Stockholms stad

GDPR Årsrapport

2021

Stockholms Stadshus AB

GDPR årsrapport
Maj 2021

Dnr: SSAB 2021/74
Utgivningsdatum: 2021-05-19
Kontaktperson: Simon Jernelöv

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

Simon Jernelöv, JP Infonet AB lämnar i egenskap av externt dataskyddsombud (DSO) åt Stockholms Stadshus AB (bolaget) följande årsrapport.

I denna rapport redovisas resultatet av den granskning som DSO har genomfört av bolagets efterlevnad av dataskyddsförordningen. För att kunna hantera skyldigheterna som följer av dataskyddsförordningen krävs tillräckliga resurser och arbetet med dataskyddsförordningen gäller alla anställda som är delaktiga i dataskyddsarbetet och hanterar personuppgifter. Rapporten är därmed tillställd hela bolaget.

Ansvarssituationen för bolagets personuppgiftshantering kompliceras i någon mån, som ofta för kommunala bolag, av ägarstrukturen, där Stockholms stad i sin ägarroll fattar större delen av besluten gällande vilka datasystem bolaget ska använda, hur personuppgifter och annat ska behandlas i dessa system och hur rutinerna för detta ser ut. Även säkerhetsklassningen av systemen och frågan om konsekvensanalyser vid eventuella förändringar hamnar således utanför bolagets rådighet, i någon bemärkelse.

DSO anser att bolaget generellt har en god lagefterlevnad i förhållande till kraven i dataskyddsförordningen och att bolaget uppnått en acceptabel mognad gällande anpassningarna till lagstiftningen. Efter vår genomgång av verksamheten har vi dock identifierat nedanstående enskilda förbättringsåtgärder som nödvändiga.

Dataskyddsorganisationen
För att kunna hantera skyldigheterna som följer av dataskyddsförordningen krävs tillräckliga resurser och en mer robust dataskyddsorganisation i bolaget. En stor del av informationssäkerhets- och dataskyddsarbetet sköts centralt av Stockholms Stad och DSO ser positivt på att det finns en möjlighet för bolaget att kontakta stadsledningskontorets juridiska avdelning eller avdelningen för it och digitalisering i frågor som rör dataskydd och IT-säkerhet. Bolaget är dock fortfarande personuppgiftsansvarigt för de personuppgiftsbehandlingar det utför, även om detta sker i system som ägarna bestämt. För att den interna dataskyddsorganisationen ska vara tillräckligt stor och för att bolaget också på egen hand ska kunna hantera kraven i

dataskyddsförordningen anser DSO därför att bolaget behöver tillse att fler personer har kunskaper, behörigheter och arbetsuppgifter inom informationssäkerhet, dataskydd och integritetsfrågor.

Utbildning
För att uppnå en hög grad av mognad i sitt dataskyddsarbete krävs en organisation där den generella kunskapsnivån om organisationens personuppgiftsbehandling är relativt hög. Denna skyldighet framgår inte direkt av bestämmelse i dataskyddsförordningen men kan tolkas som en nödvändig åtgärd för att kunna uppfylla andra skyldigheter i förordningen.

En stark central dataskyddsorganisation kommer inte att göra avtryck på organisationens generella lagefterlevnad om inte organisationen som helhet har tillräcklig kunskap om utvalda delar av dataskyddsförordningen. En hög generell kunskapsnivå är även en riskminimerande omständighet gällande de personuppgifter som organisationen har ansvar för.

En förutsättning för att dataskyddsarbetet ska fungera effektivt i bolaget är därför att samtliga medarbetare i bolaget har grundläggande kunskaper om de skyldigheter som följer av dataskyddsförordningen. Det är enligt DSO:s bedömning inte tillräckligt att endast erbjudas en utbildning vid nyanställning; Kontinuerliga utbildningsinsatser är en viktig del i arbetet med dataskyddsförordningen. Avsaknaden av kontinuerlig utbildning till samtliga medarbetare kan riskera att leda till brister vid hanteringen av personuppgifter.

DSO har identifierat att behov av kontinuerliga utbildningsinsatser finns hos bolaget och anser att en utbildningsplan för samtliga medarbetare i bolaget bör tas fram, innehållandes en målsättning för att tillförsäkra att dataskyddsarbetet implementeras i det vardagliga arbetet hos samtliga. Utbildningsplanen bör särskilt fokusera på att schemalägga regelbundna fortbildningsinsatser för att upprätthålla en jämn och hög kunskapsnivå hos samtliga medarbetare.

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 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?	Cirka 50 stycken.
Har nödvändiga uppdateringar gjorts?	Efter första granskningen ja - efter andra granskningen har DSO inte fått mer information.
Bedöms registerförteckningen vara fullständig?	Nej.
Har verksamheten lämpliga rutiner för registerföring?	Nej.

3.1.2 Syfte

Enligt dataskyddsförordningens artikel 30 måste en registerförteckning upprättas. Eftersom registerförteckningen är ett levande dokument som ska uppdateras löpande i takt med att nya personuppgiftsbehandlingar införs i verksamheten eller att vissa personuppgiftsbehandlingar upphör måste artikel 30-registret även uppdateras löpande.

3.1.3 Resultat

Resultatet baseras på den version av registerförteckning som DSO granskade den 1 april 2021.

Cirka 50 stycken behandlingar har registrerats i bolagets registerförteckning.

Efter den första granskningen som DSO genomförde, den 13 oktober 2020, åtgärdades de brister som DSO uppmärksammade och nödvändiga uppdateringar gjordes. Efter senaste granskningen den 1 april 2020 har DSO ännu inte tagit del av en uppdaterad version av registerförteckningen där de påtalade åtgärderna vidtagits.

Registerförteckningen är på god väg att bedömas som fullständig (beaktat det faktum att det är ett levande dokument som ska ändras

varje gång en personuppgiftsbehandling påbörjas eller upphör). Det återstår dock ett antal kommentarer från DSO med åtgärder som behöver vidtas innan registret kan anses fullständigt.

Följande kommentarer har DSO lämnat vid sin senaste granskning av registerförteckningen:

”Lämna inga fält tomma. Ange t.ex. "Nej", "Sker inte" eller "Ej tillämpbart" istället för att lämna tom, för att registret inte ska framstå som ofullständigt.

Undvik förkortningar; tänk på att registret ska kunna förstås av en helt utomstående utan insyn i verksamheten.

Undvik att klumpa ihop flera behandlingar som inte har exakt samma syften, kategorier av registrerade, kategorier av personuppgifter, gallringsrutiner och så vidare. Alternativt var tydliga i varje kolumn t.ex. vilka personuppgifter som behandlas för varje kategori av registrerad "inom en behandling" och vilken gallringstid som gäller för vilken "del" av behandlingen. På en del ställen har nämligen väldigt många olika personuppgiftsbehandlingar klumpats ihop som en och samma behandling. Har ni exakt samma syften, ändamål, laglig grund, eventuellt PUB-avtal, kategorier av registrerade, kategorier av personuppgifter för dessa behandlingar? Om inte - dela upp behandlingarna så informationen blir korrekt.”

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

Eftersom att registret innehåller ganska många personuppgiftsbehandlingar och är nästintill fullständigt ifyllt

bedömer DSO att bolaget har god kunskap om ifyllande av registerförteckningen. Det krävs dock att de föreslagna åtgärderna/ändringarna som DSO lämnat som kommentarer i registret genomförs innan det kan bedömas vara fullständigt. DSO råder därför bolaget att fortsätta arbeta med registerförteckningen utifrån dessa kommentarer.

Enligt DSO saknas en utarbetad, skriftlig rutin för översyn/uppdatering av registret. Bolaget bör därmed etablera ett fungerande systematiskt arbetssätt avseende inventering av de behandlingar som sker i verksamheten samt utarbeta och implementera en rutin för att registerförteckningen ska uppdateras så fort en ny behandling har identifierats eller när en befintlig behandling förändras. En översyn av registerförteckningen bör ske ett par gånger årligen, även i en mindre organisation som bolagets.

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?	Inte till alla dokument.

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

Bolaget har en del egna styrdokument men majoriteten av bolagets styrdokument är stadsgemensamma, framtagna av och granskade centralt inom Stockholms stad. Dokumenten publiceras på stadens intranät och kommuniceras ut via mail till ansvariga i respektive verksamhet i staden.

Bolaget saknar dock en rutin för hantering av offentlighetsprincipen i relation till dataskyddsförordningen. Eftersom dataskyddsförordningen har uppgiftsminimering som en grundläggande princip, samtidigt som offentlighetsprincipen och

arkivlagstiftningen har som huvudregel att alla upprättade och inkomna handlingar ska sparas finns kolliderande synsätt som behöver hanteras. Bolaget behöver även rutiner för hur man ska hantera handlingar med personuppgifter som inkommer exempelvis via mail utan att bolaget efterfrågat uppgifterna.

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

Stockholms stad har visserligen mycket information på sitt intranät, men att endast ha informationen tillgänglig på en hemsida är inte tillräckligt, utan det måste tillförsäkras att den information som finns också är förankrad ute hos medarbetarna.

DSO råder därför bolaget att säkerställa att de dokument som staden publicerar på intranätet också kommuniceras ut i hela bolaget, så att samtliga medarbetare dels har kunskaper om vilka dokument som finns, dels har kunskaper om innehållet i dokumenten och vet vilka rutiner och policys som finns.

Dokumentet ”Rutiner för registrerades rättigheter” måste uppdateras med kontaktuppgifter/ägare, så att uppdateringar kan bli gjorda vid behov.

Ta fram en rutin för hantering av offentlighetsprincipen i relation till dataskyddsförordningen.

Ta fram rutiner för att reglera hur ni ska hantera personuppgiftbehandlingar som uppstår då handlingar med personuppgifter inkommer via mail och liknande kanaler utan att bolaget efterfrågat uppgifterna, för att säkerställa att ni möter

kraven i dataskyddsförordningen gällande uppgiftsminimering och behörighetsbegränsning.

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?	Detta är en fråga som bolaget har på bordet men inte hunnit långt med. Det handlar i praktiken inte bara om personuppgifter utan data generellt. Tanken är att staden ska bli bättre på att klassa alla processer, men detta är ett arbete som man ligger efter i. Det saknas tid och kompetens att klassa alla system. De är inte så många som bevakar frågan och det är en lite bräcklig organisation i detta avseende p.g.a. få som har kompetens i detta arbete.
Är klassade personuppgiftsbehandlingar 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.

3.3.3 Resultat

I sin dagliga hantering använder bolaget bara av ett system, Agda, som inte tillhandahålls genom Stockholms stad. Enligt DSO:s bedömning är det i första hand detta system bör överväga att göra en informationsklassning för.

Funktionen för stadsövergripande informationssäkerhet, Stadsledningskontoret, har uppgivit att för att inte ny konsulthjälp ska behöva köpas in för varje enskild informationsklassning, har SLK istället gjort en FKU (förnyad konkurrensutsättning) för löpande konsulthjälp under hela 2021 i ett svep. De som vill göra egna liknande FKU:er kan ta hjälp av den.

Ni hittar dokumentet ”Informationsklassning - exempel på FKU för konsulthjälp (SLK 2021)” i dokumentlistan på samarbetsytan Nätverket för stadens informationssäkerhetssamordnare och dataskyddsombud.

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

Sätt som mål för 2021 att ha gjort en informationsklassning av Agda.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Ja. Bolaget använder främst system som är stadsgemensamma, för vilka bolaget saknar rådighet. Eventuella konsekvensbedömningar för dessa system är således inte bolagets ansvar utan görs centralt i staden. Exempelvis är det Stockholms stad som sköter ISO-certifieringar.
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Sannolikt (se ovan).
Är de genomförda bedömningarna aktuella?	Sannolikt (se ovan).

3.4.2 Syfte

Om en personuppgiftsbehandling sannolikt leder till en hög risk för personers rättigheter och friheter ska en konsekvensbedömning genomföras, innan behandlingen påbörjas. Detta följer av artikel 35 i dataskyddsförordningen.

En konsekvensbedömning ska innehålla följande fyra grundläggande delar vilka är minikriterier enligt dataskyddsförordningen (artikel 35.7 och skälen 84 och 90):

- en systematisk beskrivning av den planerade behandlingen och behandlingens syfte,
- en bedömning behovet av och proportionaliteten hos behandlingen,
- en bedömning av riskerna för de registrerades rättigheter och friheter
- De åtgärder som planeras dels för att hantera riskerna och dels för att visa att dataskyddsförordningen efterlevs.

3.4.3 Resultat

Bolaget använder i dagsläget inga egna system i vilka personuppgiftsbehandlingar utförs som kräver att en konsekvensbedömning upprättas. Bolaget använder främst system som är stadsgemensamma, för vilka bolaget saknar rådighet. Eventuella konsekvensbedömningar för dessa system är således inte bolagets ansvar utan görs centralt i staden. Exempelvis är det Stockholms stad som sköter ISO-certifieringar.

DSO kan inte bedöma huruvida alla system som bolaget använder sig av har genomgått nödvändiga konsekvensbedömningar eftersom det faller utanför bolagets rådighet. DSO ser däremot positivt på att bolaget är medvetet om begreppen informationsklassning, riskbedömning och konsekvensbedömning samt vad de innebär.

DSO mottog även ett mail den 12 november 2020 med information om att det lagts upp en ny och godkänd mall för konsekvensbedömning på sidan ”Dataskyddsförordningen (GDPR) och personuppgiftsbehandling”, samt även en tillhörande utbildning på stadens intranät.

Vidare ser DSO positivt på att samtliga DSO respektive informationssäkerhetssamordnare i staden nyligen fick ta del av en remiss på en ny stadsgemensam mall för upprättande av konsekvensbedömningar. DSO får därtill regelbundet ta del av information via mail om hur stadens olika organisationer ska/bör använda olika system, molntjänster och liknande samt riktlinjer härvid. Sammantaget anser DSO att det finns en väl fungerande struktur generellt i staden med ett informationsflöde som sträcker sig utåt och nedåt i stadens organisationer.

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

3.4.5 DSO ger råd och rekommendationer till PUA

Förutsatt att bolaget fortsätter följa stadens direktiv och säkerställa att endast godkända system/mallar/tjänster används för de personuppgiftsbehandlingar som bolaget utför, bedömer DSO att bolaget inte behöver vidta ytterligare åtgärder vad gäller konsekvensbedömningar.

3.5 Individens rättigheter

3.5.1 Sammanfattning

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

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.

Den personuppgiftsansvarige måste säkerställa att de registrerade har möjlighet att utöva dessa rättigheter. För att tillse att de registrerade kan utöva sina rättigheter bör rutiner finnas för att hantera de registrerades begäran, så att bolaget kan hantera dem på korrekt sätt inom föreskriven tidsfrist.

3.5.3 Resultat

DSO bedömer att bolaget har en fungerande rutin för hantering av registrerades rättigheter inom föreskriven tidsfrist.

Bolaget har dessutom tagit fram dokumentet ”Rutin för registrerades rättigheter” som DSO granskat. Det är mycket informativt och tydligt, och innehåller bilaga för loggning av rättighetshantering, bilaga med mall för att kommunicera till registrerade vid olika steg av hanteringen av rättighetsbegäran, bilaga med mall för registerutdrag och bilaga med formulär för rättighetsutövande.

Rutindokumentet är inte helt färdigställt ännu men DSO ser positivt på att arbetet med detta dokument är nästintill färdigställt. Det

måste dock uppdateras så att det innehåller rutiner för och information om samtliga rättigheter, inte endast ett fåtal av dem (idag innehåller dokumentet instruktioner för att hantera rätten till tillgång och rätten till radering).

DSO har även haft löpande dialog med bolagets informationssäkerhetssamordnare i frågor som rör det praktiska tillgodoseendet av registrerades rättigheter, vilket visar att bolagets arbete med hantering av de registrerades rättigheter har implementerats på ett tillfredsställande sätt i det dagliga arbetet i bolaget, att det finns en medvetenhet och vilja att arbeta proaktivt och förbättra hanteringen av de registrerades rättigheter.

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

Färdigställ dokumentet ”Rutin för registrerades rättigheter” och säkerställ att rutinerna implementeras hos fler anställda i bolaget. Dokumentet ”Rutiner för registrerades rättigheter” måste även uppdateras med kontaktuppgifter/ägare, så att uppdateringar kan bli gjorda vid behov. DSO kan vara behjälplig med det fortsatta arbetet med rutindokumentet.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Bolagets anställda har kunskap om var de ska vända sig om det inträffar en misstänkt incident. Rutin precis fastställd. Vice vd är den som tar emot anmälningen och rapporterar till staden centralt.
Hur många personuppgiftsincidenter har dokumenterats?	En misstänkt personuppgiftsincident har dokumenterats.
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Vice vd informerades om situationen. Stockholms Stadshus AB gjorde bedömningen att det är osannolikt att incidenten medfört en risk för de registrerades fri- och rättigheter. Bolaget ansåg att detta inte var en incident som behöver anmälas till tillsynsmyndigheten. Efter kontroll visade det sig att ingen exponering av data skett och incidenten/ärendet avslutades utan åtgärd eller anmälan till tillsynsmyndigheten.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Inte aktuellt. Skulle bedömning gjorts att incidenten skulle rapporteras skulle detta anmälas inom 72 från att information om incidenten inkom (25/2 2020 kl. 11.55).

3.6.2 Syfte

En personuppgiftsincident är ”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.”, artikel 4.12 GDPR.

Alla personuppgiftsincidenter ska dokumenteras internt, artikel 33.5 GDPR. Det finns även incidenter som, utöver intern dokumentation, också ska anmälas till tillsynsmyndigheten inom 72 timmar. Därtill ska en del incidenter också informeras till de berörda registrerade.

För att undgå allvarliga konsekvenser för enskildas fri- och rättigheter och tillsynsmyndighetens korrigerande åtgärder samt för att arbeta proaktivt och därmed förhindra att incidenter inträffar eller i vart fall att dess konsekvenser inte blir så allvarsamma, är det viktigt att ha en etablerad rutin för hur personuppgiftsincidenter ska hanteras.

Därtill bör utbildning kring personuppgiftsincidenter erbjudas samtliga medarbetare så att alla vet vad en incident är, när en incident har inträffat och hur en incident ska hanteras.

Dokument med rutiner för incidenthantering bör förankras i hela verksamheten. Det vore även önskvärt att DSO får information gällande de incidenter som inträffar och som är anmälningspliktiga till tillsynsmyndigheten eftersom DSO blir bolagets kontaktpunkt gentemot tillsynsmyndigheten. Förslagsvis kan DSO få en kopia av rapporten som skickas till tillsynsmyndigheten.

3.6.3 Resultat

Stadsledningskontoret har en rutin för informationssäkerhetsincidenter på intranätet, DSO har också fått information om att en rutin precis är fastställd på bolaget. Efter genomförd granskning bedömer DSO att bolaget generellt har en tillfredsställande kunskapsnivå om vad personuppgiftsincidenter är och hur samt av vem de ska hanteras, men att kunskaper om incidenter inte finns hos samtliga medarbetare. Medarbetarna vet dock var de ska vända sig för vidare stöd.

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

Säkerställ att samtliga medarbetare har nödvändiga kunskaper om personuppgiftsincidenter (vad en incident är och hur de ska hanteras). Säkerställ också att DSO kopplas in vid inträffande av en incident och att samtliga medarbetare har kännedom om bolagets rutin för informationssäkerhetsincidenter.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Integritetspolicy
- Registerförteckning
- Rutin för registrerades rättigheter
- Utkast på PUB-avtal mellan Stockholms stad, Stadsrevisionen och EY.
- Intervjuer med anställda och ledning.

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 (bolaget) 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 – Integritetspolicy

Integritetspolicyn riktar sig i första hand till allmänheten för att förklara den behandling av personuppgifter som sker inom ramen för Stockholms Stadshus ABs personuppgiftsansvar. Integritetspolicyn har genomgått granskningar av DSO och är sedan den 15 januari 2021 färdigställd och publicerad på bolagets hemsida, https://stadshusab.stockholm.se/integritetspolicy/.

	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

Granskning 2 – Registerförteckning

Efter den första granskningen som DSO genomförde, den 13 oktober 2020, åtgärdades de brister som DSO uppmärksammade och uppdateringar gjordes. Efter senaste granskningen den 1 april 2020 har DSO ännu inte tagit del av en uppdaterad version av registerförteckningen där de föreslagna åtgärderna vidtagits.

Registerförteckningen är på god väg att bedömas som fullständig (beaktat det faktum att det är ett levande dokument som ska ändras varje gång en personuppgiftsbehandling påbörjas eller upphör). Det återstår dock ett antal kommentarer från DSO med åtgärder som behöver vidtas innan registret kan anses fullständigt.

Följande kommentarer har DSO lämnat vid sin senaste granskning av registerförteckningen:

”Lämna inga fält tomma. Ange t.ex. "Nej", "Sker inte" eller "Ej tillämpbart" istället för att lämna tom, för att registret inte ska framstå som ofullständigt.

Undvik förkortningar; tänk på att registret ska kunna förstås av en helt utomstående utan insyn i verksamheten.

Undvik att klumpa ihop flera behandlingar som inte har exakt samma syften, kategorier av registrerade, kategorier av personuppgifter, gallringsrutiner och så vidare. Alternativt var tydliga i varje kolumn t.ex. vilka personuppgifter som behandlas för varje kategori av registrerad "inom en behandling" och vilken gallringstid som gäller för vilken "del" av behandlingen. På en del ställen har nämligen väldigt många olika personuppgiftsbehandlingar klumpats ihop som en och samma behandling. Har ni exakt samma syften, ändamål, laglig grund, eventuellt PUB-avtal, kategorier av registrerade, kategorier av personuppgifter för dessa behandlingar? Om inte - dela upp behandlingarna så informationen blir korrekt.”

Eftersom att registret innehåller ganska många personuppgiftsbehandlingar och är nästintill fullständigt ifyllt bedömer DSO att bolaget har god kunskap om ifyllande av registerförteckningen. Det krävs dock att de föreslagna åtgärderna/ändringarna som DSO lämnat som kommentarer i registret genomförs innan det kan bedömas vara fullständigt. DSO råder därför bolaget att fortsätta arbeta med registerförteckningen utifrån dessa kommentarer.

Enligt DSO saknas även en utarbetad och skriftlig rutin för översyn/uppdatering av registret. Bolaget bör därmed etablera ett fungerande systematiskt arbetssätt avseende inventering av de behandlingar som sker i verksamheten samt utarbeta och implementera en rutin för att registerförteckningen ska uppdateras så fort en ny behandling har identifierats eller när en befintlig behandling förändras. Även en översyn av registerförteckningen bör ske ett par gånger årligen.

	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 3 – Rutin för registrerades rättigheter

DSO bedömer att bolaget har en fungerande rutin för hantering av registrerades rättigheter inom föreskriven tidsfrist.

Bolagets dokument ”Rutin för registrerades rättigheter” som DSO granskat är mycket informativt och tydligt, och innehåller bilaga för loggning av rättighetshantering, bilaga med mall för att kommunicera till registrerade vid olika steg av hanteringen av rättighetsbegäran, bilaga med mall för registerutdrag och bilaga med formulär för rättighetsutövande.

Rutindokumentet är dock inte helt färdigställt ännu men DSO ser positivt på att arbetet med detta dokument är nästintill färdigställt.

Det måste dock uppdateras så att det innehåller rutiner för och information om samtliga rättigheter, inte bara de allmänt efterfrågade (idag innehåller dokumentet instruktioner för att hantera rätten till tillgång och rätten till radering). Dokumentet måste också uppdateras med kontaktuppgifter/ägare.

	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 3 – PUB-avtal mellan Stockholms stad, Stadsrevisionen och EY

Den 26 november 2020 översände DSO ett mail innehållandes ett granskat PUB-avtal med tillhörande kommentarer och följande meddelande:
”Vi har lagt in några frågor/synpunkter som kommentarer i respektive dokument. I dokumentet ”kommentarer” hittar du de viktigaste sammanfattade och svaret på era frågor.”

DSO fick då svaret att dokumentet skickats vidare till de ansvariga för avtalen och att bolaget skulle återkomma med de efterfrågade bilagorna och svar på frågorna.

4.4 DSO ger råd och rekommendationer till PUA

Se råd och rekommendationer ovan i anslutning till varje granskat dokument.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

1. Sårbarhet med anledning av att endast en person i bolaget är ansvarig över informationssäkerhets- och dataskyddsarbetet.
2. Säkerställande av att alla relevanta dokument, rutiner och avtal finns på plats och att ingenting missas, eftersom en del av det sköts centralt av Stockholms stad medan annat sköts inom bolaget.
3. Avsaknad av tid och kompetens att klassa alla system.
4. Avsaknad av nödvändiga rutiner.

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 dataskyddsförordningen efterföljs är det viktigt att identifiera och minimera eller eliminera alla typer av risker i verksamheten.

5.3 Resultatet av riskkartläggningen

Risk 1

Bolaget är en mindre organisation och det är i dagsläget endast en person som har det övergripande ansvaret över informations- och dataskyddsarbetet. Det medför en sårbarhet för en verksamhet att endast förlita sig på en person, inte minst för ett så pass brett område som informationssäkerhet och dataskydd.

	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

Avsaknad av tillräckliga resurser kan leda till att viktiga åtgärder på området inte vidtas, vilket i sin tur kan leda till att kraven i dataskyddsförordningen inte möts.

Risk 2

Idag sköts en stor del av arbetet vad gäller framtagande av styrdokument och upphandling/ingående av avtal av Stockholms stad. Oklarheter i ansvarsfördelningen mellan PUA/Bolaget och dess ägare Stockholms stad, riskerar att leda till att alla nödvändiga dokument och avtal inte finns på plats.

	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

DSO har ännu inte noterat att denna risk har realiserats, men efter att ha granskat bolaget är det en risk som DSO bedömer skulle kunna inträffa. Det är därför viktigt att bolaget fortsätter ha en öppen och snabb kommunikation med Stockholms stad i alla frågor som rör informationssäkerhet och dataskydd.

Risk 3

Informationsklassning gällande data generellt. Här har DSO fått information om att tanken är att staden ska bli bättre på att klassa alla processer men att de för närvarande saknar tid och kompetens att klassa alla system. De är inte så många som bevakar frågan och har en bräcklig organisation så tillvida att det är få som kan arbetet.

	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

Personuppgifter måste skyddas på ett tillfredsställande sätt. Om personuppgifter behandlas i system som inte informationsklassas riskerar bolaget att behandla personuppgifter utan att skydda dem på ett tillräckligt sätt.

Risk 4

Bolaget saknar en rutin för hantering av offentlighetsprincipen i relation till dataskyddsförordningen. Eftersom dataskyddsförordningen har uppgiftsminimering som en grundläggande princip, samtidigt som offentlighetsprincipen och arkivlagstiftningen har som huvudregel att alla upprättade och inkomna handlingar ska sparas finns kolliderande synsätt som behöver hanteras.

Bolaget saknar även rutiner för hur de ska hantera om handlingar med personuppgifter inkommer via mail och liknande kanaler utan att bolaget efterfrågat uppgifterna.

	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

De grundläggande principerna i artikel 5 GDPR gäller oavsett kategorier av personuppgifter och typ av behandling. Den personuppgiftsansvariga måste följa samtliga dessa principer – att inte göra det utgör ett brott mot GDPR.

Principerna innebär bland annat att den personuppgiftsansvariga

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

Utan rutin för hantering av offentlighetsprincipen i relation till dataskyddsförordningen och utan rutiner för hur personuppgifter som inkommer via mail ska hanteras riskerar bolaget att bryta mot artikel 5 GDPR vilket bland annat kan leda till att tillsynsmyndigheten utdömer en sanktionsavgift mot bolaget.

5.4 DSO ger råd och rekommendationer till PUA

De åtgärder som DSO föreslår för att eliminera eller minska de identifierade riskerna framgår av tidigare avsnitt av rapporten. Som externt DSO avstår vi från att lämna förslag på vem i organisationen som lämpligen bör anförtros uppgifterna att åtgärda de ovan påtalade bristerna. Vi uppfattar dock att samtliga risker bör ha kunna hanterats innan årets slut.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Att övervaka efterlevnaden av dataskyddsförordningen är ett uppdrag som kräver ett kontinuerligt och systematiskt arbete. En tillsynsperiod rymmer inte tillsyn av en hel organisation mot dataskyddsförordningens alla element, varför tillsynen är ett kontinuerligt projekt.

Vi har denna dag nåtts av besked att vi upphandlats av bolaget som DSO för ytterligare en avtalsperiod, och ber att få återkomma med förslag på kommande granskningsområden inom ramen för detta förnyade förtroende, inom en snar framtid.

7 Övrigt att rapportera

7.1 Sammanfattning

DSO har inget övrigt att rapportera.