



Stockholms
stad

GDPR Årsrapport

År 2022

Stockholms Stadshus AB

GDPR årsrapport
2022

Dnr: SSAB 2023/19
Kontaktperson: Ingrid Storm

1 Bakgrund

EU:s Dataskyddsförordning, GDPR, trädde i kraft 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 hanteringen 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 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 en nämnd eller bolagsstyrelse ska kunna *visa* att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna *dokumentationsskyldighet*. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

| | | |
|----------|---|-----------|
| 1 | Bakgrund | 3 |
| 2 | Sammanfattning | 5 |
| 3 | Obligatoriska rapporteringsområden | 6 |
| 3.1 | Registerförteckning | 7 |
| 3.2 | Styrdokument | 10 |
| 3.3 | Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar | 13 |
| 3.4 | Konsekvensbedömningar | 15 |
| 3.5 | Individens rättigheter | 18 |
| 3.6 | Personuppgiftsincidenter | 20 |
| 4 | Genomförda granskningar under året | 23 |
| 4.1 | Sammanfattning | 23 |
| 4.2 | Syfte | 23 |
| 4.3 | Genomförda granskningar och deras resultat | 23 |
| 4.4 | DSO ger råd och rekommendationer till PUA | 25 |
| 5 | Risker inom dataskydd | 26 |
| 5.1 | Sammanfattning | 26 |
| 5.2 | Syfte | 26 |
| 5.3 | Resultatet av riskkartläggningen | 26 |
| 5.4 | DSO ger råd och rekommendationer till PUA | 26 |

2 Sammanfattning

I egenskap av Dataskyddsombud i Stockholms Stadshus AB lämnar jag följande årsrapport.

DSO har under tillsynsåret involverats i verksamhetens dataskyddsarbete på ett aktivt och löpande sätt. Således har DSO haft god insyn i verksamhetens handlingssätt och upplever att samarbetet mellan verksamheten och DSO har lett till att verksamheten utför dataskyddsarbete på en god nivå.

DSO konstaterar att verksamhetens dataskyddsarbete håller en hög nivå och att majoriteten av förra tillsynsårets föreslagna åtgärder har åtgärdats på ett lämpligt sätt.

DSO har granskat de sex obligatoriska granskningsområdena samt ett antal områden utöver de obligatoriska. Inledningsvis konstaterar DSO att verksamheten i hög utsträckning uppfyller de krav som ställs enligt dataskyddsförordningen och enligt den aktuella rapporten. DSO återger nedan de områden där vissa brister ändå finns som kan och behöver åtgärdas.

- DSO rekommenderar att registerförteckningen justeras så att den kan förstås av en utomstående person.
- DSO rekommenderar att verksamheten säkerställer att samtlig personuppgiftsbehandling informationklassas.
- DSO rekommenderar bolaget att göra en sammanställning över vilka system de använder i sin verksamhet och vilka av dessa som föranleder en riskanalys/konsekvensbedömning för att säkerställa att alla nödvändiga bedömningar genomförs.
- DSO rekommenderar bolaget att lägga särskilt fokus på att sprida kunskap i personalgruppen om vad personuppgiftsincidenter är och hur de ska hanteras.

3 Obligatoriska rapporteringsområden

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

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

Nedan redogörs för nämndens eller bolagets status och DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|------------|
| Antal behandlingar som är registrerade? | 91 stycken |
| Har nödvändiga uppdateringar gjorts? | Ja |
| Bedöms registerförteckningen vara fullständig? | Ja |
| Har verksamheten lämpliga rutiner för registerföring? | Ja |

3.1.2 Syfte

I artikel 30, GDPR, anges en skyldighet för varje personuppgiftsansvarig och personuppgiftsbiträde att upprätta ett register över samtliga personuppgiftsbehandlingar som utförs under dess ansvar.

När registerförteckningen är upprättad skapar den en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Registerförteckningen är därför dataskyddsarbetets centrala utgångspunkt och bas som bl.a. säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling man utför.

Det är viktigt att personuppgiftsansvarige får information om hur komplett verksamhetens förteckning är. Om dokumenteringskravet uppfylls kan verksamheten arbeta effektivt, systematiskt och riskbaserat och samtidigt värna individens integritet, särskilt när känsliga och särskilt skyddsvärda personuppgifter behandlas av verksamheten.

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

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

Eftersom inventeringen av personuppgifter i sig är avgörande för allt det fortsatta dataskyddsarbetet inom verksamheten, är denna lägesbild en av de viktigaste slutsatserna som personuppgiftsansvarige behöver förstå och ta ställning till inför det planerade åtgärdsarbetet under nästa verksamhetsår.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

91 stycken behandlingar finns registrerade i registerförteckningen av den 28 december 2022.

DSO kontrollerar om nödvändiga uppdateringar gjorts

DSO konstaterar att den senast uppdaterade versionen av registerförteckningen som tillhandahållits till DSO är daterad 28 december 2022, vilket indikerar att registerförteckningen hålls uppdaterad och levande. Bedömningen att registerförteckningen hålls uppdaterad understöds av bolagets internkontrollplan och av uppgifter från de intervjuer som hållits i samband med tillsynsarbetet.

DSO bedömer hur fullständig registerförteckningen är

DSO bedömer att registerförteckningen är att anse som fullständig. Det framgick under tillsynen att verksamheten har arbetat noggrant med sin registerförteckning och lagt ned ett stort arbete på att säkerställa att verksamhetens samtliga personuppgiftsbehandlingar ingår. DSO bedömer att verksamhetens samtliga personuppgiftsbehandlingar tycks ingå i registerförteckningen. Det finns definitivt en sådan ambition i verksamheten.

Registreringarna håller i regel en god kvalitet innehållsmässigt och exempelvis är fältet *Laglig grund* ifyllt i samtliga registreringar. I den föregående årsrapporten noterades att de tidigare

uppmärksammade bristerna i registerförteckningen åtgärdats i den uppdaterade registerförteckningen.

Den nuvarande registerförteckningen innehåller ett antal tomma fält, framför allt vad avser fältet ”Vidtagna säkerhetsåtgärder”. DSO rekommenderar verksamheten att undvika att lämna fält tomma då det kan framstå som oklart om registret är färdigställt. Fyll därför i alla tomma fält, och skriv exempelvis ”Sker inte”, ”Ej tillämpligt” eller ”Nej” istället för att lämna ett fält tomt.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

DSO konstaterar att verksamheten har nedtecknade rutiner som anger att registerförteckningen ska överses årligen. Det innebär att verksamheten arbetar med registerförteckningen som ett levande dokument på ett löpande sätt. Tjänstemän i verksamheten har dock uppgett att registerförteckningen är utformad på ett sådant sätt att den kan vara svår att förstå för någon annan än dokumentägaren. Detta är något som bör åtgärdas då syftet med en registerförteckning är att den ska kunna förstås även av en utomstående utan insyn eller insikt i verksamheten.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

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

3.1.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att verksamheten fortsätter att arbeta löpande med registerförteckningen utifrån att nya behandlingar införs eller att gällande behandlingar förändras. Verksamheten rekommenderas även fylla i alla tomma fält i registerförteckningen. Tomma fält kan få registerförteckningen att framstå som ofullständig. DSO

rekommenderar även att registerförteckningen justeras så att den kan förstås av en utomstående person utan insyn i verksamheten.

3.2 Styrdokument

3.2.1 Sammanfattning

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

3.2.2 Syfte

Området syftar till att personuppgiftsansvarige genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar personuppgiftsansvarige till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna, när de hanterar personuppgifter. Att styrdokument finns nedtecknade, beslutade och kommunicerade medför att medarbetaren får dataskyddsinformation och kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt. En röd tråd i dataskyddsförordningen är att viktiga arbetsätt och rutiner ska vara dokumenterade. Detta följer bland annat av kravet på att den personuppgiftsansvarige måste kunna visa att dataskyddsförordningens principer för behandling av personuppgifter efterlevs (artikel 5).

Rapporteringen av området är tvådelad: dels ska DSO bedöma om verksamheten har relevanta styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt

håller en lämplig kvalitet, i vilket ingår bl.a. att dokumentationen ska vara uppdaterad och aktuell.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?

DSO konstaterar att verksamhetens styrande dokumentation i dagsläget omfattar en stor del av dataskyddsområdet. I föregående årsrapport konstaterade DSO att det saknades rutiner för översyn av registerförteckningen vilket verksamheten har åtgärdat genom att införa översynen som ett moment i internkontrollplanen. Vid föregående tillsyn konstaterade även DSO att rutinen för registrerades rättigheter behöver uppdateras avseende rutiner för och information om samtliga rättigheter samt att rutinen behöver innehålla kontaktuppgifter och ägare. Rutinen har nu uppdaterats så att den innehåller kontaktuppgifter och ägare och arbetet med rutiner för och information om samtliga rättigheter är nästan slutfört. DSO rekommenderade även verksamheten att ta fram en rutin för hantering av offentlighetsprincipen i relation till dataskyddsförordningen och verksamheten har tagit fram ett utkast på denna rutin. DSO bedömer därmed att den styrande dokumentationen är godtagbart omfattande.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

DSO bedömer att innehållet i de tillhandahållna dokumenten håller god kvalitet. Rutinerna är överskådliga, lättillgängliga, omfattande och är utformade för att kunna användas av samtliga anställda. Även i övrigt bedömer DSO att dokumenten är relevanta och väl uppdaterade.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

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

| | |
|---|--|
| x | Inga brister av nämnvärd betydelse identifierade |
|---|--|

3.2.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att verksamheten fortsätter arbetet med att implementera styrande dokument. Verksamheten uppmuntras att färdigställa rutinen för hantering av offentlighetsprincipen i relation till dataskyddsförordningen.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlings

3.3.1 Sammanfattning

| Fråga/kontroll | Svar |
|--|---------------------|
| Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats? | 0 av bolaget själv. |
| Är klassade personuppgiftsbehandlingar aktuella? | |

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd så ska verksamheten informationsklassa sin information. Stockholms stads riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Utan informationsklassningen saknar verksamheten förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att personuppgiftsansvarige ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

Ansvar för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. En första kontrollpunkt måste därför vara om en informationsägare eller en informationsägarrepresentant med ansvar för klassning är identifierad i verksamheten. Om en ansvarig för klassningen inte har pekats ut och känner till sitt ansvar för uppdraget, minskar sannolikheten avsevärt att en klassning faktiskt initieras.

Notera att enbart sådan informationsklassning som avser behandling eller system som omfattar personuppgifter är av intresse för DSO:s årsrapportering.

3.3.3 Resultat

I föregående årsrapport konstaterade DSO att verksamheten inte informationsklassat lönehanteringssystemet Visma Agda. Verksamheten uppger att arbetet med att genomföra en

informationsklassning av Visma Agda har påbörjats och att koncernledningen deltar i grundläggande utbildning i informationsklassningsarbetets olika delar. Bland annat har verksamheten haft möte med andra bolag för att kunna genomföra en gemensam informationsklassning av systemet. De involverade bolagen använder systemet på ett identiskt sätt och en gemensam informationsklassning är därmed effektivt ur ett tids- och resursperspektiv.

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 rekommenderar att verksamheten fortsätter med det planerade informationsklassningsarbetet i fråga om lönehanteringssystemet Visma Agda. DSO rekommenderar att verksamheten slutför informationsklassningen så snart som möjligt.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

| Fråga/kontroll | Svar |
|--|------|
| Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av? | Ja |
| Har alla potentiella högriskbehandlingar konsekvensbedömts? | Ja |
| Är de genomförda bedömningarna aktuella? | Ja |

3.4.2 Syfte

Konsekvensbedömningen hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas i projekt eller linjeverksamhet. En konsekvensbedömning har till syfte att identifiera och dokumentera risker kopplade till en viss behandling, samt att bedöma sannolikheten och konsekvensen om riskscenariot skulle inträffa. Baserat på bedömningen kan/ska riskförebyggande åtgärder vidtas.

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning som ett viktigt verktyg för verksamhetens dataskyddsarbete. Kravet på konsekvensbedömning är dessutom uttryckligen angivet i GDPR och ska utföras för alla nya behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1). Det är viktigt att personuppgiftsansvarige genom årsrapporten får en uppdaterad bild av hur fullständig verksamhetens situation är i fråga om konsekvensbedömningar avseende dataskydd.

3.4.3 Resultat

Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?

Bolaget använder i dagsläget inga egna system i vilka personuppgiftsbehandlings 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. Detta minimerar även risken för att bolaget ensamt använder sig av ett system som skulle innebära en hög risk för de registrerades integritet, utan att ha genomfört en konsekvensbedömning.

DSO noterar att kunskapsläget och medvetenheten kring dataskyddsfrågor bland de anställda är på så pass hög nivå att det enligt vår bedömning föreligger en låg risk att någon högriskbehandling som inte konsekvensbedömts skulle pågå i dagsläget. DSO rekommenderar dock bolaget att göra en inventering av pågående personuppgiftsbehandlings som kan tänkas innebära hög risk för fysiska personers rättigheter och friheter och som därmed föranleder en konsekvensbedömning. Förslagsvis kan bolaget göra en förteckning över vilka system de har och vilka system som föranleder en konsekvensbedömning för att sedan säkerställa att antingen stadsledningskontoret utfört en konsekvensbedömning eller att bolaget själva utfört en konsekvensbedömning.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Vid nya eller kraftigt förändrade behandlingar kontaktar bolaget DSO för att avgöra om en konsekvensbedömning ska genomföras, vilket ökar sannolikheten för att alla nödvändiga konsekvensbedömningar genomförs. Dessutom är kunskapsläget och medvetenheten kring dataskyddsfrågor på en så pass hög nivå att det föreligger låg risk att någon högriskbehandling som inte konsekvensbedömts skulle pågå i dagsläget. DSO rekommenderar ändå bolaget att genomföra en inventering av pågående personuppgiftsbehandlings för att säkerställa att alla högriskbehandlingar föranletts av en konsekvensbedömning.

Är de genomförda konsekvensbedömningarna aktuella?

Med hänsyn till den medvetenhet och kunskap som finns inom bolaget avseende dataskydd utgår DSO från att de genomförda konsekvensbedömningarna är aktuella.

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 rekommenderar bolaget att göra en inventering av samtliga pågående personuppgiftsbehandlingar som kan tänkas innebära hög risk för fysiska personers rättigheter och friheter och som därmed föranleder en konsekvensbedömning. Bolaget kan förslagsvis göra en förteckning över vilka system de har och vilka system som föranleder en konsekvensbedömning för att sedan säkerställa att alla nödvändiga konsekvensbedömningar genomförts av antingen bolaget eller av stadsledningskontoret. Detta är en viktig del av att kunna bevisa regelefterlevnad av dataskyddsförordningen.

3.5 Individens rättigheter

3.5.1 Sammanfattning

| Fråga/kontroll | Svar |
|--|------|
| Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer? | 0 |
| Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar? | |

3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt garanterar att den registrerade personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att den personuppgiftsansvarige tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, exempelvis att lämna ut ett så kallat registerutdrag eller att rätta vissa uppgifter. (Radering, den så kallade ”rätten att bli glömd”, är sällan aktuell i någon större mån eftersom stadens organ lyder under krav på bevarande till följd av offentlighetsprincipen.) Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran. (Notera även att det finns undantagssituationer angivna i artikel 12.3, där svarsfristen kan förlängas till mer än en månad.)

Dataskyddsbudet har en roll i att granska efterlevnaden, identifiera brister samt ge råd och stöd i hur processer och rutiner för att tillgodose rättigheterna bör utformas.

Om verksamheten inte klarar av att hantera en begäran från registrerade personer i enlighet med dataskyddsförordningens krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsändan från IMY:s sida, med sanktioner som följd. Det är därför viktigt att

personuppgiftsansvarige regelbundet ges en bild av i vilken mån verksamheten klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Verksamheten har under tillsynsåret inte tagit emot någon begäran från registrerade avseende registerutdrag, begränsning eller radering.

DSO konstaterar att verksamheten har goda förutsättningar för att hantera registrerades rättigheter på ett mycket gott sätt. Rutinen för hantering av dessa ärenden tycks vara fullt ut förankrad i verksamheten. Det är väl känt för medarbetarna vem de ska kontakta om en begäran från en registrerad inkommer till bolaget. DSO bedömer att de rutiner som finns nedtecknade för att tillvarata de registrerades rättigheter är mycket goda.

3.5.4 DSO anger hur allvarliga bristerna är på en skala

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

3.5.5 DSO ger råd och rekommendationer till PUA

Under tillsynen 2021 noterade DSO att rutinen för registrerades rättigheter saknade information om samtliga rättigheter. Rutinen innehöll endast instruktioner för att hantera rätten till tillgång och rätten till radering. Arbetet med att införa instruktioner för samtliga rättigheter är så gott som slutfört. DSO rekommenderar bolaget att säkerställa att rutinerna implementeras fullt ut i verksamheten.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

| Fråga/kontroll | Svar |
|--|--|
| Hur upptäcks personuppgiftsincidenter? | Genom att medarbetare i verksamheten anmäler till dataskyddsansvarig, eller genom att det centralt (SLK) noteras signaler om incidenter i gemensamma system. |
| Hur många personuppgiftsincidenter har dokumenterats? | 0 |
| Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte? | 0 |
| Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten? | 0 |

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 bland dataskyddsförordningens olika verktyg för att åstadkomma en god personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering. Stadens mall för DSO:s årsrapport är avsedd att fokusera på rapporteringen.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se

artikel 33). Detta innebär att de flesta personuppgiftsincidenter ska rapporteras till IMY, och då inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, ska rapportering även ske till de berörda registrerade personerna, utan dröjsmål. Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering även till de berörda personerna.

Om en organisation brister i förmåga att rapportera personuppgiftsincidenter i tid kan det leda till sanktioner från IMY:s sida. DSO:ns årsrapportering är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad etc.

Notera att enligt dataskyddsförordningen artikel 33.5 ska alla personuppgiftsincidenter dokumenteras, det vill säga även i de fall då incidenten inte ska rapporteras till IMY. Bristande dokumentering står i strid med dataskyddsförordningen och leder även till problem med att ta fram korrekta siffror till årsrapporteringen avseende hur väl verksamheten lever upp till rapporteringsfristerna. Enligt artikel 33.5 är det ett krav att dokumentera omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för den egna organisationen att förbättra sin personuppgiftshantering genom systematiskt kvalitetsarbete och för tillsynsmyndigheten (IMY) att kontrollera efterlevnaden. Bristande dokumentation är sanktionsgrundande.

3.6.3 Resultat

Hur väl förmår verksamheten att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?

Eftersom inga personuppgiftsincidenter har skett under tillsynsåret så kan inte DSO uttala sig om bolagets förmåga att rapportera personuppgiftsincidenter i tid till IMY. Verksamheten har uppgett att de har svårt att bedöma vilka händelser de behöver dokumentera. Som nämnt ovan ska alla händelser som är att betrakta som personuppgiftsincidenter dokumenteras internt, oavsett om

incidenten ska anmälas till IMY eller om de registrerade ska informeras om incidenten.

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

Verksamheten uppger att de har svårt att bedöma vilka händelser som är att betrakta som personuppgiftsincidenter och därmed behöver dokumenteras. Av dataskyddsförordningen följer en skyldighet att registrera och dokumentera incidenter. Bolaget behöver även motivera beslut som tagits i samband med personuppgiftsincidenten, exempelvis varför incidenten inte anmäls till IMY eller varför de registrerade inte blivit informerade om incidenten.

Av den anledningen rekommenderar DSO att bolaget lägger särskilt fokus på att sprida kunskap i sin organisation om vad personuppgiftsincidenter är och hur de ska hanteras.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- *Granskning 1 – Implementering av åtgärder från förra årets tillsynsrapport*
- *Granskning 2 – Agerande med anledning av Schrems II-domen*

4.2 Syfte

En av dataskyddsombudets centrala uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En viktig del av detta arbete är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten behöver fatta i fråga om dataskyddsåtgärder. För personuppgiftsansvarige är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under tillsynsåret och vad resultaten av granskningarna är.

4.3 Genomförda granskningar och deras resultat

Granskning 1 - Implementering av åtgärder från förra årets tillsynsrapport

I föregående årsrapport föreslog DSO ett antal åtgärder, däribland:

- Kontinuerlig utbildning för medarbetarna,
- Utbildning kring personuppgiftsincidenter,
- Införande av en utarbetad, skriftlig rutin för översyn och uppdatering av registerförteckningen,
- Uppdatering av rutiner för registrerades rättigheter,
- Framtagande av en rutin för hantering av offentlighetsprincipen i relation till dataskyddsförordningen.
- Att dokument som staden publicerar på intranätet också kommuniceras ut i hela bolaget,

- Informationsklassning av lönehanteringssystem Visma Agda.

DSO konstaterar att majoriteten av de rekommenderade åtgärderna har implementerats väl av bolaget. Den åtgärd som ännu inte implementerats, enligt den information som tillhandahållits DSO, är:

- Informationsklassning av lönehanteringssystem Visma Agda.

DSO har fått information om att bolaget börjat planera informationsklassningsarbetet av Visma Agda och att koncernledningen deltar i grundläggande utbildning i informationsklassningsarbetets olika delar. Bolaget har även haft möte med andra bolag för att kunna genomföra en gemensam informationsklassning av Visma Agda. De involverade bolagen använder systemet på ett identiskt sätt och en gemensam informationsklassning är därmed effektivt ur ett tids- och resursperspektiv. DSO rekommenderar att bolaget genomför informationsklassningen av Visma Agda så snart som möjligt.

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

Granskning 2 – Agerande med anledning av Schrems II-domen

Under 2020 kom avgörandet Schrems II från EU-domstolen. Där slog domstolen fast att Privacy Shield-avtalet mellan EU och USA inte gav ett tillräckligt skydd för personuppgifter när dessa förs över till USA. Ogiltigförklarandet innebär att verksamheter inte längre kan stödja sig på Privacy Shield som grund för att överföra personuppgifter till USA. DSO har därför valt att granska verksamhetens agerande med anledning av Schrems II-avgörandet.

DSO konstaterar inledningsvis att verksamheten uppvisar god kunskap om avgörandet och de konsekvenser avgörandet har fått på dataskyddsområdet i stort. Det finns en tydlig förståelse i verksamheten om de problem som tredjelandsöverföring till USA innebär.

Som exempel på den goda medvetenheten så har bolaget gjort en kartläggning av sina pub-avtal och system som de har rådighet över för att säkerställa att ingen tredjelandsöverföring sker. Vidare anges det alltid i bolagets pub-avtal att alla tredjelandsöverföringar måste godkännas av bolaget. Bolaget publicerar dessutom inte personuppgifter på sociala medier.

| | |
|---|--|
| | 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

DSO rekommenderar bolaget att fortsätta följa det som händer på dataskyddsområdet med anledning av Schrems II-domen. Bolaget rekommenderas även att vara fortsatt restriktiva och att i den mån det är möjligt undvika tredjelandsöverföringar fram till dess att frågan om överföring till framför allt USA har kommit närmare en lösning.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- *DSO har inte identifierat eller blivit uppmärksammat på några risker i verksamheten som inte redan är hanterade i riskanalyser och konsekvensbedömningar.*

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. DSO behöver som underlag för sin planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, gällande verksamhetens samtliga personuppgiftsbehandlingar. Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som dataskyddsombudet behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

5.3 Resultatet av riskkartläggningen

| | |
|---|--|
| | 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 |

5.4 DSO ger råd och rekommendationer till PUA

Bolaget tillhör inte typiskt sett den del av en kommuns verksamhet där det hanteras stora mängder känsliga personuppgifter eller vars personuppgiftsrisiker på annat sätt kan förväntas vara framträdande.

Givet detta och att DSO i dagsläget inte har kännedom om några nämnvärda risker i bolagets verksamhet, lämnas inga rekommendationer på detta område.