Stockholms stad

GDPR Årsrapport

2021

Stockholm Business Reigon

GDPR årsrapport
Januari 2021

Dnr: SBR 2022/7
Utgivningsdatum: 2022-03-08
Kontaktperson: Mattias Rindberg

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 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

Inom koncernen Stockholm Business Region (SBR) finns tre personuppgiftsansvariga (PUA), Stockholm Business Region AB, Invest Stockholm Business Region AB och Visit Stockholm AB.

SBR har utsett ett dataskyddsombud och en informations-säkerhetssamordnare vilka även innehar rollerna inom koncernens två dotterbolag.

Under 2021 har SBR genomfört riskanalyser avseende tredjelandsöverföring av bolagens sociala medier, följt av pågående implementering av skyddsåtgärder. Vidare pågår rekrytering av ny kompetens med syfte att hantera verksamhetens aktiviteter inom området.

I egenskap av DSO överlämnar jag följande årsrapport innefattande råd och rekommendationer för samtliga tre personuppgiftsansvariga i koncernen.

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som PUA, som ett minimum, ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter.

Nedan redogörs för PUAs status och DSOs slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSOs genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	Totalt 109. Fördelade enligt följande: Stockholm Business Region 45 st. Invest Stockholm 40 st. Visit Stockholm 24 st.
Har nödvändiga uppdateringar gjorts?	Nej.
Bedöms registerförteckningen vara fullständig?	Nej.
Har verksamheten lämpliga rutiner för registerföring?	Nej.

3.1.2 Syfte

Det är ett krav enligt dataskyddsförordningen (artikel 30) att sammanställa information om alla slags behandlingar av person-uppgifter som en organisation utför och dokumentera dessa, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde. På så sätt skapa ett register över allting som man gör med personuppgifter.

Dessa register ska upprättas skriftligen, vara tillgängliga i elektronisk format och hållas uppdaterade. På begäran ska registret göras tillgängligt för Integritetsskyddsmyndigheten (IMY).

3.1.3 Resultat

Resultatet är baserat på den version av registerförteckning som DSO granskade den 24 september 2021.

Total är 109 behandlingar registrerade i koncernens registerförteckning. Dessa behandlingar är fördelade mellan koncernens respektive PUA enligt följande;

- Stockholm Business Region 45 st.
- Invest Stockholm 40 st.
- Visit Stockholm 24 st.

10 september 2020 genomförde DSO senast en översyn av koncernens registerförteckning. Då konstaterades bl.a. att merparten av behandlingarna saknade obligatoriska uppgifter, att ingen behandling var granskad och klar och att det inte sker något systematiskt arbete för att registret ska hållas aktuellt.

Vid granskningen genomförd den 24 september 2021 kan konstateras att viss uppdatering har genomförts i registerförteckningen. Dock saknas obligatoriska uppgifter i flertal behandlingar och ingen behandling är granskad och klar.

Vidare kan konstateras att vissa behandlingar finns i registret trots att behandlingarna inte längre sker av PUA. Personuppgifts-behandlingarna är upprättade i tre olika formulär varför de inte är enhetligt upprättade och vissa uppgifter behöver rättas. Ingen behandling är granskad och godkänd då ansvarsroller inte är tydliggjorda.

PUA har inte en utvecklad rutin för att hålla registerförteckningen enhetlig och aktuell vilket medför att registerförteckningen inte uppdateras när en ny behandling identifierats eller när en befintlig behandling förändras.

Sammanfattningsvis bedömer DSO att det inte sker något kontinuerligt arbete för att hålla registret enhetligt och aktuellt samt att PUA saknar ett systematiskt arbetssätt för att säkerställa detta.

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

Utan en enhetlig upprättad och aktuell registerförteckning saknar PUA en överblick över vilka behandlingar som sker och att dessa sker i enlighet med GDPR. DSO har därför bedömt denna brist som högre jämfört med andra brister redogjorda för i denna årsrapport.

3.1.5 DSO ger råd och rekommendationer till PUA

Registerförteckningen är en grundförutsättning för allt annat dataskyddsarbete. För att PUA systematiskt ska kunna styra och följa upp dataskyddsarbetet och för att kunna säkerställa att detta arbete följer gällande lagar och regler och rättsutvecklingen inom området behöver registerförteckningen vara enhetlig och aktuell.

PUA behöver därför regelbundet och systematiskt arbeta med inventering av personuppgiftsbehandlingarna i verksamheten och säkerställa att registerförteckningen är enhetlig och aktuell.

DSOs råd och rekommendation är att PUA beslutar om en tillfällig insats för att säkerställa att PUAs personuppgiftsbehandlingar inom en bestämd tid ska vara enhetligt registerförtecknad och aktuell.

Vidare rekommenderar DSO att befintlig rutin utvecklas, tydliggörs och implementeras i respektive PUA för att säkerställa att registerförteckningen fortsättningsvis hålls enhetlig och aktuell.

DSO rekommenderar även att PUAs kompetens på området stärks genom utbildningsinsatser.

3.2 Styrdokument

3.2.1 Sammanfattning

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

3.2.2 Syfte

Dataskyddsförordningen ställer krav på att en organisation ska kunna visa att och hur dataskyddsförordningen efterlevs. Detta innebär att det ställs stora krav på en organisation att ha dokumentation om dataskyddsförordningen upprättad.

Dokumentationen är både ett verktyg för att organisationen ska få en bild av vilka rutiner som finns på plats, men också för att organisationen ska kunna uppvisa arbetet för tillsynsmyndigheten vid en eventuell tillsyn.

3.2.3 Resultat

PUAs styrdokument inom detta område är stadsgemensamma, framtagna av och granskade centralt inom Stockholms stad. Dessa styrdokument är publicerade på stadens intranät vilket PUA hänvisar sina medarbetare till.

PUA har en verksamhetsspecifik handbok för att ge grundläggande information och stöd till medarbetarna vad gäller vid behandling av personuppgifter inom verksamheten. Denna handbok innehåller även PUAs verksamhetsspecifika rutiner.

PUAs handbok fyller ett syfte i att ge grundläggande information och stöd till medarbetarna vad gäller vid behandling av personuppgifter. De verksamhetsspecifika rutinerna som finns i handboken behöver utvecklas och kompletteras då dessa mer generellt beskrivs i handboken.

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

3.2.5 DSO ger råd och rekommendationer till PUA

DSOs råd och rekommendation är att PUA säkerställer att stadens information är förankrad bland medarbetarna och att dessa har tillräcklig kompetens inom området för att tillgodogöra sig informationen.

DSOs råd och rekommendation är vidare att PUA utvecklar och implementerar verksamhetens rutiner avseende;

- Rutiner för att tillgodose registrerades samtliga rättigheter.
- Rutin för hur personuppgiftsincidenter ska utredas, analyseras, rapporteras och dokumenteras.
- Rutin för att hålla registerförteckningen enhetlig och aktuell.

Dessa rutiner bör separeras från PUAs handbok så att de tydliggöras som styrdokument, implementeras och kommuniceras som verksamhetsspecifika rutiner på PUAs intranät. Dessa rutiner bör vidare ha en ägare som säkerställer att uppdateringar görs vid behov.

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?	Tio system finns registrerade i SKRs verktyg KLASSA. Därtill har ett system enligt uppgift klassats enligt en tidigare metod.
Är klassade personuppgiftsbehandlingar aktuella?	Ja. Ansvariga bedömer informationsklassningarna vara aktuella.

3.3.2 Syfte

För att kunna skydda information och personuppgifter på ett tillräckligt sätt ska en verksamhet informationsklassa sin information. Att klassa informationen är ett sätt att utreda vilket skydd informationen ska ha.

Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKRs verktyg KLASSA.

3.3.3 Resultat

Då PUAs registerförteckning inte bedöms vara enhetlig och aktuell har granskningen inom detta område tagit utgångspunkt i SKRs verktyg KLASSA för att undersöka om PUA genomfört informationsklassning för alla behandlingar som rör personuppgifter.

Resultatet är baserat på den version av KLASSA som DSO granskade den 4 oktober 2021.

En personuppgiftsbehandling kan innefatta ett eller flera system. I KLASSA har PUA tagit upp totalt tio system. Därtill har ett system enligt uppgift klassats enligt en tidigare metod. Uppgifter huruvida dessa system täcker PUAs samtliga personuppgiftsbehandlingar saknas.

Därutöver har ingen stickprovskontroll genomförts för att verifiera att lämpliga tekniska och organisatoriska åtgärder från KLASSA vidtagits för att skydda dessa system.

DSOs samlade bedömning, tillsammans med verksamhetens informationssäkerhetssamordnare, är att PUA inte genomfört informationsklassning för alla behandlingar som rör 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
	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

3.3.5 DSO ger råd och rekommendationer till PUA

DSOs råd och rekommendation är att PUA beslutar om en tillfällig insats för att säkerställa att PUAs personuppgiftsbehandlingar inom en bestämd tid ska vara informationsklassade med stöd av KLASSA.

Vidare rekommenderar DSO att PUA utvecklar sin kompetens generellt inom området it-tjänster för att stärka PUAs förmåga inom området på ett sätt som överensstämmer med lagstiftningen.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	DSOs kontroll har tagit avstamp i PUAs registerförteckningen. Av registerförteckningen framgår att 13 behandlingar har konsekvensbedömts. I 12 av dessa fall framgår dock att det avser en informationsklassning av ett enskilt system i verktyget KLASSA. Den konsekvensbedömning som genomförts bedöms av ansvarig för behandlingen vara aktuell. DSO har tidigare i denna rapport bedömt att inte sker något kontinuerligt arbete för att hålla registerförteckning enhetlig och aktuell (punkt 3.1). Därigenom saknar DSO grundläggande förutsättningar för att identifiera eventuella behandlingar där konsekvens-bedömningar borde genomföras. Av den anledningen har ingen djupare granskning genomförts av detta granskningsområde.
Har alla potentiella högrisk-behandlingar konsekvensbedömts?	N/a
Är de genomförda bedömningarna aktuella?	Ja. Ansvarig för behandlingen bedömer konsekvensbedömning vara aktuell.

3.4.2 Syfte

Konsekvensbedömningen hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas. 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 vidtas riskförebyggande åtgärder.

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning som viktiga verktyg för 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

DSOs kontroll på detta område har tagit avstamp i PUAs registerförteckningen för att kontrollera vilka behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”. Registerförteckningen ger en översiktsbild av vilka kategorier av uppgifter som behandlas och vad som görs med uppgifterna.

Resultatet är baserat på den version av registerförteckning som DSO granskade den 24 september 2021.

Av registerförteckningen framgår att 13 personuppgiftsbehandlingar konsekvensbedömts. Vid närmare granskning av dessa framgår dock att 12 av dessa avser en informationsklassning av ett enskilt system i verktyget KLASSA.

Den konsekvensbedömning som genomförts bedöms av ansvarig för behandlingen vara aktuell.

DSO har i denna rapport bedömt att inte sker något kontinuerligt arbete för att hålla registerförteckning enhetlig och aktuell (punkt 3.1). Därigenom saknar DSO grundläggande förutsättningar för att identifiera eventuella behandlingar där konsekvensbedömningar borde genomföras. Av den anledningen har ingen djupare granskning genomförts av detta granskningsområde.

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
	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

3.4.5 DSO ger råd och rekommendationer till PUA

DSOs råd och rekommendation är att PUA beslutar om en tillfällig insats för att, inom en bestämd tid, säkerställa att erforderliga konsekvensbedömningar har genomförts med användande av stadens rutin för konsekvensbedömning av dataskydd.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	Under den granskade perioden har ingen begäran om information inkommit.
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	N/a.

3.5.2 Syfte

De registrerade har ett antal rättigheter enligt dataskyddsförordningens artikel 15-22. Rättigheterna är tillgång till information, tillgång till registerutdrag, rättelse, radering, begränsning av behandling, dataportabilitet, invändning mot behandling.

PUA måste säkerställa att de registrerade har möjlighet att utöva dessa rättigheter. Det bör därför finnas rutiner så PUA kan hantera de registrerades begäran på korrekt sätt inom föreskriven tidsfrist (30 dgr).

3.5.3 Resultat

Resultatet är baserat tidsperioden from 2021-01 tom 2021-12 vilken DSO granskat.

Under den granskade tidsperioden har ingen begäran om information inkommit.

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

3.5.5 DSO ger råd och rekommendationer till PUA

DSO kan konstatera att PUA saknar skriftliga rutiner för hur en begäran från en registrerad person ska hanteras. Vid avsaknad av detta finns risken att PUA inte kan hanterar en sådan begäran på korrekt sätt inom föreskriven tidsfrist (30dgr).

DSOs råd och rekommendation är att PUA tar fram skriftliga rutiner för hur registrerades samtliga rättigheter ska hanteras och att dessa rutiner implementeras i respektive PUA.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Inträffar något i verksamheten som kan vara en personuppgiftsincident ska det anmälas till respektive chef som har ansvar för rapportering, analys och åtgärder av inträffade incidenter. IA är Stockholms stads system för incidentrapportering vilket innebär att personuppgiftsincidenter rapporteras och följs upp i verktyget. VD fattar beslut om att anmäla incidenten till IMY och VD eller vid dennes frånvaro administrativ chef fattar beslut om att informera de registrerade.
Hur många personuppgiftsincidenter har dokumenterats?	Under den granskade perioden har en personuppgiftsincident dokumenterats.
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Bolaget har, efter samråd med DSO, bedömt det osannolikt att incidenten medfört en risk för de registrerades fri- och rättigheter. Med anledning av detta har incidenten inte anmälts till IMY.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	N/a.

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.”

3.6.3 Resultat

Resultatet är baserat på den version av IA som DSO granskade den 22 december 2021 och omfattar tidsperioden from 2021-01 tom 2021-12.

Under den granskade perioden har en personuppgiftsincidenter inträffat. Incidenten har inte bedömts föranleda en anmälan till IMY. Med anledning av incidenten valde SBR att informera samtliga medarbetare om det inträffade och bad samtliga vara vaksamma avseende onormala e-postmeddelanden som innehåller anspråk, klickbara länkar eller bilagor etc.

Av koncernens rutin för personuppgiftsincident framgår bl.a. att om något inträffar i verksamheten som kan vara en personuppgifts-incident ska det anmälas till respektive chef som har ansvar för rapportering, analys och åtgärder av inträffade incidenter.

Vidare framgår att IA är Stockholms stads system för incidentrapportering vilket innebär att personuppgiftsincidenter ska rapporteras och följas upp i verktyget. VD fattar beslut om att anmäla incidenten till IMY.

DSO ska alltid vara inblandad i konsekvensbedömningar av en personuppgiftsincident samt ha en rådgivande roll. VD eller vid dennes frånvaro administrativ chef fattar beslut om att informera de registrerade.

I samband med incidenten har DSO konstaterat att PUAs rutin avseende personuppgiftsincidenter behöver kompletteras och att rutinen behöver implementeras i respektive PUA.

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

3.6.5 DSO ger råd och rekommendationer till PUA

DSO har konstaterat att PUAs rutin avseende personuppgifts-incidenter behöver kompletteras och att rutinen behöver implementeras i respektive PUA.

Med anledning av den begränsade anmälningstiden av en incident till IMY (72h) bör även PUAs förmåga att hantera incidenter stärkas genom utbildnings- och övningsinsatser så att alla vet vad en incident är, när en incident har inträffat och hur en incident ska hanteras.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Registerförteckningen.
- Obligatorisk utbildning.

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 samt resultaten av granskningarna.

4.3 Genomförda granskningar och deras resultat

Granskning 1 - Registerförteckningen

10 september 2020 genomförde DSO senast en översyn av koncernens registerförteckning. Då konstaterades bl.a. att merparten av behandlingarna saknade obligatoriska uppgifter, att ingen behandling var granskad och klar och att det inte sker något systematiskt arbete för att registret ska hållas aktuellt.

Vid granskningen genomförd den 24 september 2021 kan konstateras att viss uppdatering har genomförts i registerförteckningen. Dock saknas obligatoriska uppgifter i flertal behandlingar och ingen behandling är granskad och klar.

Vidare kan konstateras att vissa behandlingar finns i registret trots att behandlingarna inte längre sker av PUA. Personuppgifts-

behandlingarna är upprättade i tre olika formulär varför de inte är enhetligt upprättade och vissa uppgifter behöver rättas.

Ingen behandling är granskad och godkänd då ansvarsroller inte är tydliggjorda. PUA har inte en utvecklad rutin för att hålla registerförteckningen enhetlig och aktuell vilket medför att registerförteckningen inte uppdateras när en ny behandling identifierats eller när en befintlig behandling förändras.

Sammanfattningsvis bedömer DSO att det inte sker något kontinuerligt arbete för att hålla registret enhetligt och aktuellt samt att PUA saknar ett systematiskt arbetssätt för att säkerställa detta.

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

Granskning 2 - Obligatorisk utbildning

E-utbildningarna ”Grundkurs i dataskydd” är obligatoriska utbildningar.

Uppföljning av ”Grundkurs i dataskydd” genomförs av DSO månatligen och respektive PUA hålls löpande informerad om resultatet. Av genomföranderapporterna framgår att samtliga tillsvidareanställda medarbetare genomfört den obligatoriska e-utbildningen.

PUA informerar löpande nyanställda medarbetare om att detta är en obligatorisk utbildning vilket även framgår av att nyanställda genomfört den obligatoriska e-utbildningen.

	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

4.4 DSO ger råd och rekommendationer till PUA

DSOs råd och rekommendationer avseende granskning 1 – Registerförteckning.

Registerförteckningen är en grundförutsättning för allt annat dataskyddsarbete. För att PUA systematiskt ska kunna styra och följa upp dataskyddsarbetet och för att kunna säkerställa att detta arbete följer gällande lagar och regler och rättsutvecklingen inom området behöver registerförteckningen vara enhetlig och aktuell.

PUA behöver därför regelbundet och systematiskt arbeta med inventering av personuppgiftsbehandlingarna i verksamheten och säkerställa att registerförteckningen är enhetlig och aktuell.

DSOs råd och rekommendation är att PUA beslutar om en tillfällig insats för att säkerställa att PUAs personuppgiftsbehandlingar inom en bestämd tid ska vara enhetligt registerförtecknad och aktuell.

Vidare rekommenderar DSO att befintlig rutin utvecklas, tydliggörs och implementeras i respektive PUA för att säkerställa att registerförteckningen fortsättningsvis hålls enhetlig och aktuell.

DSO rekommenderar även att PUAs kompetens på området stärks genom utbildningsinsatser.

DSOs råd och rekommendationer avseende granskning 2 – Obligatorisk utbildning

Inga brister av nämnvärd betydelse har identifierats.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- Avsaknad av verksamhetsspecifika och implementerade rutiner.
- Bristande införande av skyddsåtgärder (tekniska och organisatoriska) efter genomförda informationsklassningar.
- Bristande kompetensnivå.

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. Det kan därtill finnas mer övergripande, generella eller specifika risker ur ett dataskyddsperspektiv, ur såväl tekniskt som organisatoriskt perspektiv. För att säkerställa att dataskydds-förordningen efterföljs är det viktigt att identifiera och minimera eller eliminera alla typer av risker i verksamheten.

5.3 Resultatet av riskkartläggningen

Risk 1

Verksamhetsspecifika och implementerade rutiner krävs för att koncernens tre PUA, på ett enhetligt sätt och korrekt sätt ska kunna hantera personuppgifter.

Vid avsaknad av verksamhetsspecifika och implementerade rutiner finns risken att koncernen inte hanterar ansvaret för personuppgifter på det sätt som Dataskyddsförordningen föreskriver.

	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

Risk 2

Att genomföra en informationsklassning är första steg mot att skydda information. Det måste följas av införande av skyddsåtgärder (tekniska och organisatoriska) identifierade vid informationsklassningen.

Ett bristande införande av identifierade skyddsåtgärder (tekniska och organisatoriska) medför risken att informationen inte får det skydd som motsvarar dess betydelse för verksamheten.

	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

Risk 3

Korrekt kompetensnivå krävs bland medarbetarna som på ett eller annat sätt hanterar personuppgifter. Kompetens är en färskvara som bibehålls och utvecklas genom löpande utbildnings- och övningsinsatser.

Vid bristande kompetensnivå finns risken att PUAs förmåga inom området inte överensstämmer med lagstiftningen.

	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

DSOs råd och rekommendationer framgår av tidigare avsnitt i denna rapport.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Registerförteckningen.
- Verksamhetsspecifika rutiner.

6.2 Syfte

En av DSOs viktigaste uppgifter är det granskande arbetet.

Granskningsområdena har DSO valt utifrån ett riskbaserat synsätt, dvs. de områden där DSO anser verksamhetens mest relevanta risker och brister identifierats.

PÅ så sätt 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.

6.3 Planerade granskningar

Granskning 1

- En översyn av att registerförteckningen är aktuell och fullständig.

Översynen innefattar samtliga tre PUA och att registerförteckningen är enhetligt registerförtecknad och aktuell.

Vidare innefattar granskningen att befintlig rutin utvecklats, tydliggjorts och implementerats i respektive PUA för att säkerställa att registerförteckningen fortsättningsvis hålls enhetlig och aktuell.

Granskning 2

- En översyn av att PUA uppdaterat och implementerat rutin avseende informationsklassning.

Vidare innefattar granskningen att en ägare är utsedd till rutinen som säkerställer att uppdateringar görs vid behov.

7 Övrigt att rapportera

7.1 Sammanfattning

DSO har inget övrigt att rapportera.