Stockholms stad

Bilaga 4

ÖST 2023/12

GDPR Årsrapport

År 2022

Östermalms stadsdelsnämnd

GDPR årsrapport
Januari 2023

Dnr: ÖST 2023/12
Utgivningsdatum: 2023-02-21
Kontaktperson: Jennifer Gavin, kanslichef

1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd och bolagsstyrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett Dataskyddsombud (”DSO”). DSO:n har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

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

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

Innehåll

2 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

Årsrapporten består dels av granskning kring sex obligatoriska rapporteringsområden som Personuppgiftsansvarig (”PUA”) som ett minimum ska informera sig om årligen, dels granskningar som DSO på egen hand genomfört utifrån separata riskbedömningar.

Det kan sammanfattningsvis konstateras att förvaltningen redovisat goda resultat vid granskning kring följande områden:

- Uppdaterade styrdokument
- Individens rättigheter
- Personuppgiftsincidenter

Vad gäller nedanstående områden har dock brister identifieras:

- Registerförteckning
- Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar
- Konsekvensbedömningar

För de områden som brister identifierats har åtgärder föreslagits. Vissa av dessa åtgärder är redan påbörjade och kommer slutföras under våren 2023.

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.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	524
Har nödvändiga uppdateringar gjorts?	Nej
Bedöms registerförteckningen vara fullständig?	Registerförteckningen kan inte anses vara fullständig
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

Dataskyddsförordningens artikel 30 ställer krav på att PUA måste inventera alla personuppgifter som behandlas i verksamheten och dokumentera dem i en så kallad registerförteckning.

En registerförteckning skapar en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Registerförteckningen är dataskyddsarbetets centrala utgångspunkt.

Syftet med detta rapporteringsområde är således att rapportera till PUA hur väl verksamheten har lyckats inventera sina personuppgifter och upprätta en registerförteckning.

3.1.3 Resultat

Förvaltningen upprättade inför införandet av Dataskyddsförordningen i maj 2018 en registerförteckning. Förteckningen är upprättad i en excel-fil. Under hösten 2020 och våren 2021 gick förvaltningens samtliga avdelningar igenom sina behandlingar i registerförteckningen och reviderade uppgifterna vid behov. Inför 2022 beslutade förvaltningsledningen om att ett omfattande arbete för att säkerställa en fullständig och ändamålsenlig registerförteckning skulle genomföras med slutdatum 31 maj 2023. I detta arbete ingår det att se över samtliga dokumenterade behandlingar och komplettera dessa i ett samlat dokument med en överskådlig struktur. Arbetet med detta har påbörjats men inte slutförts. Förvaltningen bedömer dock att arbetet kommer att vara slutfört till den 31 maj 2023.

I dagsläget har förvaltningen totalt 524 granskningar registrerade i förteckningen. Vid granskning av förteckningen kan det konstateras att det finns behov av revidering för att säkerställa att den är komplett och ändamålsenlig. Detta bedöms vara slutfört senast den 31 maj 2023.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.1.5 DSO ger råd och rekommendationer till PUA

DSO bedömer att det finns brister i förvaltningens registerförteckning. För att åtgärda dessa brister pågår det ett arbete som syftar till att säkerställa att registerförteckningen är komplett, ändamålsenlig och tydlig. Slutdatum för detta arbete är 31 maj 2023 och förvaltningen bedömer att arbetet kommer att slutföras inom denna tidsperiod. Mot bakgrund av detta bedömer DSO att det i dagsläget inte behöver vidtas några ytterligare åtgärder.

3.2 Styrdokument

3.2.1 Sammanfattning

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

3.2.2 Syfte

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

Syftet med rapporteringen av området är tvådelad: dels att bedöma om verksamheten har styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket ingår bl.a. att dokumentationen ska vara uppdaterad och aktuell.

3.2.3 Resultat

På förvaltningens intranät finns en sida med rubriken ”GDPR på Östermalm”. På denna sida finns samlad information för chefer och medarbetare. Utöver informationen som är sammanställd för förvaltningens chefer och medarbetare finns länkar till stadens

övergripande information och styrande dokument. Ett urval av dokumentationen:

- Rutin för hantering av personuppgiftsincident samt checklista
- Checklista för rensning av e-post
- Vägledning vid de registrerades begäran om tillgång, rättelse och radering av personuppgift
- Mallar för konsekvensbedömning, riskbedömning

Utöver rutindokument finns utförligt informationsmaterial på intranätet med instruktioner för vad verksamheten bör uppmärksamma och utföra. Till exempel kan nämnas informationsmaterialet ”GDPR i korthet för dig som chef” och ”GDPR i korthet för dig som medarbetare”. Det finns även hänvisningar till stadens gemensamma information på intranätet.

Sammanfattningsvis bedöms det finnas grundläggande styrdokument och informationsmaterial lättillgängligt på intranätet. Överlag är texterna anpassade till målgruppen. Inom områdena konsekvensbedömningar och riskbedömningar finns dock behov av kompletterande material för att underlätta för verksamheterna att genomföra dessa aktiviteter när behov finns av dessa.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

3.2.5 DSO ger råd och rekommendationer till PUA

DSO bedömer att det finns relevanta och uppdaterade styrdokument. DSO har gått igenom samtliga dokument och har gjort uppdateringar där det varit nödvändigt.

Då inga brister identifierats lämnas inga förslag på åtgärder. Däremot är det viktigt att säkerställa att befintliga dokument

ständigt hålls uppdaterade och att nya dokument, vid behov, upprättas.

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?	10
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av Sveriges kommuner och regioners 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 personuppgiftsansvarig ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

3.3.3 Resultat

Förvaltningen har totalt informationsklassat 10 behandlingar varav 3 är genomförda under 2022. Samtliga klassningar är inte mer än två år gamla och bedöms därmed som fortsatt aktuella.

Granskning visar att förvaltningen har påbörjat ett arbete med att informationsklassa sina behandlingar, men att det återstår mycket arbete med att utföra klassningar.

Förvaltningens informationssäkerhetssamordnare har under året tagit fram en konkret plan för när informationsklassningar ska genomföras för att säkerställa att arbetet med informationsklassning intensifieras under 2023.

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

3.3.5 DSO ger råd och rekommendationer till PUA

DSO bedömer att det finns brister kopplat till förvaltningens arbete med informationsklassning. För att åtgärda dessa brister behöver arbetet med att genomföra klassningar intensifieras under kommande år. För detta finns redan en upprättad plan. Mot bakgrund av detta bedömer DSO att det i dagsläget inte behöver vidtas några ytterligare åtgärder.

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 anses liksom registerförteckning och informationsklassning som ett viktigt verktyg för verksamhetens dataskyddsarbete. En konsekvensbedömning ska enligt dataskyddsförordningens artikel 35 utföras om en behandling av personuppgifter sannolikt leder till en hög risk för den registrerades integritet, rättigheter och friheter. 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.

En konsekvensbedömning är en arbetsrutin som ska utföras av verksamheten innan en behandling påbörjas. Däremot medför dock även kravet på konsekvensbedömning att även personuppgiftsbehandlingar som redan existerade när dataskyddsförordningen trädde i kraft behöver kartläggas och utredas i fråga om behovet av att utföra en konsekvensbedömning.

Det är viktigt att PUA genom årsrapporten får en uppdaterad bild av hur fullständig verksamhetens situation är i fråga om konsekvensbedömningar avseende dataskydd.

3.4.3 Resultat

Under året har förvaltningen genomfört 5 konsekvensbedömningar. Samtliga avser nya system och behandlingar som inrättats inom förvaltningens verksamheter och dessa bedöms därmed vara aktuella. Däremot har en inventering av befintliga personuppgiftsbehandlingar inte gjorts under året. Det kan därför inte uteslutas att det saknas konsekvensbedömningar.

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

3.4.5 DSO ger råd och rekommendationer till PUA

DSO bedömer att det finns brister kopplat till förvaltningens arbete med konsekvensbedömningar och att det inte kan uteslutas att förvaltningen inte fullgjort sin skyldighet att upprätta konsekvensbedömningar för samtliga behandlingar där det krävs. För att åtgärda detta rekommenderas förvaltningen att i det pågående arbetet med att upprätta en fullständig registerförteckning särskilt identifiera behovet av behandlingar där konsekvensbedömningar ska genomföras samt att säkerställa att dessa blir genomförda.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	3
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	3

3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt ska garantera att den registrerade personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att den verksamhet som är personuppgiftsansvarig – dvs. 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 så kallat registerutdrag eller att rätta vissa uppgifter. Radering, den så kallade ”rätten att bli glömd”, är dock sällan aktuell i någon större mån eftersom stadens verksamheter lyder under krav på bevarande till följd av offentlighetsprincipen. Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran.

3.5.3 Resultat

Under året har 3 begäran om registerutdrag, begränsning eller radering inkommit. Samtliga tre har hanterats av verksamheten inom 30 dagar. Förvaltningen har rutiner för hur begäran ska hanteras.

3.5.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten

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

3.5.5 DSO ger råd och rekommendationer till PUA

DSO bedömer att det inte finns några brister identifierade kopplat till förvaltningens arbete med att säkerställa den enskildes rättigheter. Då inga brister identifierats lämnas inga förslag på åtgärder.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Vanligtvis genom anställd eller utomstående/registrerad informerar förvaltningen
Hur många personuppgiftsincidenter har dokumenterats?	4
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	3
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	2

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.”

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att de flesta personuppgiftsincidenter ska rapporteras till Integritetsskyddsmyndigheten (IMY), inte senare än 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.

3.6.3 Resultat

Under året har 4 incidenter rapporterats i förvaltningen varav 3 incidenter har anmälts till Integritetsskyddsmyndigheten (IMY). Av

de 3 incidenterna som anmälts har 2 anmälts inom 72 timmar från upptäckt av incidenten.

Kunskapsnivån gällande personuppgiftsincidenter bedöms vara god inom förvaltningen. Vid inträffade incidenter vidtas åtgärder snabbt och verksamheterna genomför aktiviteter för att minska risken att incidenterna inträffar igen.

Det finns information på intranätet om hur verksamheterna ska gå tillväga för att utreda och anmäla personuppgiftsincidenter. En checklista vägleder verksamheten om vilken information som behöver tas fram för att hantera incidenten. Av delegationsordningen framgår vilken funktion som anmäler 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
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

3.6.5 DSO ger råd och rekommendationer till PUA

DSO bedömer att det inte finns några brister identifierade kopplat till förvaltningens arbete med att säkerställa den enskildes rättigheter. Då inga brister identifierats lämnas inga förslag på åtgärder däremot vill DSO påpeka att det är av största vikt att förvaltningen vidtar åtgärder för att underhålla den höga kunskapsnivån under kommande år.

4 Genomförda granskningar under året

4.1 Sammanfattning

I 2021 års årsrapport föreslogs följande granskningar för 2022:

- *Översyn av registerförteckningen*
- *Konsekvensbedömningar*
- *Personuppgiftsbiträdesavtal*

Under 2022 har samtliga områden granskats av förvaltningens dataskyddsombud. Nedan följer en beskrivning och resultat av dessa granskningar.

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 – Översyn av registerförteckningen

Under året har DSO granskat förvaltningens registerförteckning. Granskningen visar att det finns behov av revidering för att säkerställa att den är komplett och ändamålsenlig.

För närmare beskrivning och mer information se avsnitt 3.1.

	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 – Konsekvensbedömningar

Under året har DSO granskat förvaltningens genomförda konsekvensbedömningar. Granskningen visar att det för nya behandlingar och system genomförs konsekvensbedömningar där det bedöms nödvändigt. Det går dock inte att utesluta att det saknas konsekvensbedömningar för äldre behandlingar och system.

För närmare beskrivning och mer information se avsnitt 3.4.

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
X	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Granskning 3 – Personuppgiftsbiträdesavtal

Under året har DSO granskat förvaltningens personuppgiftsbiträdesavtal. Granskningen visar att det enbart upprättats två (2) personuppgiftsbiträdesavtal med leverantörer under 2022. Det framgår dock att det vid direktupphandlingar upprättas personuppgiftsbiträdesavtal. Sammanfattning av granskningen är att det är oklart huruvida förvaltningen fullgjort sina skyldigheter enligt dataskyddsförordningen och upprättat personuppgiftsavtal med personuppgiftsbiträden. DSO rekommenderar därför att en inventering av samtliga avtal med personuppgiftsbiträden genomförs samt att det skyndsamt, i de fall det behövs, upprättas personuppgiftsbiträdesavtal.

	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

Utifrån 2022 års granskningar lämnar DSO följande råd:

- PUA bör följa upp förvaltningens arbete med att säkerställa en komplett, ändamålsenlig och tydlig registerförteckning. Slutdatum för detta arbete är satt till 31 maj 2022.
- PUA bör följa upp förvaltningens arbete med att säkerställa att det finns konskensbedömningar för de behandlingar där det är nödvändigt. Detta görs genom uppföljning av ovanstående punkt.
- PUA bör följa upp förvaltningens arbete med att genomföra en inventering av samtliga avtal med personuppgiftsbiträden för att säkerställa att personuppgiftsbiträdesavtal upprättas i de fall det behövs.

5 Risker inom dataskydd

5.1 Sammanfattning

De primära riskerna som identifierats i verksamheten utifrån ett dataskyddsperspektiv under 2022 bedöms utgöras av:

- *Personuppgiftsbiträdesavtal* – risk att personuppgifterna hanteras utan att ansvarsfrågan för hanteringen är reglerad.
- *Registerförteckning* – personuppgifter hanteras felaktigt.

Utöver ovanstående risker som löper som en röd tråd genom denna slutrapport ska det påtalas att förvaltningen har hela tio (10) kontrollmoment kopplat till dataskydd i internkontrollplanen för 2023.

5.2 Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser som exempelvis konsekvensbedömningar och informationsklassningar. Dessa riskanalyser ger dock inte en heltäckande bild av samtliga personuppgiftsrisker 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 - Personuppgiftsbiträdesavtal

Att personuppgifter hanteras utan att ansvarsfrågan för hanteringen är utredd och reglerad i avtal har bedöms som en stor risk. Granskning av personuppgiftsbiträdesavtal under 2022 visar att det saknas en heltäckande bild av förvaltningens upprättade personuppgiftsbiträdesavtal, se ovan under rubrik 4.3. Risken är identifierad och integrerad i förvaltningens internkontrollplan för 2023 och kommer således även att följas upp inom ramen för denna.

	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 – Registerförteckning

Att förvaltningen har bristande kontroll över sina personuppgiftsbehandlingar till följd av en ofullständig registerförteckning har bedöms som en stor risk. Granskning av registerförteckningen under 2022 visar att det saknas en komplett och ändamålsenlig registerförteckning, se ovan under rubriken 3.1. Risken är identifierad och integrerad i förvaltningens internkontrollplan för 2023 och kommer således även att följas upp inom ramen för denna.

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

5.4 DSO ger råd och rekommendationer till PUA

PUA bör följa förvaltningens arbete för att säkerställa att ovanstående risker minimeras och elimineras. För detta har det föreslagits åtgärder i denna rapport, se avsnitt 4.4. Vidare kommer riskerna löpande att följas upp inom ramen för förvaltningens internkontrollplan.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

De största och återkommande riskerna och där DSO identifierat behov av störst åtgärder under 2022 bör följas upp under 2023 för att säkerställa att arbetet genomförts i enlighet med plan. Relevanta granskningsområden inom verksamheten under 2023 bedöms därmed utgöras av:

- *Registerförteckning* – personuppgifter hanteras felaktigt.
- *Personuppgiftsbiträdesavtal* – risk att personuppgifterna hanteras utan att ansvarsfrågan för hanteringen är reglerad.

6.2 Syfte

En av uppgifterna i rollen som dataskyddsombud är att granska personuppgiftsansvarigs efterlevnad av dataskyddsförordningen. Granskningsområdena bör lämpligen väljas utifrån ett riskbaserat synsätt, det vill säga att fokus bör ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därigenom åstadkoms en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

Följande granskningar planeras att genomföras under 2023. Utifrån kontinuerlig riskbedömning kan planering och prioritering av granskningar förändras under året.

6.3 Planerade granskningar

Granskning 1 - Registerförteckning
Kontroll av att förvaltningen per den 31 maj 2022 har en komplett, ändamålsenlig och tydlig registerförteckning.

Granskning 2 - Personuppgiftsbiträdesavtal
Kontroll av att förvaltningen under 2023 genomfört en inventering av samtliga avtal med personuppgiftsbiträden för att säkerställa att personuppgiftsbiträdesavtal upprättas i de fall det behövs.