Stockholms stad

Dataskyddsombudets årsrapport

2023

Äldrenämnden

Dataskyddsombudets årsrapport 2023
Januari 2024

Dnr: ALD 2023/205
Utgivningsdatum: 2023-02-07
Kontaktperson: Jonathan Storm

Innehåll

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. Med personuppgifter avses varje upplysning som avser en identifierad eller identifierbar fysisk person.

Enligt dataskyddsförordningen är varje myndighet, såsom äldrenämnden, personuppgiftsansvarig (”PUA”), d.v.s. ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Personuppgiftsansvarig är alltså den organisation, som bestämmer för vilka ändamål personuppgifter ska behandlas och hur behandlingen ska gå till. Det är alltså inte chefen på en arbetsplats eller en anställd som är personuppgiftsansvarig.

Personuppgiftsansvaret innebär vidare att nämnden behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd i Stockholms stad har i enlighet med dataskyddsförordningen utsett ett Dataskyddsombud (”DSO”).

Den övergripande och viktigaste uppgiften för DSO:n är att övervaka att organisationen följer dataskyddsförordningen. Det innebär bl.a. att

- samla in information om hur organisationen behandlar personuppgifter
- kontrollera att organisationen följer bestämmelser och interna styrdokument
- informera och ge råd inom organisationen

Dataskyddsombudet ska också

- ge råd om konsekvensbedömningar
- vara kontaktperson för tillsynsmyndigheten Integritetsskyddsmyndigheten (”IMY”)
- vara kontaktperson för de registrerade, d.v.s. de vilkas personuppgifter behandlas, och personalen inom organisationen
- samarbeta med IMY, till exempel vid inspektioner.

DSO:n har alltså till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

DSO:n har inget eget ansvar för att organisationen följer dataskyddsförordningen. Det ansvaret ligger alltid hos den personuppgiftsansvariga eller hos personuppgiftsbiträdet. Vidare ska DSO:n kunna arbeta självständigt och oberoende, utan att bli påverkad av andra inom organisationen. Det är därför viktigt att DSO:n inte har andra arbetsuppgifter som kan komma i konflikt med rollen som DSO.

Denna årsrapport är således ett medel för nämnden 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 den 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 dataskyddsarbete

2 Sammanfattning

I egenskap av Dataskyddsombud lämnar jag följande årsrapport.

Följande slutsatser har dragits av uppgifterna i årsrapporten:

- Registerförteckningen (registret över alla personuppgiftsbehandlingar som görs i verksamheten) är ofullständig och har omfattande behov av utveckling.
  Innebörden av detta är bland annat att organisationen kan sakna kännedom om ifall känsliga eller extra skyddsvärda personuppgifter behandlas i verksamheten.

Utöver detta behöver följande områden fortsätta utvecklas:

- Styrdokument
- Hantering av personuppgiftsincidenter
- Konsekvensbedömningar
- Säkerhetsåtgärder
- Hantering av den registrerades rättigheter

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 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?	22 verksamhetsområden eller verksamhetsprocesser, vissa ofullständigt registrerade.
Har nödvändiga uppdateringar gjorts?	Nej.
Bedöms registerförteckningen vara fullständig?	Nej.
Har verksamheten lämpliga rutiner för registerföring?	Nej.

3.1.2 Syfte

Syftet med detta rapporteringsområde är att rapportera till PUA hur väl verksamheten har lyckats inventera sina personuppgifter och de personuppgifter som behandlas för annans räkning och upprätta en registerförteckning.

För att något ska gå att skydda måste det först vara synligt för verksamheten. 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 samt säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling.

Att ha en registerförteckning på plats leder till att verksamheten kan arbeta mer resurs- och kostnadseffektivt med sitt systematiska och riskbaserade dataskyddsarbete. Man kan styra insatserna dit de gör störst nytta.

3.1.3 Resultat

Antalet personuppgiftsbehandlingar som var registerförda vid det förra verksamhetsårets utgång: 22 verksamhetsområden (typer av behandlingar). Behov av uppdateringar av registerförteckningen kvarstår.

Det finns ytterligare system och behandlingar som ännu inte dokumenterats i registerförteckningen. Denna slutsats baseras på DSO:s egen erfarenhet av organisationens system och behandlingar som görs inom organisationen.

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

Eftersom registerförteckningen är en grundförutsättning och således av avgörande betydelse för allt annat dataskyddsarbete, innebär handlingen i sitt nuvarande skick att det föreligger risk för att organisationen saknar kännedom om känsliga eller extra skyddsvärda personuppgifter behandlas i olika sammanhang och situationer samt om det överhuvudtaget sker några tredjelandsöverföringar av personuppgifter, oavsett vilken kategori uppgifterna tillhör.

3.1.5 DSO ger råd och rekommendationer till PUA

PUA har tidigare beslutat om uppdragsbeskrivning för personal som operativt ska arbeta med dataskyddsfrågor (dataskyddshandläggare). Bedömningen är att det fortsatt finns ett behov att implementera rollen i den löpande verksamheten.

Bedömningen är vidare att verksamheten fortsatt är i behov av att utveckla strukturer för arbetet med registerförteckning.

3.2 Styrdokument

3.2.1 Sammanfattning

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

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.

3.2.3 Resultat

- Rutin för hur verksamheten hanterar inbyggt dataskydd och dataskydd som standard i verksamhetens processer och rutiner behöver utvecklas. Detta innebär bl.a. att minska risken för att medarbetarna gör manuella fel när de ska distribuera information till medborgare eller andra. Dessutom behöver organisationen ta höjd för och genomföra analyser av hur de grundläggande principerna i dataskyddsförordningen ska beaktas i relevanta processer och rutiner.

De grundläggande principerna innebär bl.a. att PUA

- måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter
- bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål
- inte ska behandla fler personuppgifter än vad som behövs för ändamålen
- ska se till att personuppgifterna är riktiga
- ska radera personuppgifterna när de inte längre behövs
- ska skydda personuppgifterna, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs
- ska kunna visa att och hur organisationen lever upp till dataskyddsförordningen

- Personuppgiftsincidentrutinen behöver kompletteras så att det tydligt framgår hur personuppgiftsincidenter ska utredas, analyseras, rapporteras och dokumenteras samt vilken roll som ansvarar för vad i detta förfarande.

- Rutinen för konsekvensbedömning behöver ses över med anledning av dokument som tagits fram av staden centralt och som alltså ska ligga till grund för organisationens egen rutin. Det behöver även fortsättningsvis framgå av rutinen när och av vem en konsekvensbedömning avseende dataskydd ska genomföras i verksamheten samt innefatta hur bedömningen ska dokumenteras och av vem den ska tas om hand.

Kännedom om styrdokumenten bland organisationens medarbetare är av väsentlig betydelse, varför det bör vara ett utvecklingsområde för år 2024.

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

Relevant dokumentation finns delvis. Befintliga dokument behöver uppdateras och kompletteras.

Om dokumentation saknas finns risker för enskildas rättigheter, att personuppgiftsincidenter kan uppstå, att organisationen behandlar personuppgifter i onödan eller på fel sätt samt för agerande eller underlåtenhet som i övrigt strider mot regelverket. På lite längre sikt kan det resultera i sanktionsavgifter eller skadeståndskrav.

3.2.5 DSO ger råd och rekommendationer till PUA

DSO ser behov av återkommande insatser i form av internutbildningar och praktiska övningar i syfte att förvaltningens medarbetare ska lära sig om bland annat rutiner samt inbyggt dataskydd och dataskydd som standard. Verksamheten skulle kunna integrera hela eller delar av dessa insatser i befintliga forum.

Utöver det rekommenderas att befintliga rutiner och styrdokument ses över och uppdateras, eller upprättas i de fall de saknas.

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?	Delvis.

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

3.3.3 Resultat

Informationsklassning har under året genomförts för ett antal områden som innefattar personuppgiftsbehandlingar, men det kvarstår flera områden där det är pågående eller i behov att göras. Det innebär att det är rimligt att anta att lämpliga tekniska och organisatoriska åtgärder måste vidtas för klassning av övriga behandlingar.
För centralt upphandlade system har tekniska och organisatoriska åtgärder som utgångspunkt vidtagits på central nivå i Staden. Detta innebär dock inte att organisationen kan avstå från att på lokal nivå tillse att organisatoriska åtgärder vidtas, exempelvis genom behörighetsbegränsningar gällande dessa system.

Utöver detta måste varje organisation enligt Stadens riktlinjer för informationssäkerhet göra egna klassningar, vilket också inkluderar information som organisationen hanterar i centralt upphandlade system. Detsamma gäller frågan om konsekvensbedömningar enligt dataskyddsförordningen, i de fall det följer av ovan nämnda regelverk att konsekvensbedömning ska göras.

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

Arbetet med informationsklassning är i behov av utveckling. Frågan om lämpliga tekniska och organisatoriska skyddsåtgärder är av grundläggande betydelse för informationssäkerheten, däribland för känsliga och integritetskänsliga personuppgifter och således för de registrerades (enskildas) rättigheter, varför risken är medelhög.

3.3.5 DSO ger råd och rekommendationer till PUA

PUA bör utse ansvarig för att säkerställa att informationsklassningar görs av samtliga verksamhetsprocesser, i synnerhet de som omfattar personuppgiftsbehandlingar.

PUA bör se över och förtydliga styrningen av behörighetstilldelning för de system som omfattar personuppgiftsbehandlingar, i synnerhet de som omfattar känsliga eller extra skyddsvärda personuppgifter.

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

Konsekvensbedömningen hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas i verksamheten. 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 eller 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”.

3.4.3 Resultat

Det återstår ett betydande arbete med att identifiera alla konsekvensbedömningar som borde genomföras. I det arbetet ingår också att göra konsekvensbedömningar för alla potentiella högriskbehandlingar av personuppgifter.

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

Arbetet med att identifiera alla behandlingar där konsekvensbedömning bör göras är eftersatt, varför det, särskilt med avseende på syftet med konsekvensbedömningar och de kategorier av personuppgifter som för närvarande behandlas av organisationen, föreligger förhållandevis hög risk.

3.4.5 DSO ger råd och rekommendationer till PUA

PUA bör utveckla rutiner för att säkerställa att konsekvensbedömning görs i anslutning till informationsklassningen i de fall där personuppgiftsbehandling förekommer.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många förfrågningar (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	En.
Hur många av dessa förfrågningar 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 personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att den verksamhet som enligt förordningen är att se som personuppgiftsansvarig – d.v.s. i stadens fall nämnder och bolag – tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, som exempelvis att lämna ut ett s.k. registerutdrag eller att rätta vissa uppgifter. Verksamheten har enligt dataskyddsförordningen 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 Intetgritetsskyddsmyndighetens (”IMY”) sida, med 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
	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 anledning av att det endast inkommit en förfrågan inom detta område bedöms risken vara medellåg. Risken kan inte anses låg då organisationens strukturerade arbetssätt, såsom rutiner, är i behov av utveckling. Den risk som trots allt identifieras på detta område ansluter sig också till föregående områden, i det avseende att samtliga behandlingar inte är kartlagda och därför potentiellt missas.

3.5.5 DSO ger råd och rekommendationer till PUA

PUA bör utse ansvarig för att säkerställa att det finns en uppdaterad och tillämplig rutin för hantering av förfrågningar av registerutdrag m.m.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Det finns rutiner för detta.
Hur många personuppgiftsincidenter har dokumenterats?	Två.
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Två incidenter har rapporterats till IMY.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Samtliga.

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen 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.

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”. Detta innebär att det gällande samtliga personuppgiftsincidenter ska göras en bedömning om de ska rapporteras till IMY, och eventuell rapportering ska 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.
Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering till de berörda personerna.

Enligt dataskyddsförordningen 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

Under det gångna året har två incidenter inträffat som rapporterats till integritetsskyddsmyndigheten. Båda incidenterna har rapporterats inom 72 timmar, men har ändå gett skäl att understryka att de hade kunnat hanteras snabbare om verksamheten haft väl etablerade rutiner för upptäckt, utredning och bedömning av personuppgiftsincidenter.

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
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

Utifrån de personuppgiftsincidenter som rapporterats under året är bedömningen att risken är medelhög då det funnits onödiga dröjsmål från identifiering till utredning och rapportering av de personuppgiftsincidenter som uppstått.
Det finns också, utifrån DSO:s kunskap om verksamheten, vissa skäl att tro att incidenter som uppstått under året kanske inte rapporterats och dokumenterats.

Bedömningen är att det är angeläget för verksamheten att utveckla och implementera såväl kunskap kring som rutiner för incidenthantering för att säkerställa att personuppgiftsincidenter identifieras och anmäls i tid.

3.6.5 DSO ger råd och rekommendationer till PUA

Alla chefer bör få i uppdrag av PUA att till slutet av året tillse att personal är insatta i rutiner och övriga dokument på området samt har en tillräcklig kunskap för att kunna upptäcka och rapportera personuppgiftsincidenter i tid.

4 Genomförda granskningar under året

4.1 Sammanfattning

Då en stor del av arbetet med dataskydd och informationssäkerhet ännu är pågående och en tillfredsställande organisation för dataskyddsarbetet och DSO-rollen inte finns etablerade har det inte gjorts några granskningar under året.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten redovisas ovan, under respektive rapporteringsområde.

6 Planerade granskningar för 2024

6.1 Sammanfattning

Med anledning av att någon granskning inte gjorts under 2023 anses det vara angeläget att arbetet med granskningar påbörjas under 2024, förutsatt att det bedöms vara relevant i relation till det pågående arbetet med utveckling av dataskyddsarbetet samt genomförande av informationsklassningar och konsekvensbedömningar.