Stockholms stad

Bilaga 7 till
VB 2023

GDPR Årsrapport

År 2023

Farsta stadsdelsnämnd

GDPR årsrapport
Januari 2024

Dnr: FAR 2023/924
Utgivningsdatum: 2024-01-23
Kontaktperson: Charlotte Sundvall

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. Farsta stadsdelsnämnd är personuppgiftsansvarig (”PUA”) för alla personuppgiftsbehandlingar som sker inom ramen för nämndens verksamheter.

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 nämnden ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

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

Ordlista

PUA = Personuppgiftsansvarig, i det här fallet Farsta stadsdelsnämnd
DSO = Dataskyddsombud
IMY= Integritetsskyddsmyndigheten, tillsynsmyndighet för GDPR
GDRP = General Data Protection Regulation, i Sverige kallat dataskyddsförordningen

Innehåll

2 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport. Årsrapporten spänner över sex obligatoriska rapporteringsområden, riskmatris för dataskydd samt andra genomförda granskningar under året.

Årets granskning visar att PUA under 2023 har vidtagit flera åtgärder för att stärka arbetet med dataskydd i nämndens verksamheter. Bland annat har takten för informationsklassningar av verksamhetssystem ökat jämfört med tidigare år vilket satt fokus på implementering av nödvändiga organisatoriska och tekniska skyddsåtgärder för skydd av personuppgifter. Flera konsekvensbedömningar än tidigare har genomförts samtidigt som det skapats en förvaltningsövergripande organisation för implementering och omhändertagande av dataskyddsarbetet. Utbildning i dataskydd har prioriterats och flera rutiner har uppdaterats. Genom en systeminventering har också PUA skapat sig en bättre bild över vilka system används inom verksamheterna samt gjort en prioriteringsordning för informationsklassning av system. Inventeringen är också en grund för planerad uppdatering av registerförteckning samt för att kartlägga vilka behandlingar som behöver konsekvensbedömas.

Trots att PUA vidtagit flera åtgärder har årets granskning identifierats brister inom varje obligatoriskt rapporteringsområde under framtagandet av årsrapporten. Bristerna bedöms ligga på samma nivåer som tidigare år. I vissa fall handlar det omfattande brister med behov av omgående åtgärder, i andra delar handlar det om åtgärder som behöver åtgärdas men som inte bedöms vara lika omfattande och brådskande. Precis som föregående års rapport så visar granskningen på störts brister när det gäller registerförteckningen, organisatoriska och tekniska skyddsåtgärder samt avsaknaden av konsekvensbedömningar.

Granskningen visar även att det finns utmaningar inom stadens organisation när det gäller nämndens ansvar i relation till andra personuppgiftsansvariga nämnder inom staden i system som är stadsgemensamma. DSO:s bedömning är att det försvårar PUA:s dataskyddsarbete. Dels då det emellanåt är svårt att få rätt underlag och information i samband med klassningar, dels otydlig information vid incidenthantering.

DSO rekommenderar fortsatt PUA att utveckla arbetet med registerförteckningen, öka takten i informationsklassningen av system i syfte att vidta lämpliga organisatoriska och tekniska skyddsåtgärder samt genomföra konsekvensbedömningar för de personuppgiftsbehandlingar som har behov av det. DSO rekommenderar också PUA att föra en dialog med stadsledningskontoret kring organisation, rutiner och ansvar för stadsgemensamma verksamhetssystem.

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som 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 status och DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	392 st
Har nödvändiga uppdateringar gjorts?	Delvis
Bedöms registerförteckningen vara fullständig?	Delvis
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

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

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

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

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

PUA har upprättat en registerförteckning i systemet ”Visma draftit”. I december 2023 fanns det totalt 392 registrerade behandlingar i registerförteckningen, sex stycken fler än föregående år. I samband med registrering av en behandling får man även besvara frågan ”Är du klar med registerbeskrivningen?”. Av de registrerade behandlingarna är 158 registrerade behandlingar markerade som klara jämfört med föregående år då 152 var klarmarkerade. 24 stycken har markerats som inte färdiga och återkommer. I övriga behandlingar har frågan lämnats obesvarad.

Många behandlingar är registrerade av flera olika verksamheter. Dessa behandlingar behöver registreras samlat och övergripande för att minska antalet dubbletter, göra registerförteckningen mer översiktlig samtidigt som det kan minska administrationstrycket på enheterna.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Innehållsmässigt har uppdateringar inte skett i den utsträckning som varit nödvändig. Majoriteten av de registrerade behandlingarna är fortfarande inte fullständigt registrerade i registerförteckningen. Endast ett fåtal registreringar har uppdaterats under 2023.

DSO bedömer hur fullständig registerförteckningen är

I registerförteckningen saknas ett flertal registreringar som borde finnas upptagna i en registerförteckning. Under året har en inventering påbörjats men det arbetet behöver fortsätta under 2024. Därtill har flera registreringar registrerats flera gånger fast på olika enheter.

I rapporten för 2022 konstaterades att de behandlingar som finns beskrivna i registerförteckningen många gånger också är bristfälligt beskriven, oaktat om frågan är obligatorisk eller inte. Detta gäller särskilt frågan om ändamål. Frågan besvaras väldigt kort till exempel anges ”avtal”, ”lätt tillgängligt” och ”administration” som ändamål vilket inte beskriver ändamålet med personuppgiftsbehandlingen tillräckligt. Dessa brister kvarstår även 2023.

Vidare noterar DSO att registreringar ibland registreras utifrån system, ibland utifrån ändamål vilket gör det svårt att följa och säkerställa att alla delar finns med.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Det finns ett utbildningsmaterial, *Dataskyddsförordningen och registerförteckning* för hur registerförteckningen ska fyllas i och vad den bör innehålla för att uppfylla kraven i dataskyddsförordningen.

Utöver utbildningsmaterialet för registerförteckningen finns en vägledning ”GDPR för dig som chef” som redogör för chefernas ansvar enligt dataskyddsförordningen. Enligt vägledningen ska cheferna säkerställa att de personuppgiftsbehandlingar som görs i deras verksamhet registreras i systemverktyget Draftit och att alla obligatoriska frågor ska besvaras för varje behandling. Utöver det ska cheferna ansvara för att registerförteckningen hålls uppdaterad och att alla nya personuppgiftbehandlingar registreras samt att registerförteckningen minst en gång om året kontrolleras för att säkerställa att den är komplett och korrekt. Det ansvaret har förtydligats genom en separat rutin som tagits fram under 2023 i syfte att tydliggöra ansvaret. Det finns även en lathund för hur systemet Draftit ska användas vid en registrering.

DSO noterar att en ny rutin som tydliggör ansvar för registerförteckningen har tagits fram under året och bedömer att rutinen är tillräcklig men att tillämpningen av den är möjlig att följa upp först under 2024. DSO noterar också att försök att underlätta för verksamheterna att fylla i registerförteckningen har vidtagits under året.

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
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

De identifierade bristerna är omfattande och kräver omgående åtgärder. Grunden för fastställandet är både registerförteckningens kvalitet och omfattning men även en bedömning av de obligatoriska frågorna i registerförteckningen.

PUA behöver ha kontroll över vilka behandlingar som utförs i verksamheterna, särskilt vilka behandlingar som omfattar känsliga och särskilt skyddsvärda personuppgifter, för att kunna vidta rätt skyddsåtgärder och i övrigt leva upp till kraven i dataskyddsförordningen.

3.1.5 DSO ger råd och rekommendationer till PUA

PUA bör under kommande år prioritera att strukturera om registerförteckningen för att tydliggöra syfte, ändamål och underlätta för verksamheterna att fylla i registerförteckningen. I Samband med det bör också ansvariga för gemensamma registreringar utses. Granskningen visar att många verksamheter upplever det som svårt att besvara frågorna vilket leder till att många registreringar förblir ofärdiga.

PUA bör också prioritera så att sammanhållna registreringar görs på övergripande förvaltningsnivå för att komplettera registerförteckningen med alla personbehandlingar i centrala system så som LISA, Sociala System etc. De behandlingar som å andra sidan är registrerade av flera olika verksamheter, exempelvis vissa typer av protokoll eller faktureringar, skulle även dessa behöva registreras samlat och förvaltningsövergripande för att minska antalet dubbletter och göra registerförteckningen mer översiktlig och korrekt. PUA bör också prioritera att identifiera de områden som inte alls finns upptagna i registerförteckningen, till exempel registreringar kopplade till förtroendevalda, centrala IT-system med mera.

PUA bör i samband med omstrukturering av registerförteckning fundera över om man ska utgå från ändamål eller utifrån system vid registreringar. DSO rekommenderar med fördel att utgå från ändamål för att effektivisera och förenkla registreringarna för verksamheterna.

Ett samlat stöd bör erbjudas verksamheterna i samband med uppdatering, översyn och upprättande av registerförteckning. Information om ansvar och befintliga styrdokument behöver också spridas.

Dessa åtgärder bedöms förbättra kvaliteten på registerförteckningen avsevärt och motivera medarbetarna till att fullfölja registreringarna av samtliga personuppgiftsbehandlingar.

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 den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna, när de hanterar personuppgifter. Att styrdokument finns nedtecknade, beslutade och kommunicerade medför att medarbetaren får dataskyddsinformation och kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt. En röd tråd i Dataskyddsförordningen är att viktiga arbetssätt och rutiner ska vara dokumenterade. Detta följer bland annat av kravet på att den personuppgiftsansvarige måste kunna visa att dataskyddsförordningens principer för behandling av personuppgifter efterlevs (artikel 5).

Rapporteringen av området är tvådelad: dels ska DSO bedöma om verksamheten har de styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en

lämplig kvalitet, i vilket ingår bl.a. att dokumentationen ska vara uppdaterad och aktuell.

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

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?

Lista över befintliga styr- och stöddokument:

- Handbok för personuppgiftsbehandling.
  Omfattar information om hur verksamheten hanterar information till den registrerade samt information om den registrerades rättigheter.
- Integritetspolicy Farsta Stadsdelsnämnd
- Hantering av anställdas personuppgifter
- Mall för information om hantering av personuppgifter
- Mall för hur redovisning av personuppgiftsbehandling ska utformas
- Handbok för informationsklassning
- Rutin för hantering av personuppgiftsincidenter (uppdaterad 2023)
- Vägledning för personuppgiftsincidenter
- Checklista och mall för konsekvensbedömning
- Stockholms stads policy används för instruktioner om publicering på sociala medier
- Arkiv och gallring i förhållande till GDPR.
- Mall för personuppgiftsbiträdesavtal (Stadens)
- Instruktion till personuppgiftsbiträdesavtalet (Stadens)
- Checklista för inbyggt dataskydd samt dataskydd som standard (Stadens)
- Lokal tillämpningsanvisning för informationssäkerhet
- Rutin för inventering av personuppgifter
- GDPR för dig som chef

Under året har flera styrdokument uppdaterats. Det handlar om den lokala rutinen för inventering av personuppgifter,

personuppgiftsincidenter, Arkiv och gallring samt mallar för information till registrerade.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

Dokumentation som finns på plats bedöms vara lättillgänglig för verksamheten genom att all dokumentation finns samlad på samma plats i förvaltningens dokumentbibliotek, tillgängligt för alla medarbetare via intranätet. Dokumentationen är tydligt strukturerad genom uppdelningen i underrubriker. Genom att dokumentationen är samlad på samma plats blir det enkelt för medarbetarna att veta var de ska leta efter rätt information.

Information till den registrerade samt om dennes rättigheter
I handboken för personuppgiftsbehandling redogörs för den registrerades rättigheter. Information i handboken är utförligt och tydligt förklarad vilket gör det enkelt för användaren att ta till sig informationen. Informationen är generellt formulerad och kan tjäna på att konkretiseras med exempel från verksamheterna.

Avseende den registrerades rättigheter finns även en integritetspolicy, vilken riktas till stadsdelsförvaltningens invånare. I policyn ges en kortfattad bakgrund till dataskyddsförordningen, där bland annat information om vad som utgör en personuppgift innefattas. Det ges dessutom en generell beskrivning över hur verksamheten behandlar personuppgifter, där det bland annat beskrivs att verksamheten behandlar personuppgifter för ändamålet att utföra myndighetsutövning. Integritetspolicyn fungerar som generell information till invånarna med hänvisning vidare för mer information och uppfyller inte kraven i artikel 13 avseende information om rättslig grund, information om mottagare av personuppgifterna och information om överföringar till tredjeland, eller kraven i artikel 14. PUA måste tillhandahålla särskild information om personuppgifterna inte har erhållits från den registrerade själv, detta görs bäst i en integritetspolicy som finns publicerad på hemsidan för samtliga att nå. Detta är svårt att åstadkomma med nuvarande utformning av stadens hemsida.

För att uppfylla artikel 13 och 14 finns Mall för information om hantering av personuppgifter. Den grundläggande utformningen av mallen är framtagen av staden, men under året har en lokal anpassning till Farsta stadsdelsnämnd tagits fram samt ett stödmaterial till verksamheterna i att utforma den utifrån den personuppgiftsbehandling som de olika verksamheterna har.

Det finns även en information om hantering av anställdas personuppgifter. Detta dokument är strukturerat på samma sätt som ovan nämnda integritetspolicy, detta gör att ovan nämnda brister även återfinns i aktuellt dokument. Informationen om hantering av anställdas personuppgifter uppfyller inte kraven i artikel 13 avseende information om rättslig grund, information om mottagare av personuppgifterna och information om överföringar till tredjeland, och bör därför uppdateras.

Informationsklassning
Det finns en väldigt omfattande handbok för informationsklassning på 28 sidor som föredömligt beskriver hur informationsklassning ska genomföras steg för steg. Handboken anses heltäckande och är enkel för användaren att följa. Utöver handboken finns även två olika mallar för "Informations-klassningsprotokoll" som stöd i arbetet och är tydliga i vad och hur man ska göra. Dessa dokument anses vara fullt tillräckliga för användare att följa för att kunna fullgöra informationsklassningar.

Personuppgiftsincident
Det finns en rutin för hantering av personuppgiftsincident. Rutinen för hantering av personuppgiftsincident har uppdaterats under året och tydliggjort ansvar och process för hantering av incidenter.

Registerförteckning och inventering av personuppgifter
Under året har en rutin för inventering av personuppgifter och ansvarsfördelning för registerförteckningen tagits fram i syfte att tydliggöra ansvarsfördelningen. Rutinen beskriver tydligt vem som ansvarar för vad och tidpunkt för detta.

Konsekvensbedömning
Det finns en mall för konsekvensbedömning och en checklista för konsekvensbedömning. Mallen för konsekvensbedömning kommer från Stockholms stad och fungerar som en stödmall i processen för konsekvensbedömningar. Farsta stadsdelsnämnds checklista för konsekvensbedömningar tar snarare sikte på att fungera som ett stöd för organisationen vid bedömningen om en konsekvensbedömning behöver genomföras. Checklistan är tydligt strukturerad och formulerad med exempel på varje bedömningsdel. I checklistan stadgas att rutinen för konsekvensbedömningen är att den ska dokumenteras och att DSO ska kontaktas.

Gallring och GDPR

Det finns ett kort dokument; Arkiv och gallring i förhållande till GDPR som redogör för principen i dataskyddsförordningen om att personuppgifter inte ska sparas längre än nödvändigt. Dokumentet har uppdaterats under året och tydliggör vidare att radering (gallring) enbart får ske enligt gallringsbeslut fattade av Stadsarkivet. Frågorna kring detta i registerförteckningen har också uppdaterats för att underlätta för verksamheterna att svara på frågan om gallring och radering.

Tredjelandsöverföring till USA
Stadsledningskontoret har tagit fram Reviderat inriktningsbeslut avseende tredjelandsöverföring till USA med anledning av EU-kommissionens nya adekvansbeslut som kom i jul 2023. I Farsta har man valt att ta SLK:s inriktningsbeslut som sitt eget.

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

Några dokument, till exempel integritetspolicyn, kan kompletteras med exempel från verksamheten och instruktioner bör beskrivas mer utförligt.

Verksamheten ska i första hand hänvisa till Stockholm stads integritetspolicy, men det finns en specifik integritetspolicy för personuppgiftsbehandling i Farsta stadsdelsnämnd. Denna finns dock för tillfället inte öppet tillgänglig för de registrerade vilket är problematiskt då själva syftet med informationen är att informera de registrerade om deras rättigheter. Tidigare fanns Farstas integritetspolicy tillgänglig under stadsdelsområdets dokument på stadens hemsida, men togs bort när Stockholm ändrade domän.

På stadens nya hemsida listas de områden som stadsdelsförvaltningen ansvarar över, men dessa överensstämmer inte med de områden som listas i integritetspolicyn. Problemet med att hänvisa till stadens policy är därmed att den inte är anpassad efter stadsdelsförvaltningens olika verksamhetsområden och är

heller inte komplett utformad. Det leder dessutom till att det är svårt för den registrerade att få en helhetsbild över verksamhetens behandlingar.

Utöver avsaknaden på publicering är det en brist att det inte tydligt framgår ur integritetspolicyn hur personuppgifterna behandlas. Ett exempel på detta är om lagring av uppgifter där det framkommer av policyn att uppgifter inte lagras längre än vad som är nödvändigt för ändamålet. Då ändamålet för behandlingen beskrivs vara myndighetsutövning är det svårt för den registrerade att skapa sig en uppfattning om hur länge uppgifterna i praktiken lagras.

Det finns också ett behov av att säkerställa att rutinerna efterlevs samt att rutinerna för personuppgiftsbehandlingar vävs in i den ordinarie verksamhetens uppdrag för att få full effekt.

3.2.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att alla verksamheter går igenom sina processer för att säkerställa att verksamhetens rutiner tar höjd för efterlevnaden av Dataskyddsförordningen.

Dokumenten bör kontinuerligt ses över och om möjligt slås ihop för att minimera risken för fel i arbetet. Det ska vara tydligt vilket syfte varje dokument har och var medarbetaren kan hitta hjälp.

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?	15 st som är informationsklassade i sin helhet.
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

För att kunna skydda personuppgifter med rätt slags skydd så ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information och de personuppgifter som behandlas. 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. Det är därför viktigt att en ansvarsfördelning och utpekad ansvarig finns.

3.3.3 Resultat

Informationsklassning sker efter protokoll framtaget av SLK. Dokumentet ger en första bedömning och stöd innan den större aktiviteten med verktyget KLASSA. Under 2023 har 13 klassningar slutförts och ytterligare åtta har påbörjats.

PUA har totalt 15 stycken verksamhetssystem som är fullt ut informationsklassade. Dock ska man beakta att samtliga personuppgiftsbehandlingar klassas utifrån vilken typ av personuppgifter som behandlas och lämpligt skydd vidtas för respektive behandling. Detta kan vara behörighetsbegränsning, skydd av lösenord på dokument osv. Detta ska dokumenteras i

Draftit, men är i majoriteten av de registrerade behandlingarna inte ifylld.

Under året har en lokal tillämpningsanvisning tagits fram vad gäller informationssäkerhet. I den tydliggörs och formaliseras enhetschefernas ansvar jämfört med tidigare. Ett lokalt nätverk med samtliga enheter finns representerade har bildats. Genom nätverket har arbetet med att öka kunskap påbörjats och tanken är att takten på informationsklassningarna ska kunna öka en raskare takt än tidigare.

Under året har en systeminventering genomförts och en process för införandet av nya tjänster tagits fram i syfte att säkerställa att informationsklassning och nödvändiga skyddsåtgärder för att skydda personuppgifter vidtas. Detta ger en bra bild och kunskap över status och behov framåt. Genom inventeringen har rollen som system- och informationsägare tydliggjorts och dokumentet ”Ledningens genomgång” säkerställer att det finns en prioriteringsordning för informationsklassning av system. DSO konstaterar att det därmed finns en bättre överblick hos organisationen för att genomföra klassningar framöver. De brister som identifierats i 2022 års rapport i allt väsentligt kvarstår sett till utfallet under 2023.

Under året har kontroller på organisatoriska tekniska och organisatoriska skyddsåtgärder genomförts för de system som är informationsklassade, alternativt är i en process för informationsklassning. Granskningen visar att flera av de system som är i informationsklassnings process har avstannat på grund av bristande information från systemägare/leverantör. Ofta handlar det om system som staden, genom ansvarig facknämnd, tagit in och implementerat och där stadsdelarna förväntas börja använda systemet utan att en lokal klassning har hunnit genomföras. När de lokala klassningarna påbörjas är systemet ofta redan infört och det PUA beskriver att det har varit svårt att få svar på de frågor som ställs i klassningen. Det försvårar PUAs möjligheter att vidta lämpliga organisatoriska och tekniska skyddsåtgärder för att skydda personuppgifter.

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

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

Bedömningen är att bristerna som identifieras kräver åtgärder, vilket beror på att flera system fortfarande inte har informationsklassats. Informationsklassningar behöver genomföras för att säkerställa att rätt tekniska- och organisatoriska säkerhetsåtgärder finns på plats. Detta är framför allt av vikt i de personuppgiftsbehandlingar där känsliga och särskilt skyddsvärda personuppgifter behandlas.

3.3.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar PUA att uppdra åt avdelnings- och enhetschefer att, i samråd med informationssäkerhetssamordnare och DSO, göra en prioriteringsordning av sina verksamhetssystem. Prioriteringen bör utgå från parametrar som känsliga personuppgifter, mängd personuppgifter och eventuell tredjelandsöverföring. Därefter bör klassningarna påbörjas och organisatoriska och tekniska skyddsåtgärder vidtas i syfte att leva upp till kraven i Dataskyddsförordningen avseende skydd för personuppgifter.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

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

3.4.2 Syfte

Konsekvensbedömningen hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas i projekt eller linjeverksamhet. En konsekvensbedömning har till syfte att identifiera och dokumentera risker kopplade till en viss behandling, samt att bedöma sannolikheten och konsekvensen om riskscenariot skulle inträffa. Baserat på bedömningen kan/ska riskförebyggande åtgärder vidtas.

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning som ett viktigt verktyg för verksamhetens dataskyddsarbete. Kravet på konsekvensbedömning är dessutom ett uttryckligt krav enligt dataskyddsförordningen. och ska utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1).

3.4.3 Resultat

Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?
Verksamheten har inte identifierat alla behandlingar som det borde upprättas konsekvensbedömningar av. Däremot har systeminventeringen gett en bra bild över vilka system som används och i vilket syfte. Utifrån den listan är det möjligt att få en indikation på vilka behandlingar som kräver en konsekvensbedömning i enlighet med dataskyddsförordningen.

Det finns en funktion i Draftit där risknivån för personuppgiftsbehandlingar anges (låg/mellanhög/hög), men den används i mycket liten utsträckning.

De konsekvensbedömningar som genomförts under 2023 har gjorts i samband med informationsklassningar och på initiativ av informationssäkerhetssamordnare och DSO. Verksamheterna saknar i stor utsträckning kunskap och processer för att själva kunna identifiera och bedöma behov av konsekvensbedömningar.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Genom att utföra ett stickprov ur registerförteckningen kan det konstateras att det gjorts några fler riskbedömningar jämfört med 2022, men att det inte gjorts konsekvensbedömningar av alla behandlingar där det finns ett behov att göra en sådan. Mot

bakgrund av att det är flera behandlingar som innefattar känsliga personuppgifter, uppgifter om barn, äldre, funktionsnedsatta och andra personer som befinner sig i underläge eller beroendeställning samt personuppgifter i stor omfattning, bör fler konsekvensbedömningar gjorts.

Då registerförteckningen i vissa delar är bristfälligt ifylld, särskilt i detta fall med avseende på risknivå, går det visserligen att konstatera att det saknas konsekvensbedömningar men det är inte möjligt att besvara i vilken omfattning.

Är de genomförda konsekvensbedömningarna aktuella?

De konsekvensbedömningar som finns är aktuella och i de flesta fall genomförda under 2022 och 2023.

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
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

Då verksamheten behandlar en stor mängd personuppgifter, däribland känsliga personuppgifter, är det viktigt att den har utrett de potentiella riskerna som finns med behandlingen ur ett integritetsperspektiv. Detta görs bland annat genom en konsekvensbedömning.

Konsekvensbedömningar saknas för majoriteten av de behandlingar som utförs i verksamheten, inklusive högriskbehandlingar.

3.4.5 DSO ger råd och rekommendationer till PUA

Respektive avdelning rekommenderas att omedelbart initiera arbete med att identifiera och ta fram de konsekvensbedömningar som saknas. I denna rapport ges endast exempel på behandlingar som behöver konsekvensbedömningar, men det finns sannolikt fler behandlingar där konsekvensbedömningar behöver genomföras. Det är viktigt att komma ihåg att kravet på konsekvensbedömning inte

endast gäller för nya behandlingar, utan även gäller för behandlingar som verksamheten genomfört innan dataskyddsförordningen trädde ikraft.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	0 st
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	0 st

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 är att se personuppgiftsansvarig tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, som exempelvis att lämna ut ett så kallat registerutdrag eller att rätta vissa uppgifter. Radering, den så kallade ”rätten att bli glömd”, är sällan aktuell i någon större mån eftersom stadens verksamheter lyder under krav på bevarande till följd av offentlighetsprincipen. Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran.

Om verksamheten inte klarar av att hantera en begäran från en registrerad person i enlighet med dataskyddsförordningens krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från Integritetsskyddsmyndighetens (”IMY”) sida, med sanktioner som följd. Det är därför viktigt att PUA regelbundet ges en bild av i

vilken mån verksamheten klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Den interna processen är uppbyggd så att en begäran om registerutdrag går till DSO, som sedan vidarebefordrar frågan till utsedda funktioner med behörighet att genomsöka systemen. Invånare informeras i första hand om att de kan kontakta DSO för detta, men den registrerade ska dock kunna kontakta vem som helst i organisationen med en begäran och ansvariga chefen ska se till så att begäran hanteras korrekt. Det ställer höga krav på medarbetare och chefers kunskap om den registrerades rättigheter.

I handboken för personuppgiftsbehandlingen beskrivs alla rättigheter på ett utförligt sätt vilket är positivt. Det saknas dock konkreta exempel och beskrivning av hur hanteringen av begäran ska gå till. I dokumentet ”GDPR för dig som chef” beskrivs rutinen för registerutdrag, men de övriga rättigheterna nämns inte.

Den här typen av process ökar risken för att hanteringen sker på ett felaktigt sätt eller att begäran inte hanteras överhuvudtaget. En stickprovskontroll som DSO genomförts under året visar dock att ingen förfrågan har inkommit samt att kunskaperna om de registrerades rättigheter samt rutiner vid begäran om registerutdrag var god. Även om samtliga saknade detaljkunskap om hur en förfrågan skulle hanteras så angav samtliga att de visste var de kunde hitta mer information om rutiner för registerutdrag samt angav att de skulle söka stöd hos DSO om förfrågan skulle inkomma.

En förutsättning för att den registrerade ska inkomma med begäran är att den har information om dennes rättigheter och hur verksamheten behandlar den registrerades personuppgifter. Genom att inte erbjuda tillräcklig information till den registrerade garanteras därmed inte heller dennes rättigheter. Avsaknaden av en separat integritetspolicy för verksamheten utgör en av bristerna, men det kan även röra sig om övrig kommunikation med de registrerade. Under året har PUA/DSO hållit utbildningar om informationskravet och stöttat verksamheter i att ta fram ändamålsenliga och verksamhetsanpassade informationsutskick till de registrerade.

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

Givet att ingen begäran har inkommit under 2023 är det svårt att göra en bedömning om organisationens kapacitet och förutsättningar att tillgodose kravet om registerutdrag inom utsatt tid. DSO noterar dock att bristerna i registerförteckningen är en risk, likväl som de tidigare identifierade riskerna med de registrerades rätt till information.

3.5.5 DSO ger råd och rekommendationer till PUA

Det finns fortsatt ett behov av utbildning för att öka kunskaperna om de registrerades rättigheter, inklusive rätten till information.

PUA rekommenderas att säkerställa att åtgärder vidtas för att leva upp till de krav som ställs på registerförteckningen i dataskyddförordningen. Detta är grundläggande för att säkerställa den registrerades rättigheter.

Slutligen rekommenderar DSO att PUA genomför en inventering på enhetsnivå för att säkerställa att det finns rutiner och anpassad information till verksamheternas målgrupper i enlighet med dataskyddsförordningens bestämmelser. Parallellt med detta bör PUA föra en dialog med SLK om möjligheten att publicera integritetspolicys på extern webb.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom medarbetare och chefer.
Hur många personuppgiftsincidenter har dokumenterats?	20 st
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	8 st rapporterats till IMY, i 9 st fall har den registrerade informerats.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	8 st

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen (artikel 4.12) ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering. Stadens mall för årsrapport är avsedd att fokusera på rapporteringen.

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

personers rättigheter och friheter, ska rapportering även ske till de berörda registrerade personerna, utan dröjsmål. Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering till de berörda personerna.

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

Notera att enligt dataskyddsförordningen artikel 33.5 ska alla personuppgiftsincidenter dokumenteras, det vill säga även i de fall då incidenten inte ska rapporteras till IMY. Bristande dokumentering står i strid med Dataskyddsförordningen och leder även till problem med att ta fram korrekta siffror till årsrapporteringen avseende hur väl verksamheten lever upp till rapporteringsfristerna. Enligt artikel 33.5 är det ett krav att dokumentera omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden och bristande dokumentering är sanktionsgrundande.

3.6.3 Resultat

Hur väl förmår verksamheten att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?

Verksamheten förmår att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten. Samtliga personuppgiftsincidenterna har hanterats i tid. Ett stort ansvar läggs på cheferna gällande personuppgiftsincidenter. Enligt befintliga rutiner ska den som är chef för den verksamhet där en personuppgiftsincident har inträffat utreda och dokumentera incidenten. Chefen uppmanas att följa förvaltningens rutin för hantering av personuppgiftsincidenter. Chefen har också ett ansvar att säkerställa att medarbetare genomgått stadens e-utbildning för grundläggande dataskydd. Huruvida en incident därför upptäckts och anmäls i tid beror också på chefernas agerande och medarbetarnas kunskaper.

Under 2023 har fler personuppgiftsincidenter rapporterats jämfört med 2023 och en högre andel har rapporterats korrekt. Detta är förmodligen en följd av att utbildningen i dataskydd genomförts i större utsträckning samt att alla chefer och nyckelpersoner fått fyra särskilda utbildningstillfällen kring chefsansvaret för dataskyddsarbetet i praktiken.

Bland det incidenter som har rapporterats under året består en övervägande majoritet av information som skickats till fel mottagare. Vissa incidenter har varit mer allvarliga än andra och i de fallen har också den registrerade kontaktats. Vissa verksamheter är mer frekventa i att rapportera personuppgiftsincidenter men noterar att rapporteringsbenägenheten möjligen kan vara en faktor.

Bedömningen är dock att det finns ett stort mörkertal kring personuppgiftsincidenter som inte rapporteras. Det finns ett behov av att öka kunskaperna även bland medarbetarna kring vad en personuppgiftsincident är och hur den ska hanteras.

DSO noterar också att det finns en osäkerhet i verksamheten när incidenter inträffar i stadsgemensamma system. Det är ett problem att olika nämnder och bolag gör olika bedömningar kring hur incidenter ska rapporteras. Informationsöverföringen kring incidenter i stadsgemensamma system är också bristfällig vilket försvårar för Farsta stadsdelsnämnd som PUA när gäller rapporteringen av incidenter. Ibland får inte PUA information och ibland finns det utmaningar att få tag i rätt information som krävs för att kunna göra bedömningar om det är en incident som ska rapporteras eller ej. Ett exempel är den incident som i juni slog ut alla telefoner inom hemtjänsten under fler dagar och där PUA gjorde en bedömning att det var en allvarlig personuppgiftsincident då verksamheten inte kom åt informationen alls. Det tog PUA tre månader att få information från systemägaren om att detta endast rörde sig om en uppdatering av systemet som inte kommunicerats.

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
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga

	Inga brister av nämnvärd betydelse identifierade

Sedan 2022 har mer än dubbelt så många personuppgiftsrapporter rapporterats vilket tyder på att det finns en ökad kännedom om vad en personuppgift är och hur den ska hanteras. Det finns ett behov av att fortsatt ha fokus på incidenthanteringen och öka rapporteringen men bedömningen är att det finns väl kända rutiner. Däremot finns ett behov av att följa upp och se hur man tar om hand de incidenter som inträffar och hur man drar lärdomar som ett sätt att utveckla verksamheten och säkerställa att det inte sker igen.

3.6.5 DSO ger råd och rekommendationer till PUA

PUA bör föra dialog med SLK och systemförvaltande facknämnder kring rutiner, informationsdelning och hantering av incidenter i gemensamma system.

Arbetet med att kontinuerligt utbilda samtliga medarbetare om grundläggande dataskydd och vad som utgör en personuppgiftsincident behöver fortsätta och upprätthållas för att eventuella personuppgiftsincidenter ska identifieras och hanteras på korrekt sätt. Den obligatoriska utbildningen ”Grundkurs i dataskydd” bör skickas ut årligen till alla medarbetare och det bör säkerställas att den är en del av introduktionen för alla nya medarbetare. Avsnittet gällande personuppgiftsincidenter bör särskilt lyftas. Det är positivt att utbildningen avslutas med ett kunskapstest.

Eftersom ett stort ansvar läggs på cheferna bör dessa få stöd och exempel på vad en personuppgiftsincident kan vara för att lära sig vilka personuppgiftsincidenter som är vanligast i verksamheten och hur dessa hanterats samt vad som förväntas av dem i de fallen.

I IA-systemet rapporteras alla incidenter som sker i verksamheten, som till exempel att någon skadar sig fysiskt. Ibland sker felregistreringar av händelsetyp, vilket kan leda till att identifiering av personuppgiftsincidenter fördröjs eller inte hanteras på rätt sätt. En rekommendation är att löpande kontrollera huruvida övriga rapporterade incidenter också utgör en personuppgiftsincident.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Registerförteckning
- Individens rättigheter
- Informationsklassning

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 PUA 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 – Registerförteckning

Under året har utbildningar genomförts riktat till enhetschefer och utvalda ombud per enheter. PUA har tagit fram en ny rutin med fokus på att inventera personuppgifter och skapa ett årshjul för uppdateringar av registerförteckning. Rutinen syftar också till att tydliggöra ansvar för att registerförteckningen är komplett och uppdaterad.

Granskningen visar att många verksamheter upplever det svårt att fylla i registerförteckningarna och det är uppenbart att det finns ett behov av att förenkla och stötta verksamheterna i deras arbete. Ett nätverk för dataskyddshandläggare har upprättats på förvaltningen och där alla enheter finns representerade. De har fått utbildning i hur man ska registrera och ett försök att underlätta för verksamheterna att fylla i regiterförteckningen har genomförts under året.

En ny struktur för registerförteckning har tagits fram som ett sätt att effektivisera och underlätta registreringar med fokus på att minska antalet registreringar genom bland annat samregistreringar.

DSO noterar att det under året har gjorts ett ordentligt arbete med att sätta strukturerna för arbetet med registerförteckningen men att det under året 2024 finns ett behov att också implementera det i verksamheten. Vid denna rapports framtagande finns det fortfarande stora brister i nämndens registerförteckning och behovet av att komplettera registreringarna kvarstår.

	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

Granskning 2 – individens rättigheter

Granskningen gällande avsaknaden av individens rättigheter genomfördes inte helt som planerades i årsrapport 2022.

Under året har en inventering av förvaltningens styrdokument och rutinbeskrivningar påbörjats med fokus individens rättigheter. Inventeringen, som inte slutförts och därmed inte är heltäckande, visar samstämmigt att det verksamheterna inte önskar egna rutiner och tillämpningar utan tycker att de förvaltningsövergripande dokumenten är tillräcklig. Därmed lyfter verksamheterna att det finns behov att få med dataskyddsperspektivet i befintliga processer och rutiner. Det finns dock ett behov att fortsätta inventeringen för att få en mer heltäckande bild samt säkerställa behovet av lokala rutiner.

Under 2024 bör inventeringen fokusera på informationskravet och inventera hur enheternas rutiner för att säkerställa att informationskravet uppfylls i alla delar. DSO bör leda den fortsatta inventeringen tillsammans med förvaltningens nätverk för dataskysshandläggare och enhetschefer.

	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 – avsaknad av informationsklassningar

I 2022 års granskning identifierades en avsaknad av informationsklassningar som en risk med behov av granskning i slutet av 2023. Syftet är att säkerställa om lämpliga tekniska och organisatoriska säkerhetsåtgärder har vidtagits i enlighet med kraven i artikel 32.

DSO har granskat alla informationsklassningar som genomförts under 2023 med fokus på tekniska och organisatoriska säkerhetsåtgärder. Granskningen visar att verksamheten i allt väsentligt har vidtagit lämpliga åtgärder i de klassningar som har genomförts.

Den systeminventering som förvaltningen gjort under 2023 visar dock att det finns flera verksamhetssystem som inte är informationsklassade, varav känsliga och skyddsvärda personuppgifter förekommer i flera fall. DSO har inom ramen för denna granskning inte granskat dessa system och kan därför inte bedöma huruvida nödvändiga tekniska och organisatoriska skyddsåtgärder har vidtagits. Det finns dock ett behov att fortsätta och påskynda informationsklassningen av organisationens verksamhetssystem för att säkerställa att lämpliga tekniska och organisatoriska säkerhetsåtgärder har vidtagits i enlighet med kraven i artikel 32.

	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

4.4 DSO ger råd och rekommendationer till PUA

Mot bakgrund av bristerna i registerförteckningen bör granskning fortsätta under följande år, där det följs upp att samtliga enheter fyller i förteckningen.

För att stötta enhetschefer och de som ansvarar för att fylla i registerförteckningen bör utbildning och gemensamma workshops genomföras i syfte att samordna och stötta verksamheterna i arbetet.

Inventering av lokala rutiner bör fortsätta. DSO bör leda arbetet tillsammans med enheter och nätverket av dataskyddshandläggare.

PUA bör fortsatt prioritera resurser för att informationsklassa verksamhetssystem och vidta lämpliga organisatoriska och tekniska säkerhetsåtgärder.

5 Risker inom dataskydd

5.1 Sammanfattning

Det finns ett antal identifierade risker hos PUA kopplat till dataskydd. Riskerna är i allt väsentligt samma som tidigare år och nedan beskrivs de mest relevanta risker inom verksamheten:

- Den personuppgiftsansvariga (PUA) har inte fullständig överblick över sina personuppgiftsbehandlingar.
- Dataskydd tas inte i beaktande vid upphandlingar, införanden av nya system eller arbetssätt
- Bristen på konsekvensbedömningar oh hantering av känsliga personuppgifter
- Medarbetarnas kunskaper om dataskydd är bristfälliga

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 - Den personuppgiftsansvariga (PUA) har inte fullständig överblick över sina personuppgiftsbehandlingar.

För att verksamheten ska kunna garantera de registrerades rättigheter och se till så att dataskyddsarbetet sker på ett korrekt sätt är det viktigt att verksamhetens registerförteckning är korrekt ifylld. Utan en fullständig registerförteckning är det inte möjligt för verksamheten att hålla koll på de olika behandlingar som görs. Registerförteckningen utgör dessutom grunden för den interna kontrollen och speglar verksamhetens kunskap om sina behandlingar. En bristfällig registerförteckning tyder därmed på att verksamheten inte har koll på de behandlingar som utförs, vilket i sin tur leder till risker som avsaknad av konsekvensbedömningar och personuppgiftsbiträdesavtal avseende de behandlingar som kräver det.

Det är svårt att besvara hur allvarliga konsekvenser kan bli om den aktuella risken skulle realiseras, men då flera andra risker är nära anknutna till den aktuella risken bör det kunna antas att konsekvenserna kan bli allvarliga. De identifierade bristerna bör därför anses som omfattande och kräver omedelbara insatser.

	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

Risk 2 - Dataskydd tas inte i beaktande vid upphandlingar, införanden av nya system eller arbetssätt

Det är ett krav om inbyggd dataskydd och dataskydd som standard i alla processer. Trots det förekommer det att verksamhetssystem köps in eller implementeras trots att behandlingen inte informationssäkerhetsklassats, konsekvensbedömts eller att nödvändiga skyddsåtgärder vidtagits för att skydda personuppgifter hos de registrerade.

Det finns också ett identifierat behov av att få in dataskyddsfrågorna i befintliga verksamhetsprocesser och arbetssätt.

Vidare finns det risker kopplat till att verksamheterna inte har systematiserat arbetet med att omhänderta lärdomar från inträffade personuppgiftsincidenter. Det riskerar att obehöriga får tillgång till personuppgifter som de inte har rätt till.

	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

Risk 3 – Bristen på konsekvensbedömningar och hantering av känsliga och särskilt skyddsvärda personuppgifter

PUA behandlar många känsliga personuppgifter samt personuppgifter i stor omfattning i flera behandlingar. Trots det är konsekvensbedömningarna få. Under 2023 har flera av de rapporterade personuppgiftsincidenterna involverat känsliga eller särskilt personuppgifter.

Att hantera känsliga personuppgifter ställer högre krav på säkerhetsåtgärder och behovet av såväl konsekvensbedömningar som att sätta ljus på organisatoriska rutiner och tekniska skyddsåtgärder är därför viktigt. Det innebär en hög risk att PUA inte har genomfört konsekvensbedömning av alla aktuella systemen eller har ett systematiskt arbetssätt för att dra lärdomar av de incidenter som inträffar.

Risk 4 – Medarbetarnas kunskaper om dataskydd är bristfälliga

Trots utbildningsinsatser finns en okunskap om dataskydd och vad det ställer för krav på organisationen. Tillräckliga kunskaper om dataskyddsarbetet i alla delar av en personuppgiftsbehandling saknas samt en okunskap kring frågorna har identifierats som ett hinder för en komplett registerförteckning.

Kunskapsbristerna kan leda till allvarliga brister och konsekvenser om de inte hålls färska och uppdaterade hos alla medarbetare.

	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

5.4 DSO ger råd och rekommendationer till PUA

Ovan identifierade risker ligger i linje med de obligatoriska arbetssätten som redovisats tidigare i rapporten, för råd och rekommendationer hänvisas därför till relevanta avsnitt i rapporten.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Implementering och efterlevnad av nya rutiner
- Hantering av personuppgiftsbehandlingar, myndighetsutövande och utredande enheter inom avdelningen IOF och äldreomsorg

6.2 Syfte

Som nämnts ovan är det granskande arbetet en av dataskyddsombudets viktigaste uppgifter. Granskningsområdena har valts utifrån ett riskbaserat synsätt, det vill säga med fokus på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Dessa har valts för att åstadkomma 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 – Implementering och efterlevnad av nya rutiner

Under 2023 har PUA tagit fram nya rutiner inom dataskyddsområden. Det handlar om följande rutiner som har tagits fram:

- Lokal anvisning för informationssäkerhet
- Rutin för inventering av personuppgifter (inklusive ansvar för registerförteckning)
- Rutin för att rapportera saknade personakter enligt SoL/LSS

Under året ska efterlevnaden av de nya arbetssätten granskas för att säkerställa att de är tillämpade inom organisationen.

Granskning 2 - Hantering av personuppgiftsbehandlingar, myndighetsutövande och utredande enheter inom avdelningen IOF och äldreomsorg

På myndighetssidan (utredandende enheter på avdelning individ- och familjeomsorg samt beställarenheten äldre) hanteras många känsliga och särskilt skyddsvärda personuppgifter samtidigt som personuppgifter delas med många andra parter som en del i

myndighetsutövandet. Trots att många känsliga och särskilt skyddsvärda personuppgifter hanteras är det få av de verksamhetssystem som används där en konsekvensbedömning är genomförda. Det är därför osäkert vilka risker som finns kopplat till behandlingarna samt om lämpliga skyddsåtgärder vidtagits för att skydda de registrerades personuppgifter i enlighet med dataskyddsförordningen.

Under året har ett flertal personuppgiftsincidenter rapporterats från beställarenheterna inom socialtjänsten, varav många med liknande karaktär, dvs att man skickat information till fel mottagare. Vissa har varit mer allvarliga än andra men det noteras att det finns ett behov av att se över befintliga rutiner.

Med anledning av ovan har DSO beslutat att genomföra en särskild granskning av ovan nämnda enheter under 2024 för att se hur väl PUA lever upp till dataskyddsförordningen och lokala arbetssätt/rutiner.

7 Övrigt att rapportera

7.1 Sammanfattning

Utöver ovan har DSO i detta avsnitt valt att lyfta två delar som inte fullt ut ryms i de andra delarna av rapporten. Det handlar dels om behovet av att avsätta mer resurser för dataskyddsarbetet hos PUA och dels om de organisatoriska utmaningar med dataskyddsarbetet som finns inom Stockholms stads organisation.

7.2 Syfte

Avsikten med denna punkt i årsrapporten är att ge möjlighet att komplettera bilden av statusen i dataskyddsarbetet hos PUA. Under denna rubrik anges därför sådant som inte på ett naturligt sätt kunde tas upp under någon av punkterna i rapporteringsstrukturen ovan.

7.3 Övriga observationer

Observation 1

DSO noterar att det under året har skett framsteg hos PUA inom dataskyddsarbetet. Takten på informationsklassningar av verksamhetssystem har ökat, flera rutiner har utvecklats och förtydligats och det finns – i och med dokumentet ”Ledningens genomgång” en tydlig plan för klassningen av system framåt.

Utbildningar har genomförts och ett samlat grepp finns taget om registerförteckningen.

För att kunna genomföra detta krävs att tillräckliga resurser avsätts. Dataskyddsarbetet är i allmänhet mycket krävande och i dagsläget, vilket framkommer ovan, har flera allvarliga brister identifierats. Även om arbetet har prioriterats i högre utsträckning under 2023 så finns det en skuld som behöver betas av för att komma ikapp och ligga i takt inom dataskyddsarbetet. Eftersom bristerna är omfattande förutsätter det fortsatta arbetet att det finns resurser som kan arbeta med det löpande dataskyddsarbetet för att minimera riskerna.

Detta särskilt eftersom det inte ingår i DSO:s arbetsuppgifter att arbeta med det operativa arbetet. Det är viktigt att PUA möjliggör för DSO att utföra sin granskande roll. En granskning av dataskyddsombudets roll i en nationell och europeisk kontext har genomförts under 2023 och utifrån den nationella granskningen det är tänkbart att det också kommer att påverka arbetet lokalt.

Observation 2

Utifrån stadens organisationsstruktur finns det en utmaning i gränsdragningen mellan stadens nämnder och bolag vilket emellanåt försvårar dataskyddsarbetet. Även om det är tydligt att varje nämnd/bolag är personuppgiftsansvarig för informationen som de lägger in i systemen så är det uppenbart att olika nämnder och bolag gör olika bedömningar av olika incidenter och hantering av information.

Det är också utmaningar när facknämnder upphandlar system som stadsdelsnämnderna sedan förväntas ta in utan att ha möjlighet att själv informationsklassa det. Detta sker inte sällan i efterhand och/eller med bristande tillgång till information från ansvariga nämnder. Vid en granskning av PUA:s informationsklassningar av centrala system under året visar utfallet att flera klassningar inte kunnat slutföras på grund av bristande tillgång till information från berörd facknämnd.

Under granskningen av personuppgiftsincidenter noterar DSO att olika nämnder och bolag hanterat incidenter på olika sätt och att bristen på information från ansvarig facknämnd många gånger varit bristfällig. Så pass bristfällig att det varit svårt för Farsta stadsdelsnämnd som PUA att bilda sig en uppfattning ifall det är en incident och ifall den i så fall bör rapporteras vidare till tillsynsmyndighet.

DSO noterar att det finns en otydlig ansvarsfördelning och brist på rutiner om hur incidenter ska hanteras och hur stadsdelsnämnderna ska involveras i implementeringen och införandet av nya verksamhetssystem. Det skiljer sig också åt mellan hur olika facknämnder involverar och informerar om brister i de system där de har systemförvaltningen. Det hade varit önskvärt att detta tydliggörs på ett sätt som underlättar för stadens nämnder och bolag att agera i egenskap av PUA.

7.4 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att fler resurser avsätts för att ytterligare öka takten i dataskyddsarbetet för att kunna leva upp till kraven i dataskyddsförordningen.

DSO rekommenderar PUA att föra en dialog med SLK och berörda facknämnderna kring rutiner och hantering av stadsgemensamma verksamhetssystem. Både avseende incidenthantering men också vad gäller informationsklassningar av gemensamma verksamhetssystem.