Stockholms stad

Bilaga 4

GDPR Årsrapport

År 2024

Äldrenämnden

GDPR årsrapport
Januari 2025

Dnr: ALD 2024/446
Utgivningsdatum: 2025-01-07
Kontaktperson: Désirée Veschetti

1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskydds-regler 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 också 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 i dess hantering av personuppgifter följer dataskyddslagstiftningen. Det innebär att äldrenämnden såsom personuppgiftsansvarig behöver hålla sig informerad, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter inom nämndens verksamhet.

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 rapportera resultatet av granskningen och ge sina rekommendationer direkt till högsta förvaltningsnivå. DSO:n ska arbeta självständigt och oberoende, utan att bli påverkad av andra inom organisationen.

Denna årsrapport är således ett medel för äldrenämnden att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till personuppgiftsansvarig 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 äldrenämnden att visa hur den som personuppgiftsansvarig, (”PUA”), efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att äldrenämnden 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.

Innehåll

2 Sammanfattning

I egenskap av ert Dataskyddsombud (DSO) lämnar jag följande årsrapport.

Årets granskning av äldreförvaltningen dataskyddsarbete visar i stort sätt på samma brister som påpekades i förra årets rapport. Sammanfattningsvis visar granskningen på följande brister.

- Registerförteckningen och struktur för registervård är fortfarande ofullständig och i behov av genomgående revidering. Bristen innebär att äldrenämnden och äldreförvaltningen har begränsad kännedom om hur känsliga eller extra skyddsvärda personuppgifter behandlas i olika verksamhetsprocesser och situationer.

- Endast ett par konsekvensbedömningar har genomförts. Den begränsade kännedomen om vilka personuppgifter som behandlas inom äldreförvaltningen får till följd att nödvändiga konsekvensbedömningar inte blir gjorda, vilket även här innebär en hög risk för att fysiska personers rättigheter och friheter inte kan garanteras.

- Handläggningen av dataskyddsfrågor är reaktivt då det idag saknas samordnade gemensamma rutiner, med undantag för incidenthanteringsrutinen. Bristerna innebär att skyddet av enskildas uppgifter kan hanteras olika inom äldreförvaltningens verksamhetsprocesser.

- Äldreförvaltningen saknar idag rutiner och ett strukturerat för att hantera registrerades rättighetsbägarna. Vidare saknas information till de registrerade och för äldreförvaltningen anpassade blanketter för rättighetsbegäran på äldreförvaltningens del av stadens hemsida. Det sammantaget med de brister som identifieras inom föregående områden, bland annat registerförteckning, innebär det att vissa behandlingar som kan vara aktuella vid en rättighetsbegäran kan komma att missas. Det innebär också att handläggare får lägga mycket tid på att försöka hitta rätt och utreda vad som behöver göras, exempelvis när en registrerad lämnar in en rättighetsbegäran eller ett klagomål.

Positivt är att äldreförvaltningen under hösten har påbörjat ett utvecklingsarbete i syfte att åtgärda delar av de ovan beskrivna bristerna. Som DSO rekommenderar jag starkt att arbetet med att ta fram en registerförteckning, genomföra konsekvensbedömningarna samt utarbeta nödvändiga rutiner fortsätter. På så sätt läggs en viktig grund för att uppnå kraven enligt dataskyddsförordningen.

För att undvika att personuppgifter och de enskildas rättigheter hanteras olika är det också viktigt för att etablera en struktur för äldreförvaltningens dataskyddsarbete.

Äldrenämnden bör under året följa upp hur arbetet fortskrider.

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporterings-områden som äldrenämnden 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 äldrenämndens 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?	54 personuppgiftsbehandlingar har identifierats och en registerförteckning över dessa har påbörjats
Har nödvändiga uppdateringar gjorts?	Nej
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Nej

3.1.2 Syfte

För att någonting ska gå att skydda måste det också vara synligt för verksamheten och för den som ska granska regelefterlevnaden. Det följer därför i klartext av dataskyddsförordningen att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde och dokumentera dem i en så kallad registerförteckning (även kallat behandlingsregister). 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 som säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling.

Syftet med rapporteringsområdet är att redovisa för äldrenämnden i dess roll som PUA hur väl verksamheten har lyckats inventera och registrera de personuppgifter som behandlas inom respektive verksamhetsområde och de personuppgifter som behandlas för annans räkning, samt att upprätta en registerförteckning över dessa behandlingar.

Att ha en registerförteckning på plats leder vidare till att verksamheten kan arbeta mer resurs- och kostnadseffektivt med sitt

systematiska och riskbaserade dataskyddsarbete. Verksamheten kan därmed styra insatserna dit de gör störst nytta.

3.1.3 Resultat

Antalet personuppgiftsbehandlingar som var registerförda vid det förra verksamhetsårets utgång angavs vara 22 stycken. Under pågående översyn av förvaltningens behandlingar har totalt 54 personuppgiftsbehandlingar identifierats hittills. Den slutliga analysen och registreringen av samtliga personuppgiftsbehandlingar kvarstår att slutföras.

Äldreförvaltningen saknar idag rutiner för att identifiera nya eller följa upp registrerade personuppgiftsbehandlingar inom förvaltningens verksamhetsområden. För att verksamheten ska kunna hålla en korrekt, komplett och uppdaterad registerförteckning behöver sådana rutiner och arbetssätt etableras.

Denna slutsats baseras på DSO:s granskning av de behandlingar av personuppgifter som finns registrerade i systemet Draftit i förhållande till äldreförvaltningens verksamhetsprocesser och de personuppgiftsbehandlingar som utförs inom dessa. Att notera är att de behandlingar som registrerats i Draftit påbörjades 2019 och är inte slutförda. Den nu pågående kartläggningen förväntas utmynna i en ny och uppdaterad registerförteckning.

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

Som anges ovan är registerförteckningen en grundförutsättning för äldreförvaltningens dataskyddsarbete, exempelvis verksamhetens kännedom om huruvida verksamheten behandlar känsliga eller extra skyddsvärda personuppgifter. Nuvarande brister i

registerförteckningen och rutiner för registervård innebär att det föreligger en hög risk för att organisationen har en begränsad kännedom om och hur personuppgifter oavsett hur de klassas behandlas i olika verksamhetsprocesser och situationer. Därför bedömer jag som DSO att risken för de registrerades integritetsskydd fortfarande är hög och att den trots det påbörjade kartläggningsarbetet ligger kvar på samma nivå som förra årets bedömning, dvs. medelhög.

3.1.5 DSO ger råd och rekommendationer till PUA

I Äldreförvaltningens lokala anvisningar för informationssäkerhet, Dnr ALD 2024/453, finns en uppdragsbeskrivning för det operativa arbetet med dataskyddsfrågor och att det ska tillsättas en dataskyddshandläggare.

- PUA bör säkerställa att nödvändiga resursen tillsätts och att dataskyddshandläggaren ges tillräckliga förutsättningar, i form av tid och kompetensutveckling, samt för att genomföra löpande dataskyddsarbetet.

Vidare har förvaltningen påbörjat ett arbete för att ta fram en långsiktig struktur till registerförteckning och för förvaltningen av den samma.

- PUA bör fortsätta arbetet med att utarbeta rutiner för att följ upp och förvalta registervården inom äldreförvaltningens verksamhet.

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?	Delvis
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Delvis
Är dokumenten uppdaterade?	Delvis
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Delvis

3.2.2 Syfte

En röd tråd i dataskyddsförordningen regler och krav är att viktiga arbetssätt och rutiner ska vara dokumenterade och kommunicerade inom organisationen. Med stöd av tydliga och relevanta styrdokument kan PUA visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Med stöd av styrdokumenten kommunicerar PUA vad som gäller och vad som förväntas av medarbetarna när de hanterar personuppgifter i den dagliga verksamheten.

Stockholms stads övergripande styrdokument för dataskyddsarbetet inom staden är, Riktlinjer för informationssäkerhet i Stockholms stad, beslutad av kommunfullmäktige 2022-02-21. I dokumentet anges bland annat nämnderna ansvarar för dataskyddsarbetet inom den egna verksamheten. Den övergripande styrningen ska därefter förtydligas i lokala tillämpningsanvisningar och anpassas till förvaltningsnivån genom interna rutiner och mallar. 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.

3.2.3 Resultat

Under 2024 har förvaltningens informationssäkerhetssamordnare, ISAM, utarbetat lokala anvisningar för äldreförvaltningen. Vidare har det under året tagits fram rutiner och en mall för rapportering av personuppgiftsincidenter.

Kvarstår att ta fram är:

- En rutin för hur verksamheten hanterar inbyggt dataskydd och dataskydd som standard i verksamhetens olika processer. Syftet är bland annat att minska risken för att medarbetarna gör manuella fel när de ska distribuera information till medborgare eller andra parter.

- En rutin för konsekvensbedömning avseende dataskydd. Rutinen bör utarbetas i enlighet med de dokument som tagits fram av staden centralt och anpassas till en rutin för äldreförvaltningen. Av den lokala rutinen ska det framgå: när en konsekvensbedömning ska genomföras, vem som ska genomföra bedömningen, samt innefatta hur bedömningen ska dokumenteras och hur den ska tas om hand.

- En rutin för hur verksamheten hanterar information till den registrerade gällande personuppgiftsbehandlingen.

- En rutin för hur verksamheten hanterar den registrerades rättigheter och klagomål från dem.

Kännedom om styrdokumenten bland organisationens medarbetare samt chefer och ledningspersoner på alla styrnivåer är av väsentlig betydelse. Det är därför viktigt att det återkommande görs insatser för att öka kännedomen om äldreförvaltningens dataskyddsarbete och de styrdokument som gäller för verksamheten. Detta bör därför vara ett utvecklingsområde även för år 2025.

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
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

Relevanta styrdokument finns på stadsövergripande nivå men de behöver kompletteras med lokala anvisningar och rutiner. Styrdokumenten är viktiga grundläggande delar i dataskyddsarbetet och är ett stöd för att begränsa risken för att:

- enskildas rättigheter åsidosätts,
- personuppgiftsincidenter uppstår,
- äldreförvaltningen behandlar personuppgifter i onödan eller på fel sätt, samt
- äldreförvaltningen hanterar personuppgifter på sätt som i övrigt strider mot regelverket.

Bristerna kan på sikt vid klagomål från registrerade eller granskning från tillsynsmyndigheten kan resultera i sanktionsavgifter eller skadeståndskrav.

3.2.5 DSO ger råd och rekommendationer till PUA

- PUA bör fortsätta att se över befintliga styrdokument samt upprätta nya där sådana saknas idag.
- PUA bör etablera rutiner för återkommande kommunikationsinsatser i form av internutbildningar i syfte att höja och bibehålla förvaltningens lednings och medarbetares kunskaper om vilka krav och rutiner som gäller vid verksamhetens behandling av personuppgifter.

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?	Okänt
Är klassade personuppgiftsbehandlingar aktuella?	----

3.3.2 Syfte

Informationssäkerhetsklassningen av förvaltningens information är en grundläggande förutsättning för att verksamheten ska kunna välja rätt åtgärder för att skydda sin information, inkl. de personuppgifter som behandlas. Därför är det av stor betydelse för dataskyddsarbetet att PUA varje år ges en uppdaterad bild av om och vilka av verksamhetens personuppgiftsbehandlingar som säkerhetsklassats.

3.3.3 Resultat

Av de underlag jag som DSO fått ta dela av, rörande centralt upphandlade eller utvecklade system, utgår jag från att tekniska och organisatoriska skyddsåtgärder vidtagits på central nivå i Staden. Det har dock som DSO varit svårt att få tillgång till relevant information och den dokumentation som finns rörande systemen.

De åtgärder som vidtagits på central nivå behöver följas upp och kompletterande lokala organisatoriska åtgärder vidtas. Äldreförvaltningens bedömning av vilka skyddsåtgärder som förvaltningen behöver vidta sker i samband med verksamhetens informationsklassning med tillhörande risk- och sårbarhetsanalys samt i den konsekvensbedömning som göras av personuppgiftsbehandlingar enligt dataskyddsförordningen.

Arbetet med informationsklassningar som påbörjades på central nivå 2023 har fortsatt även under 2024 och äldreförvaltningen har deltagit i normerande klassningar för it-system som driftas av Sociala system. Det kvarstår dock flera områden där informationsklassningen nyligen påbörjats eller är i behov av att klassningar genomföras. Äldreförvaltningens verksamheter behöver därför fortsätta att granska och bedöma lämpliga tekniska och organisatoriska åtgärder i det fortsatta arbetet med klassning av verksamhetens behandlingar av personuppgifter.

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

Arbetet med normerande klassningar är under fortsatt utveckling vilket kommer att påverka klassningsarbetet positivt då möjligheten att ta del av information om genomförda klassningar i sociala system ökar.

Eftersom frågan om lämpliga tekniska och organisatoriska skyddsåtgärder är av grundläggande betydelse för förvaltningens informationssäkerhet och därmed också för behandlingen av känsliga och integritetskänsliga personuppgifter och därmed för de registrerades (enskildas) rättigheter, bedöms risken som medellåg. Det förutsätts emellertid att det pågående arbetet fortsätter som planerat och inte stannar av.

3.3.4 DSO ger råd och rekommendationer till PUA

- PUA bör säkerställa att arbetet med informationsklassningar av äldreförvaltningens samtliga verksamhetsprocesser, i synnerhet de som omfattar personuppgiftsbehandlingar, som planerats under 2025 genomförs.

- PUA bör säkerställa att behörighetstilldelning för de system som omfattar personuppgiftsbehandlingar, och då särskilt de som omfattar känsliga eller extra skyddsvärda personuppgifter ses över och att rutiner för hanteringen av dessa tas fram.

- PUA bör ge äldreförvaltningen i uppdrag att utreda vilka organisatoriska och tekniska skyddsåtgärder som behöver vidtas för att begränsa risken för att enskildas integritet skadas genom att personuppgifter, särskilt känsliga sådana, sprids på olämpligt sätt.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

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

3.4.2 Syfte

I datasskyddsförordningen ställs ett uttryckligt krav på att konsekvensbedömningar ska utföras för alla behandlingar av personuppgifter som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”. Syftet med bedömningarna är att identifiera och dokumentera risker kopplade till verksamhetens olika behandlingar av personuppgifter. Baserat på resultatet av konsekvensbedömningen kan PUA vidta lämpliga riskförebyggande åtgärder vid hanteringen av personuppgifter inom verksamheten.

I likhet med registerförteckningen och informationsklassningen är konsekvensbedömningen ett viktigt verktyg för verksamhetens dataskyddsarbete. Genom att genomföra konsekvensbedömningar kan äldreförvaltningen identifiera och minimera integritetsriskerna vid hanteringen av de personuppgifter som behandlas i verksamheten.

3.4.3 Resultat

Under senhösten 2024 har ett större arbete påbörjats för att identifiera äldreförvaltningens olika personuppgiftsbehandlingar. I arbetet ingår att bedöma vilka av dessa behandlingar som innebär en ”hög risk för den registrerade” och som därför förutsätter att en konsekvensbedömning genomförs. Efter en genomgång av de personuppgiftsbehandlingar som utförs inom verksamhetsområdet ”Bistå stadens äldre” är den initiala bedömningen att flera konsekvensbedömningar kommer att behöva genomföras inom området.

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

Trots det arbete som påbörjats under hösten 2024 är äldreförvaltningens dataskyddsarbete eftersatt, särskilt med avseende på att identifiera och förteckna förvaltningens behandlingar samt genomföra konsekvensbedömningar. Sammantaget innebär det att underlagen och förutsättningarna för att bedöma behovet av konsekvensbedömningar och att genomföra dess saknas. Det i sin tur innebär att förvaltningen idag saknar dokumenterad kunskap om vilka bristerna i behandlingarna är och vilka åtgärder som den behöver och kan vidta för att stärka skyddet för den enskildes integritet.

3.4.5 DSO ger råd och rekommendationer till PUA

- PUA bör säkerställa att det påbörjade arbetet med att identifiera äldreförvaltningens personuppgiftbehandlingar slutförs och att nödvändiga konsekvensbedömningar genomförs.

- PUA bör utveckla rutiner för att förvalta och revidera gjorda och tillkommande konsekvensbedömningar.

3.5 Individens rättigheter

3.5.1 Sammanfattning

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

3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen ett antal rättigheter som på olika sätt ska garantera att den registrerade individen har insyn i hur den enskildes personuppgifter hanteras.

Rättigheterna medför en rätt för den registrerade att ställa krav på att den verksamhet som är personuppgiftsansvarig på begäran vidtar vissa åtgärder, som exempelvis att lämna ut ett s.k. registerutdrag eller att rätta felaktiga uppgifter. Äldreförvaltningen har enligt dataskyddsförordningen en skyldighet att vidta åtgärden inom trettio dagar efter att den ha mottagit begäran.

Om förvaltningen inte klarar av att hantera en begäran från en registrerad person i enlighet med dataskyddsförordningens krav, kan det skada allmänhetens förtroende för hur staden och äldreförvaltningen hanterar personuppgifter. Det kan också leda till tillsynsärenden från Integritetsskyddsmyndighetens (”IMY”) sida, med förelägganden och eventuella sanktioner som följd.

3.5.3 Resultat

Under året har en begäran om registerutdrag inkommit. Begäran hanterades inom tidsrymden om 30 dagar.

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

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

Av granskningen framgick att det under året endast kommit in en rättighetsförfrågan till äldreförvaltningen och att handläggningen av ärendet kunde hanteras trots avsaknaden av rutiner för hanteringen av sådana förfrågningar. Oavsett det att handläggarna kunnat hantera situationen innebär äldreförvaltningens avsaknad av ett strukturerat arbetssätt, såsom

- rutiner för hanteringen av förfrågningar,
- bristande i information till de registrerade och
- anpassade blanketter för rättighetsbegäran på äldreförvaltningens hemsida,

en betydande risk för de registrerades möjligheter att utöva sina rättigheter. Det sammantaget med de brister som identifieras inom föregående områden är risken stor för att vissa behandlingar som kan vara aktuella vid en rättighetsbegäran inte beaktas i samband med begäran och att den enskildes rättigheter inte kan uppfyllas. Sammantaget innebär det att jag som DSO bedömer risken som medelhög.

3.5.5 DSO ger råd och rekommendationer till PUA

- PUA bör säkerställa att det finns tillämpliga och för äldreförvaltningen anpassade rutiner för hantering av förfrågningar om registerutdrag och rättighetsbegäran samt att dessa är kända inom organisationen så att ett ärende kan hanteras av samtliga verksamheter som behandlar personuppgifter.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Verksamheterna har en utarbetad rutin som verksamheten följer.
Hur många personuppgiftsincidenter har dokumenterats?	Fyra
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	En incident har rapporterats till IMY
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Samtliga

3.6.2 Syfte

Med begreppet personuppgiftsincident avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. En korrekt hanteringen av personuppgiftsincidenter är därför en viktig och obligatorisk del i dataskyddsarbetet.

I dataskyddsförordningen finns det krav på att omständigheterna kring en personuppgiftsincident, dess effekter och de korrigerande åtgärder som vidtagits ska dokumenteras och rapporteras till tillsynsmyndigheter. Syftet med dokumentationen och rapporteringen är att göra det möjligt för tillsynsmyndigheten att kontrollera verksamhetens regelefterlevnad. En bristande dokumentation är därför sanktionsgrundande.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Detta innebär att det för samtliga personuppgiftsincidenter ska göras en bedömning om de ska rapporteras till tillsynsmyndigheten, IMY. Om verksamheten beslutar att IMY ska underrättas ska rapportering ske senast 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska

personers rättigheter och friheter, ska avvägning göras om rapportering även ske till de berörda registrerade personerna, utan dröjsmål.

Incidentrapporteringen är också en indikator på hur väl verksamheten förstår vad som utgör en incident och att den ska rapporteras. Den ger kunskap om hur rutiner och arbetssätt kan utvecklas för att höja säkerheten i personuppgiftsbehandlingen.

3.6.3 Resultat

Under det gångna året har fyra incidenter inträffat, varav en har rapporterats till IMY. Incident rapporterades inom 72 timmar.

Under året har äldreförvaltningen etablerat en rutin för att snabbare upptäckt, utreda och bedöma av personuppgiftsincidenter. Rutinen är känd inom verksamheten vilket inneburit att fler incidenter rapporterats under 2024 än året innan. Det i sig innebär inte att det under 2024 inträffat fler incidenter än under tidigare år utan snarare att fler har rapporterats och därmed kunnat hanteras i enlighet med rutinen.

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

Med utgångspunkt från att det under året tagits fram och etablerats rutiner rapportering av personuppgiftsincidenter och att kännedomen om rutinen ökat bedöms risken som lägre i år än förra året. Det finns emellertid en fortsatt risk för dröjsmål från identifiering till utredning och rapportering av personuppgiftsincidenterna till tillsynsmyndigheten.

Av de rapporter som gjorts framgår att incidenterna inträffat i kontakter med externa leverantörer av tjänster inom äldreomsorgen. Tillgängliga organisatoriska och tekniska säkerhetsåtgärder för hantering av dessa kontakter bör därför ses över. Det är också

angeläget att äldreförvaltningen fortsätter att utveckla lokala hanteringsrutiner för att hantera och förebygga incidenter och att rapporteringsrutinen genomförs på utsatt tid.

3.6.5 DSO ger råd och rekommendationer till PUA

- PUA bör löpande tillse att personal är insatta i rutiner och övriga dokument på området samt har en tillräcklig kunskap för att kunna upptäcka och rapportera personuppgifts-incidenter samt avslutar rapporteringen i tid.

4 Genomförda granskningar under året

4.1 Sammanfattning

Utvecklingsarbetet av dataskydd och informationssäkerhet har fortsatt under hela 2024. Vilket innebär att det ännu inte finns en tillfredsställande organisation för dataskyddsarbetet etablerad. Den övergripande beskrivningen av dataskyddsarbetet och rollfördelningen mellan dataskyddssamordnaren, DSO och dataskyddshandläggare beskrivs i, Tillämpningsanvisning till stadens riktlinje för informationssäkerhet och i äldreförvaltningens lokala anvisning för informationssäkerhet. Den senare beslutades av äldredirektören den 16 december 2024.

I DSO:s årsrapport för 2023 angavs det som angeläget att arbetet med DSO:s granskningar skulle påbörjas under 2024, dock utan att en plan presenterades. Den granskning som genomförts under 2024 är därför övergripande och har främst varit inriktad på att fastställa aktuell status på äldreförvaltningens dataskyddsarbete.

5 Risker inom dataskydd

5.1 Sammanfattning

Resultatet för flera av de obligatoriska granskningspunkterna ligger på en medelhög risknivå. Det kan bland annat förklaras av att grundläggande förutsättningar för ett adekvat dataskyddsarbete saknas. Nedan redovisas vilka granskningspunkterna är och vilka

risker bristerna kan innebära för registrerade i äldreförvaltningens verksamhet

Relevanta risker inom verksamheten:

- Nuvarande brister i registerförteckningen och strukturen för registervård innebär:
    - att äldreförvaltningen har begränsad kännedom om hur känsliga eller särskilt skyddsvärda personuppgifter behandlas i olika verksamhetsprocesser och situationer, samt
    - att konsekvensbedömningar för dessa kategorier av personuppgiftbehandlingar inte genomförts.

- Handläggningen av dataskyddsfrågor är idag reaktivt då det saknas samordnade gemensamma rutiner som förvaltningen enkelt kan följa, vilket leder till:
    - att skyddet av enskildas uppgifter kan hanteras olika inom äldreförvaltningens olika verksamhetsprocesser, samt
    - att handläggare får lägga mycket tid på att försöka hitta rätt och utreda vad som behöver göras, exempelvis när en registrerad lämnar in en rättighetsbegäran eller ett klagomål.

Sammantaget innebär bristerna innebär en relativ hög risk för att fysiska personers rättigheter och friheter inte kan säkerställas. En närmare beskrivning av riskerna i verksamheten redovisas mer i detalj i kapitel 3 ovan.

5.2 DSO ger råd och rekommendationer till PUA

Under hösten 2024 har äldreförvaltningen påbörjat ett grundläggande arbete för att organisera verksamhetens dataskyddsarbete. I det ingår att kartlägga förvaltningens olika personuppgiftsbehandlingar, att upprätta en registerförteckning i enlighet med dataskyddsförordningen och att genomföra vissa konsekvensbedömningar. När det arbetet är slutfört kommer några av de redovisade bristerna förhoppningsvis att vara åtgärdade.

Det dock viktigt att understryka att det arbete som genomförs nu endast är en engångsinsats som just syftar att lägga grunden för äldreförvaltningens dataskyddsarbete. Den fortsatta hanteringen av förvaltningens dataskyddsarbete måste fortsätta att utvecklas och

förvaltas. Äldreförvaltningen bör därför säkerställa att resurser avsätts för hanteringen och förvaltningen av dataskyddsarbetet i verksamheten.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

1. Äldreförvaltningens organisation av dataskyddsarbetet och hur den fungerar.
2. Registerförteckningens status och behov av eventuella kompletteringar.
3. Genomförda konsekvensbedömningar samt om det finns behov av att genomföra ytterligare bedömningar.
4. Rutiner för hantering av registrerades rättigheter.

6.2 Syfte

Fokus för granskningen 2025 bör även fortsatt ligga på de risker som har identifierats i denna årsrapport för att på så sätt säkerställa en fortsatt strukturering och utveckling av äldreförvaltningens dataskyddsarbete. Målet för arbetet bör vara att åtgärda bristerna och att säkerställa skyddet för de registrerades dataskyddarbete.