



Stockholms
stad

GDPR Årsrapport

År 2024

Stockholms Stadshus AB

GDPR årsrapport

Dnr:

Utgivningsdatum:

Kontaktperson:

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	7
3.1	Registerförteckning	8
3.2	Styrdokument	12
3.3	Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar	14
3.4	Konsekvensbedömningar	16
3.5	Individens rättigheter	19
3.6	Personuppgiftsincidenter	21
4	Genomförda granskningar under året	24
4.1	Sammanfattning	24
4.2	Syfte	24
4.3	Genomförda granskningar och deras resultat	24
4.4	DSO ger råd och rekommendationer till PUA Fel! Bokmärket är inte definierat.	
5	Risker inom dataskydd	29
5.1	Sammanfattning	29
5.2	Syfte	29
5.3	Resultatet av riskkartläggningen	29
5.4	DSO ger råd och rekommendationer till PUA	29

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 relativt god insyn i verksamhetens handlingsätt 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 flera 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 de anställda får information om vad en personuppgiftsbehandling är och hur de ska gå tillväga vid en ny eller förändrad personuppgiftsbehandling, för att säkerställa att registerförteckningen återspeglar bolagets aktuella behandlingar.
- DSO rekommenderar att bolaget slutför arbetet med att kontrollera att samtliga genomförda informationsklassningar är aktuella, relevanta och att bolaget vid behov reviderar klassningarna.
- DSO rekommenderar att bolaget gör en inventering av samtliga pågående personuppgiftsbehandlingar som kan tänkas innebära hög risk för fysiska personers rättigheter och friheter för att säkerställa att alla nödvändiga bedömningar genomförs.
- DSO uppmuntrar verksamheten att färdigställa en rutin för personuppgiftsincidenthantering som är anpassad för verksamhetens arbetssätt och övriga behov.
- DSO rekommenderar att de anställda får tydlig information om hur de ska hantera sin e-post i förhållande till dataskyddsförordningen och allmänna handlingar.

- DSO rekommenderar bolaget att ta fram riktlinjer för hur AI får användas i verksamheten, för att säkerställa att AI hanteras på ett sätt som är förenligt med dataskyddsförordningen.

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?	52 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 utgör den en ökad intern synlighet och förståelse för vilka personuppgifter som behandlas i verksamheten och hur dessa hanteras. Registerförteckningen kan därför sägas utgöra 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

52 stycken behandlingar finns registrerade i registerförteckningen av den 15 november 2024.

DSO kontrollerar om nödvändiga uppdateringar gjorts

DSO konstaterar att den senast uppdaterade versionen av registerförteckningen som tillhandahållits till DSO är daterad 15 november 2024, 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 bolagets samtliga personuppgiftsbehandlingar ingår. DSO bedömer att bolagets samtliga personuppgiftsbehandlingar ingår 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 registerförteckningen

innehöll ett antal tomma fält, framför allt avseende fältet ”Vidtagna säkerhetsåtgärder”.

De tidigare uppmärksammade bristerna avseende de tomma fälten har åtgärdats och den uppdaterade registerförteckningen framstår som fullständigt ifylld.

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 systematiskt sätt. Det finns även ett utpekat ansvar för uppdatering och översyn av registerförteckningen.

DSO har fått information om att det finns ett behov av att påminna de anställda om vad en personuppgiftsbehandling är och hur de ska gå tillväga om en ny typ av behandling påbörjas eller om en etablerad personuppgiftsbehandling förändras. För att säkerställa att registret återspeglar bolagets aktuella personuppgiftsbehandlingsar är det viktigt att det finns rutiner för att fånga upp nya behandlingar och föra in dessa i registerförteckningen.

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. DSO rekommenderar att de anställda får information om vad en personuppgiftsbehandling är och hur de ska gå tillväga vid en ny eller förändrad

personuppgiftsbehandling, för att säkerställa att registerförteckningen återspeglar bolagets aktuella behandlingar.

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 den personuppgiftsansvarige genom styrdokument ska kunna visa att man bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar den 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 arbetssätt och rutiner ska vara dokumenterade. Detta följer bland annat av kravet på att den personuppgiftsansvarige måste kunna visa att dataskyddsförordningens principer för behandling av personuppgifter efterlevs (artikel 5).

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. DSO bedömer därmed att den styrande dokumentationen är av tillräcklig omfattning.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

DSO har vid tidigare tillsyn bedömt att verksamhetens rutiner på dataskyddsområdet är överskådliga, lättillgängliga, omfattande och utformade för att kunna användas av samtliga anställda. Dessa rutiner har inte förändrats under tillsynsåret och inga nya rutiner har tillkommit.

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.

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?	2 av bolaget själva samt 16 centralt informationsklassade.
Är klassade personuppgiftsbehandlingar aktuella?	Inte säkerställt

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slag och nivå av skydd, så behöver verksamheten klassa 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 både genomförd och aktuell för de personuppgifter som verksamheten hanterar.

Ansaret 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 genomförs på ett bra sätt.

Notera att enbart sådan informationsklassning som avser behandling eller system som omfattar personuppgifter är av intresse för DSO:s årsrapportering. Annan typ av data ligger utanför dataskyddförordningens reglering och DSO:s uppdrag.

3.3.3 Resultat

Bolaget använder sig av flera system som Stockholms stad äger och för dessa system har bolaget tagit del av stadens genomförda informationsklassningar. Bolaget har jämfört stadens informationsklassningar med bolagets egen användning av systemen och kontrollerat att det inte finns behov av ytterligare klassning.

Översyn av klassningarna sker kontinuerligt och vid behov. Verksamheten har vid föregående tillsyn uppgett att några av de genomförda informationsklassningarna kan vara i behov av revidering. I föregående årsrapport rekommenderade DSO bolaget att kontrollera att samtliga genomförda informationsklassningar var aktuella, relevanta och att bolaget vid behov reviderade klassningarna. DSO har fått information om att arbetet med detta är påbörjat men inte slutfört.

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 bolaget slutför arbetet med att kontrollera att samtliga genomförda informationsklassningar är aktuella, relevanta och att bolaget vid behov reviderar klassningarna.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

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

3.4.2 Syfte

En konsekvensbedömning hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas i projekt eller linjeverksamhet. Konsekvensbedömningen 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 personuppgiftsbehandlingar utförs som kräver att en konsekvensbedömning upprättas. Bolaget använder främst system som är stadsgemensamma, som bolaget saknar faktisk rådighet över. Eventuella konsekvensbedömningar för dessa system torde således inte vara bolagets ansvar utan bör istället göras centralt i staden, där beslutet om upphandling och användning fattas. Något som också minimerar risken för att bolaget ensamt använder sig av ett system som kunde 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 bara föreligger en låg risk att någon högriskbehandling som inte konsekvensbedömts skulle pågå eller vara på väg att påbörjas. DSO rekommenderade ändå bolaget vid föregående tillsyn att göra en inventering av pågående personuppgiftsbehandlingar som kan tänkas innebära hög risk för fysiska personers rättigheter och friheter och som därmed föranleder en konsekvensbedömning. DSO har ännu inte fått information om att bolaget genomfört en sådan inventering. DSO föreslår att bolaget gör en förteckning över vilka system de har och vilka av dessa som föranleder en konsekvensbedömning, för att sedan säkerställa att en konsekvensbedömning utförts antingen av stadsledningskontoret/annan del av Stockholms stad, eller att bolaget själva utfört den.

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 bedöms kunskapsläget och medvetenheten kring dataskyddsfrågor ligga 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 för säkerhets skull genomföra en inventering av pågående personuppgiftsbehandlingar, för att säkerställa att alla högriskbehandlingar föregåtts 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. För att säkert kunna ta ställning till detta bör dock en inventering göras (se ovan).

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, av stadsledningskontoret eller annat organ inom staden. 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 begäranden (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	0
Hur många av dessa begäranden har hanterats av verksamheten inom 30 dagar?	0

3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt garanterar att den registrerade personen ges 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 lagkrav på handlingars och uppgifters 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 tillsynsärenden 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?

Under 2024 har ingen begäran om att utöva registrerades rättigheter inkommit till bolaget.

DSO konstaterar att verksamheten har goda förutsättningar 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 väl utformade.

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

Eftersom ingen begäran om att utöva de registrerades rättigheter har inkommit under tillsynsåret så kan inte DSO fullt ut uttala sig om bolagets förmåga att hantera dessa. Verksamheten har dock tidigare år visat god förmåga att hantera dessa inom föreskriven tidsfrist. DSO uppmuntrar verksamheten att fortsättningsvis tillmötesgå begäran om att utöva registrerades rättigheter på en sådan god nivå som de hittills har gjort.

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.

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

artikel 33). Detta innebär att flera 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 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. Syftet är att de ska kunna användas i det kvalitetsutvecklande arbetet hos den personuppgiftsansvarige. Bristande dokumentation 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 vid IMY:S tillsyn.

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 verksamhetens förmåga att rapportera personuppgiftsincidenter i tid till IMY. Verksamheten har dock tidigare uppgett att de emellanåt har svårt att bedöma när och hur de ska hantera händelser som kan utgöra personuppgiftsincidenter.

Vid föregående tillsyn rekommenderade därför DSO bolaget att sprida kunskap till de anställda om vad en personuppgiftsincident är och hur den ska hanteras. Under tillsynsåret har bolaget genomfört kortare utbildningsinsatser för att sprida kunskap om detta. Bolaget har uppgett att det finns en ambition om att återkommande genomföra utbildningsinsatser om personuppgiftsincidenter. DSO uppmuntrar detta.

Verksamheten har uppgett att de använder en rutin för personuppgiftsincidenthantering som är baserad på den rutin som stadsledningskontoret tagit fram. Verksamheten upplever att rutinen är omfattande och innehåller delar som inte är relevanta för ett bolag av deras storlek. Vid föregående tillsyn fick DSO information om att verksamheten hade påbörjat arbetet med att ta fram en rutin för personuppgiftsincidenthantering som var anpassad för deras behov. DSO har inte fått information om att det arbetet har slutförts.

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 uppmuntrar verksamheten att färdigställa en rutin för personuppgiftsincidenthantering som är anpassad för verksamhetens arbetssätt och övriga behov.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- *Granskning 1 – Implementering av åtgärder från förra årets tillsynsrapport*
- *Granskning 2 – Artificiell intelligens*
- *Granskning 3 – PUB-avtal*

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:

- att bolaget skulle fylla i alla tomma fält i registerförteckningen.
- att bolaget skulle kontrollera att samtliga genomförda informationsklassningar är aktuella, relevanta och vid behov reviderar klassningarna.
- att bolaget skulle göra en inventering av samtliga pågående personuppgiftsbehandlingar som kan tänkas innebära hög risk för fysiska personers rättigheter och friheter för att säkerställa att alla nödvändiga bedömningar genomförs.

- att bolaget skulle lägga särskilt fokus på att sprida kunskap i sin organisation om vad personuppgiftsincidenter är och hur de ska hanteras om de inträffar.
- att bolaget skulle färdigställa en rutin för personuppgiftsincidenthantering som är anpassad för verksamhetens arbetssätt och övriga behov.
- att de anställda skulle få tydlig information om hur de ska hantera sin e-post i förhållande till dataskyddsförordningen och allmänna handlingar.

DSO konstaterar att flera av de rekommenderade åtgärderna har implementerats väl av bolaget. De åtgärder som fortfarande är aktuella, enligt den information som tillhandahållits DSO, är:

- att bolaget kontrollerar att samtliga genomförda informationsklassningar är aktuella, relevanta och vid behov reviderar klassningarna.
- att bolaget gör en inventering av samtliga pågående personuppgiftsbehandlingar som kan tänkas innebära hög risk för fysiska personers rättigheter och friheter för att säkerställa att alla nödvändiga bedömningar genomförs.
- att bolaget färdigställer en rutin för personuppgiftsincidenthantering som är anpassad för verksamhetens arbetssätt och övriga behov.
- att de anställda får tydlig information om hur de ska hantera sin e-post i förhållande till dataskyddsförordningen och allmänna handlingar.

DSO har fått information om att bolaget under tillsynsåret lagt särskilt fokus på att sprida kunskap i sin organisation om hantering av offentlighetsprincipen i relation till dataskyddsförordningen. Verksamheten har dock uppgett att det finns ett fortsatt behov av att öka kunskapen inom detta. Av den anledningen bedömer DSO att åtgärden fortsatt är aktuell.

	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 – Artificiell intelligens

Artificiell intelligens, AI, bygger på maskininlärning. Det är en teknik som innebär att AI:n själv skapar sitt regelsystem genom att tränas på en stor mängd data. De data som matas in i en AI blir en del av träningsdatan och kan potentiellt användas av AI:n. Om personuppgifter matas in i en AI kan det innebära risker för de registrerade.

Dataskyddsförordningen gäller för all behandling av personuppgifter, inklusive den som sker vid användning av AI. Precis som all behandling av personuppgifter behöver den personuppgiftsbehandling som sker i AI ha en rättslig grund. Behandlingen behöver även vara förenlig med de grundläggande principer som finns i dataskyddsförordningen, såsom att enbart samla in personuppgifter för specifika ändamål, att radera personuppgifterna när de inte längre behövs och att skydda uppgifterna från spridning eller från att obehöriga får tillgång till dem.

Som personuppgiftsansvarig har man således ett ansvar för att säkerställa att all behandling som sker i den egna organisationen eller på den personuppgiftsansvariges uppdrag vid användning av AI, uppfyller kraven som uppställs i dataskyddsförordningen.

DSO konstaterar att verksamheten är medveten om riskerna med användning av AI. Bolaget har tillgång till AI-system via staden och bolaget har på eget initiativ använt OpenAI. Det finns riktlinjer från Stadsledningskontoret som anger att användningen av AI ska ske på ett restriktivt sätt. Bolaget uppger dock att det finns behov av tydligare information om hur AI får användas. För att säkerställa att AI hanteras på ett sätt som är förenligt med dataskyddsförordningen, rekommenderar DSO att bolaget tar fram riktlinjer för hur AI får användas i verksamheten. Därefter behöver informationen spridas till de som berörs inom organisationen.

	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

Ett personuppgiftsbiträdesavtal (PUB-avtal) ska tecknas när en part har rollen som personuppgiftsansvarig och den andra parten har rollen som personuppgiftsbiträde. Kravet framgår av artikel 28.3 dataskyddsförordningen, där det anges att ett personuppgiftsbiträdes hantering av personuppgifter ska regleras i ett särskilt avtal.

En personuppgiftsansvarig är ett företag eller en organisation som fastställer för vilka ändamål personuppgifter behandlas och genom vilka medel. En personuppgiftsansvarig har det yttersta ansvaret för personuppgiftsbehandlingen och har som ansvar att se till att dataskyddsförordningen följs, att information lämnas till de personer vars personuppgifter behandlas och att personuppgiftsbiträdet uppfyller sina skyldigheter vid behandlingen av personuppgifter.

Ett personuppgiftsbiträde är ett företag eller en organisation som behandlar personuppgifter för den personuppgiftsansvariges räkning. Ett personuppgiftsbiträde har som ansvar att säkerställa att det används lämpliga tekniska och organisatoriska säkerhetsåtgärder vid personuppgiftsbehandlingen.

För att reglera relationen mellan den personuppgiftsansvarige och personuppgiftsbiträdet ska ett PUB-avtal ingås. PUB-avtalet avser främst att ge instruktioner om vilka personuppgifter som ska behandlas och hur behandlingen får ske.

DSO konstaterar att verksamhetens visar god kunskap för hur PUB-avtal ska hanteras. Verksamheten använder Stadens mall för PUB-avtal vid centrala upphandlingar som omfattar personuppgiftsbehandling av personuppgiftsbiträden. Ifall leverantörer uppdaterar sina tjänster finns det ett utpekat ansvar för vem som ska hantera detta. För frågor som rör PUB-avtal som ingåtts efter centrala upphandlingar får bolaget stöd av Stadsledningskontoret. Inga nödvändiga åtgärder har identifierats av DSO.

	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 att verksamheten säkerställer att samtliga rekommenderade åtgärder från tidigare årsrapport implementeras. DSO rekommenderar bolaget att ta fram riktlinjer för hur AI får användas i verksamheten, för att säkerställa att AI hanteras på ett sätt som är förenligt med dataskyddsförordningen.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- *DSO har inte identifierat eller blivit uppmärksammas 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 den del av en kommuns verksamhet där det typiskt sett hanteras stora mängder känsliga personuppgifter eller vars personuppgiftsrisker på annat sätt kan förväntas vara framträdande.

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

Stockholm 2025-02-28

Simon Jernelöv
Externt DSO

Ebba Holm
Jurist