Rapport

FAMILJEBOSTÄDER

Dataskyddsombudets årsrapport 2023

Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.
Dataskyddsåret har varit fullt av både upp och nergångar. Den 25:e maj firade GDPR 5 år sedan införandet och mycket har hänt och kommer hända. En snabb omvärldsbevakning pekar på att GDPR och det kommande NIS2-direktivet[1] kommer att ligga till grund för flera kommande förordningar inom EU. Bland annat kan det omnämnas att regleringar kommer ske inom områdena AI, IoT (Internet of Things) och DMA, Förordningen om Digitala Marknader[2] vilket alla påverkar bolagets dagliga arbete. År 2023 var också året då terrorhotsnivån i Sverige höjdes och flertalet uppmärksammade incidenter med attacker mot myndigheter och organisationer skedde. Det i sin tur har också lett till en ny syn på behov av säkerhetskontroller och krisorganisation.

Som Dataskyddsombud, DSO, för Familjebostäder har jag främst arbetat med frågan om ZoomX under år 2023. Kraven på digital kommunikation och lösningar för detta har varit stora sedan första dagarna av pandemin. Det befintliga verktyget Skype har börjat bli föråldrat och uppdateras inte av leverantören i den takt som behövts. Stockholm stad har nu implementerat en europeisk variant av Zoom kallad ZoomX och är baserad i Tyskland. Verktyget implementerades under hösten 2023. I spåren av detta har också flera andra tankar om verktyg för kommunikation också diskuterats inom organisationen då nya krav tillkommit. Bland annat behövs lösningar för socialtjänsten för säkra möten över starkare kryptering och identifiering.

Året har fortsatt inneburit behov och krav på säkra digitala meddelanden, en tjänst att kunna skicka e-post krypterat. Vid rapportens framtagande finns det nu ett pågående projekt på stadsledningskontoret för att genomföra en stadsgemensam konsekvensbedömning. En remiss för underlag är framtaget och nästa steg är work-shops med verksamhetsrepresentanter. Med arbetet har också behovet av en process som styr stadsgemensamma konsekvensbedömningar synliggjorts ytterligare i nätverket av DSO: er till SLK.

Ett förnyat inriktningsbeslut (KS 2023/241) kom hösten 2023 angående användande av tredjelandsöverföringar i Stockholm stad. Detta har öppnat upp för att bolaget kan fatta beslut i frågorna men med förbehållet att exit-plan behöver finnas på plats. Detta då överenskommelsen mellan USA och EU/EES bygger på en så kallad ”President order” och kan rivas upp av en ny amerikansk

[1] NIS2; Syftet med NIS2-direktivet är att harmonisera de olika medlemsländernas cybersäkerhetskrav och tillämpning av säkerhetsåtgärder samt stärka medlemsländernas samarbete för samhällsviktiga tjänster. NIS2-direktivet fastställer miniminivåer för regelverket och mekanismer för ett effektivt samarbete mellan tillsynsmyndigheterna i varje medlemsland.
[2] Förordningen om digitala marknader; Syftet är att hindra så kallade grindvakter från att bland annat ställa oskäliga villkor för företag och slutanvändare och att säkerställa öppenhet när det gäller viktiga digitala tjänster. EU-kommissionen utsåg i september 2023 för första gången sex grindvakter: Alphabet, Amazon, Apple, ByteDance, Meta och Microsoft. Detta gjorde de med stöd av olika kriterier i DMA som avgör om ett företag är en grindvakt. Efter att ha betecknats som grindvakter har företagen sex månader på sig att följa listan över vad de får göra och inte får göra enligt DMA, så att slutanvändare och företagsanvändare av grindvakternas tjänster får mer valmöjligheter och större frihet.

president efter valet 2024 eller vid en rättslig prövning. Detta ställer i sin tur höga krav på förvaltningen av informationstillgångar.

År 2024 kommer med stor sannolikhet fortsatt bli prioriteringar inom kontinuitetsplanering för att kunna hantera informationssäkerhet och dataskydd i krig och kris. Omvärlden har blivit kallare och vi ser en ökad påverkan efter så kallade hybridattacker där myndigheter och företags hemsidor stängs ner. Det är ett sätt att skapa otrygghet och instabilitet i samhället för antagonister. Samtidigt finns en stor problematik med efterfrågan av era hyresgäster på kamerabevakning efter flera våldsamma händelser där integritetsfrågan är högst aktuell. Allt detta påverkar oss dagligen och min förhoppning är att jag nästa gång kan ge en ljusare bild i min sammanfattande omvärldsbevakning och dataskyddsåret 2024.

Jessica Hillergård

Dataskyddsombud

Innehållsförteckning

Sammanfattning **2**

1 Inledning **5**

2 Obligatoriska rapporteringsområden **6**

2.1 Registerförteckning 7

2.2 Styrdokument 9

2.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar 11

2.4 Konsekvensbedömningar 14

2.5 Individens rättigheter 16

2.6 Personuppgiftsincidenter 18

3 Genomförda granskningar under året **20**

3.1 Sammanfattning 20

3.2 Syfte 20

3.3 Genomförda granskningar och deras resultat 20

3.4 DSO ger råd och rekommendationer till PUA 21

4 Risker inom dataskydd **22**

4.1 Sammanfattning 22

4.2 Syfte 22

4.3 Resultatet av riskkartläggningen 22

4.4 DSO ger råd och rekommendationer till PUA 24

5 Planerade granskningar under det nya verksamhetsåret **25**

5.1 Sammanfattning 25

5.2 Syfte 25

5.3 Planerade granskningar 25

6 Övrigt att rapportera **27**

6.1 Klagomål ..... **Fel! Bokmärket är inte definierat.**

6.2 Intern arbetsgrupp 27

1 Inledning

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 styrelse 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. Denna roll 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 styrelsen att ta emot de råd och rekommendationer som dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen. I rapporten får styrelsen insyn i vad dataskyddsombudets granskningar visat av verksamheten och status avseende integritet och dataskydd. Årsrapporten syftar till att styrelsen ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig styrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att styrelsen ska kunna *visa* att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna *dokumenteringsskyldighe*t. Årsrapporten är även ett medel för styrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

2 Obligatoriska rapporteringsområden

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

De obligatoriska rapporteringsområdena är:

- registerförteckning
- styrdokument
- tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar
- konsekvensbedömningar
- individens rättigheter
- personuppgiftsincidenter

Nedan redogörs för styrelsens status och dataskyddsombudets slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter genomförd uppföljning och granskning.

2.1 REGISTERFÖRTECKNING

2.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	148
Har nödvändiga uppdateringar gjorts?	Nej
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Nej

2.1.2 Syfte

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför i klartext av dataskyddsförordningen (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i en så kallad registerförteckning (även kallat behandlingsregister eller register av register).

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 samt säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling. Det är därför viktigt att PUA får information om hur komplett verksamhetens förteckning är. Om dokumenteringskravet uppfylls kan verksamheten arbeta effektivt, systematiskt och riskbaserat och samtidigt värna om 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 PUA 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 PUA behöver förstå och ta ställning till inför det planerade åtgärdsarbetet under nästa verksamhetsår.

2.1.3 Resultat

Registerförteckningen i finns i ett digitalt verktyg kallat DraftIt och består av ett frågeformulär per personuppgiftsbehandling vilket i sin tur blir funktionen av en checklista att alla krav i GDPR dokumenteras korrekt. Under 2023 har en översikt av registerförteckningen gjorts och anpassats mot den hanteringsanvisning med processer som Stadsarkivet har tagit fram. Ett 40-tal behandlingar har rensats bort då de varit inaktuella eller dubbletter.

Totalt har 148 behandlingar registrerats i DraftIt.

Arbetet saknar fortfarande en rutin och utpekade ansvariga personer för uppdateringar. Detta sker ad hoc idag och är individberoende.

2.1.4 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

2.1.5 DSO ger råd och rekommendationer till PUA

Det saknas en skriven och kommunicerad rutin för arbetet med registerförteckningen. Åtgärden behövs för att det ska bli ett systematiskt arbete med registerförteckningen och inte personberoende.

Det saknas ansvarig person för varje registrering, d.v.s. en anställd som de facto utför den i verksamheten. Det behövs en sådan rutin och att personer utses och dokumenteras hos organisationen. Detta för att vid en incident rätt bedömningars ska kunna göras snabbt och en tydlig kontaktyta som förstår omfattningen och påverkan. Den ansvarige för processen/arbetsuppgiften arbetar med personuppgiftsbehandlingen i sina ordinarie arbetsuppgifter och står i kontakt med dataskyddssamordnaren som hanterar registerförteckningen vid sin del i organisationen.

2.2 STYRDOKUMENT

2.2.1 Sammanfattning

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

2.2.2 Syfte

Området syftar till att PUA genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar PUA 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 de 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.

En brist inom detta område bör förstås ses som en brist i förhållande till direkta lagkrav, men det finns fler nyanser av detta som bör lyftas fram till PUA. Bristande styrning på grund av att lämplig styrande dokumentation saknas leder exempelvis ofta till bristande kvalitet i hur verksamheten utför aktiviteterna, men även till att verksamheten slösar värdefulla resurser när exempelvis för många personer blir involverade i en incidenthantering eller för att en analys behöver

göras om från grunden varje gång istället för att man återanvänder redan uppfunnen kunskap. Dessa effekter drabbar
verksamheter ur ett vidare perspektiv och är något som ligger i PUA:s intresse att förstå för att fatta rätt beslut om.

2.2.3 Resultat

Familjebostäder har egen handledning för hur personuppgiftsincidenter ska hanteras samt en förklaring om vad GDPR/ Dataskyddsförordningen innebär. Dessa finns publicerade på Familjebostäders intranät, Porten. Innehållet på intranätet är gediget och länkar även vidare till tillsynsmyndighet och viktiga vägledningar.

När tillämpningsanvisningen för informationssäkerhet finns på plats och implementerats kommer också det bli tydligare vilken roll som har ansvaret att uppdateringar av dokument sker och nya rutiner tas fram.

2.2.4 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

2.2.5 DSO ger råd och rekommendationer till PUA

Organisationen har en god grund att stå på. Den nya stadsövergripande informationssäkerhetsriktlinjen och dess tillämpningsanvisningar behöver implementeras och kommuniceras under 2024.

2.3 TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER FÖR PERSONUPPGIFTSBEHANDLINGAR

2.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	60 st.
Är klassade personuppgiftsbehandlingar aktuella?	Nej

2.3.2 Syfte

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

Ansvaret 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 klassning, minskar sannolikheten avsevärt att en klassning faktisk initieras.

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

Viktigt är också att notera att dataskyddsombudet omhändertar den registrerades intresse och informationssäkerhetssamordnaren har fokus på verksamhetens krav på informationen i form av tillgänglighet, riktighet och konfidentialitet. Verktyget för DSO är i första hand registerförteckningen och dokumentationen där. Informationssäkerhetssamordnaren har KLASSA som verktyg för att se till att verksamhetens krav efterlevs i form av dokumentation i förvaltningsplaner, systembeskrivningar etc.

Eftersom informationsklassning är ett arbete som görs inom ramen för informationssäkerhetsarbetet, bör DSO samråda och planera uppföljningen tillsammans med informationssäkerhetssamordnare. Enligt stadens metodik klassas personuppgifter och övrig information i samma workshop, och slutsatserna kring klassningen dokumenteras i samma protokoll.

2.3.3 Resultat

Under år 2023 har fortsatt arbete skett med förklassningsprotokoll och då i tre steg vilka är: A-klassning i designfasen, B-klassning vid införandet och C-klassning vid årlig uppföljning. Protokollet från dessa ska signeras av informationsägaren, i dagsläget direktören, och har konkretiserat skyddsvärdet för informationen och då även personuppgifterna som kan ingå i dessa. Dataskyddsombudet har blivit inbjuden till sådana vid flertalet tillfällen och metoden börjar sätta sig i organisationen parallellt med implementeringen av förvaltningsmodellen PM3. Arbetet har tagit ett stort kliv fram och en prioriteringsordning har följts.

Värt att notera är att det inte är informationstillgången som klassats tidigare utan systemet/informationsbäraren. Under slutet av 2023 påbörjades metodiken att klassa informationstillgångar vilket ger en mer rättvis bild.

Samtliga personuppgiftsbehandlingar klassas utifrån vilken typ av personuppgifter som behandlas och lämpligt skydd vidtas för respektive behandling. Detta kan vara behörighetsbegränsning, skydd av lösenord på dokument osv. Detta dokumenteras i DraftIT. En klassificeringsstruktur med märkning av dokument finns inte

2.3.4 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

2.3.5 DSO ger råd och rekommendationer till PUA

Tidigare år har klassningar skett ad hoc och varit drivna av enskilda individer. Med PM³ eller liknande som förvaltningsmodell kan detta problem reducerats då ansvariga inom organisationen utses.

Rekommendationen från DSO är att fortsätta se till nästa steg i införandet förvaltningsmodellen av informationssäkerhet och klassificera de processer som ingår i hanteringsanvisningen. Identifierar man processer och inte ser endast till system, blir klassningen av information/ personuppgifterna än mer konkret och verklig.

2.4 KONSEKVENSBEDÖMNINGAR

2.4.1 Sammanfattning

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

2.4.2 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 ett uttryckligt krav enligt dataskyddsförordningen och ska utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1).

2.4.3 Resultat

Organisationen arbetar med konsekvensbedömningar. Rutiner finns på plats på intranätet, Porten. Aktiviteten sker dock individberoende, d.v.s. individer har kunskapen men inte bredden vilket kan försvåra processen med att använda verktyget. Med införande av PM[3] blir ansvaret tydligare för vem som ska tillse att resurs avsätts för att uppgiften konsekvensbedömning sker.

Under året har en stor konsekvensbedömning skett gemensamt i staden för ZoomX. Det har synliggjorts under året hur viktigt det är med gemensam konsekvensbedömningsprocess och behovet av att ha utsedd ledare för det. Det uppstår ofta tidspress i det här arbetet då konsekvensbedömningar görs väldigt sent i framtagande av tjänster. Värt att notera är att bolaget självt löser ut sina

egna aktiviteter inom konsekvensbedömningar utan drabbas negativt vid det gemensamma arbetet.

2.4.4 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

2.4.5 DSO ger råd och rekommendationer till PUA

Konsekvensbedömningen som verktyg skapar bättre kravställningar redan i designstadiet och förenklar/förtydligar i avtal och kommunikation med leverantörer. I förvaltningsmodellen PM3 är det ett ansvarsområde som tilldelas en specifik roll. Vid implementering av modellen kommer det att förflytta individberoendet vilket det är idag, till ett mer systematiskt använt verktyg. Nämnden behöver också fortsatt arbeta för att process för gemensamma konsekvensbedömningar i staden implementeras, därav den gula bedömningen.

2.5 INDIVIDENS RÄTTIGHETER

2.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	Kan ej anges då endast nekande registreras enligt Stadsarkivariens gallringsregler.
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Kan ej anges då endast nekande registreras enligt Stadsarkivariens gallringsregler.

2.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt ska garantera 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 verksamhet som enligt förordningen är att se som personuppgiftsansvarig – dvs. i stadens fall nämnder och bolag – tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, som 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 verksamheter 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 dock att det finns undantagssituationer angivna i artikel 12.3, där fristen kan förlängas till mer än en månad.)

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

Om verksamheten inte klarar av att hantera en begäran från en registrerad person i enlighet med dataskyddsförordningen krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från Integritetsskyddsmyndighetens, IMY:s sida, med sanktioner som följd. Det är därför viktigt att PUA regelbundet ges en bild av i vilken mån verksamheten klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

2.5.3 Resultat

På Familjebostäder.com finns information om personuppgiftsbehandling och inhämtning av personuppgifter. Det finns även ett formulär för begäran om registerutdrag. Kundservice tar emot begäran om rättning vid namnbyte etc. Organisationen har också en portal för hyresgäster där man själv kan administrera sina uppgifter.

Information till medarbetarna om hur deras personuppgifter sparas och används saknas.

2.5.4 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

2.5.5 DSO ger råd och rekommendationer till PUA

Informationen till de anställda behöver uppdateras med om hur länge personuppgifter sparas, vilka och vem som får ta del av dem.

2.6 PERSONUPPGIFTSINCIDENTER

2.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	En utomstående eller medarbetare upptäcker incidenten.
Hur många personuppgiftsincidenter har dokumenterats?	8
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

2.6.2 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 sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering.

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, inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter ska de berörda registrerade personerna, utan dröjsmål underrättas.

Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering till de berörda personerna.

Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY. DSO:ns årsrapportering är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad osv.

2.6.3 Resultat

Under år 2023 har åtta personuppgiftsincidenter uppmärksammats i organisationen. Det är fyra fler än året innan. Det har blivit en något ökad kunskap i organisationen efter att utbildningsinsatser skett av dataskyddsombudet och informationssäkerhetssamordnaren. Efter en utbildning ses direkt att uppmärksamheten blir bättre att upptäcka incidenter och frågorna ökar.

Det gångna året har också översyn av verktyget som personuppgiftsincidenter rapporteras i. Brister i det verktyg som staden använder, IA, har lett till att det nu finns ett förslag att använda IT:s rapporteringsverktyg TopDesk. Att använda det skulle bli bättre för uppföljning och spårbarhet.

2.6.4 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

2.6.5 DSO ger råd och rekommendationer till PUA

Kunskap om vad och hur man hanterar personuppgiftsincidenter är en färskvara. Det finns en tydlig korrelation mellan att personalen haft utbildning i Dataskyddsförordningen och en ökad benägenhet att anmäla personuppgiftsincidenter.

Styrelsen rekommenderas att ta fram en organisation att omhänderta lessons learned. Det är en naturlig del av det förbättringsarbete som en mer mogen verksamhet kan ta nästa steg emot.

DSO rekommenderar också att verktyget TopDesk implementeras för att få bättre uppföljning i incidenthanteringsarbetet.

3 Genomförda granskningar under året

3.1 SAMMANFATTNING

Genomförda granskningar:

- *Problem vid tredjelandsöverföringar*
- *Implementationen av nya informationssäkerhetsriktlinjen och dess tillämpningsanvisningar*

3.2 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 personuppgiftsansvarig är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är.

3.3 GENOMFÖRDA GRANSKNINGAR OCH DERAS RESULTAT

3.3.1 Problem vid tredjelandsöverföringar

Då verksamheten har stort behov av att använda molntjänster behövde detta område granskas extra under det gånga året. Under hösten 2023 kom dock ett nytt inriktningsbeslut av SLK som öppnar upp för möjligheten för tredjelandsöverföringar. Dock med vissa förbehåll. (Se vidare i kapitel 4 Risker inom dataskydd.)

Med tredjelandsöverföringar och det nya inriktningsbeslutet följer flera insatskrävande åtgärder vilket ställer höga krav på verksamheten. Idag är denna kunskap delvis spridd i organisationen och är individberoende. Tydligare rutiner och ansvar saknas i och med förvaltningsmodellen inte är införd fullt ut.

	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

3.3.2 Implementationen av nya informationssäkerhetsriktlinjen och dess tillämpningsanvisningar

Arbetet med att ta fram tillämpningsanvisning för informationssäkerhet har skett under 2023. Den är framtagen men inte implementerad och kommunicerad. Detta ska ske 2024.

En anpassad förvaltningsmodell för informationshantering har tagits fram men är inte fullt ut anpassad till alla informationstillgångar. Roller och ansvarsområden är inte tillsatta.

	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

3.4 DSO GER RÅD OCH REKOMMENDATIONER TILL PUA

3.4.1 Problem vid tredjelandsöverföringar

Dataskyddsombudet rekommenderar att organisationen inför den förvaltningsmodell som finns beskriven i tillämpningsanvisningen med ansvarområden och roller. Därefter bör beröra rollinnehavare utbildas inom området och rutiner tas fram för att underlätta arbetet med tredjelandsöverföringar. PUA behöver också bestämma vilken riskaptit man har för att kunna ta höjd för vilka risker man är villig att ta vid ett aktuellt underkännande av nuvarande överföringsmekanism och tredjelandsöverföringar förbjuds.

3.4.2 Implementationen av nya informationssäkerhetsriktlinjen och dess tillämpningsanvisningar

Dataskyddsombudets råd är att fortsätta arbetet med att implementera förvaltningsmodell för informationshantering och göra arbetet med informationstillgångar/ personuppgifter mindre individberoende. På det sättet kommer mognadsgraden öka i organisationens informationssäkerhets- och dataskyddsarbete.

4 Risker inom dataskydd

4.1 SAMMANFATTNING

Relevanta risker inom verksamheten:

- Brist på kunskap om dataskyddsförordningen
- Tredjelandsöverföringar
- Osäker e-posthantering med personuppgifter

4.2 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. Dataskyddsombudet behöver som underlag för sin egen planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, i 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.

4.3 RESULTATET AV RISKKARTLÄGGNINGEN

4.3.1 Risk 1 Brist på kunskap om dataskyddsförordningen (Kvarstår)

En konsekvensbedömning avseende dataskydd enligt artikel 35 i GDPR ska alltid göras om en planerad personuppgiftsbehandling kan medföra en hög risk för de registrerade individerna. Att det sker förutsätter att det finns en allmän förståelse i organisationen för att stödfunktioner likt informationssäkerhetssamordnare och dataskyddsombud kan behöva bli inblandade i en mängd olika sammanhang i verksamheten när personuppgifter förekommer, och
i synnerhet innan personuppgifter börjar behandlas i stor skala eller med hjälp av ny teknik.

I dagsläget har flera medarbetare goda kunskaper och arbetar noggrant med dataskyddsfrågorna. Dock sker det inte i hela organisationen. Risken är också att brist på förståelse skapar frustration och man ser det som ett hinder och inte en möjlighet att lagstiftningen finns.

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

4.3.2 Risk 2 Tredjelandsöverföringar

Det nya inriktningsbeslutet från stadsledningskontoret som kom under hösten 2023 innebar en öppning för bolaget att använda leverantörer som använder sig av tredjelandsöverföringar. Förutsättningen är att verksamheten har en väl utformad exit-plan om överföringsmekanismen ”Data Privacy Framwork” ogiltigförklaras likt ”Privacy Shield” gjorde år 2020 och ”Safe Harbour” innan dess.

Flertalet leverantörer erbjuder idag endast molntjänster och de stora leverantörerna av sådana är amerikanskägda. Därav är detta en risk som behöver uppmärksammas extra.

	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

4.3.3 Risk 3 Osäker e-posthantering med personuppgifter

Varje personuppgift som ska hanteras måste behandlas säkert. När en personuppgift e-postas med någon av stadens leveranser sker själva överföringen krypterat, men är okrypterad i in- och utboxen. Det är också inte säkert att maila externt då exempelvis en medborgares adress inte kan kontrolleras på ett tillräckligt bra sätt.

Stadsledningskontoret har tagit fram en tjänst kallad ”Säkra meddelanden” eller ”TDialog”. Kvarstående aktivitet för verksamheten, är att se över och bedöma vad tjänsten kan användas till.

Jag som DSO kan inte rekommendera i dagsläget att tjänsten används efter att jag tagit del av analysmaterialet. Samtidigt är behovet kvarstående från verksamheten att möjligheten att e-posta personuppgifter säkert och krypterat.

Vid denna rapports framtagande är ett projekt med att en gemensam konsekvensbedömning med systembeskrivning, informationsklassning och riskanalys ska ske 2024 av SLK. Detta för att kunna besvara de risker som framkommit inom de verksamheter som gjort ena konsekvensbedömningar och riskanalyser. Rekommendationen att inte använda tjänsten utan att analysmaterialet finns på plats kvarstår, då riskerna inte har besvarats av

systemförvaltaren och informationsmängderna som ska skickas i det är så pass känsligt och skyddsvärt.

X	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
	Inga brister av nämnvärd betydelse identifierade

4.4 DSO GER RÅD OCH REKOMMENDATIONER TILL PUA

Alla medarbetare inom Stockholm stad ska årligen genomgå utbildningsplattformens utbildningar:

- Grundkurs i dataskydd
- Informationssäkerhet grundkurs

Rekommendationen från DSO är att en tidsperiod avsätts varje år för att samtliga medarbetare går utbildningarna och tydlig kommunikation sker på Porten med påminnelser.
För chefer finns också utbildningen:

- Informationssäkerhet för chefer.

Risken att tredjelandsöverföringsproblematiken kommer att uppstå igen är sannolikt rätt stor. Nätaktivistorganisationen NOYB, Non Of Your Business, har sagt att man kommer göra en rättslig prövning och då trolige redan årsskiftet 2023-2024. Samtidigt bygger överföringsmekanismen på en presidentorder vilken kan rivas upp av nästa president efter valet 2024. Nämnden rekommenderas att ta höjd för risken och bestämma aptiten för vad man är villig att riskera när man ingår nya avtal med leverantörer där överföringar till tredjeland sker. Rådet är också att ha en tydlig exitplan och genomlysa marknaden i förstahand inom Sverige och EU/EES.

Dataskyddsombudets rekommendation för att minimera risken att personuppgifter e-postas utan tillräckligt skydd, är att delta i det gemensamma arbetet med konsekvensbedömning och riskanalys och därefter implementera verktyget.

5 Planerade granskningar under det nya verksamhetsåret

5.1 SAMMANFATTNING

Relevanta granskningsområden inom verksamheten:

- Kontinuitetshantering
- Implementationen av nya informationssäkerhetsriktlinjen och dess tillämpningsanvisningar

5.2 SYFTE

Som nämnts tidigare är det granskande arbetet en av dataskyddsombudets viktigaste uppgifter. Eftersom dataskyddsombudet ofta har begränsat med tid, behöver granskningsplanen för det nya året utformas med eftertanke. Som en tumregel bör två-tre granskningar ses som en rimlig granskningsinsats under ett verksamhetsår. Granskningsområdena bör lämpligen väljas utifrån ett riskbaserat synsätt, det vill säga att fokus bör ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därigenom åstadkoms en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

5.3 PLANERADE GRANSKNINGAR

5.3.1 Granskning 1 Kontinuitetshantering

I händelse av avbrott i tjänster ska en kontinuitetsplan finnas för att tjänsterna ska kunna återupptas så snart som möjligt, om än eventuellt i begränsad funktion. Den ska innehålla en enkel plan och checklistor med:

- Reservrutin – Hur arbetar vi på alternativa sätt under en störning? Inklusive roller och ansvar.
- Återställningsrutin – Hur återställer vi den kritiska aktiviteten eller resursen efter en störning? Inklusive roller och ansvar.
- Återgångsrutin – Hur återgår vi till ordinarie arbetssätt när den kritiska aktiviteten eller resursen fungerar igen? Inklusive roller och ansvar.
- Nödvändiga kontaktuppgifter – Vilka kontaktuppgifter behövs för att kunna utföra uppgifterna? Vilka behöver informeras om läget, internt och externt?

Ändamålet att granska kontinuitetsplanerna är att ombesörja att dataskyddets krav på säkerhetsåtgärder och de registrerades intressen omhändertas även i kriser.

5.3.2 Granskning 2 Implementationen av nya informationssäkerhetsriktlinjen och dess tillämpningsanvisningar

Den nya tillämpningsanvisningen ska omhänderta även dataskyddsförordningen och praktiskt arbete där lagstiftningen är aktuell. Under 2023 kommer DSO att granska text och att implementationen, dvs förståelse och kommunikationen av den samt att den sprids ut i hela organisationen.

6 Övrigt att rapportera

6.1 INTERN ARBETSGRUPP

Under år 2024 behöver den arbetsgrupp som jobbade internt med dataskyddsfrågor under 2021, startas upp igen. Representanter i denna behöver vara utsedda utifrån förvaltningen av informationsmängderna. Syftet med en sådan grupp är att verksamheten kommer närmare Dataskyddsombudet och informationssäkerhetssamordnaren och ett utbyte av kunskap och behov flödar lättare. Arbetssättet har visat sig vara lyckat i andra verksamheter.