Stockholms stad

Bilaga 7 till
VB 2024

GDPR Årsrapport

År 2024

Farsta stadsdelsnämnd

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

Ordlista

PUA = Personuppgiftsansvarig, i den här rapporten menas Farsta stadsdelsnämnd
DSO = Dataskyddsombud
IA = stadens verktyg för incidentrapportering
IMY= Integritetsskyddsmyndigheten, tillsynsmyndighet behnadling av personuppgifter
GDRP = General Data Protection Regulation, i Sverige omsatt till nationell lagstifning genom framför allt dataskyddsförordningen
PUB = personuppgiftsbiträde, en aktör som behandlar personuppgift åt PUA:s räkning. Till exempel en leverantör av en digital tjänst.
PUB-avtal = Avtal (som ofta följer med huvudavtal) mellan PUA och PUB och som reglerar hur PUB får behandla personuppgifter för PUA:s räkning

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 Farsta stadsdelsnämnd (PUA) under 2024 stärkt sitt dataskyddsarbete på flera områden, framför allt när det gäller arbetet med registerförteckningen. Även om det fortsatt finns behov av att komplettera registerförteckningen så är den mer heltäckande än föregående år. Utifrån att registerförteckningen är en grundplatta för resterande dataskyddsarbete så har det också skapat en bättre överblick av dataskyddsarbetet även i de andra rapporteringsområdena i denna rapport.

Utöver registerförteckningen har Farsta stadsdelsnämnd även ökat antalet konsekvensbedömningen och utvecklat arbetet med att kartlägga i vilka system som känsliga personuppgifter finns. Genom det arbetet finns också en bättre grund att stå på i fråga om prioriteringar för konsekvensbedömningar samt informationsklassningar framöver med utgångspunkten att börja med de system/behandlingar med flest personuppgifter och mest känsliga personuppgifter.

Även om Farsta stadsdelsnämnd stärkt sitt dataskyddsarbete under året så finns det fortsatt en del brister som behöver hanteras. Behovet av konsekvensbedömningar för personuppgiftsbehandlingar med stora mängder känsliga personuppgifter är fortsatt stort. En utmaning som identifierats i årets granskning är att PUA behöver förtydliga vem som bär ansvar för att genomföra konsekvensbedömningar, särskilt behandlingar som sträcker sig över flera verksamhetsområden. Det samma gäller för bedömningen av vidtagna organisatoriska och tekniska säkerhetsåtgärder. Där är ansvarsfördelningen tydligare men det är fortsatt många behandlingar som saknar dokumentation av vidtagna säkerhetsåtgärder. PUA rekommenderas särskilt att under kommande åren prioritera arbetet med att inventera och teckna nödvändiga pub-avtal samt säkerställa en korrekt behörighetshantering i system, särskilt när det handlar om känsliga personuppgifter.

Slutligen visar årets granskning att det finns ett behov av att samtliga nämnder och bolag samordnar sitt dataskyddsarbete. Idag

hanterar olika facknämnder dataskyddsfrågorna på olika sätt vilket gör det svårt för PUA att agera och planera sitt dataskyddsarbete. Stadens facknämnder har idag olika syn på incidenthantering, tecknandet av pub-avtal när det gäller gemenensamma leverantörer samt behovet av gemensamma tekniska och organisatoriska säkerhetsåtgärder. En rekommendation är därför att PUA fortsatt är aktiv i samtalet och fortsätter att driva på för att Stockholms stad gemensamt ska samordna sitt dataskyddsarbete.

Stockholm 3 januari 2024

Charlotte Sundvall
Dataskyddsombud
Farsta stadsdelsnämnd

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:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

De obligatoriska områdena är gemensamma för hela staden och har valts ut till årsrapportmallen eftersom de tillsammans kan ses som ett nödvändigt minimum för PUA att informera sig om för att upprätthålla ett fungerande och lagenligt dataskyddsarbete år från år. Att de definieras som ett minimum baseras på en bedömning av dataskyddsförordningens syfte och tillsynsmyndigheternas praxis.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	96
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 nämnden måste inventera alla personuppgifter som behandlas i verksamheten och dokumentera dem i en så kallad registerförteckning.

Inventeringen av personuppgifter i sig är avgörande för allt det fortsatta dataskyddsarbetet inom verksamheten och registerförteckningen är därför en central utgångspunkt.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats
PUA har upprättat en registerförteckning i systemet ”Visma draftit” och i december 2024 så fanns det 96 registreringar i Draftit. Det är en minskning jämfört med tidigare år men det beror på att PUA under året har omarbetat hela registerförteckningen för att öka systematiken och fokusera på processerna. Tidigare registrerades varje behandling för sig medan den nya registerförteckningen fokuserar på processer och täcker in flera behandlingar i samma registrering.

DSO kontrollerar om nödvändiga uppdateringar gjorts
DSO noterar att hela registerförteckningen har uppdaterats under året och att nödvändiga uppdateringar har i allt väsentligt gjorts men att inte allt granskats av närmaste chef enligt rutinen samt att några registreringar fortsatt saknar nödvändig information. Processerna och personuppgiftsbehandlingar bedöms dock identifierade och att registerförteckningen är mer ändamålsenlig och i betydligt högre grad än tidigare lever upp mot de krav som finns i Dataskyddsförordningen.

DSO bedömer hur fullständig registerförteckningen är
DSO bedömer att registerförteckningen i större utsträckning än tidigare är fullständig. Jämfört med tidigare är den mer överblickbar genomarbetad. Vid granskning kan DSO dock konstatera att några registreringar fortsatt behöver kompletteras innan registerförteckningen kan anses vara fullständig.

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 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 hos PUA som fastslår ansvar för uppdatering samt när uppdatering ska ske. Det verkar dock som att det finns utrymme att öka efterlevnaden av rutinen, särskilt nu när en ny registerförteckning finns på plats.

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

DSO bedömer att de brister som påtalats i tidigare års årsrapporter till viss del har åtgärdats i och med det arbete som gjorts under året kopplat till registerförteckningen. Däremot kvarstår fortsatt ett arbete med att komplettera och avsluta det påbörjade arbetet innan bristerna kan anses fullt ut åtgärdade.

3.1.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar PUA att hålla i det arbete som genomförts under året och att prioritera implementeringen av den rutin som finns kopplat till ansvar och årshjul för uppdatering av registerförteckning.

I samband med den årliga översikten rekommenderas PUA även att komplettera de registreringar som inte är klara.

Det är viktigt att verksamheterna fortsatt får stöd i göra och avsluta sina registreringar då det fortsatt finns kunskapsluckor hos medarbetarna. Det är också synligt att det utifrån registreringarna finns områden som behöver jobba särskilt med, detta gäller framför allt på utförarsidan inom äldreomsorgen och funktionsnedsättning.

3.2 Styrdokument

3.2.1 Sammanfattning

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

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.

Detta följer bland annat av kravet på att den personuppgiftsansvarige måste kunna visa att dataskyddsförordningens principer för behandling av personuppgifter efterlevs (artikel 5).

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 (inkl instruktion)
- Handbok för informationsklassning
- Rutin för hantering av 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 (uppdaterad 2024)
- Rutin för inventering av personuppgifter
- GDPR för dig som chef
- Reviderat inriktningsbeslut avseende tredjelandsöverföring till USA
- Rutin för att rapportera saknade personakter enligt SoL/LSS

Utöver ovan finns även lokala behörighetsrutiner för flera verksamhetssystem.

DSO konstaterarar att PUA i stora delar har lämpliga styrdokument. Däremot är det inte i befintliga rutiner och styrdokument vem som ansvarar för att till exempel initiera och genomföra konsekvensbedömningar samt gemensamma rutiner på hur personuppgiftsincidenter ska följas upp. Även om behörighetsrutin finns för många system så finns det idag flera system som saknar detta. Enligt granskade underlag kan DSO se att det finns en tydlig koppling mellan lokala behörighetsrutiner och huruvida systemet genomgått en komplett informationsklassningsprocess.

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.

Däremot finns en del av de stadsgemensamma styrdokumenten inte i dokumentbiblioteket utan behöver finnas på annat sätt. Det kan vara mer utmanande men ofta handlar det om mer specifika frågor och där expertfunktioner ofta kallas in, personer som har kunskap om var informationen finns. De styrdokument som finns bedöms tillräckliga och uppdaterade.

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

DSO konstaterar att nödvändiga styrdokument i allt väsentligt finns på plats. Det som saknas är behörighetsrutiner för alla system, styrdokument som tydliggör vem som ansvarar för att genomföra konsekvensbedömningar samt tydlighet i hur enheterna förväntas implementera Dataskyddsförordningen och förvaltningsgemensamma rutiner i sina löpande processer och verksamheter. Det saknas också rutiner för ett systematiskt följa upp incidenter vilket är en viktig del i att utveckla verksamheten och förebygga eventuella brister/risker.

3.2.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar PUA att ta fram styrdokument för att tydliggöra ansvar kring konsekvensbedömningar och uppföljning av incidenter. DSO rekommenderar även att behörighetsrutiner tas fram för samtliga system som behandlar personuppgifter,

inledningsvis med särskilt fokus på system som behandlar känsliga och särskilt skyddsvärda personuppgifter.

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

DSO rekommenderar även PUA att inventera hur de förvaltningsgemensamma rutinerna finns omhändertagna i enheternas lokala rutiner.

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?	36 st i sin helhet. Utöver det är 22 stycken påbörjade och för en behandling har riskanalys genomförts.
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd så ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att PUA ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare.

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 2024 har 21 klassningar slutförts och ytterligare 22 har påbörjats.

Under året har en inventering av befintliga pub-avtal påbörjats men inte slutförts. Inventeringen har tagit fasta på vilka system/processer som har pub-avtal men inte på vilka behandlingar där det finns ett behov av pub-avtal. PUA har också deltagit i de stadsinterna diskussioner som påbörjats kring stadens interna hantering av biträdessituationer. Diskussionerna har påvisat svårigheter med stadens interna hantering av pub-avtal och där olika facknämnder hanterar frågan på olika sätt vilket försvårat PUA:s hantering av pub-avtal.

Under året har den lokala tillämpningsanvisningen för informationssäkerhet uppdaterats. Ett lokalt nätverk med samtliga enheter finns representerade har bildats och de har varit drivande i att antalet klassade system har ökat. Under året har PUA beslutat om en organisation för utveckling och omhändertagande av sina it-system. I den har rollerna i det här arbetet förtydligats i syfte att säkerställa att informationsklassning och nödvändiga skyddsåtgärder för att skydda personuppgifter vidtas.

DSO konstaterar att PUA är bättre rustad för att genomföra klassningar framöver. Under året har kontroller på 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 informationsklassade saknar svar på flera organisatoriska eller tekniska säkerhetsåtgärder, alternativt att informationsklassning som pågår fastnad på samma grunder och att detta beror på 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 är 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

PUA behandlar en stor mängd känsliga och särskilt skyddsvärda personuppgifter i sin verksamhet. Trots det finns inte tekniska och organisatoriska skyddsåtgärder dokumenterade. Det framgår dock att PUA har en plan för att genomföra informationsklassningar (och därmed identifiera behov av tekniska och organisatoriska skyddsåtgärder) de kommande åren men att arbetet behöver resurs-sättas och prioriteras.

3.3.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar PUA att initiera och föra dialog med facknämnderna när det gäller informationsklassningar (och vidta rätt tekniska och organisatoriska säkerhetsåtgärder) för att säkerställa att PUA lokalt kan säkerställa att rätt åtgärder har vidtagits för att skydda personuppgifter i enlighet med befintlig lagstiftning.

DSO rekommenderar även PUA att höja tempot i informationsklassningar av de verksamhetssystem/processer som finns i organisationen. 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.

DSO rekommenderas att under året inventera behovet av pub-avtal i alla behandlingar som görs. DSO rekommenderar även PUA att fortsätta ligga på stadsledningskontoret kring behovet av att tydliggöra hur stadens nämnder och bolag ska förhålla sig till frågor om interna pub-avtal (alternativt PUA-PUA situationer).

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 och uppdateringen av registerförteckningen 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. Fler system har också informationsklassat

och bedömningen är därför att PUA har en bättre överblick nu jämfört med för ett år sedan.

De konsekvensbedömningar som genomförts under 2024 har gjorts i samband med informationsklassningar och på initiativ av informationssäkerhetssamordnare och DSO. I en granskning under året har visat att endast en av fem enhetschefer vet vad en konsekvensbedömning är och att den behöver göras. 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?
Under året har flera konsekvensbedömningar genomförts och DSO bedömer att fler högriskbehandlingar än tidigare har konsekvensbedömts. Däremot kvarstår fortsatt flera högriskbehandlingar som inte har konsekvensbedömts. I vissa fall finns centrala bedömningar inom Stockholms stad men där PUA behöver göra en egen bedömning lokalt.

Är de genomförda konsekvensbedömningarna aktuella?

De konsekvensbedömningar som finns är aktuella och genomförda de senaste två åren.

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

Även om PUA under året skaffat sig en bättre överblick av behovet av konsekvensbedömningar samt genomfört konsekvensbedömningar för fler behandlingar än tidigare så finns det många behandlingar som saknar en konsekvensbedömning. Givet att konsekvensbedömningar är centrala för att förebygga risker och vidta rätt säkerhetsåtgärder för att skydda personuppgifter i de behandlingar som innebär större risker för den registrerade så är det centralt för PUA att prioritera denna fråga.

3.4.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar PUA att omedelbart initiera ett arbete med att identifiera och genomföra konsekvensbedömningar för de behandlingar som bedöms behöva det.

DSO rekommenderar PUA att genomföra informationsinsatser och utbildning riktat till dataskyddshandläggare och chefer kring konsekvensbedömningar. Det finns ett behov för hela organisationen att öka sina kunskaper om *vad* en konsekvensbedömning är och *när* en sådan behöver genomföras.

Vidare rekommenderar DSO även PUA att tydliggöra vem som ansvarar för att initiera och genomföra konsekvensbedömningar i system/behandlingar som omfattar flera enheter.

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.

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. Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran.

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 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.

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/tillgång att slå i system och behandlingar.

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

En stickprovskontroll som DSO genomförts under året visar dock att ingen förfrågan, utöver de som passerat DSO, har inkommit. Sedan tidigare har kontroller visat att chefernas kunskaper om de registrerades rättigheter samt rutiner vid begäran om registerutdrag är god.

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 DSO stöttat flera verksamheter som uppdaterat sin information till registrerade och bedömningen är att rutinerna kring information i allt väsentligt fungerar.

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

DSO bedömer att det finns bra rutiner och arbetssätt men att det fortsatt finns utmaningar inom stadens samlade dataskyddsarbete när det gäller information på hemsidan, till exempel att den integritetspolicy/information som finns på stadens hemsida inte är anpassad till stadsdelarnas verksamheter fullt ut.

3.5.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar PUA att fortsätter föra en dialog med SLK om möjligheten att publicera integritetspolicys på extern webb. Men även med andra facknämnder för att säkerställa att informationskravet finns med i stadens gemensamma system och personuppgiftsbehandlingar.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Medarbetare, chefer, information från andra PuA i standen.
Hur många personuppgiftsincidenter har dokumenterats?	43
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	26
Hur många av incidenterna har rapporterats i tid till	24

tillsynsmyndigheten?	

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 DSO:s årsrapport är avsedd att fokusera på rapporteringen.

Rapporteringsskyldigheten omfattar alla personuppgiftsincidenter som ska rapporteras i stadens incidenthanteringssystem, IA. Incidenter som bedöms kunna medföra en risk för fysiska personers rättigheter och friheter (se artikel 33) ska även rapporteras till tillsynsmyndigheten, IMY, inom 72 timmar efter 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.

Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY:s sida. 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. Med några få undantag har personuppgiftsincidenterna har rapporterats och hanterats i tid. I de fall där så inte skett har det funnits särskilda skäl till detta. 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 2024 har fler personuppgiftsincidenter rapporterats jämfört med 2023. Detta är förmodligen en följd av att förvaltningens dataskyddshandläggare under året fått utbildning i personuppgiftsincidenter samt att några enheter rapporterat många incidenter och därmed har en ökad medvetenhet kring den typen av incidenter. Däremot noterar DSO fortsatt en låg kvalitet på många rapporter i IA och att förvaltningens rutin inte efterlevs i fråga om vad en rapport ska innehålla (dokumentationskravet).

Bland de 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 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.

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

Kunskapen och benägenheten att rapportera incidenter har ökat vilket är bra. Även rapporteringen till IMY har stärkts. Det noteras dock att det fortsatt är vissa enheter som rapporterar mycket medan andra verksamheter knappt rapporterat något. Det finns anledning att tro att det beror på en okunskap i de verksamheter som rapporterar färre incidenter snarare än en bristfällig hantering i de verksamheter som rapporterar många. Det saknas idag också en systematik i hur man ska följa upp rapporterade incidenter. Det är viktigt att verksamheten ser incidenter som ett tillfälle att identifiera och åtgärda eventuella brister i verksamheter för att säkerställa att det finns ett lärande i detta.

Vidare konstaterar DSO också att det finns brister i innehållet i de incidentrapporter som finns. I rutinen framgår tydligt vad som ska finnas med i rapporteringen men trots det är det få IA-rapporter som innehåller den information som krävs enligt Dataskyddsförordningen.

Vidare konstateras brister i hantering av incidenter som inträffar i stadsgemensamma system. Detta är inte en fråga som PUA kan hantera på egen hand utan en fråga som staden gemensamt behöver hitta rutiner för. Den delen har därför inte tagits med i bedömningen av bristerna hos PUA.

3.6.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar PUA att fortsatt föra dialog med SLK och systemförvaltande facknämnder kring rutiner, informationsdelning och hantering av incidenter i gemensamma system.

DSO rekommenderar PUA att utveckla efterlevnaden av rutinen för rapportering av personuppgifter så att de innehåller den information som PUA enligt lag är ålagda att dokumentera.

DSO rekommenderar PUA att ta fram en rutin för uppföljning av incidenter. DSO rekommenderar även PUA att genomföra risktade insatser om personuppgiftsincidneter till verksamheter som redovisar få incidenter, bland annat utförarna inom funktionsnedsättning, fritidens verksamhet samt förskolan.

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:

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

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 –Implementering och efterlevnad av nya rutiner

Under året har DSO granskat efterlevnaden av följande nya rutiner;

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

<u>Lokal anvisning informationssäkerhet</u>
Under året har en handfull enhetschefer fått frågan om de har kännedom om den lokala anvisningen för informationssäkerhet. Av de tillfrågade svarade alla utom en att de hade kännedom om den men kunskapen om vad den innehåller samt vilket ansvar som medföljer var begränsat. Granskningen visar att det fortsatt finns ett behov av att informera om detta framöver, och DSO rekommenderar att detta följs upp även framåt.

<u>Inventering av personuppgifter</u>

När det gäller rutin för inventering av personuppgifter så har den varit svår att granska i år. Bakgrunden är att nämnden under året beslutat att ta in en resurs för att driva arbetet med att komplettera och uppdatera PUA:s registerförteckning. Därmed har rutinen inte testats skarpt under året och granskningen för aktuell rutin kvarstår därmed till nästkommande år. Den rapporteras då inte som särskild granskning utan rapporteras under registerförteckningen.

Rapportera saknade personakter

Rutinen för att rapportera saknade personakter enligt SoL/LSS har till viss del efterlevts. Under vårens gallring av personakter saknades cirka 30 akter. Alla berörda enheter hade försvunna akter men endast fyra enheter rapporterade detta som personuppgiftsincidenter. Granskningen visar att information och rutinen har kommunicerats men att verksamheterna har upplevt det som svårt att veta vad som ska rapporteras och hur. Arbetet har också identifierat behov av att fortsätta arbeta med frågan men också att ansvarsfördelningen kring de förlorade akterna blir tydligare. Utifrån tillämpningsanvisningen är det dock tydligt att det är upp till respektive enhetschef att säkerställa att rapportering av personuppgiftsincidenten rapporteras vilket inte skett i enlighet med rutin.

	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 – Hantering av personuppgiftsbehandlingar, myndighetsutövande och utredande enheter inom avdelningen Individ- och familjeomsorg samt avdelningen äldreomsorg

Vad som har granskats

Granskningen avser hantering av personuppgiftsbehandlingar inom myndighetsutövande och utredande enheter på avdelningen individ. Och familjeomsorg samt avdeningen äldreomsorg. Enheterna som har granskats är beställarenheten äldre, beställarenheten

funktionsnedsättning, enheten för barn och ungdom, vuxenenheten samt enheten arbete, integration och bistånd.

Bakgrund till granskning
Bakgrunden är att dessa verksamheter hanterar stora mängder känsliga och särskilt skyddsvärda personuppgifter samtidigt som person. Samtidigt är det de verksamheterna som rapporterar in flest personuppgiftsincidenter, varav flera incidenter påminner om varandra och där känsliga personuppgifter spridits till obehöriga. GDPR:s årsrapport har under flera år också belyst behovet av att öka antalet konsekvensbedömningar för dataskydd i syfte att säkerställa att rätt tekniska och organisatoriska skyddsåtgärder har vidtagits för att skydda de personuppgifter som hanteras i verksamheten.

Genomförande av granskning
Granskningen genomfördes under perioden maj-juni 2024. Granskningen har skett genom mail till berörda enhetschefer, genom inventering av konsekvensbedömningar samt inrapporterade personuppgiftsincidenter.

Därefter har följdfrågor ställts i de fall där det kvarstått frågor. Efter att frågorna besvarats av enhetschefer har dataskyddsombudet via eDok och registerförteckningar i Drafit inventerat hur många av de personuppgiftsbehandlingar som är konsekvensbedömda. En del av slutsatserna kring incidentrapporteringen har även fångats upp i andra sammanhang.

Utfall av granskning
Alla enheter förutom en har redovisat personuppgiftsincidenter, i flera fall liknande incidenter där känsliga personuppgifter skickats till fel mottagare. Underlaget baseras på en genomgång av rapporterade personuppgiftsincidenter de senaste 12 månaderna. Bland de enheter som anger att de har haft incidenter redogör också på ett tillfredsställande sätt för hur de har omhändertagit incidenterna genom att till exempel lyfta frågan på APT eller sett över rutiner. Det är dock viktigt att frågan lyfts till en avdelningsövergripande nivå för att gemensamt se över behovet av gemensamma rutiner och arbetssätt samt lärande utifrån inträffade incidenter.

I samtal med enhetschefer har dataskyddsombudet även fångat upp att det finns incidenter som inte rapporterats. Det går många gånger att härleda till bristande kunskap om vad en personuppgiftsincident

är eller en arbetssituation som gör det svårt att hinna med att rapportera alla incidenter när de bedöms som mindre allvarliga.

Däremot upplever flera enheter att det är svårt att överföra information på ett säkert sätt då mailen inte är krypterad och alternativet som kvarstår då är vanlig post eller fax. Det finns en vilja att göra rätt men ett behov av bättre digitala verktyg. En del enheter har skriftliga rutiner kring vad som gäller för hantering av känslig information i samband med hemarbete medan andra har muntliga avstämningar om det i samband med APT. Utifrån granskningen verkar det dock inte finnas en förvaltningsgemensam hållning i frågan.

Det som är viktigt att lyfta är att de medarbetare som arbetar på enheterna och som löpande hanterar känsliga personuppgifter ofta har en utbildning i hur man ska hantera känslig och sekretessbelagd information. Även om det inte är specifik utbildning i dataskyddslagstiftningen så är det ett förhållningssätt som underlättar för att säkerställa efterlevnad av Dataskyddsförordningen. Det finns således upparbetade arbetssätt och rutiner för att hantera och säkerställa att känslig information inte når obehöriga. Alla enhetschefer anger att de löpande påminner medarbetare om att gå stadens obligatoriska digitala utbildningar i dataskydd och informationssäkerhet. Detta bekräftas också av det uppföljningsarbete som nämnden gör i samband med delårsbokslut och årsbokslut. Flera enhetschefer anger att medarbetarna har rätt kunskaper om aktuella frågor medan andra bedömer att det finns ett behov av att stärka medarbetarnas kunskaper.

Granskningen visar vidare att enhetschefernas kunskap om behovet av konsekvensbedömningar är bristfälliga. Endast en av de svarande kunde redogöra för vad en konsekvensbedömning är och behovet av det i den egna verksamheten. Frågan om konsekvensbedömningen har under många år flaggats som en stor risk i GDPR:s årsrapport och den här granskningen visar att det finns ett stor behov av att öka kunskapen om vad en konsekvensbedömning för dataskydd är och vilka krav det ställer på verksamheten. Det är allvarligt att processer som hanterar så mycket känsliga personuppgifter inte har konsekvensbedömts.

Genomgången av eDok och registerförteckning i Draftit bekräftar bilden och visar att endast två verksamhetsspecifika processer/system kopplat till de granskade verksamheterna har en lokal konsekvensbedömning. Det är e-signeringsverktyget och e-ansökan för ekonomiskt bistånd. Granskningen visar dock att inga

av stadens sociala system eller processer är konsekvensbedömda vilket är allvarligt utifrån att det innehåller så mycket känsliga personuppgifter. Dataskyddsombudet bedömer dock att det finns väl upparbetade rutiner och att staden centralt arbetar med den tekniska säkerheten kopplat till aktuella system. Det är dock viktigt att dokumentera detta i en konsekvensbedömning.

	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

- Kompetenshöjande insatser kring konsekvensbedömningar för dataskydd samt för personuppgiftsincidenter
- Att inventera och göra konsekvensbedömningar för de system som behandlar känsliga personuppgifter
- Införa verktyg för en säker digital kommunikation
- Undersöka behovet av gemensamma riktlinjer för hemarbete och sekretessbelagd information/känsliga personuppgifter.
- Information till chefer i samband med att rutinen uppdateras

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- Bristen på konsekvensbedömningar (inklusive tekniska och organisatoriska säkerhetsåtgärder) och hantering av känsliga personuppgifter
- Medarbetarnas kunskaper om dataskydd är bristfälliga
- Avsaknad av, och otydligheter, vad gäller Pub-avtal
- Ansvarsfördelningen inom Stockholms stad

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 - Bristen på konsekvensbedömningar och hantering av känsliga personuppgifter

PUA behandlar många känsliga personuppgifter samt personuppgifter i stor omfattning i flera behandlingar. Trots det är konsekvensbedömningarna få. Under 2024 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/processer och därmed inte har dokumenterat vilka säkerhetsåtgärder som vidtagits för att skydda de registrerade rättigheter.

	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 – Medarbetarna och chefernas kunskaper om dataskydd är bristfälliga

Trots utbildningsinsatser finns en okunskap om dataskydd och vad det ställer för krav på organisationen samt vem som är ansvarig för detta. Tillräckliga kunskaper om dataskyddsarbetet i alla delar av en personuppgiftsbehandling saknas.

Kunskapsbristerna kan leda till allvarliga brister och konsekvenser om de inte hålls färska och uppdaterade hos alla medarbetare. Till exempel har årets granskningar visat att det finns en stor okunskap kring vad en konsekvensbedömning är och när den behöver göras. Även kunskaperna kring personuppgiftsincidenter och pub-avtal har visat sig bristande i olika sammanhang där DSO har deltagit tillsammans med verksamheten. Ytterst kan de bristerna leda till incidenter där PUA förlorar kontrollen över de registrerades personuppgifter, personuppgifter som många gånger kan vara av känslig karaktär utifrån de myndighetsuppdrag som PUA har.

	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 Avsaknad av, och otydligheter, vad gäller Pub-avtal

PUA har idag en bristande bild av behovet av pub-avtal. Uppdateringen av registerförteckningen har också visar att det finns en kunskapslucka om när ett pub-avtal ska tecknas eller huruvida pub-avtal finns tecknade för de behandlingar som genomförs idag. Vidare har DSO även tidigare i denna rapport konstaterat att det föreligger oklarheter hur staden intern kan och ska hantera pub-situationer nämnderna emellan vilket försvårar PUA:s möjligheter att faktiskt få en bra överblick av när ett pub-avtal behöver tecknas eller ej.

	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 4 Ansvarsfördelningen inom Stockholms stad
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 och pub-avtal 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.

	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

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

Utifrån identifierade risker, samt utöver de obligatoriska granskningarna ovan (som täcker in stora delar av identifierade riskerna) så bedömer DSO att följande är relevanta granskningsområden inom verksamheten:

- Pub-avtal
- Behörighetshantering

6.2 Syfte

Som nämnts ovan är det granskande arbetet en av dataskyddsombudets viktigaste uppgifter. Granskningsområdena Utgår från riskerna i avsnittet ovan då det är områden där verksamhetens mest relevanta risker har identifierats.

6.3 Planerade granskningar

Granskning 1- Pub-avtal

Under 2024 har DSO identifierat att det finns brister i organisationens hantering av pub-avtal. Området har tidigare identifierats av DSO och av stadsrevisionen men då andra områden bedömts mer prioriterade tidigare så har denna fråga fått vänta. Nu bedömer dock DSO att det är rimligt att återigen genomföra en granskning av PUA:s hantering av pub-avtal.

PUA har också infört ett antal olika stadsgemensamma system där frågan om pub-avtal funnits med i diskussionerna och där det funnits oklarheter om hur pub-avtal ska hanteras internt men också mellan PUA och leverantör.

Granskning 2 - Behörighetshantering

I samband med konsekvensbedömningar och informationsklassningar (tekniska och organisatoriska skyddsåtgärder) har genomförts har behörighetshantering varit en återkommande fråga. Det är också ett prioriterat område inom staden. Behörighetshantering är en viktig del i att begränsa medarbetares tillgång till personuppgifter och därmed säkerställa att inte obehöriga får tillgång till personuppgifter som de inte ska ha tillgång till. Samt principen om ändamålsbegräning. Givet att PUA hanterar mycket känsliga personuppgifter bedömer DSO att det är viktigt att särskilt granska efterlevnaden av befintliga behörighetsrutiner.