Stockholms stad

# Dataskyddsombudets årsrapport 2025

## Bromma Stadsdelsnämnd

start.stockholm

**Dataskyddsombudets årsrapport 2025**
Januari 2026
**Dnr**: BRO 2026/40
**Kontaktperson**: Maria Palme
**Konsult**: Jessica Hillergård

# Sammanfattning

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

Dataskyddsåret som gått har varit präglat av arbete med flera stora konsekvensbedömningar, ny AI-förordning att ta hänsyn till och framförallt nya hot från och i omvärlden. I skrivandets stund vid årsskiftet, har kartan ritats om på vem som är allierad och inte vilket påverkar vilka tekniska val en organisation behöver ta och prioritera.

Ett område som påverkas av omvärlden, är frågorna om tekniska säkerhetsåtgärder, AI och tredjelandsöverföringar. I årets dataskyddsraport lyfts tredjelandsöverföringar in som ett eget kapitel. Slutsatsen är att med övergång till fler molntjänster behöver beställaren vara än mer tydlig i sina krav på leverantörerna. Detsamma gäller tjänster med AI, där risken finns att nya oväntade personuppgiftsbehandlingar skapas och lagras osäkert. Där rekommenderar jag som DSO att det tas fram en AI-riktlinje och -strategi i staden så att stadsdelsförvaltningen kan luta sig mot dem hur nästa steg i digitaliseringen ska ske.

En årsrapport 2025 kan inte utesluta den stora personuppgiftsincidenten i slutet av augusti och som utvecklades med nya vändningar under hela hösten. I dagsläget har IMY, Integritetsskyddsmyndigheten, bestämt att inte inleda granskning mot Stockholm stad och dess stadsdelsförvaltningar, utan mot två kommuner, en region och leverantören. Det som är tydligt i min slutsats av årets incidenter, är att det behöver bli tydligare kommunikationsvägar när incidenter sker. DSO informeras sent och riskerar att sakna pusselbitar när rekommendationer ska ges. Miljödataincidenten kommer också bli vägledande vad som krävs innan personuppgiftsbehandlingar börjar, att det gäller även från implementationsstadiet och kan inte göras i efterhand.

IMY har också omorganiserats vid årsskiftet och får en operativ avdelning som kommer arbeta med riskbaserad tillsyn och klagomål. Det tyder på att personuppgiftsansvarig behöver ha god kontroll på sina dataskyddsrisker och arbeta aktivt med dem. Risker redovisas i ett eget kapitel som jag uppmanar dig som läsare att ta del av lite extra.

Med förhoppning om ett spännande och säkert dataskyddsår!

*Jessica Hillergård*

*Dataskyddsombud*

## Innehåll

**Sammanfattning ..... 3**
**1. Inledning ..... 6**
1.1. Bakgrund ..... 6
1.2. Beskrivning och förklaring av granskningsmetod och resultat ..... 6
1.3. Obligatoriska rapporteringsområden ..... 8
**2. Resultatsammanställning och centrala iakttagelser inom dataskyddsarbetet ..... 9**
*2.1. Registerförteckning ..... 9*
*2.1.1. Syftet med området ..... 9*
*2.1.2. Resultat ..... 9*
*2.1.3. Sammanfattning ..... 10*
*2.1.4. DSO ger råd och rekommendationer till PUA ..... 10*
*2.2. Tekniska och organisatoriska åtgärder ..... 11*
*2.2.1. Syftet med området ..... 11*
*2.2.2. Resultat ..... 11*
*2.2.3. Sammanfattning ..... 12*
*2.2.4. DSO ger råd och rekommendationer till PUA ..... 13*
*2.3. Konsekvensbedömning avseende dataskydd ..... 14*
*2.3.1. Syftet med området ..... 14*
*2.3.2. Resultat ..... 14*
*2.3.3. Sammanfattning ..... 15*
*2.3.4. DSO ger råd och rekommendationer till PUA ..... 16*
*2.4. Den registrerades rättigheter ..... 17*
*2.4.1. Syftet med området ..... 17*
*2.4.2. Resultat ..... 17*
*2.4.3. Sammanfattning ..... 18*
*2.4.4. DSO ger råd och rekommendationer till PUA ..... 18*
*2.5. Personuppgiftsincidenter ..... 19*
*2.5.1. Syftet med området ..... 19*
*2.5.2. Resultat ..... 19*
*2.5.3. Sammanfattning ..... 20*
*2.5.4. DSO ger råd och rekommendationer till PUA ..... 21*
*2.6. Överföring till tredje land ..... 22*
*2.6.1. Syftet med området ..... 22*
*2.6.2. Resultat ..... 22*
*2.6.3. Sammanfattning ..... 22*
*2.6.4. DSO ger råd och rekommendationer till PUA ..... 23*
**3. Genomförda granskningar under året ..... 24**
*3.1. Sammanfattning ..... 24*
*3.2. Syfte ..... 24*

*3.3. Genomförda granskningar och deras resultat ..... 24*
*3.3.1. Granskning 1 Granska förskolans införande av Infomentor ..... 24*
*3.3.2. Granskning 1 Utbildning i dataskydd ..... 25*
*3.4. DSO ger råd och rekommendationer till PUA ..... 25*
**4. Risker inom dataskydd ..... 26**
*4.1. Sammanfattning ..... 26*
*4.2. Syfte ..... 26*
*4.3. Resultatet av riskkartläggningen ..... 27*
*4.4. DSO ger råd och rekommendationer till PUA ..... 31*
**5. Planerade granskningar under det nya verksamhetsåret ... 33**
*5.1. Sammanfattning ..... 33*
*5.2. Syfte ..... 33*
*5.3. Planerade granskningar ..... 33*
*5.3.1. Granskning 1 Förskolans införande av Infomentors nya modul för specialpedagogik ..... 33*
*5.3.2. Granskning 2 Utbildning i dataskydd ..... 33*
*5.3.3. Granskning 3 AI (Styrdokument och metod för infoklassning och anpassning mot AI-förordningen och GDPR) ..... 34*
**6. Omvärldsbevakning ..... 35**
*6.1. Tillsynsmyndigheten omorganiseras ..... 35*
*6.2. Kommande förändringar av Dataskyddsförordningen ..... 35*
*6.3. Tillsyn av Miljödata incidenten ..... 35*
*6.4. Övrigt ..... 36*
**7. Övrigt att rapportera ..... 37**
*7.1. Interna arbetsgruppen med ambassadörer för dataskydd och informationssäkerhet ..... 37*
*7.2. Gemensamt arbete inom Trillingen ..... 37*
*7.3. Samarbete och kommunikation i dataskydd i staden ..... 37*

# 1. Inledning

## 1.1. Bakgrund

Dataskyddsförordningen, GDPR, 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 eller styrelse 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 personuppgiftsansvarig att ta emot de råd och rekommendationer som dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen. I rapporten får personuppgiftsansvarig insyn i vad dataskyddsombudets granskningar visat av verksamheten och status avseende integritet och dataskydd. Årsrapporten syftar till att personuppgiftsansvarig ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd eller styrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att personuppgiftsansvarig ska kunna visa att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna dokumenteringsskyldighet. Årsrapporten är även ett medel för personuppgiftsansvarigs uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

## 1.2. Beskrivning och förklaring av granskningsmetod och resultat

Dataskyddsombudet 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 dataskyddsombudet 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 som kräver åtgärder. |

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

## 1.3. 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
- Tekniska och organisatoriska säkerhetsåtgärder i samband med personuppgifts behandling[1]
- Konsekvensbedömningar
- Överföring till tredje land
- Individens rättigheter
- Personuppgiftsincidenter

Utöver dessa obligatoriska områden rapporteras även om de fördjupade granskningar som skett under föregående år samt planerade granskningsaktiviteter för år 2026. Ett specifikt kapitel om risker och omvärldsbevakning är också prioriterat i rapporten för att underlätta beslut angående dataskyddsarbetet framåt för personuppgiftsansvarig.

[1] I tidigare årsrapporter är denna punkt uppdelat i rubrikerna ”tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar” och ”styrdokument”

# 2. Resultatsammanställning och centrala iakttagelser inom dataskyddsarbetet

## 2.1. Registerförteckning

### 2.1.1. Syftet med området

I GDPR framkommer det att personuppgiftsansvariga (och personuppgiftsbiträden) ska föra ett register över sina personuppgiftsbehandlingar. Registret brukar benämnas ”behandlingsregister” eller ”registerförteckning”. Registret ska finnas tillgängligt i elektronisk form och ska omfatta samtliga personuppgiftsbehandlingar som personuppgiftsansvarig utför. Det ska hållas uppdaterat vilket innebär att det ska uppdateras vid nya eller förändrade personuppgiftsbehandlingar.

Syftet med detta rapporteringsområde är att beskriva om verksamheten har ändamålsenliga rutiner som möjliggör att nya/förändrade personuppgiftsbehandlingar registreras, huruvida personuppgiftsbehandlingar registreras/uppdateras såsom det krävs samt huruvida de uppgifter som är obligatoriska har besvarats kopplat till de registrerade personuppgiftsbehandlingarna.

### 2.1.2. Resultat

Registerförteckningen finns i det digitala verktyget DraftIT. Det har funnits problem med användarvänligheten i verktyget då behörighetsnivåerna inte varit lämpliga. Under sommaren var det även problem med att granska och validera registerförteckningen. Men, hösten 2025 släpptes en ny version av plattformen och felen åtgärdades av leverantören. Det nya utseendet och behörighetsnivåerna kommer innebära nya möjligheter att ge läs- och ändringsbehörigheter på en mer detaljerad nivå. I samarbetet för Trillingen kommer Järva att gå ut först i den nya plattformen som pilot, Bromma och Hässelby-Vällingby står därefter på tur att gå över under vintern 2026 till den nya plattformen.

Rekommendationen inför 2025 var att ge en kortare utbildning i DraftIT så att ambassadörerna lättare skulle kunna uppdatera registerförteckningen. Under det gånga året har delar av ambassadörerna uppdaterat i sina behandlingar men det finns behov av att flera gås igenom och uppdateras. Dock var det som tidigare nämnt stora problem under sommaren med verktyget då flera signaler kom att det inte gick att skicka in behandlingar för granskningar/ slutföra dem då och medarbetarna brukar ha tid att jobba med arbetsuppgiften under den perioden.

### 2.1.3. Sammanfattning

| Fråga/kontroll | Risk | Rekommendationer |
|---|---|---|
| Antal behandlingar som är registrerade? | | *186* |
| Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar? | | *Verksamheten har rutiner och utpekat ansvar att uppdatera.* |
| Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför? | | *Registerförteckningen saknar uppdateringar på en del områden. Uppdateringar sker efter aktiviteter i årshjulet.*<br><br>*Det är bra att hänvisning till hanteringsanvisningen finns kopplat till varje personuppgiftsbehandling.* |
| Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna? | | *Registerförteckningar har identifierat de personuppgiftsbehandlingar som finns i organisationen och kopplat dem till hanteringsanvisningen. Dock behöver vissa informationsluckor täppas till. Det kommer med sannolikhet lättare kunna göras i den nya plattformen som är mer användarvänliga och det går att fokusera bättre på obligatoriska frågor.* |

### 2.1.4. DSO ger råd och rekommendationer till PUA

Under vintern 2026 kommer den nya plattformen implementeras och under våren behöver dataskyddshandläggarna utbildas i det nya formatet. De som inom stadsdelsförvaltningen har rollerna systemägare behöver även de få en information om verktyget.

## 2.2. Tekniska och organisatoriska åtgärder

### 2.2.1. Syftet med området

Personuppgiftsansvarig ska tillse att personuppgifter skyddas med lämpliga säkerhetsåtgärder, detta för att till exempel undvika att obehöriga får tillgång till uppgifterna, att uppgifterna förloras eller förstörs.

Personuppgiftsansvarig behöver alltid bedöma vilka tekniska- och organisatoriska säkerhetsåtgärder som ska vidtas för de behandlingar som utförs. Till tekniska säkerhetsåtgärder räknas till exempel kryptering, behörighetsbegränsning, pseudonymisering och säkerhetskopiering. Organisatoriska säkerhetsåtgärder avser till exempel interna riktlinjer och rutiner.

För att skapa förutsättningar för att skydda all information inom verksamheten och ha rätt nivå på skyddsåtgärder, ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare.

Genom att använda arbetssättet i metodhandboken värderas informationen utifrån konfidentialitet, riktighet och tillgänglighet. Verktyget KLASSA hjälper sedan till att ta fram tekniska och organisatoriska krav att ställa internt och mot leverantörer. Detta innefattar även bedömning och värdering av personuppgifter. Genom att genomför riskanalyser identifierar informationsägaren risker och väljer åtgärder för att hantera riskerna.

Den personuppgiftsansvariga måste kunna visa hur GDPR efterlevs och att det finns styrdokument och rutiner är en viktig del i detta. Det görs genom att det finns skriftliga, beslutade och kommunicerade styrdokument samt kända rutiner så att medarbetarna vet hur de ska agera avseende frågor som rör dataskydd.

Syftet med detta rapporteringsområde är att redogöra för huruvida DSO bedömer att det tas hänsyn till risker för den registrerade och om dessa beaktas i tillräcklig mån i genomförda informationsklassningar och riskanalyser samt att rätt bedömningen för både tekniska och organisatoriska åtgärder är gjorda. Vidare bedömer DSO också huruvida det finns tillräckligt mycket reglerat om dataskydd i styrdokument och rutiner samt om dessa är tillräckligt implementerade och kända.

### 2.2.2. Resultat

Tidigare år har jag noterat att det är svårt för medarbetare att hitta de lokala rutinerna för dataskydd och informationssäkerhet på intranätet. Den iakttagelsen kvarstår då det fortfarande är en hel del klickande och scrollande för att hitta rätt. Styrdokumenten som finns är bra och pedagogiska men behöver uppdateras och synliggöras 2026.

Under 2025 har flera gemensamma informationssäkerhetsklassningar och dataskyddsworkshops skett. Några att flagga extra för är de inom ”Sociala system” som kopierat Trillingens modell för samarbete under året. Det har inneburit att stadsdelsförvaltningarna i staden delat upp sig i tre block och på det sättet bidragit med medarbetare ur olika kompetenser. Det har lett till mer korrekta analyser och underlag som sedan kunnat mer effektivt anpassas till varje respektive personuppgiftsansvarigs egna behov och rutiner.

Det finns fortfarande brister inom andra verksamhetsområden från central förvaltning, där informationen sent kommer till ISAM och DSO så att det blir svårt att implementera tjänster för verksamheten. Ett exempel på det är Miljödata incidenten som omnämns i kapitel 2.5. Ett annat exempel på bra samarbete är förskolans arbete med Infomentor. Se kapitel 2.3.2.

Som dataskyddsombud har jag återkommande avstämningar med ISAM från både hela Trillingen månadsvis, och enskilda veckomöten med varje respektive stadsdelsförvaltnings ISAM. Det som bland annat tas upp på dessa avstämningar är utförda informationssäkerhetsklassningar och resultat. DSO är också involverad i de informationsklassningar där de registrerade är i fokus som informationsmängd och konfidentialitetsnivån är bedömd som hög.

Bromma har under året påbörjat informationsklassningar av processer för att få kontroll över flöden av information och inte bara enskilda system. Arbetet utgår från hanteringsanvisningen och synkas med riskarbetet som sker av säkerhetssamordnaren och ISAM. Ett bra arbete som fortgår 2026.

### 2.2.3. Sammanfattning

| Fråga/kontroll | Risk | Rekommendationer |
|---|---|---|
| Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att | | *Verksamheten är bra på att informationsklassa. Dock är det personberoende av nyckelmedarbetare.* |

| | | |
|---|---|---|
| resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter? | | |
| Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd? | | *Styrande dokument är bra och pedagogiska, men behöver en mindre uppdatering. Bland annat saknas hur AI:n ska behandlas.* |
| Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända? | | *Styrande dokument är svåra att hitta för medarbetare på intranätet på grund av dess utseende att de publiceras långt ner på en sida som innebär mycket scrollande.* |

### 2.2.4. DSO ger råd och rekommendationer till PUA

Rekommendationen från tidigare år kvarstår att förbättra synligheten för de styrande dokumenten på intranätet.

Rådet för informationssäkerhetsklassningar och arbetet med verktyget KLASSA är att fortsätta enligt den inslagna effektivare vägen och regelbundna avstämningar. Önskemålet är också att utbildning sker av samtliga chefer som kan bli föremål för att ta emot information om nya system och IT-tjänster så att de kan fånga upp och förmedla information när dem får det.

## 2.3. Konsekvensbedömning avseende dataskydd

### 2.3.1. Syftet med området

En konsekvensbedömning avseende dataskydd krävs när personuppgiftsansvarig planerar att inleda en personuppgiftsbehandling som innebär hög risk för de registrerade. Huruvida en behandling innebär hög risk eller inte behöver personuppgiftsansvarig avgöra genom att genomföra en s.k. tröskelanalys.

En konsekvensbedömning ska vara genomförd för samtliga behandlingar som innebär hög risk, vilket innebär att personuppgiftsansvarig även behöver kontrollera huruvida denne utför befintliga behandlingar som innebär hög risk. Om högriskbehandlingar utfös för vilka en konsekvensbedömning inte har gjorts, behöver personuppgiftsansvarig genomföra en sådan.

Genom att genomföra en konsekvensbedömning kan personuppgiftsansvarig identifiera risker med en personuppgiftsbehandling, hantera riskerna genom åtgärder och rutiner samt påvisa ansvarsskyldighet. Genom konsekvensbedömningar kan risker identifieras och förebyggas samt korrekta och relevanta skyddsåtgärder identifieras i kravställning på leverantörerna.

Syftet med detta rapporteringsområde är att rapportera huruvida verksamheten har ändamålsenliga rutiner som möjliggör att tröskelanalyser och konsekvensbedömningar genomförs, huruvida sådana genomförs när det krävs samt huruvida personuppgiftsansvarig har genomfört konsekvensbedömningar för de behandlingar som kräver det.

### 2.3.2. Resultat

Under det gånga året har IMY, Integritetsskyddsmyndigheten levererat mer vägledningar än bestraffningar. Det har bland annat syns genom ett mycket bra material innehållande vägledning och mallar för konsekvensbedömningar. Stadsdelsförvaltningen har anpassat sina mallar efter detta.

Stadsdelsförvaltningen och samarbetet i Trillingen, har genomfört flera konsekvensbedömningar under året. En av dem är ersättaren till Skolplattformen kallad Infomentor.

Ett av de området som fortfarande brister är de stadsgemensamma konsekvensbedömningarna som saknar process. I dagsläget är de dokument som tas fram alldeles för generellt hållna och har inte haft med verksamhetsrepresentanter eller dataskyddsombud. Det leder till att det blir merarbete lokalt på stadsdelsförvaltningen och många frågetecken att försöka reda ut i efterhand. Det förekommer också

händelser där personuppgiftsansvarig tvingas använda en tjänst utan att den är färdigdokumenterad.

### 2.3.3. Sammanfattning

| Fråga/kontroll | Risk | Rekommendationer |
|---|---|---|
| Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys? | | *Det finns ett förklassningsprotokoll där bland annat frågan om personuppgifter lyfts och det ska bifogas en bilaga (ny 2025) som heter tröskelanalys. Bilagan behöver implementeras mer under 2026.* |
| Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar? | | *En diskussion har tidigare genomförts och dokumentation i handlingsplan och förklassningsprotokoll om frågan om fullständig konsekvensbedömning ska göras. Dokumentationen i det nya protokollet som omnämns ovan behöver implementeras bättre under 2026.* |
| Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd? | | *Lokal nivå- JA* |
| | | *Stadsgemensamma konsekvensbedömningar genomförs ad hoc och efter att det är nyckelpersoner som tar initiativ. Det behöver bli tydligare process och rollfördelning för att detta ska bli mer effektivt.* |
| Genomförs | | *Lokal nivå- JA* |

| | | |
|---|---|---|
| konsekvensbedömning avseende dataskydd i de fall det krävs? | | *Centrala system delvis* |
| Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta? | | *Lokal nivå JA* |
| | | *Det finns brister som påtalats av lokala medarbetare till centrala funktioner.* |

### 2.3.4. DSO ger råd och rekommendationer till PUA

Rådet som personuppgiftsansvarig får är att fortsätta den inslagna vägen med samarbeten. Det är också en rekommendation att det tas fram en central process för metod och roller i referenskonsekvensbedömningarna så att de kan användas mer effektivt lokalt. Den nya bilagan för tröskelanalys behöver implementeras under 2026.

## 2.4. Den registrerades rättigheter

### 2.4.1. Syftet med området

Den registrerade har ett antal rättigheter enligt GDPR. Den registrerade kan bland annat begära tillgång (registerutdrag), rättelse eller radering. Den som är personuppgiftsansvarig har att tillmötesgå en begäran enligt de krav som finns i dataskyddsförordningen. (För registerutdrag säger GDPR 30 dagar och för övriga begäran skyndsamt.)

Syftet med detta rapporteringsområde är att kontrollera huruvida det finns ändamålsenliga mallar samt rutiner för besvarande av rättighetsbegäran, huruvida inkomna begäranden har hanterats inom den tidsram som finns att förhålla sig till samt huruvida svaren till de registrerade, baserat på ett antal stickprov, uppfyller lagkraven.

### 2.4.2. Resultat

Stadsförvaltningen har interna rutiner för hur begäran ska omhändertas från registrerade. Under det gånga året har begäran om registerutdrag inkommit en dessa registreras inte i diariet enligt hanteringsanvisningen. Det är endast nekade beslut som diarieförs.

En rättighet den registrerade har är att lämna klagomål och begära skadestånd. I samband med Miljödataincidenten inkom också krav på ersättning från tidigare anställda som fått sina personuppgifter röjda. (De handläggs av SLK juridiska avdelning.)

Ett av förbättringsområden som kvarstår sedan tidigare år är informationen till de registrerade på externwebben start.stockholm. Ärendet har lyfts av samtliga stadsdelsförvaltningars DSO:er och är ett pågående område som vi försöker trycka på ska bli bättre. Det är svårt för en stadsdel att presentera sin egen information om personuppgiftsbehandlingar då det inte finns en hemsida att publicera det på.

### 2.4.3. Sammanfattning

| Fråga/kontroll | Risk | Rekommendationer |
|---|---|---|
| Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade? | | *Det finns interna instruktioner men är inte publicerade på intranätet.* |
| Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade? | | *Antalet har inte diarieförts då de raderas så fort begäran inkommit och färdigställts. Endast nekande begäran diarieföres enligt hanteringsanvisningen.* |
| Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad? | | *Inga avvikelser har identifierats.* |
| Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven? | | *Ja* |

### 2.4.4. DSO ger råd och rekommendationer till PUA

Arbetet med att omhänderta registrerades begäran om rättigheter är bra och fungerar. Rådet är att se över rutinerna och sprida dem under 2026 samt påverka att informationen till den registrerade blir bättre på externwebben.

## 2.5. Personuppgiftsincidenter

### 2.5.1. Syftet med området

Med begreppet personuppgiftsincident avses 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.

Om en inträffad personuppgiftsincident medför en risk/ konsekvens för fysiska personers rättigheter och friheter ska den anmälas till Integritetsskyddsmyndigheten, IMY, inom 72 timmar från att den upptäckts. Om personuppgiftsincidenten sannolikt leder till hög risk för de registrerade måste individen informeras utan onödigt dröjsmål. Om en personuppgiftsincident inte bedöms vara anmälningspliktig ska den dokumenteras. Det görs i verktyget IA.

Syftet med detta rapporteringsområde är att kontrollera huruvida det säkerställs att samtliga medarbetare har den kunskap som krävs om personuppgiftsincidenter, huruvida det finns ändamålsenliga rutiner för att hantera händelser som kan utgöra personuppgiftsincidenter och huruvida dessa rutiner följs.

### 2.5.2. Resultat

Det finns rutiner för hur personuppgiftsincidenter ska hanteras och utredas. Det fungerar bra lokalt, men kan bli svåra att hantera när incidenterna är stadsgemensamma.

Främst är kommunikationsvägarna inte alltid tydliga och information kommer sent fram till DSO som får kunskap ofta flera steg från källan. Med det menar jag att en incident upptäcks eller förmedlas från central IT-förvaltning/ IT-leverantör, som i sin tur kontaktar sin kontakt på central förvaltning vid ex. SLK, Stadsledningskontoret. Därefter kontaktar de olika personer i verksamheten vid varje separat tillfälle, likt direktören, HR-chef, ISAM, IT-ansvarig osv. som i sin tur informerar ISAM och/eller DSO. (Ibland informeras ISAM först och därefter DSO vilket lägger till ett steg.) Då det är olika medarbetare som har olika intresseområden som får budskapet, riskerar informationen att bli förändrad av misstag och det blir svårt att ge korrekt råd som dataskyddsombud när delar av pusslet saknas.

#### Miljödataincidenten

I slutet av augusti 2025 spreds nyheten att IT-tjänsteleverantören Miljödata hade drabbats av en IT-attack. Det tog sedan ett par dagar innan det uppmärksammades för stadsdels- och fackförvaltningarna att även medarbetare där var drabbade. Detta då den centrala HR-avdelningen har påbörjat att implementera deras arbetsmiljöverktyg på delar av staden utan att information framkommit till DSO och

ISAM om personuppgiftsbehandlingen. Under veckorna som följde och utredningen vidgades, klarnade också bilden för alla inblandade. Det som är problematiskt är att främst personuppgiftsansvaret inte var utrett, f.d. anställda och även vissa med skyddad ID har förts över i implementationsfasen. Anmälningar i ärendet har skett till IMY vartefter uppdateringar har framkommit i ärendet.

Stadsdelsförvaltningen har försökt att följa incidenten och meddela sina medarbetare och omhändertagit de med skyddad ID som drabbats. En hel del frågor inkom initialt från oroliga medarbetare. När rapporten skrivs har ännu inte slutrapporten och lessons learned meddelats från SLK då utredning pågår. Integritetsskyddsmyndigheten har inte beslutat att i det första läget granska Stockholm stads användning av Miljödatas verktyg. Mer om granskningen kan läsas i kapitlet 6.3.

Tydligt är att incidenten kommer leda till en klar syn på vad som behöver göras innan en sådan här personuppgiftsbehandling kan starta och att det gäller även innan man testar tjänster.

### 2.5.3. Sammanfattning

| Fråga/kontroll | Risk | Rekommendationer |
|---|---|---|
| Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident? | | *Samtliga medarbetare genomgår en digital dataskyddsutbildning varje år.*<br><br>*Dataskyddshandläggarna påminns på varje kvartalsträff där ämnet är en stående informations- och diskussionspunkt.* |
| Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa? | | *Lokalt följs de rutiner som finns.* |
| | | *När incidenter sker med personuppgifter i centrala system är inte kommunikationsvägarna tydliga och det blir en del förvirring. Det tar lång tid innan DSO och ISAM får information vilket försvårar arbetet.* |

| | | |
|---|---|---|
| | | *Lessons learned kommuniceras inte från centrala funktioner med DSO:er utan oftast endast med ISAM eller andra medarbetare. Därav blir det svårt att bedöma hur hela staden och också i slutändan verksamheten i stort drar lärdom av incidenter och förbättras.* |
| Hur många personuppgiftsincidenter har dokumenterats under året? | | *21* |
| Hur många personuppgiftsincidenter har anmälts till IMY under året? | | *1* |

### 2.5.4. DSO ger råd och rekommendationer till PUA

Som ett led av händelserna med Miljödataincidenten så är det tydligt att det är viktigt att öva och testa sina incidentrutiner.

Kommunikationsvägar och förberedelser är A och O då det uppstår mycket snabba behov av beslut och åtgärder. Rådet är att under 2026 öva och testa organisationen med en personuppgiftsincident likt den som drabbade staden 2025. Rollerna i ett incidentteam behöver vara tydliga, kommunicerade och våga även att involvera personer utanför ordinarie kristeam.

## 2.6. Överföring till tredje land

### 2.6.1. Syftet med området

För att säkerställa att den nivå av skydd för personuppgifter som ställs i GDPR inte undergrävs, får överföringar av personuppgifter till länder utanför EU/EES (tredje land) endast ske under särskilda förutsättningar. Det innebär att sådan överföring måste stödjas på antingen ett beslut från EU-kommissionen om att landet ifråga upprätthåller en adekvat skyddsnivå, att överföringen omfattas av en lämplig skyddsåtgärd eller i särskilda undantagsfall. Vidare behöver även kompletterade skyddsåtgärder, utöver de lämpliga skyddsåtgärderna, vidtas i vissa fall.

Syftet med detta rapporteringsområde är att rapportera huruvida personuppgiftsansvarig har identifierat de tredjelandsöverföringar som utförs, huruvida personuppgiftsansvarig tillämpar överföringsverktyg på de tredjelandsöverföringar som utförs och om nödvändiga bedömningar har gjorts avseende tredjelandsöverföringarna.

### 2.6.2. Resultat

I tidigare rapporter har tredjelandsöverföringar angetts som en risk. Nytt för 2025 årsrapport är att detta är ett separat kapitel.

Stadsdelen har en god insyn i vad tredjelandsöverföringar innebär och det är ett område som ofta diskuteras. Det finns en spridd kompetens som gör att frågor ställs i merparten av tillfällen om ett verktyg är bra att använda eller inte baserat just på detta kriterium. Medarbetarna som har insyn försöker också att hitta alternativ aktivt. Stadsdelsförvaltningen använder sig av tredjelandsöverföringar, men omhändertas korrekt under 2025 genom analys och medvetenhet.

Tredjelandsöverföringar är problematiska om de inte analyseras korrekt och att rätt avtal finns för underbiträden som leverantörer använder sig utav. Tredjelandsöverföringar är fortsatt omnämnt som en risk av den anledningen.

### 2.6.3. Sammanfattning

| Fråga/kontroll | Risk | Rekommendationer |
|---|---|---|
| Har personuppgiftsansvarig identifierat de | | *De tredjelandsöverföringar som finns är identifierade i verksamheten.* |

| | | |
|---|---|---|
| tredjelandsöverföringar som utförs? | | |
| Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs? | | *När tredjelandsöverföringar har varit aktuella finns det omnämnt hur de omhändertagits i personuppgiftsbiträdesavtalets instruktion.* |
| Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar? | | *När tredjelandsöverföring är aktuell efterfrågas TIA av leverantören/ personuppgiftsbiträdet. Denna bedöms sedan av ISAM och DSO som ger rekommendation om fortsatt progress eller inte med leverantören.* |

### 2.6.4. DSO ger råd och rekommendationer till PUA

Sannolikheten att tredjelandsöverföringar kommer öka, är stor i och med att flera IT-leverantörer flyttar sina tjänster från on-prem (egna servrar) till molntjänster. Under 2026 rekommenderas organisationen att arbeta aktivt med att informera utvalda medarbetare om tredjelandsöverföringar. Det finns också ett behov

av att bestämma vilken riskaptit verksamheten har för tredjelandsöverföringar exempelvis genom en molnstrategi.

Det är en utmaning att upphandla tjänster och förvirring finns hos leverantörerna om vad som gäller. Därför är det viktigt att verksamheten fortsätter vara en bra kravställare och kan fånga upp otydligheter med rätt frågeställningar till leverantörer

# 3. Genomförda granskningar under året

## 3.1. Sammanfattning

Genomförda granskningar:

- *Granskning 1* Granska förskolans införande av Infomentor, en ersättare till Skolplattformen
- *Granskning 2* Utbildning i dataskydd

## 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 2024-års dataskyddsrapport.

## 3.3. Genomförda granskningar och deras resultat

### 3.3.1. Granskning 1 Granska förskolans införande av Infomentor

Bakgrunden till granskningen är den sanktionsavgift som tilldelats Utbildningsförvaltningen[2] år 2020 av IMY, Integritetsskyddsmyndigheten, för den tidigare IT-tjänsten Skolplattformen. Sanktionsavgiften har fastställts till fyra miljoner. I årsrapporten redovisades granskning om det första steget i förnyelsen oh då modulen kallad Tempus. Det fanns brister i det införandet och farhågor att inte skyddade personuppgifter skulle omhändertas korrekt.

Granskningen 2025 är av nästa steg i implementationen av en ny digital plattform som kallas Infomentor. Det är positivt att projektet har dragit lärdom och utvecklats sedan början av arbetet med Tempus. Det har varit lätt att hitta information och tidsplanen realistisk. Skyddad ID omhändertas bra och det har lett att risker

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

omhändertagits korrekt. De frågeställningar som kvarstod i projektets slutskede var snabbt besvarade och vid behov åtgärdade.

Under 2026 kommer en ny modul implementeras i Infomentor. Det är för specialpedagogik och kommer innehålla mycket känslig information om barn. Därför kommer jag att granska detta också då tidsramarna är snävare och personuppgifternas natur ännu mer känslig.

#### 3.3.2. Granskning 1 Utbildning i dataskydd

Det har tidigare identifierats att flera medarbetare inte har en egen dator eller saknar möjlighet att genomgå den digitala utbildningen. Tanken var att i Trilling-nätverket ta fram en icke-digital utbildning som skulle kunna användas på informationsträffar i organisationen. Under 2025 har detta fått nedprioriteras och rekommendationen kvarstår att utbildning behöver spridas i organisationen och då även till de utan egen dator.

Det framkommer också i mailutskick till ISAM, att 2026 kommer inte certifieringen finnas kvar att medarbetaren klarat utbildningen. Det innebär också att inga automatiska påminnelser kommer skickas ut till medarbetare att genomgå utbildningen och det blir upp till organisationens chefer att påminna alla att gå utbildningen.

### 3.4. DSO ger råd och rekommendationer till PUA

Vad som framkommer i granskningen av Infomentor så har lärdomar av tidigare implementationer av nya system inom förskolan, omhändertagits i projektet. Det är ett bra exempel på när samarbete där projektet har varit lyhört mot verksamhetsbehov och önskemål om metod från ISAM och DSO:er.

Rekommendationen till personuppgiftsansvarig är att 80 procent av medarbetarna ska genomgå en utbildning i dataskydd under 2026. Riktvärdet är med tanke på medarbetare som kan vara långidsfrånvarande av olika anledningar. För att fortsätta ha ett gott systematiskt arbete med dataskydd är kunskap A och O för verksamheten.

# 4. Risker inom dataskydd

## 4.1. Sammanfattning

Prioriterade risker inom verksamheten:

1. Osäker e-posthantering med personuppgifter (Kvarstår)
2. Brister inom dokumentationen i informationssäkerhets- och GDPR-frågor (Kvarstår)
3. Tredjelandsöverföringar (Kvarstår)
4. Skyddade personuppgifter inom förskolan (Kvarstår)
5. Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (Stadsdelsförvaltningens) objektförvaltning (Kvarstår)
6. Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation (Kvarstår)
7. Användning av appar (Ny)
8. Lagringsytor utan kontroll (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.

**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 (Kvarstår)*

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.

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.

Rekommendationen kvarstår att inte använda tjänsten utan att analysmaterialet finns färdigt. Riskerna har inte besvarats av central förvaltning, då ny tillsattes november 2025, 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.

Under 2025 har tjänster införts utan att dokumentationen är färdigställd centralt vilket påverkar personuppgiftsansvarigs efterlevnad av GDPR. Positiva initiativ till förbättring finns i IT-projekt men det är på grund av handlingskraftiga nyckelpersoner.

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

### *Risk 3 Tredjelandsöverföringar (Kvarstående)*

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. Att använda en tjänst som innefattar tredjelandsöverföringar behöver analyseras både ur konfidentialitetsperspektivet men också tillgänglighet. Organisationen måste vara beredd att med kort varsel inte kunna använda en tjänst.

Med ökad osäkerhet i omvärlden är det här en risk som kvarstår som hög.

| | |
|---|---|
| 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 (Kvarstående)*

Problem har uppdagats under år 2023 och 2024 att det finns brister inom hanteringen av skyddade personuppgifter inom förskolan. Det gäller både för personal och barn med vårdnadshavare. Eftersom ny modul ska införas under 2026 med snäva tidsramar behöver risken fortsatt bevakas.

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

### *Risk 5 Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (Stadsdelsförvaltningens) objektförvaltning (Kvarstår)*

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. Under slutet av 2025 tillfördes resurs men vid rapportens framställning har inte den kommit igång.

| | |
|---|---|
| | 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 startade efterfrågan på AI och möjligheten att effektivisera arbetet. År 2025 har det blivit än mer vardag och efterfrågan ökar konstant. 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? Osv. AI är ett oerhört bra och kraftfullt hjälpmedel som vi måste använda medvetet och till rätt saker.

AI-förordningen har också tillkommit under 2025 vilket ställer högre krav på den som upphandlar tjänster att ha kontroll på sina informationsflöden. Staden saknar ett styrande dokument likt AI-riktlinje och AI-strategi. Det gör det svårt för stadsdelsförvaltningen att själva bestämma väg i frågorna.

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

### *Risk 7 Vitlistning av appar och användning av digital utrustning*

Det går att ladda ner appar i tjänstetelefonerna och använda sitt eget AppleID utan begränsning när rapporten skrivs. Detta gäller dock ej förskolan som har teknisk lösning för detta på plats.

Att lägga in sitt AppleID kan innebära att information riskerar att synkas felaktigt vilket har lett till sanktionsavgift för Tullverket[3].

Risk finns att appar laddas ner och används av andra än tjänstepersonen under privat tid. T.ex. ett barn använder tjänstemobiltelefonen för spel.

[3] https://www.imy.se/nyheter/sanktionsavgift-mot-tullverket-for-bristande-rutiner/

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

*Risk 8 Lagringsytor utan kontroll*

I den nya plattformen Nordic for Zoom (ersätter ZoomX) kommer det finnas möjlighet att dela dokument och skapa egna grupper fritt för samarbete både inom den egna organisationen och med andra. En bra möjlighet, men i en gemensam mapp eller i en samarbetsyta på SharePoint kan administratörer med särskild behörighet följa upp och gallra information som inte längre är relevant. I Nordic for Zoom finns inte denna administrativa kontroll vilket gör att kraven i dataskyddsförordningen om transparens (registerutdrag) och lagringsminimering inte kan efterlevas.

| | |
|---|---|
| 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.

7. Vitlistning och styrning av appar behöver implementeras på samtliga digitala kommunikationsverktyg. Det behöver också finnas en uppdaterad gemensam riktlinje för mobiltelefoner får användas privat. Det är stor skillnad på hur mobiler används mot hur det var för ett par år sedan och i dagsläget. Det är inte längre så att mobiltelefonen används för telefonsamtal, det är mer en dator i miniformat som kan innebära en sårbarhet om den används felaktigt.

8. Under arbetet med införande av Nordic for Zoom behöver risken omhändertas. En rekommendation är att minst skapa en organisatorisk åtgärd med rutiner och förbud, om det inte går att tekniskt stänga av filöverföring, begränsa lagringstiden eller på annat sätt kontrollera ytorna.

# 5. Planerade granskningar under det nya verksamhetsåret

## 5.1. Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Granskning 1* Förskolans införande av Infomentors nya modul för specialpedagogik
- *Granskning 2* Utbildningar i dataskydd
- *Granskning 3*: AI (Styrdokument och metod för infoklassning och anpassning mot AI-förordningen och GDPR)

## 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 Förskolans införande av Infomentors nya modul för specialpedagogik

Under 2026 ska nästa modul i Skolplattformen ersättas med en ny del kallad Infomentor specialpedagogik. Tidsplanen är den här gången snäv och det gör att jag som DSO vill fortsätta hålla området extra under lupp. Granskningen syftar till att följa upp att de tidigare lärdomarna som drogs vid tidigare projektet. Det är betydligt mer integritetskänsliga uppgifter som kommer hanteras i denna modul vilket gör att området prioriteras även under år 2026.

### 5.3.2. Granskning 2 Utbildning i dataskydd

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.

### 5.3.3. Granskning 3 AI (Styrdokument och metod för infoklassning och anpassning mot AI-förordningen och GDPR)

Den nya tekniken är här för att stanna och det saknas styrande dokument för hur området ska omhändertas. Under 2026 kommer jag som DSO att följa upp kvalitet på styrande dokument, hur väl de efterlevs och hur användarvänliga de är.

# 6. Omvärldsbevakning

## 6.1. Tillsynsmyndigheten omorganiseras

Den 1:a januari 2026 omorganiserades Integritetskyddsmyndighetens, IMY:s, operativa del. Det har nu inrättats en avdelning för tillsyn och klagomål och en för vägledning, innovation och teknik. Syftet är att:

- stärka myndighetens förmåga att genomföra riskbaserad tillsyn,
- stärka myndighetens förmåga att ge tydlig och effektiv vägledning samt
- effektivisera myndighetens hantering av klagomål

Sannolikt kommer det här leda till fler tillsyner baserade på klagomål och som pressmeddelandet säger, genomföra riskbaserade granskningar av organisationer. Det innebär att organisationen behöver ha god kontroll över sina dataskyddsrisker och arbeta aktivt med dem.

## 6.2. Kommande förändringar av Dataskyddsförordningen

Ett förslag har lämnats från Europakommissionen i november på förändringar i dataskyddslagstiftningarna inom EU. Förslaget syftar främst till att öka möjligheten för innovation och minska administrativa krav på mindre verksamheter. Förslaget var helt annorlunda än det som levererades som första utkast sex månader tidigare då fokus var att minska kravet på registerförteckning.

Analysen jag som DSO gör är, att områdets fokusområden svänger fort men tydligt är att en organisation fortsatt behöver vara en tydlig beställare till leverantörer av IT-tjänster och ha kontroll på sina legala- och informationssäkerhetskrav. Behovet av att göra riskanalyser och tänka till före och ta medvetna risker är en viktig fortsatt nyckelaktivitet inom dataskyddsarbetet.

## 6.3. Tillsyn av Miljödata incidenten

Under hösten 2025 skedde en större personuppgiftsincident hos leverantören Miljödata. Den berörde även delar av Stockholm stad då Stadsledningskontorets HR-avdelning hade beslutat att använda plattformen leverantören erbjöd. Stadsdelsförvaltningens medarbetare och tidigare anställda från och med januari 2024 har i och med läckan hamnat på Darknet. (Se vidare under kapitel 2.5.2) Med anledning av IT-angreppet och den efterföljande läckan av personuppgifter har Integritetsskyddsmyndigheten, IMY, beslutat att inleda granskningar mot Miljödata samt två kommuner och en

region som har använt företagets tjänster. (Göteborgs stad, Älmhults kommun och Region Västmanland)

Urvalet av de granskade aktörerna har gjorts baserat på typ av verksamhet som bedrivs och indikationer på risker då det var många aktörer berörda. Det finns i nuläget inga planer på ytterligare granskningar från IMY men det är heller inte uteslutet att det kommer att ske. Granskningarna kommer bli vägledande i hur en organisation måste agera innan en personuppgiftsbehandling sker.

### 6.4. Övrigt

IMY har mer fokus på vägledning än bestraffning sedan ett år tillbaka. Det innebär att en organisation kan söka delaktighet i regulatoriska sandlådor där man testar sig fram till ex. ett nytt AI skulle kunna användas.

Under år 2025 lättades kamerabevakningslagen upp. Ett område som troligen kommer att granskas under 2026 av tillsynsmyndigheten är nog att efterlevnaden av lagen, dokumentationskrav och bedömningar.

# 7. Övrigt att rapportera

## 7.1. Interna arbetsgruppen med ambassadörer för dataskydd och informationssäkerhet

Den interna arbetsgruppen för GDPR och informationssäkerhet med representanter från verksamheterna har börjat arbeta under året som gått. Den har hunnit med att träffas tre gånger. Aktiviteter som de arbetat med är registerförteckningen och förstå DraftIT samt hjälpa sin verksamhet att komma igång med att ta fram egna rutiner för dataskydd och informationssäkerhet. Det arbetar fortgår under 2026.

## 7.2. 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.

När vi gick in i år 2025 hade vi som ambition att arbeta närmare varandra i Trillingen på informationssäkerhetssamordnarna, ISAM och DSO. Så har skett och resultatet har blivit mycket bra, så bra att det är en kvalitetsstämpel om deltagare från Trillingen varit med i framtagande av underlag.

Under 2026 kommer fortsatt ett regelbundet arbete ske mellan stadsdelsförvaltningarnas informationssäkerhetssamordnare ISAM, 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.

## 7.3. Samarbete och kommunikation i dataskydd i staden

Stadsdelsförvaltningarnas DSO:er har ett informellt nätverk kallat ”GUG, GDPR Utan Gränser”. Nätverkets syfte är att användas som bollplank och säkerställa att alla DSO:er inte ska gå på samma frågor som andra DSO:er redan arbetar med och minska belastningen på rådgivande verksamheter likt SLK juridiska avdelning. Nätverket är välfungerande och har även med DSO:er från fackförvaltningar och bolag samt arkivarie och ISAM. Det finns inget formellt nätverk för DSO:er sedan 2020 i Stockholm stad, därför är det här samarbetet än viktigare att vårda.