Stockholms stad

GDPR Årsrapport

2022

Stockholm Business Reigon

GDPR årsrapport
Januari 2023

Dnr: 2022/304
Utgivningsdatum: 2023-03-07
Kontaktperson: Mattias Rindberg

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

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.

Rapporten omfattar sex obligatoriska rapporteringsområden som PUA som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskydds-förordningen avser.

De obligatoriska rapporteringsområdena är;

- Registerförteckning.
- Styrdokument.
- Tekniska och organisatoriska åtgärder för personuppgifts-behandlingar.
- Konsekvensbedömningar.
- Individens rättigheter.
- Personuppgiftsincidenter.

I fem av dessa rapporteringsområden har DSO bedömt det finns brister som bör åtgärdas men som ej bedöms vara brådskande, omfattande eller allvarliga. I det sjätte rapporteringsområdet, registerförteckningen, bedömer DSO bristen vara omfattande och/eller kräva omgående åtgärder.

Vid granskningen av registerförteckningen kan konstatera att PUA upprättat ett nytt formulär för registrering av personuppgifts-behandlingar. Personuppgiftsbehandlingarna som tidigare var upprättade i tre olika formulär har förts över till det nya formuläret och registerförteckningen är på så sätt enhetligt upprättade.

I samband med detta har även viss uppdatering och revidering genomförts av den registrerade informationen där vissa behandlingar som inte längre är aktuella har tagits bort och vissa behandlingar har slagits samman.

Dock kan konstateras att uppgifter saknas i flertal behandlingar, vissa behandlingar finns i registret trots att behandlingarna inte

längre sker, vissa uppgifter är felaktiga och vissa behandlingar är inte registrerade i förteckningen.

Vidare kan konstateras att PUA inte har en lämplig rutin för att hålla registerförteckningen aktuell vilket medför att registerförteckningen inte uppdateras när en ny behandling identifierats eller när en befintlig behandling upphör eller förändras.

DSOs råd och rekommendation är att PUA fortsätter arbetet med att aktualisera registerförteckningen. Vidare rekommenderar DSO att befintlig rutin utvecklas, tydliggörs och implementeras för att säkerställa att registerförteckningen fortsättningsvis hålls enhetlig och aktuell samt att PUAs kompetens på området stärks genom utbildningsinsatser.

Granskning av PUAs styrdokument genomfördes av DSO i samarbete med verksamhetens informationssäkerhetssamordnare den 17 november 2022.

Av granskningen kan konstateras att PUAs styrdokument dels är stadsgemensamma och dels verksamhetsspecifika. PUAs verksamhetsspecifika styrdokument beskrivs i verksamhetens handbok för behandling av personuppgifter.

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

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

- Rutin för att tillgodose registrerades rättigheter.
- Rutin för hur personuppgiftsincidenter ska utredas, analyseras, rapporteras och dokumenteras.
- Rutin för att hålla registerförteckningen enhetlig och aktuell.
- Rutin för att konsekvensbedömningar vid behov genomförs, och dokumenteras.
- Rutin för att genomföra informationsklassningar, implementera eventuella skyddsåtgärder samt vid behov och minst årligen ta ställning till om informationens skyddsvärde fortfarande gäller.

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.
- Personuppgiftsincidenter.

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

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

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 100 st. Fördelade enligt följande: Stockholm Business Region, 49 st. Invest Stockholm, 28 st. Visit Stockholm, 26 st.
Har nödvändiga uppdateringar gjorts?	Ja, delvis
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, i samarbete med verksamhetens informations-säkerhetssamordnare, granskade den 28 december 2022.

Total är 100 behandlingar registrerade i koncernens registerförteckning. Dessa behandlingar är fördelade mellan koncernens respektive PUA enligt följande;

- Stockholm Business Region 49 st.
- Invest Stockholm 28 st.
- Visit Stockholm 26 st.

Den 24 september 2021 genomförde DSO senast en översyn av koncernens registerförteckning. Då konstaterades bl.a. att det saknades uppgifter i flertal behandlingar, att vissa behandlingar finns i registret trots att behandlingarna inte längre sker, att förteckningen är upprättade i tre olika formulär varför de inte är enhetligt och att PUA inte har en 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.

Vid årets granskning, genomförd den 28 december 2022 kan konstateras att PUA upprättat ett nytt formulär för registrering av personuppgiftsbehandlingar. Personuppgiftsbehandlingarna som tidigare var upprättade i tre olika formulär har förts över till det nya formuläret och registerförteckningen är på så sätt enhetligt upprättade.

I samband med detta har även viss uppdatering och revidering genomförts av den registrerade informationen där vissa behandlingar som inte längre är aktuella har tagits bort och vissa behandlingar har slagits samman.

Dock kan konstateras att uppgifter saknas i flertal behandlingar, vissa behandlingar finns i registret trots att behandlingarna inte längre sker, vissa uppgifter är felaktiga och vissa behandlingar är inte registrerade i förteckningen.

Vidare kan konstateras att PUA inte har en lämplig rutin för att hålla registerförteckningen aktuell vilket medför att registerförteckningen inte uppdateras när en ny behandling identifierats eller när en befintlig behandling upphör eller förändras.

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 aktuell registerförteckning saknar PUA en överblick över vilka behandlingar som sker och att dessa sker i enlighet med dataskyddsförordningen. 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 fortsätter arbetet med att aktualisera registerförteckningen. Vidare rekommenderar DSO att befintlig rutin utvecklas, tydliggörs och implementeras för att säkerställa att registerförteckningen fortsättningsvis hålls enhetlig och aktuell samt 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

Granskning av PUAs styrdokument inom detta område genomfördes av DSO i samarbete med verksamhetens informations-säkerhetssamordnare den 17 november 2022.

Av granskningen kan konstateras att PUAs styrdokument dels är stadsgemensamma och dels verksamhetsspecifika.

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

PUA har vidare 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 beskrivs i handboken behöver dock 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 utvecklar och implementerar rutiner avseende;

- Rutin för att tillgodose registrerades rättigheter.
- Rutin för hur personuppgiftsincidenter ska utredas, analyseras, rapporteras och dokumenteras.
- Rutin för att hålla registerförteckningen enhetlig och aktuell.
- Rutin för att konsekvensbedömningar vid behov genomförs, och dokumenteras.
- Rutin för att genomföra informationsklassningar, implementera eventuella skyddsåtgärder samt vid behov och minst årligen ta ställning till om informationens skyddsvärde fortfarande gäller.

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?	Åtta (8) klassningar finns registrerade i verktygstödet KLASSA 3.5 och KLASSA 4. Därtill är enligt uppgift en klassning genomförd enligt en tidigare metod.
Är klassade personuppgiftsbehandlingar aktuella?	Ja. Ansvariga bedömer att klassningarna är aktuella.

3.3.2 Syfte

För att kunna vidta relevanta tekniska och organisatoriska åtgärder för att skydda information (däribland personuppgifter) behöver informationsägaren avgöra vilket skyddsvärde informationen har för verksamheten.

Den nämnd/styrelse som ytterst ansvarar för att informationen är riktig samt för det sätt informationen används och sprids av både medarbetare och it-tjänster, är formellt sett informationsägare tillika PUA.

Informationsägaren ansvarar för att initiera informations-klassningar samt för att kraven från informationsklassningen kommuniceras och ställs till rätt part. Informationens skyddsvärde fastställs utifrån en skala (0-3). Ju större skadan bedöms kunna bli om informationen inte skyddas, desto högre skyddsvärde anges för informationen.

Standardiserade skyddsåtgärder genereras därefter med hjälp av verktygsstödet KLASSA. Den grundläggande principen är att ju större skyddsvärde informationen har desto mer omfattande åtgärder krävs för att skydda informationen (tekniska och organisatoriska). Därefter ska informationsägaren ta ställning till vilka skyddsåtgärder som redan finns på plats och vilka som behöver arbetas in i verksamheten. När skyddsåtgärderna är införda som informationen får det skydd som motsvarar dess betydelse för verksamheten.

Minst årligen, eller vid betydande förändringar i verksamheten eller omvärlden, ska informationsägaren ta ställning till om informationens skyddsvärde fortfarande gäller eller om nya risker och behov av skydd har uppstått.

3.3.3 Resultat

DSOs granskning inom området har dels tagit utgångspunkt i verktygsstödet KLASSA och dels systemstödet för ärende- och dokumenthantering, eDok för att identifiera klassade personuppgiftsbehandlingar.

Granskning har genomförts i samarbete med verksamhetens informationssäkerhetssamordnare. Resultatet är baserat på granskningen av systemstödet som genomfördes den 17 november 2022.

Åtta (8) klassningar har registrerats i verktygstödet KLASSA. Sju stycken (7) i KLASSA 3.5 och en (1) har under året registrerats i KLASSA 4. Därtill är enligt uppgift en klassning genomförd enligt en tidigare metod. Samtliga nio klassningar bedöms vara aktuella av ansvariga.

Stickprovskontroll har inte genomförts för att verifiera att skyddsåtgärderna, som genererats av klassningen införts för att skydda informationen.

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

DSO har under punkt 3.2.5 lämnat råd och rekommendation att PUA behöver utveckla och implementera skriftliga rutiner för att genomföra informationsklassningar, implementera eventuella skyddsåtgärder samt vid behov och minst årligen ta ställning till om informationens skyddsvärde fortfarande gäller.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	DSO bedömning är att grundläggande förutsättningar för att identifiera eventuella behandlingar där konsekvensbedömningar borde genomföras saknas.
Har alla potentiella högriskbehandlingar konsekvensbedömts?	N/a
Är de genomförda bedömningarna aktuella?	Ja, delvis. En konsekvens-bedömning är aktuell och en har ansvarig bedömt behöver förnyas.

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 28 december 2022.

Av registerförteckningen framgår att 13 personuppgiftsbehandlingar konsekvensbedömts. Vid närmare granskning av dessa framgår att 12 av dessa i själva verket inte är konsekvensbedömningar utan avser en informationsklassning av ett enskilt system i verktygsstödet KLASSA 3.5. Den trettonde konsekvensbedömning, som är registrerad i registerförteckningen, har ansvarig bedömt behöver förnyas.

Därutöver har, under 2022, en konsekvensbedömning genomförts avseende användningen av CRM systemet Salesforce. Detta mot bakgrund av Schrems II-domen och dess följdeffekter. Dock finns varken denna konsekvensbedömning eller själva personuppgifts-behandling, i vilken CRM systemet Salesforce används, registrerad i PUAs registerförteckning.

DSO har under punkt 3.1.3 bl.a. konstaterat att uppgifter saknas i registerförteckningen, vissa uppgifter är felaktiga och att vissa behandlingar inte är registrerade.

DSO bedömning är därför att grundläggande förutsättningar för att identifiera eventuella behandlingar där konsekvensbedömningar borde genomföras saknas. 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

DSO har under punkt 3.2.5 lämnat råd och rekommendation att PUA behöver utveckla och implementera skriftliga rutiner för att konsekvensbedömningar, vid behov, genomförs och dokumenteras.

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 inkommit från någon registrerad person.
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 innefattar:

- Rätt till information.
- Rätt till tillgång.
- Rätt till rättelse.
- Rätt till radering.
- Rätt till begränsning av behandling.
- Rätt att göra invändningar.
- Rätt till dataportabilitet.
- Automatiserade beslut.

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

Om verksamheten inte har förmåga att hantera en begäran från en registrerad person i enlighet med dataskyddsförordningens krav,

kan det skada allmänhetens förtroende för hur PUA hanterar personuppgifter. Det kan även leda till tillsynsärenden från IMY.

3.5.3 Resultat

Granskningen har tagit utgångspunkt i om någon inkommen handling registrerats avseende önskan att utöva rättigheter och om VD, eller vid dennes frånvaro administrativ chef fattat något beslut rörande registrerades rättigheter.

DSOs kontroll har genomförts i samarbete med verksamhetens registrator och tagit avstamp i systemstödet för ärende- och dokumenthantering, eDok vilket bl.a. används för registrering av handlingar, remisshantering och nämnd- och styrelsehantering. Kontrollen genomfördes den 11 januari 2023 och omfattar tidsperioden fr.o.m. 2022-01 t.o.m. 2022-12.

Vid kontrollen kan konstateras att ingen (0) handling har inkommit och registrerats i eDok och att inget (0) beslut av VD, eller vid dennes frånvaro administrativ chef, rörande registrerades rättigheter registrerats.

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 har under punkt 3.2.5 lämnat råd och rekommendation att PUA utvecklar och implementerar rutin för att tillgodose registrerades rättigheter.

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 (1) personuppgiftsincident dokumenterats.
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Ingen (0).
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". Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent och består av två huvudsakliga moment – dokumentering respektive rapportering.

Varje personuppgiftsincident ska dokumenteras och ett register ska föras över uppkomna incidenter. Enligt artikel 33.5 är det ett krav att dokumentera omständigheterna kring personuppgiftsincidenten, effekterna och åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden. Bristande dokumentering är sanktionsgrundande.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag gäller enbart om det är "osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter" (artikel 33).

Detta innebär att de personuppgiftsincidenter som sannolikt leder till hög risk för fysiska personers rättigheter och friheter ska rapporteras till IMY, senast 72 timmar efter att PUA 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

DSOs kontroll har dels skett i Stockholms stads incidentrapporteringssystem IA. Kontrollen genomfördes den 28 december 2022 och omfattar tidsperioden fr.o.m. 2022-01 t.o.m. 2022-12.

Av kontrollen framgår att en (1) personuppgiftsincident dokumenterats i IA under den granskade perioden. Incidenten avsåg förlust av mobiltelefon. Av rapporten i IA framgår att mobiltelefonen rensades och spärrades samt förlusten polisanmäldes. Med anledning av att mobiltelefonen rensades från allt som var kopplat till synkronisering och Stockholms stad samt spärrades ansågs inte incidenten föranleda någon ytterligare åtgärd.

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 råd och rekommendation från föregående års GDPR rapport, att PUAs rutin avseende personuppgiftsincidenter behöver kompletteras och att rutinen behöver implementeras i respektive PUA, kvarstår.

Med anledning av den begränsade anmälningstiden av en incident till IMY (72h) rekommenderar DSO även att PUA genomför en övningsinsats i syfte att stärka PUAs förmåga att dokumentera och vid behov rapportera personuppgiftsincidenter.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Registerförteckningen.
- Verksamhetsspecifika rutiner.

4.2 Syfte

En av DSOs 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.

Vid årets granskning, genomförd den 28 december 2022 kan konstateras att PUA upprättat ett nytt formulär för registrering av personuppgiftsbehandlingar. Personuppgiftsbehandlingarna som tidigare var upprättade i tre olika formulär har förts över till det nya formuläret och registerförteckningen är på så sätt enhetligt upprättade.

I samband med detta har även viss uppdatering och revidering genomförts av den registrerade informationen där vissa behandlingar som inte längre är aktuella har tagits bort och vissa behandlingar har slagits samman.

Dock kan konstateras att uppgifter saknas i flertal behandlingar, vissa behandlingar finns i registret trots att behandlingarna inte längre sker, vissa uppgifter är felaktiga och vissa behandlingar är inte registrerade i förteckningen.

Vidare kan konstateras att PUA inte har en lämplig rutin för att hålla registerförteckningen aktuell vilket medför att registerförteckningen inte uppdateras när en ny behandling identifierats eller när en befintlig behandling upphör eller förändras.

	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 - Verksamhetsspecifika rutiner.

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 vidare 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.

	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

4.4 DSO ger råd och rekommendationer till PUA

DSOs råd och rekommendationer avseende granskning 1 – Registerförteckning.

DSOs råd och rekommendation är att PUA fortsätter arbetet med att aktualisera registerförteckningen. Vidare rekommenderar DSO att befintlig rutin utvecklas, tydliggörs och implementeras för att säkerställa att registerförteckningen fortsättningsvis hålls enhetlig och aktuell samt att PUAs kompetens på området stärks genom utbildningsinsatser.

DSOs råd och rekommendationer avseende granskning 2 - Verksamhetsspecifika rutiner.

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

- Rutin för att tillgodose registrerades rättigheter.
- Rutin för hur personuppgiftsincidenter ska utredas, analyseras, rapporteras och dokumenteras.
- Rutin för att hålla registerförteckningen enhetlig och aktuell.
- Rutin för att konsekvensbedömningar vid behov genomförs, och dokumenteras.
- Rutin för att genomföra informationsklassningar, implementera eventuella skyddsåtgärder samt vid behov och minst årligen ta ställning till om informationens skyddsvärde fortfarande gäller.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- Avsaknad av verksamhetsspecifika och implementerade rutiner.
- Informationstillgångar som inte klassificerats eller bristande införande av skyddsåtgärder (tekniska och organisatoriska) efter genomförda informationsklassningar.
- Bristande kunskap.

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 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 informationstillgångar klassificeras är första steg mot att skydda information. Därefter behöver verksamheten ta ställning till vilka skyddsåtgärder (tekniska och organisatoriska), genererade med hjälp av klassningen, som redan finns på plats och vilka som behöver arbetas in i verksamheten.

När skyddsåtgärderna är införda får informationen det skydd som motsvarar dess betydelse för verksamheten.

Informationstillgångar som inte klassificeras eller skyddsåtgärder som inte arbetas in i verksamheten 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

Kunskap krävs bland medarbetarna som på ett eller annat sätt hanterar personuppgifter för att verksamheten ska kunna leva upp till dataskyddsförordningen. Kunskap är en färskvara som bibehålls och utvecklas genom utbildnings- och övningsinsatser.

Vid bristande kunskapsnivå finns risken att PUAs förmåga inom området inte lever upp till kraven i 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 granskning av registerförteckningen.

Granskningen innefattar samtliga tre PUA och att registerförteckningen är enhetligt förtecknad och aktuell.

Granskning 2

- En granskning av verksamhetsspecifika rutiner (styrdokument).

Granskningen innefattar PUAs verksamhetsspecifika rutiner (styrdokument).