Stockholms stad

Bilaga 11

GDPR Årsrapport

År 2024

Hägersten-Älsvjö stadsdelsförvaltning

GDPR årsrapport
Januari 2025

Dnr: HÄ 2025/37
Utgivningsdatum: 2025-01-17
Kontaktperson: David Persson

1 Bakgrund

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 och bolagsstyrelse 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”). DSO:n 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 nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnd eller bolagsstyrelse ska kunna *visa* att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna *dokumenteringsskyldighe*t. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

2 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

Ur ett GDPR-perspektiv var 2024 ett år präglat av fortsatt fokus på dataskydd, särskilt i ljuset av teknologiska framsteg och nya regleringar. Några viktiga händelser och trender inkluderar:

- **Ökat fokus på AI och dataskydd**: Med den snabba utvecklingen av artificiell intelligens (AI) och dess användning i olika sektorer, växte diskussionen kring hur GDPR påverkar datainsamling och bearbetning för AI-applikationer. Det fanns en ökad oro för att AI kan innebära risker för integriteten, vilket ledde till nya vägledningar och tolkningar av reglerna för att säkerställa att AI-lösningar inte strider mot dataskyddslagarna.
- **Fler sanktioner och böter**: Flera stora företag och organisationer fick böter för GDPR-överträdelser, vilket förstärkte vikten av att följa regleringen. Myndigheter fortsatte att granska stora tech-företag för bristande transparens i datainsamling och användning.
- **Utveckling av ePrivacy-förordningen**: Diskussionerna om den nya ePrivacy-förordningen, som syftar till att reglera elektronisk kommunikation och cookie-användning, fortsatte. Det är en kompletterande lag till GDPR och väntas påverka hur företag samlar in och hanterar data via digitala plattformar.
- **Förstärkning av individers rättigheter**: Fler initiativ togs för att säkerställa att individers rättigheter till åtkomst, rättelse och radering av data inte bara respekterades utan också genomfördes på ett effektivt sätt. Ökad transparens och tydlig information till användare om hur deras data används blev en prioritet.

Dataskyddsombudet (DSO) för Hägersten-Älsvjö har främst under året arbetat med incidenthantering samt involverande i större granskningsarbeten för Zoom X, Tempus, AiAi, TDialog, med flera.

När det kommer till granskningen av Zoom X under 2024 har kraven länge funnits på att hitta en ny lösning för digital kommunikation. Det befintliga verktyget Skype har blivit föråldrat och uppdateras inte av leverantören i den takt som behövts. Stockholm stad har nu implementerat en europeisk variant av Zoom kallad ZoomX och är baserad i Tyskland. Verktyget infördes under hösten 2023 och har under 2024 gått igenom en slutlig granskning för godkänt användande.

Det har även under året fortsatt funnits ett behov av att kunna skicka e-post krypterat. Under 2024 har man gjort en ny ansträngning inom nämnden att ta tjänsten TDialog i bruk. Ett granskningsarbete genomfördes under hösten och systemet är nu godkänt av ledningen.

När det kommer till det generella GDPR-arbetet har en stor del av arbetet under 2023 gått ut på att öka medvetenheten hos medarbetare och det har visat resultat under 2024. Fler personuppgiftsincidenter anmäls, fler system har granskats under 2024 om man jämför med 2023 och verksamheten kan på ett bra sätt ta hand om förfrågningar ifrån medborgare eller andra typer av individer vars personuppgifter verksamheten behandlar.

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, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter.

Nedan redogörs för nämndens eller bolagets status och DSO:s slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:s genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	299
Har nödvändiga uppdateringar gjorts?	Nej, pågår en revidering av registerförteckningen
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Nej, men det pågår ett arbete för nya rutiner och instruktioner

3.1.2 Syfte

När en registerförteckning är upprättad skapar den en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras av verksamheten. Registerförteckningen är därför dataskyddsarbetets centrala utgångspunkt och bas samt att den säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all typ av personuppgiftsbehandling. Det är därför viktigt att PUA får information om hur komplett verksamhetens förteckning är. Om dokumenteringskravet uppfylls kan verksamheten arbeta effektivt, systematiskt, riskbaserat och samtidigt värna om individens integritet, särskilt när känsliga och särskilt skyddsvärda personuppgifter behandlas av verksamheten.

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.

3.1.3 Resultat

Registerförteckningen har under året genomgått en översyn där man har gått igenom och modifierat verktyget där PUA ska registrera sina behandlingar. En instruktion som går igenom hur detta ska gå till för den som registrerar behandlingarna är under just nu under arbete och ska sedan kommuniceras ut till ansvariga.

3.1.4 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

3.1.5 DSO ger råd och rekommendationer till PUA

Kvarstående från 2023: Nästa steg för förvaltningens arbete med registerförteckningen är att implementera de roller som anges i förvaltningsmodellen PM3 som Stockholms stads verksamheter ska följa. I den finns roll 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 behandlingar.

Ny rekommendation: För underlättande av bra hantering med registerförteckningen bör en instruktion tas fram för att kunna hantera detta centralt i DraftIt. Denna information bör också kommuniceras ut till verksamheterna med syfte att hålla registerförteckningen uppdaterad och aktuell.

3.2 Styrdokument

3.2.1 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

3.2.2 Syfte

Området syftar till att PUA genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att PUA 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 dokumenterade, 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 dataskyddsförordningens principer för behandling av personuppgifter efterlevs.

En brist inom detta område bör ses som en brist i förhållande till direkta GDPR-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 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 kunna fatta rätt beslut om.

3.2.3 Resultat

Under 2023 och början av 2024 arbetade man med att implementera tillämpningsanvisningar för både informationssäkerhet och dataskydd. Dessa rutiner, inklusive kontaktvägar finns nu på plats via intranätet för samtliga medarbetare att ta del av.

3.2.4 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
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

3.2.5 DSO ger råd och rekommendationer till PUA

Hägersten-Älvsjö stadsdelsförvaltningsnämnd rekommenderas att fortsätta arbetet med PM3 och arbetet med att se över att intranätets informationsmaterial uppdateras på regelbunden basis.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

3.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	16
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

För att skydda information (inklusive personuppgifter) med adekvata 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. 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 eller inte. Om en ansvarig för klassningen inte har pekats ut och känner till sitt ansvar för klassning, minskar sannolikheten avsevärt att klassningsarbetet initieras.

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

Eftersom informationsklassning är ett arbete som utförs 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.

3.3.3 Resultat

Under 2024 har 6 system informationsklassats, vilket innebär en ökning från 2023 där enbart 3 system informationsklassades. Däremot är det en betydande mängd system (totalt 107 stycken) som ännu inte har klassats.

Under 2024 har DSO varit involverad i ett flertal granskningar och metoden är generellt sett bra inarbetad i organisationen. Däremot sker många av dessa granskningar fortfarande ad-hoc.

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.

3.3.4 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
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.3.5 DSO ger råd och rekommendationer till PUA

Rekommendation ifrån DSO är att fortsätta arbetet med att informationsklassa fler system eftersom majoriteten av system i dagsläget inte är klassade. Informationsklassningsarbetet behöver ligga som grund så att verksamheten i nästa steg har möjlighet till att införa relevanta och adekvata skyddsåtgärder för att skydda de personuppgifter som verksamheten behandlar.

3.4 Konsekvensbedömningar

3.4.1 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

3.4.2 Syfte

Konsekvensbedömning hjälper verksamheten 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 personuppgiftsbehandling, samt att bedöma sannolikheten och konsekvensen om ett specifikt riskscenario skulle inträffa. Baserat på bedömningen bör då 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).

3.4.3 Resultat

Verksamheten arbetar med konsekvensbedömningar. Rutiner finns på plats i tillämpningsanvisningen. Aktiviteten sker dock individberoende, d.v.s. individer har kunskapen men inte bredden vilket kan försvåra processen med att använda verktyget. I dessa fall finns DSO att bistå som en hjälpande hand genom processen.

Under 2024 har en stor konsekvensbedömning av förskolans nya närvaroplattform utförts samt ett flertal andra konsekvensbedömningar av mindre system.

Problemet som ofta uppstår är tidspress i det här arbetet då konsekvensbedömningar görs väldigt sent i upphandlingsfasen av tjänster.

3.4.4 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

3.4.5 DSO ger råd och rekommendationer till PUA

Konsekvensbedömningar som verktyg skapar bättre kravställningar redan i designstadiet och förenklar/förtydligar i avtal och kommunikation med leverantörer och dess underleverantörer. I förvaltningsmodellen PM3 är det ett ansvarsområde som tilldelas en specifik roll. Vid implementering av modellen kommer det att förflytta individberoendet vilket det är idag, till ett mer systematiskt använt verktyg.

Nämnden behöver också fortsatt arbeta för att en process för gemensamma konsekvensbedömningar i staden implementeras samt att det behöver finnas en tydlig instruktion när det kommer till vilka ansvarsområden verksamheten har för att möjliggöra en korrekt bedömning.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	2
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	2

3.5.2 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.

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 Intetgritetsskyddsmyndighetens (IMY:s) sida, med sanktioner som följd. Det är därför viktigt att PUA regelbundet ges en bild av i 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 vilken mån verksamheten klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

3.5.3 Resultat

Inga avvikelser sker då personalen är engagerad och löser ut frågor som uppstår inom tidsramen för de lagstadgade kraven.

3.5.4 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

3.5.5 DSO ger råd och rekommendationer till PUA

Nämnden rekommenderas att gå igenom och kontrollera interna rutiner för att på så sätt kunna tillgodose dessa begäran på ett bättre sätt. Detta kommer att medföra snabbare hantering och att mindre resurser behöver användas för att kunna hantera en sådan typ av begäran.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom medborgare, personal som upptäcker incidenten och meddelar därefter DSO för rådgivning
Hur många personuppgiftsincidenter har dokumenterats?	24
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	3
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	3

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen (artikel 4.12) följande: ”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 dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering och 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 en betydande del av alla 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 de fysiska personers rättigheter ska de berörda registrerade personerna, utan dröjsmål underrättas.

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

3.6.3 Resultat

Nämnden har generellt en god uppmärksamhet på att upptäcka personuppgiftsincidenter. När en sådan skett vill personalen också gärna åtgärda eventuella brister och se över rutiner och processer omedelbart. Incidenter lyfts också i styrgruppen för informationssäkerhet och dataskydd samt nätverket för dataskydd/ informationssäkerhetsambassadörer. På det sättet sprids kunskap brett om så kallade ”lessons learned” efter en incident.

3.6.4 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
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

3.6.5 DSO ger råd och rekommendationer till PUA

DSO:s rekommendation gällande hantering av personuppgiftsincidenter är att få ökad kunskap i vilka ansvarsområden varje roll i incidentprocessen har. Till exempel så är det PUA:s ansvar att rapportera incidenten till IMY om man bedömer att en rapportering ska ske. Det finns tillfällen där det råder bristande förståelse om detta ansvar och bör därför ytterligare förtydligas och förankras i verksamheten.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Tempus
- Zoom X
- AiAi
- TDialog

4.2 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.

4.3 Genomförda granskningar och deras resultat

Granskning 1 - Tempus

Tempus syftar till att hantera närvaro, frånvaro och personalplanering i förskolans verksamhet. Systemet behandlar personuppgifter för barn, vårdnadshavare och personal. Systemet ska stödja verksamhetens behov av att hantera närvaro och personalplanering i verksamheten på ett säkert sätt. Samt samla in underlag för statistik gällande närvaro.

Granskningen har under våren 2024 utförts enligt de rutiner och processer som gäller vid införande av en ny tjänst till driftstart. Det som snabbt uppdagades under detta arbete var att tjänsten kommer att behandla en stor mängd med personuppgifter i och med att systemet bland annat hanterar förskolans närvaro hos eleverna. Utifrån informationsklassningen utfördes sedan en riskanalys där ett flertal risker kopplat till personuppgifter upptäcktes och några av dessa var av allvarlig karaktär. Däremot minskar verksamheten riskvärdet avsevärt med diverse åtgärder som dokumenterats i

riskanalys-dokumentet. Det finns dock fortfarande risker kvar efter att åtgärderna kommit på plats som behöver monitoreras på regelbunden basis.

	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

Granskning 2 – Zoom X

Som en del i digitaliseringsarbetet har Stadsledningskontoret under 2024 beslutat att köpa in Zoom X för digital kommunikation.

De personuppgifter som behandlas genom användandet av Zoom X varierar i viss del beroende på ändamålet med den specifika behandlingen. Detta kan i vissa fall kopplas till vilken verksamhet av staden som använder Zoom X. På ett generellt plan kan det konstateras att behandlingen av personuppgifter genom Zoom X i många fall kan vara olika former av rörliga bilder på fysiska personer som deltar i ett videomöte och namn på deltagare. Vidare kan personuppgifter som framgår av samtal behandlas; dels avseende deltagare i konversationer, dels avseende externa personer som inte deltar i konversationer men vars personuppgifter behandlas genom att digitala samtal rör dem. Utöver detta behandlas ett fåtal personuppgifter kopplade till användarkonton.

Under granskningen upptäcktes ett flertal risker med användandet av tjänsten men dessa kunde minimeras kraftigt med skyddande åtgärder på både teknisk och administrativ nivå.

Nedan följer dataskyddsombudets bedömning av Zoom X:
Då totalsträckskrypteringen är implementerad och används som standard kan Zoom X användas under förutsättning att denna funktion är påslagen. För chattar och fildelning ska Advanced Chat Encryption vara aktiverat.

Flertalet risker är sänkta med administrativa åtgärder, vilket gör att utbildning/information är en viktig kontrollpunkt att förmedla

och genomföra till alla medarbetare. Detta ska också påminnas systematiskt. När möjlighet finns ska dessa administrativa åtgärder ersättas/minimeras med tekniska lösningar för att uppfylla ”dataskydd som standard”.

	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

Granskning 3 - AiAi

Aiai är ett verksamhetssystem som är utvecklad för insatsen personlig assistans. Systemet möjliggör digital schemaläggning för personal, tidsrapportering till Försäkringskassan samt dokumentation om enskilda brukare. Aiai har funnits i verksamheten sedan ett flertal år tillbaka. Systemet hade dock inte klassats tidigare.

Under granskningen upptäcktes ett flertal risker med användandet av tjänsten kopplat till personuppgiftsbehandlingar men dessa kunde minimeras med skyddande åtgärder på både teknisk och administrativ nivå. Det finns dock fortfarande risker kvar efter att åtgärderna kommit på plats som behöver monitoreras på regelbunden basis.

	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

Granskning 4 - TDialog

Stadsledningskontoret har tagit fram en tjänst kallad ”Säkra meddelanden” även kallad ”TDialog”. I ett större projekt under 2022 med stadsdelsförvaltningarna i Bromma, Järva, Hässelby-Vällingby och Hägersten-Älvsjö, har konsekvensbedömnings och informationsklassningsarbete samt riskanalys genomförts med verksamhetsrepresentanter, informationssäkerhetssamordnare och dataskyddsombud. Kvar fanns en mängd frågetecken och behov av riskåtgärder för att denna aktivitet kunde gå i mål. Dåvarande DSO kunde därför inte rekommendera att tjänsten skulle tas i bruk.

Under 2024 gjorde man i nämnden ett försök till att igen prova detta system och det gjordes en granskning i en mindre skala. Problemet med denna granskning var att samma risker som identifierades 2022 fortfarande fanns kvar utan någon handlingsplan för hur man ska gå tillväga för att hantera dessa. Vilket innebär att rekommendationen kvarstår till att inte använda tjänsten då riskerna inte har besvarats och hanterats av systemförvaltaren. Systemet kommer också att potentiellt behandla väldigt känsliga personuppgifter vilket styrker denna rekommendation.

X	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
	Inga brister av nämnvärd betydelse identifierade

4.4 DSO ger råd och rekommendationer till PUA

Dataskyddsombudets rekommendationer är att först och främst fortsätta med arbetet att granska system oavsett om det är system som ännu inte är upphandlade eller om det är system som redan idag är i bruk. Detta är en grundförutsättning för att få koll på vilka personuppgifter som behandlas och hur de behandlas. Det krävs då att man utför en informationsklassning och en eventuell konsekvensbedömning samt riskanalys.

Den andra rekommendationen är att på regelbunden basis se över de åtgärder i redan granskade system som har syfte att minska eller eliminera risker. Syftet med den övningen är få ett grepp om huruvida dessa åtgärder fungerar i praktiken och om de faktiskt åtgärdar riskerna som de ska.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- Osäker e-posthantering med personuppgifter (kvarstående)
- Tredjelandsöverföringar (kvarstående)
- Skyddade personuppgifter inom förskolan (kvarstående)
- Användning av ännu ej granskade system (ny)

5.2 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.

5.3 Resultatet av riskkartläggningen

Risk 1 – Osäker e-posthantering med personuppgifter (kvarstående)

Varje personuppgift som ska hanteras måste behandlas säkert. När en personuppgift e-postas med någon av stadens leveranser sker själva överföringen krypterat, men är icke krypterad i när det ligger i inboxen. Det är också inte säkert att maila externt då exempelvis en medborgares adress inte kan kontrolleras och verifieras på ett tillräckligt bra sätt.

Stadsledningskontoret har tagit fram en tjänst kallad ”Säkra meddelanden” även kallad ”TDialog”. I ett större projekt under 2022 med stadsdelsförvaltningarna i Bromma, Järva, Hässelby-Vällingby och Hägersten-Älvsjö, har konsekvensbedömnings och informationssäkerhetsklassningsarbete samt riskanalys genomförts med verksamhetsrepresentanter, informationssäkerhetssamordnare och dataskyddsombud. Kvar fanns en mängd frågetecken och behov

av riskåtgärder för att denna aktivitet kunde gå i mål. Dåvarande DSO kunde därför inte rekommendera att tjänsten skulle tas i bruk.

Under 2024 gjorde man i nämnden ett försök till att igen prova detta system och det gjordes en granskning i en mindre skala. Problemet med denna granskning var att samma risker som identifierades 2022 fortfarande fanns kvar utan någon handlingsplan för hur man ska gå tillväga för att hantera dessa. Tjänsten används tillsammans med en särskild riktlinje, men ett flertal risker kvarstår.

X	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
	Inga brister av nämnvärd betydelse identifierade

Risk 2 – Tredjelandsöverföringar (kvarstående)

Det nya inriktningsbeslutet från stadsledningskontoret som kom under hösten 2023 innebar en öppning för stadsdelsförvaltningarna att använda leverantörer som använder sig av tredjelandsöverföringar. Förutsättningen är att verksamheten har en väl utformad exit-plan om överföringsmekanismen ”Data Privacy Framwork” ogiltigförklaras likt ”Privacy Shield” gjorde år 2020 och ”Safe Harbour” innan dess.

Flertalet leverantörer erbjuder idag endast molntjänster och de stora leverantörerna av sådana är amerikanskägda. Därför är detta en risk som behöver uppmärksammas extra.

	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

Risk 3 – Skyddande personuppgifter inom förskolan (kvarstående)

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.

Införandet av Tempus under 2024 sänker denna risk ifrån orange till gul. Risken kvarstår till viss del då Tempus inte är ett heltäckande skydd mot en felaktig hantering av skyddade personuppgifter inom förskolan.

	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

Risk 4 – Användning av ännu ej granskade system

Tidigare i denna rapport framgår det att nämnden har många system i bruk som ännu inte har granskat ur varken ett informationssäkerhets- eller personuppgifts-perspektiv. Detta medför en stor risk då det blir svårt att ha koll på vilken information som flödar igenom dessa system, samt hur skyddsåtgärderna ser ut för specifika system. I dagsläget har exempelvis enbart 16 av 107 system informationsklassats. Det behövs en satsning här för att granska fler system då det är en grundförutsättning för att få styrning på vilka personuppgifter som behandlas och hur de behandlas i systemen. Det krävs då att man utför en informationsklassning och en eventuell konsekvensbedömning samt riskanalys.

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

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

5.4 DSO ger råd och rekommendationer till PUA

Dataskyddsombudets rekommendation för att minimera risken att personuppgifter e-postas utan tillräckligt skydd, är att de risker som kommit fram under projektet med ”TDialog” åtgärdas.

Risken att tredjelandsöverföringsproblematiken kommer att uppstå igen är sannolikt rätt stor. 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.

Vid införandet av nya skolplattformen ombads man i 2023 års rapport att omhänderta perspektivet skyddade personuppgifter med särskild noggrannhet. Nämnden rekommenderas även detta år att fortsätta med detta arbete för att säkerställa att hanteringen av skyddade personuppgifter i förskolan sker på ett säkert sätt.

Slutligen rekommenderas nämnden att satsa på att granska fler system då det i dagsläget är för få system som har granskats. Det som krävs är att man behöver utföra informationsklassningar, konsekvensbedömningar samt riskanalyser för de system som ännu inte gått igenom denna process.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Registerförteckning och DraftIt
- Uppföljning av befintliga rutiner och processer
- Uppföljning av redan granskade system

6.2 Syfte

Det granskande arbetet en av dataskyddsombudets huvudsakliga uppgifter. 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.

6.3 Planerade granskningar

Granskning 1 - Registerförteckning och DraftIt

Under 2024 påbörjades arbetet med att överse processer och rutiner för nämndens registerförteckning. Anledningen till detta är att nuvarande registerförteckning under tidigare år inte har hållits uppdaterad med relevanta uppgifter. Arbetet under 2024 har inneburit rensning av gamla uppgifter och behörigheter samt att mallen för registrering av personuppgifter har justerats och förenklats med syfte att det ska bli enklare för ansvariga att registrera sina uppgifter i systemet.

Under 2025 kommer detta arbete att fortsätta med att ta fram en instruktion och rutin för att kunna börja använda denna mall i DraftIt. När den är på plats behöver den nya instruktionen kommuniceras ut till verksamheterna så att den kan börja användas och hållas uppdaterad.

Granskning 2 - Uppföljning av befintliga rutiner och processer

Den planerade granskningen syftar till att följa upp och utvärdera organisationens rutiner och processer för att säkerställa efterlevnad av GDPR. Fokus kommer att ligga på områden som

informationssäkerhetsklassningar, registerförteckning, hantering av registrerades rättigheter, incidentrapportering, personalutbildning samt hantering av externa leverantörer. Målet är att identifiera eventuella förbättringsområden, stärka dataskyddet och säkerställa att nämnden följer GDPR:s krav för att minimera risker och säkerställa skyddet av personuppgifter.

Granskning 3 – Uppföljning av redan granskade system

En planerad granskning kommer att genomföras för att följa upp redan granskade system ur ett personuppgiftsperspektiv. Syftet är att säkerställa att hanteringen av personuppgifter fortsatt sker enligt gällande lagstiftning, riktlinjer och interna processer. Fokus kommer att ligga på att följa upp de eventuella risker eller brister i dataskyddet som upptäckts vid den initiala granskningen, samt att bedöma om tidigare rekommendationer och åtgärder har implementerats och fått önskad effekt. Granskningen ska bidra till att stärka säkerheten och integriteten för de personuppgifter som behandlas i systemen.