under året då nya AI:n implementerats av misstag i olika digitala verktyg vid uppdateringar.

Samhället har påverkats av flera uppmärksammade informations- och personuppgiftsincidenter, bland annat en större ransomware-attack hos TietoEvry i januari 2024. Incidenten skapade stor oro och informationen var otydlig till en början. Turligt nog klarade sig Stockholm stad i den attacken, men andra kommuner drabbades samtidigt mycket hårt. Ett behov av en central CERT-funktion blir tydlig för att stadsdelsförvaltningen ska kunna ta kunskapsbaserade beslut vid incidenter. Omvärldsbevakningen visar också att fokus inte får tappas på dataskyddsfrågor även i kris och krig.

Flera risker inom dataskydd kvarstår inom stadsdelsförvaltningen även detta år. Alla risker kan inte åtgärdas eller sänkas vilket kan bero på faktorer man inte kan påverka. Att ha kunskap om sina risker och ha dem under bevakning är en styrka för en organisation. I rapporten har sex stycken prioriterade risker lyfts fram som påverkar förvaltningens förmåga och arbete med dataskydd vilket styrs av bland annat dataskyddsförordningen.

Det stora arbetet under 2024 har varit att följa den handlingsplan som tagits fram för informationssäkerhet inom Bromma stadsdelsförvaltning där dataskyddet jobbats in som en delmängd. Arbetet har lett till att samtliga IT-system och IT-tjänster nu har en tydligt utpekat förvaltningsansvar och genomgått en så kallad förklassning. Som nästa steg rekommenderas nu nämnden att arbeta vidare med att kartlägga och klassa sina processer och koppla dessa till IT-tjänsterna för att på det sättet ha en tydligare kontroll över sina informationstillgångar och personuppgiftsbehandlingar.

Jessica Hillergård

Dataskyddsombud

# Innehåll

# 1 Inledning

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

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett dataskyddsombud, DSO. Denna roll 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 dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen. I rapporten får nämnden insyn i vad dataskyddsombudets granskningar visat av verksamheten och status avseende integritet och dataskydd. Årsrapporten syftar till 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 *dokumenteringsskyldighe*t. Årsrapporten är även ett medel för nämndens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

# 2 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som personuppgiftsansvarig, PUA, som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som Dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är:

- registerförteckning
- styrdokument
- tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar
- konsekvensbedömningar
- individens rättigheter
- personuppgiftsincidenter

Nedan redogörs för nämndens status och dataskyddsombudets slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter genomförd uppföljning och granskning.

## 2.1 Registerförteckning

### 2.1.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Antal behandlingar som är registrerade? | 115 |
| Har nödvändiga uppdateringar gjorts? | Nej |
| Bedöms registerförteckningen vara fullständig? | Nej |
| Har verksamheten lämpliga rutiner för registerföring? | Ja |

### 2.1.2 Syfte

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför i klartext av dataskyddsförordningen (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i en så kallad registerförteckning (även kallat behandlingsregister eller register av register).

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. Det är därför viktigt att PUA får information om hur komplett verksamhetens förteckning är. Om dokumenteringskravet uppfylls kan verksamheten arbeta effektivt, systematiskt och riskbaserat och samtidigt värna om individens integritet, särskilt när känsliga och särskilt skyddsvärda personuppgifter behandlas av verksamheten.

Att ha en registerförteckning på plats leder till att verksamheten kan arbeta mer resurs- och kostnadseffektivt med sitt systematiska och riskbaserade dataskyddsarbete. Man kan styra insatserna där de gör störst nytta.

Syftet med detta rapporteringsområde är således att rapportera till PUA hur väl verksamhetens har lyckats inventera sina personuppgifter och de personuppgifter som behandlas för annans räkning och upprätta en registerförteckning.

Eftersom inventeringen av personuppgifter i sig är avgörande för allt det fortsatta dataskyddsarbetet inom verksamheten, är denna lägesbild en av de viktigaste slutsatserna som PUA behöver förstå och ta ställning till inför det planerade åtgärdsarbetet under nästa verksamhetsår.

### 2.1.3 Resultat

Registerförteckningen finns i ett digitalt verktyg kallat DraftIt och består av ett frågeformulär per personuppgiftsbehandling, vilket i sin tur blir funktionen av en checklista att alla krav i GDPR dokumenteras och omhändertas korrekt.

Totalt har 115 behandlingar registrerats i DraftIt. Under år 2024 har översyn gjorts av DSO samt en granskning mot hanteringsanvisningen. Det finns en del brister. Då registerförteckningen bygger på 2019-års standard och utvecklingen har gått framåt sedan dess, så finns ett behov att modernisera registerförteckningen efter dagens bästa praxis.

### 2.1.4 DSO anger hur allvarliga bristerna är på en skala

| | |
|---|---|
| | 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 ej bedöms vara brådskande, omfattande eller allvarliga |
| | Inga brister av nämnvärd betydelse identifierade |

### 2.1.5 DSO ger råd och rekommendationer till PUA

Nästa steg för förvaltningens arbete med registerförteckningen är att implementera de roller som anges i förvaltningsmodellen PM[3] som Stockholms stads verksamheter ska följa. I den finns roll angiven för vem som är informationsansvarig, den som är ansvarig att utföra kontroller osv. I rollbeskrivningen ska det också framkomma vem som är ansvarig för att hålla registerförteckningens olika personuppgiftsbehandlingar uppdaterade och lägga in nya.

För att underlätta arbetet med registerförteckningen kan man med fördel lyfta in hanteringsanvisningen från Stadsarkivet som stöd för att förtydliga i vilka processer som behandlingarna går in under.

Under år 2025 ges rekommendationen att likt samarbetspartnern Hässelby-Vällingby stadsdelsförvaltning bygga upp registerförteckningen utifrån processer och uppdatera utifrån bästa praxis.

## 2.2 Styrdokument

### 2.2.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Finns lämplig styrande dokumentation på plats? | JA |
| Håller innehållet i de existerande dokumenten lämplig kvalitet? | JA |
| Är dokumenten pedagogiska och ger de ett tillräckligt stöd? | JA |
| Är dokumenten uppdaterade? | JA |
| Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov? | JA |

### 2.2.2 Syfte

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 Dataskyddsförordningen principer för behandling av personuppgifter efterlevs (artikel 5).

Rapporteringen av området är tvådelad: dels ska DSO bedöma om verksamheten har de styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket ingår bl.a. att dokumentationen ska vara uppdaterad och aktuell.

En brist inom detta område bör förstås ses som en brist i förhållande till direkta lagkrav, men det finns fler nyanser av detta som bör

lyftas fram till PUA. Bristande styrning på grund av att lämplig styrande dokumentation saknas leder exempelvis ofta till bristande kvalitet i hur verksamheten utför aktiviteterna, men även till att verksamheten slösar värdefulla resurser när exempelvis för många personer blir involverade i en incidenthantering eller för att en analys behöver göras om från grunden varje gång istället för att man återanvänder redan uppfunnen kunskap. Dessa effekter drabbar verksamheter ur ett vidare perspektiv och är något som ligger i PUA:s intresse att förstå för att fatta rätt beslut om.

### 2.2.3 Resultat

Bromma SDF. har tagit fram flera rutiner och styrande dokument inom verksamheten och uppdaterat dessa under 2024. De är väl skrivna och informativa.

En uppdatering av intranätet våren 2023 skapade en hel del problem för stadsdelsförvaltningen att publicera information så att medarbetarna lätt kan ha access till den vid behov. Problemet kvarstår även under år 2024 och är än mer problematiskt i dagsläget.

För att nå information om dataskydd ska medarbetaren göra följande klick/ val på intranätet:

1. Stöd i arbetet
2. Rättsfrågor och juridiskt stöd
3. Informationssäkerhet i staden
4. GDPR

När en medarbetare ska ta fram information om dataskydd, möts hen av flera olika alternativa sökvägar för att hitta dokumentation och handledningar. Områdena dataskydd och informationssäkerhet har också blandats ihop vilket har uppfattas som förvirrande av medarbetarna. Järva har löst det med att lägga länkar till en plats med information som lösning, vilket fungerar hjälpligt.

Den otydlighet som är mest anmärkningsvärd, är aktiviteter som genomförs på grund av lagkrav i Dataskyddsförordningen är inblandat vid informationsklassning och riskanalys, vilket inte styrs i lag utan av riktlinjer från kommunfullmäktige. Mixen gör det svårt för medarbetarna att se den röda tråden och uppfattningen är att ämnet är krångligt och svårt att förstå.

Med tillgänglighetsdirektivet har merparten av alla sidor på intranätet gjorts om till löpande text. Medarbetaren ska först scrolla genom text med en allmän information vilket kan missförstås att

vara vägledningar, och slutligen, efter en hel del scrollande, kan den lokala informationen återfinnas med gällande vägledning och rutiner.

Under hösten 2024 publicerades en ny mall för lokal tillämpningsanvisning för informationssäkerhet av SLK. Där har dataskyddsperspektivet lyfts bort. Den har ännu inte implementerats av stadsdelsförvaltningen.

Bedömningen är att innehåll och kvalitet är **GRÖNT** men hur den bestämts att publiceras av centrala funktioner i staden är **GULT**.

### 2.2.4 DSO anger hur allvarliga bristerna är på en skala

| | |
|---|---|
| | 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 ej bedöms vara brådskande, omfattande eller allvarliga |
| X | Inga brister av nämnvärd betydelse identifierade |

### 2.2.5 DSO ger råd och rekommendationer till PUA

Bromma stadsdelsförvaltningsnämnd rekommenderas att om möjligt påverka synligheten för interna styrande dokument på intranätet.

Nämnden rekommenderas också att uppdatera den nya lokala tillämpningsanvisningen för informationssäkerhet med information om dataskydd, alternativt upprätta en lokal tillämpningsanvisning för dataskydd.

## 2.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

### 2.3.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats? | Fastställt skyddsvärde av IT-tjänster: 100 st. (100 %) |
| Är klassade personuppgiftsbehandlingar aktuella? | Ja |

### 2.3.2 Syfte

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 SKR:s 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 del av verksamheten som är informationsägare. En första kontrollpunkt måste därför vara om en informationsägare eller en informationsägarrepresentant med ansvar för klassning är identifierad i verksamheten. Om en ansvarig för klassningen inte har pekats ut och känner till sitt ansvar för klassning, minskar sannolikheten avsevärt att en klassning faktisk initieras.

***Notera att enbart sådan informationsklassning som avser behandling eller system som omfattar personuppgifter är av intresse för DSO:s årsrapportering.***

***Viktigt är också att notera att dataskyddsombudet omhändertar den registrerades intresse och informationssäkerhetssamordnaren har fokus på verksamhetens krav på informationen i form av tillgänglighet, riktighet och konfidentialitet. Verktyget för DSO är***

***i första hand registerförteckningen och dokumentationen där. Informationssäkerhetssamordnaren har KLASSA som verktyg för att se till att verksamhetens krav efterlevs i form av dokumentation i förvaltningsplaner, systembeskrivningar etc.***

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.

### 2.3.3 Resultat

Under år 2024 har fortsatt arbete skett med förklassningsprotokoll och då i tre steg vilka är: A-klassning i designfasen, B-klassning vid införandet och C-klassning vid årlig uppföljning. Protokollet från dessa ska signeras av informationsägaren och har konkretiserat skyddsvärdet för informationen samt identifierat personuppgifterna som kan ingå i dessa. Dataskyddsombudet har blivit inbjuden till sådana vid flertalet tillfällen och metoden börjar sätta sig i organisationen parallellt med implementeringen av förvaltningsmodellen PM³. Arbetet har tagit ett stort kliv fram och en prioriteringsordning följer den handlingsplan som tagits fram.

Värt att notera är att det inte är informationstillgången som klassats utan systemet/informationsbäraren.

Samtliga personuppgiftsbehandlingar klassas utifrån vilken typ av personuppgifter som behandlas och lämpligt skydd vidtas för respektive behandling. Detta kan vara behörighetsbegränsning, skydd av lösenord på dokument osv. Detta dokumenteras i DraftIT.

### 2.3.4 DSO anger hur allvarliga bristerna är på en skala

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

.

### 2.3.5 DSO ger råd och rekommendationer till PUA

Fokus under 2024 har varit att identifiera och utse ansvarsroller för förvaltning av informationsbärare. Under 2025 bör nästa steg tas att koppla ihop dessa med processer och informationstillgångar.

Rekommendationen från DSO är att fortsätta se till nästa steg i införandet förvaltningsmodellen av informationssäkerhet och klassificera de processer som ingår i hanteringsanvisningen. Identifierar man processer och inte ser endast till system, blir klassningen av information än mer konkret och verklig.

## 2.4 Konsekvensbedömningar

### 2.4.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av? | Ja |
| Har alla potentiella högriskbehandlingar konsekvensbedömts? | Ja |
| Är de genomförda bedömningarna aktuella? | Ja |

### 2.4.2 Syfte

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 som 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” (artikel 35.1).

### 2.4.3 Resultat

Organisationen arbetar fortsatt med konsekvensbedömningar enligt kraven i dataskyddsförordningen. Rutiner finns på plats. Aktiviteten sker dock fortfarande individberoende, d.v.s. individer har kunskapen men inte bredden vilket kan försvåra processen med att använda det som verktyg.

Med införande av PM[3] blir ansvaret tydligare för vem som ska tillse att resurs avsätts för att uppgiften konsekvensbedömning sker. PM[3] ska införas under 2025 och har en separat handlingsplan utifrån området informationssäkerhet.

Ett område som tidigare belysts i årsrapporterna från dataskyddsombudet avsaknad av process för när det ska ske gemensamma konsekvensbedömningar i staden. Det kan exempelvis bli aktuellt vid en central upphandling av ett IT-system som ska användas av flera organisationer inom staden. Då ingen tydlig process finns angiven från SLK blir det otydligt vem som ska sköta vad och ha ledartröjan i frågorna som uppstår i konsekvensbedömningarna. I dagsläget löser organisationerna ut det ad hoc med upparbetade inofficiella nätverk, men fastnar ofta i slutfaserna då det inte går att färdigställa dokumentationen då riskåtgärder och kravmassa har svårt att omhändertas centralt. En tydlig process ger effektivare, billigare upphandlingar. Det resulterar i en bättre beställarorganisation där stadsdelsförvaltningens krav på säkerhetsåtgärder och verksamhetens önskemål och behov omhändertas på ett korrektare sätt.

Ett tydligt exempel på detta var upphandlingen av nytt centralt IT-system under 2023-2024. En konsekvensbedömning skedde efter att designen var klar och stadsdelsförvaltningarna inte hunnit att få klart dokumentationen och gjort riskanalyserna utifrån sina verksamhetskrav och de registrerades perspektiv. Den fick ske i efterhand med flera öppna frågor. Höga kvarstående risker utan åtgärder kan leda till sanktioner.

Otydlighet vem som får/ har mandat att acceptera risker har också synliggjorts under år 2024. Problemet har lyfts i samarbetet för Trillingen vilket är bra och en förutsättning för att nå framgång i att hitta en lösning.

### 2.4.4 DSO anger hur allvarliga bristerna är på en skala

| | |
|---|---|
| | 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 ej bedöms vara brådskande, omfattande eller allvarliga |
| | Inga brister av nämnvärd betydelse identifierade |

### 2.4.5 DSO ger råd och rekommendationer till PUA

Nämnden behöver fortsatt arbeta för att process för gemensamma konsekvensbedömningar i staden implementeras. Organisationen behöver också tydliggöra hur mandatet är fördelat att äga dataskyddsrisker då dessa kan leda till sanktioner om de inte omhändertas korrekt.

## 2.5 Individens rättigheter

### 2.5.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer? | Kan ej anges då endast nekande registreras enligt Stadsarkivariens gallringsregler. |
| Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar? | Samtliga då inga avvikelser framkommit |

### 2.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) 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 den verksamhet som enligt förordningen är att se som personuppgiftsansvarig – dvs. i stadens fall nämnder och bolag – 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. (Radering, den så kallade ”rätten att bli glömd”, är sällan aktuell i någon större mån eftersom stadens verksamheter lyder under krav på bevarande till följd av offentlighetsprincipen.) Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran. (Notera dock att det finns undantagssituationer angivna i artikel 12.3, där fristen kan förlängas till mer än en månad.)

Dataskyddombudet har en roll i att granska efterlevnaden, identifiera brister samt ge råd och stöd hur processer och rutiner för att tillgodose rättigheterna bör utformas.

Om verksamheten inte klarar av att hantera en begäran från en registrerad person i enlighet med dataskyddsförordningen krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från Integritetsskyddsmyndighetens, IMY:s sida, med sanktioner som

följd. Det är därför viktigt att PUA regelbundet ges en bild av i vilken mån verksamheten klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

### 2.5.3 Resultat

Informationen till den registrerade på start.stockholm är fortsatt bristande och är en fråga som lyfts i dataskyddsombudens nätverk. Informationen har inte uppdaterats sedan 2021 och det har varit svårt att nå fram med de förbättringar som dataskyddsombuden önskar.

När förvaltningen får en begäran löser den ut frågan men rutinerna behöver förbättras och ses över i och med att det finns nya nyckelpersoner i organisationen som behöver utbildas i ämnet.

### 2.5.4 DSO anger hur allvarliga bristerna är på en skala

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

### 2.5.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet ger rådet att fortsätta samarbeta med övrig förvaltningar att i syfte att få bättre och uppdaterad information på start.stockholm till medborgarna.

## 2.6 Personuppgiftsincidenter

### 2.6.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Hur upptäcks personuppgiftsincidenter? | Genom individen/ personalen uppmärksammar dem alt meddelas av personuppgiftsbiträden. |
| Hur många personuppgiftsincidenter har dokumenterats? | 28 |
| 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? | 0 |

### 2.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt Dataskyddsförordningen (artikel 4.12) ”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.”

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland Dataskyddsförordningen olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att de flesta personuppgiftsincidenter ska rapporteras till IMY, inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska

personers rättigheter ska de berörda registrerade personerna, utan dröjsmål underrättas.

Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering till de berörda personerna.

Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY. DSO:ns årsrapportering är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad osv.

### 2.6.3 Resultat

Totalt har 28 st. incidenter med personuppgifter anmälts enligt gällande rutiner under år 2024. En bedömdes vara av den allvarlighetsgraden att den behövde anmälas till IMY, Integritetsskyddsmyndigheten. Stadsförvaltningens incidenthantering bedöms vara **GRÖN**.

Under året har en ny typ av incidenter uppmärksammats. Detta genom att AI-funktioner har implementerats vid centrala uppdateringar utan föregående konsekvensbedömningar. Risker som uppstått är t.ex. att mötesprotokoll genereras automatiskt med hjälp av ett AI där nya personuppgiftsbehandlingar skapas omedvetet och lagras utan tillräckligt skydd. AI- genererade sammanfattningar och utan kritisk granskning, kan göra att en tidigare harmlös personuppgiftsbehandling med tydlig rättslig grund plötsligt är känslig och olaglig.

Vid uppkomna incidenter som berör flera verksamheter inom hela Stockholm stad under året, har det varit tydligt att det inte fungerar med den CERT-funktion som startats centralt. Ett exempel på detta var den stora TietoEvry incidenten i januari som uppmärksammades i media. Lärdomen är att det blir snabbt ryktesspridning om inte tydlig kommunikation med korrekt, transparent och trovärdig information kommer ut vid en incident. Detta kan leda till att stadsförvaltningen inte kan göra relevanta bedömningar och åtgärder. Detta ger en **GUL** bedömning utifrån det centrala arbetet där stadsdelsförvaltningen påverkas negativt pga. andra organisationers brister.

### 2.6.4 DSO anger hur allvarliga bristerna är på en skala

| | |
|---|---|
| | 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 ej bedöms vara brådskande, omfattande eller allvarliga |
| X | Inga brister av nämnvärd betydelse identifierade |

### 2.6.5 DSO ger råd och rekommendationer till PUA

Nämndens ges rådet att fortsätta påverka och uppmuntra det centrala arbetet att utveckla CERT-funktionen vid SLK. Detta för att skapa transparent information och tydliga kontaktvägar vid incidenter.

Kunskap om vad och hur man hanterar personuppgiftsincidenter är en färskvara. Det finns en tydlig korrelation mellan att personalen haft utbildning i Dataskyddsförordningen och en ökad benägenhet att anmäla personuppgiftsincidenter.

Nämnden rekommenderas att ta fram en organisation att omhänderta lessons learned. Det är en naturlig del av det förbättringsarbete som en mer mogen verksamhet kan ta nästa steg emot.

# 3 Genomförda granskningar under året

## 3.1 Sammanfattning

Genomförda granskningar:

- *Granskning 1* Hur väl fungerar den nya ej digitala dataskyddsutbildning?
- *Granskning 2* Granska förskolans införande av ”nya skolplattformen”- Tempus

## 3.2 Syfte

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. För personuppgiftsansvarig är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är.

Granskningsområdena är planerade och aviserade vid 2023-års dataskyddsrapport.

## 3.3 Genomförda granskningar och deras resultat

### 3.3.1 *Granskning 1* Hur väl fungerar den nya ej digitala dataskyddsutbildning?

Vid starten av år 2024 togs ett icke digitalt utbildningsmaterial fram centralt. Detta för att de medarbetare som inte har access till egen dator skulle kunna få information vid APT och i kortare chefsledda lektioner. Utbildningen har inte publicerats och har således inte kunnat granskas.

Formatet är efterfrågat av verksamheterna och i Trillingen-samarbetet har det nu beslutats att ta fram en egen enklare utbildning för APT/ informationsmöten. Tanken är att närmaste chef ska kunna hålla i dragningen av informationen, alternativt enklare och kortare förinspelade föredragningar av dataskyddsombud och/ eller informationssäkerhetssamordnare.

### 3.3.2 *Granskning 2* Granska förskolans införande av ”nya skolplattformen”- Tempus.

Bakgrunden till granskningen är den sanktionsavgift som tilldelats Utbildningsförvaltningen[1] år 2020 av IMY, Integritetsskyddsmyndigheten, för den tidigare IT-tjänsten Skolplattformen. Sanktionsavgiften har fastställts till fyra miljoner.

Under slutet av 2023 och början av 2024 genomfördes dokumentationsarbete av den nya ersättningstjänsten till Skolplattformen. Den kallas Tempus. Farhågor att omhänderta alla steg i dataskyddsarbetet i den korta tidsplanen och behandlingen av risker, har varit en av mina primära arbetsuppgifter som dataskyddsombud under 2024. Granskningen har lett till ett antal åtgärder och uppmärksammande av problem som uppstår när mandat att besluta om risker är otydliga. En annan del är den centrala processen som saknas för gemensamma konsekvensbedömningar belystes igen. Det blev också tydligt att man inte använder konsekvensbedömningen som en del av ett kravarbete vid design och upphandling.

Under 2025 ska nästa del i den gamla skolplattformen ersättas med en ny tjänst kallad Infomentor. Tidsplanen för införandet har skjutits fram och som en del av granskningsarbetet för kommande år har jag som DSO beslutat att fokusera på även detta under 2025. Flera åtgärder och önskemål har lyfts fram vid det första mötet under hösten 2024 där DSO:erna informerades av Utbildningsförvaltningens införandeprojekt av Infomentor. Se vidare kapitel 5.3.1.

## 3.4 DSO ger råd och rekommendationer till PUA

Dataskyddsombudets rekommendation inför 2025 är att fortsätta säkerställa att de digitala utbildningarna inom informationssäkerhet och dataskydd genomförs i organisationen. För att säkerställa att så många som möjligt får kunskapen och att den är aktuell, behöver kortare ”mini” utbildningar som inte är digitala tas fram. Det arbete som redan omnämns under kapitel 3.3.1 är ett gott initiativ för att öka kunskapen om dataskydd och gör det till ett mer välkänt område inom hela organisationen.

[1] https://www.imy.se/nyheter/allvarliga-brister-i-skolplattformen-i-stockholm/ (2025-01-06)

# 4 Risker inom dataskydd

## 4.1 Sammanfattning

Prioriterade risker inom verksamheten:

- Osäker e-posthantering med personuppgifter (Kvarstår)
- Brister inom dokumentationen i informationssäkerhets- och GDPR-frågor (Kvarstår)
- Tredjelandsöverföringar (Kvarstår)
- Skyddade personuppgifter inom förskolan (Kvarstår)
- Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (Stadsdelsförvaltningens) objektförvaltning (Ny)
- Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation (Ny)

## 4.2 Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, men dessa ger inte en heltäckande bild av personuppgiftsriskerna i verksamheten. Dataskyddsombudet behöver som underlag för sin egen planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, i verksamhetens samtliga personuppgiftsbehandlingar. Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som dataskyddsombudet behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

Under år 2024 har en riskanalys genomförts tillsammans med informationssäkerhetssamordnaren för att hitta gemensamma åtgärder.

**Risk beräknas utifrån RISK= Sannolikhet x Konsekvens**

**Sannolikhet (1 låg - 5 hög):**
**Låg risk - Inte trolig att inträffa**
**Hög risk - Kommer med all sannolikhet att inträffa**

**Konsekvens (1 liten - 5 stor):**
**Liten konsekvens - Ingen större påverkan**
**Stor konsekvens - Omfattande, dyrt kan ändra förutsättningarna dramatiskt**

**Riskvärde**
**Låg < 4 (riskerna skall bevakas)**

**Medel 5-14 (riskerna skall hanteras eller elimineras)**

**Hög > 15 (riskerna skall elimineras)**

## 4.3 Resultatet av riskkartläggningen

*Risk 1 Osäker e-posthantering med personuppgifter*
Varje personuppgift som ska hanteras måste behandlas säkert. När en personuppgift e-postas med någon av stadens leveranser sker själva överföringen krypterat, men är okrypterad i in- och utboxen. Det är också inte säkert att maila externt då exempelvis en medborgares adress inte kan kontrolleras på ett tillräckligt bra sätt.

Stadsledningskontoret har tagit fram en tjänst kallad ”Säkra meddelanden” eller ”TDialog”. Kvarstående aktivitet för verksamheten, är att se över och bedöma vad tjänsten kan användas till. I ett större projekt med stadsdelsförvaltningarna i Bromma, Järva, Hässelby-Vällingby och Hägersten-Älvsjö, har konsekvensbedömnings och informationssäkerhetsklassningsarbete samt riskanalys genomförts med verksamhetsrepresentanter, informationssäkerhetssamordnare och dataskyddsombud.

Jag som DSO kan inte rekommendera i dagsläget att tjänsten används efter att jag tagit del av analysmaterialet. Samtidigt är behovet kvarstående från verksamheten att möjligheten att e-posta personuppgifter säkert och krypterat.

Vid denna rapports framtagande är ett projekt med att en gemensam konsekvensbedömning med systembeskrivning, informationsklassning och riskanalys ska ske 2024 av SLK. Detta för att kunna besvara de risker som framkommit inom de verksamheter som gjort ena konsekvensbedömningar och riskanalyser. Rekommendationen att inte använda tjänsten utan att analysmaterialet finns på plats kvarstår, då riskerna inte har besvarats av systemförvaltaren och informationsmängderna som ska skickas i det är så pass känsligt och skyddsvärt.

| | |
|---|---|
| X | Hög > 15 (riskerna skall elimineras) |
| | Medel 5-14 (riskerna skall hanteras eller elimineras) |
| | Låg < 4 (riskerna skall bevakas) |

*Risk 2 Brister inom dokumentationen i informationssäkerhets- och GDPR-frågor (Kvarstår)*

Vid arbete med KLASSA, vilket har varit fokus för stadsdelsförvaltningen i år, framkommer det att det saknas dokumentation (både gemensam och lokal). Vid förfrågan kan sällan förvaltningsplan, systemdokumentation etc. tas fram av leverantören eller den egna förvaltningen. Denna brist är allvarlig och gemensamma mallar för hur och vad dessa dokument ska innehålla behöver tas fram centralt. Risken är att man idag förutsätter det finns dokumentation för att det ”borde finnas” eller man ”antar” att det är på plats.

| | |
|---|---|
| X | Hög > 15 (riskerna skall elimineras) |
| | Medel 5-14 (riskerna skall hanteras eller elimineras) |
| | Låg < 4 (riskerna skall bevakas) |

*Risk 3 Tredjelandsöverföringar (Ny)*

Vid tidigare årsrapporter har risken med tredjelandsöverföringar lyfts upp. Denna risk uppmärksammas så även i år. Detta beror på att flertalet leverantörer av IT-tjänster numera går över till att endast vara molntjänstbaserade och dessa oftast är kopplade till amerikanska företag. Med den nya presidentens tillträde den 20:e januari finns en farhåga att de nuvarande överföringsmekanismerna ska ryckas upp och att det kan finnas integritetsrisker med att använda dessa tjänster.

| | |
|---|---|
| X | Hög > 15 (riskerna skall elimineras) |
| | Medel 5-14 (riskerna skall hanteras eller elimineras) |
| | Låg < 4 (riskerna skall bevakas) |

*Risk 4 Skyddade personuppgifter inom förskolan (Ny)*
Problem har uppdagats under år 2023 att det finns brister inom hanteringen av skyddade personuppgifter inom förskolan. Det gäller både för personal och barn med vårdnadshavare.

| | |
|---|---|
| | Hög > 15 (riskerna skall elimineras) |
| X | Medel 5-14 (riskerna skall hanteras eller elimineras) |
| | Låg < 4 (riskerna skall bevakas) |

*Risk 5 Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (Stadsdelsförvaltningens) objektförvaltning (Ny)*
Som tidigare nämnt flera kapitel har det uppstått problem i införande av nya tjänster beroende på resursbrist hos central förvaltning. Detta påverkar implementation av nya gemensamma IT-tjänster och det systematiska arbetet som ska ske löpande i den egna lokala organisationen.

| | |
|---|---|
| | Hög > 15 (riskerna skall elimineras) |
| X | Medel 5-14 (riskerna skall hanteras eller elimineras) |
| | Låg < 4 (riskerna skall bevakas) |

*Risk 6 Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation (Ny)*
Under år 2024 växte efterfrågan på AI och möjligheten att effektivisera arbetet. Då området är nytt och så även lagstiftningen behövs tydlig och transparent dokumentation när en sådan tjänst ska införas. Tyvärr brister ofta dokumentationen från leverantörerna och den som upphandlar verktyget behöver utbilda dem genom kravställning och möten.

Integritetsriskerna är stora då effektiviteten och möjligheten att ta fram ”smarta lösningar” tenderar att gå först i hela samhället. Mitt arbete som dataskyddsombud blir då i dessa införanden än mer viktigt att agera ombud och skydda de registrerades intressen.

En del i denna risk är också att nya funktioner införs i redan befintliga tjänster. Ett exempel på detta är en transkriberingstjänst vid digitala möten. Efter mötet är klart kommer direkt ett AI-genererat protokoll med sammanfattning, beslutspunkter och åtgärder. Det låter bra, men frågorna vi måste ställa oss då är vart sammanställdes informationen? Vem kan ta del av den? Hur känsligt blev materialet i det nya formatet? AI är ett oerhört bra och kraftfullt hjälpmedel som vi måste använda medvetet och till rätt saker.

| | |
|---|---|
| X | Hög > 15 (riskerna skall elimineras) |
| | Medel 5-14 (riskerna skall hanteras eller elimineras) |
| | Låg < 4 (riskerna skall bevakas) |

## 4.4 DSO ger råd och rekommendationer till PUA

1. Dataskyddsombudets rekommendation för att minimera risken att personuppgifter e-postas utan tillräckligt skydd, är att de risker som kommit fram under projektet att införa tjänsten ”Säkra meddelanden” åtgärdas.

2. Genom att ta fram, implementera och kommunicera tillämpningsanvisningarna för informationssäkerhet och dataskydd kommer ansvaret bli tydligare för vem som ska ta fram dokumentationen som i dag saknas.

3. Nämnden rekommenderas att ta höjd för risken och bestämma aptiten för vad man är villig att riskera när man ingår nya avtal med leverantörer där överföringar till tredjeland sker. Rådet är också att ha en tydlig exitplan och genomlysa marknaden i förstahand inom Sverige och EU/EES. Rutiner för att genomföra TIA, Transfer Impact Assessment, behöver också tas fram.

4. Vid införandet av nya tjänsterna inom förskolan behöver perspektivet skyddade personuppgifter omhändertas särskilt.

5. Att ge råd om hur den centrala organisationen ska få mer resurs att utföra sitt arbete är svårt. Men, vi kan belysa

utifrån Stadsförvaltningens perspektiv att det blir svårt att arbeta effektivt när den brister och det tenderar att byggas flaskhalsar.

6. Som DSO rekommenderar jag att ni fortsätter vara nyfikna på ny teknik och våga satsa på den. Men, rekommendationen är att göra det med stor medvetenhet och arbeta efter den metod som finns framtagen för informationsklassning, riskanalys och konsekvensbedömning. Genvägar blir kostsamma både utifrån sanktioner (både GDPR och AI-förordningen kan ge sanktioner var för sig) men också individens rättigheter får aldrig förminskas eller glömmas bort.

# 5 Planerade granskningar under det nya verksamhetsåret

## 5.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Granskning 1* Granska förskolans införande av Infomentor, en ersättare till Skolplattformen.
- *Granskning 2* Hur väl fungerar den nya icke digitala dataskyddsutbildning?

## 5.2 Syfte

Som nämnts tidigare är det granskande arbetet en av dataskyddsombudets viktigaste uppgifter. Eftersom dataskyddsombudet ofta har begränsat med tid, behöver granskningsplanen för det nya året utformas med eftertanke. Som en tumregel bör två-tre granskningar ses som en rimlig granskningsinsats under ett verksamhetsår. Granskningsområdena bör lämpligen väljas utifrån ett riskbaserat synsätt, det vill säga att fokus bör ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därigenom åstadkoms en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

## 5.3 Planerade granskningar

### 5.3.1 Granskning 1 Granska förskolans införande av nya skolplattformen

Under 2025 ska nästa del i Skolplattformen ersättas med en ny del kallad Infomentor. Tidsplanen för införandet har skjutits fram och som en del av granskningsarbetet för kommande år har jag som DSO beslutat att fokusera på även detta införande. Flera åtgärder och önskemål har lyfts fram vid det första mötet under hösten 2024 där DSO:erna informerades av Utbildningsförvaltningens införandeprojekt av Infomentor. Granskningen syftar till att följa upp att de tidigare lärdomarna som drogs vid det förra projektet nu omhändertas på ett annat sätt och processerna förbättras. Det är också av vikt att individer, både anställda, barn och vårdnadshavare, med skyddad identitet omhändertas på ett korrekt sätt.

### 5.3.2 Granskning 2 Hur väl fungerar den nya icke digitala dataskyddsutbildning?

Den nya dataskyddsutbildningen som ska tas fram för medarbetare som inte har tillgång till egen dator behöver granskas kvalitativt och hur många som deltagit i den samt deras omdöme om den.

# 6 Övrigt att rapportera

## 6.1 Projektgrupp för informationssäkerhet och dataskydd

Gruppen startades våren 2023 för att ta fram och implementera tillämpningsanvisningen för informationssäkerhet. Den har utvecklats under 2024 att fokusera på att ta fram handlingsplan och åtgärder för de brister som identifierats inom dataskydd och informationssäkerhet. Gruppen har fortsatt letts av Maria Palme med deltagande av arkivarie, informationssäkerhetssamordnare, Dataskyddsombud, telefonisamordnare och vid behov även andra medarbetare med specialistkunskaper.

Projektet har med sina gemensamma ögon kunnat bidra med en helhetssyn på området dataskydd och informationssäkerhet. Nämnden ges rådet att fortsätta med denna projektgrupp.

## 6.2 Gemensamt arbete inom Trillingen

Ett fortsatt samarbete med dataskydd och till viss del informationssäkerhet mellan stadsdelsförvaltningarna i Hässelby-Vällingby, Bromma och Järva har fortsatt under benämningen Trillingen. Synergieffekterna är fortfarande desamma och det blir särskilt tydligt när det sker en incident eller vid införanden av nya tjänster.

Under 2025 kommer också ett mer regelbundet arbete ske mellan stadsdelsförvaltningarnas informationssäkerhetssamordnare, en chefsrepresentant och dataskyddsombudet. Detta för att dra nytta av varandras arbete och kunskaper då respektive ISAM har helt olika bakgrund inom teknik, arkivkunskap osv.