Rapport

FB 2023/62

2023-01-06

Dataskyddsombudets årsrapport 2022

Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

I maj 2022 tillträdde jag som ert nya dataskyddsombud, DSO. Vid uppstarten genomfördes en analys av hur arbetet och efterlevnaden av dataskyddsförordningen är inom organisationen. Resultatet var en del mindre brister och behov av uppdateringar vilket har till viss del kunnat åtgärdas under 2022.

De områden som kvarstår är:

- Tillämpningsanvisningar för informationssäkerhet (inkluderar dataskydd)
- Utbilda och kommunicera tillämpningsanvisningarna
- Återuppta dataskyddshandläggarnas arbete i organisationen för att systematisera arbetet med registerförteckningen och informationsklassningar.

Bakgrunden till kvarstående översta två punkter är att Stockholm stads informationssäkerhetsriktlinje antogs av kommunfullmäktige vintern 2022. Därefter togs det fram mall för tillämpningsanvisningar som förvaltningar och bolag ska anpassa till sin egen verksamhet under våren och sedan blev de tillgängliga för verksamheterna under försommaren.

Granskning har genomförts av dokumentationen av kamerabevakning och arbetsmetodiken vid tecknande av personuppgiftsbiträdesavtal.

En av de risker som tydligt framkommit under hösten 2022 är behovet av molntjänster och problematiken kring tredjelandsöverföringar med Azure och liknande tjänster. Ett område som jag som dataskyddsombud får många frågor om och som behöver utredas för att organisationens vilja till både efterleva lagen och följa med i den digitala utvecklingen i samhället ska takta med alla involverade parter såsom den registrerade, medarbetaren som utför arbetsuppgiften, entreprenörer osv.

Jessica Hillergård

Dataskyddsombud

Innehåll

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?	183
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. SLK har beslutat under år 2019 att de tidigare Excel-listor med registerförteckningar som skapades 2018, ska digitaliseras i verktyget DraftIt.

Totalt har 183 behandlingar registrerats i DraftIt.

Arbetet med registerförteckningen saknar en skriven rutin, idag sker detta ad hoc och är beroende av kunskap hos den enskilde anställde.

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.

Nästa steg för att nå systematiskt arbete med registerförteckningen är att respektive dataskyddssamordnare behöver utbildas i verktyget DraftIt, då dessa ska kunna uppdatera registerförteckningen vid behov i samarbete med de ansvariga personerna för respektive personuppgiftsbehandling. Det underlättar vid de årliga genomgångarna av personuppgiftsbehandlingarna och det systematiska arbetet.

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

**Dokument som finns inom Familjebostäder är inte anpassade och uppdaterade mot Stockholm Stads informationsriktlinje och tillämpningsanvisningar från 2022. Detta har identifierats som en brist men är under framtagning under Q1 2023.*

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. Den brist som framkommer är tillämpningsanvisningen från 2022 inte är implementerade. Detta förstår jag som DSO beror på att mallarna togs fram under 2022 av stadsledningskontoret och dessa ska nu bearbetas, uppdateras och kommuniceras i organisationen under 2023.

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 2023.

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

Det finns 60 informationsklassningar registrerat i verktyget KLASSA. Dock ska man beakta att 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.

Under 2022 kom en ny version av KLASSA då ISO-standarden uppdaterades under samma år. Detta innebar att det också förändras i antal frågor och utformning av standardens krav i KLASSA.

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

DSO rekommenderar att rutin uppdateras så att dataskyddssamordnare klassar sina respektive personuppgiftsbehandlingar tillsammans med informationssäkerhetssamordnare och övriga aktuella medarbetare med informationssäkerhetsansvar enligt Familjebostäders förvaltningsmodell.

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?	Nej
Är de genomförda bedömningarna aktuella?	Nej

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 men i liten omfattning. Rutin finns publicerad med mall på Porten. Bristen är dock att den inte kommunicerats i verksamheten. Under 2022 identifierades behov att se över konsekvensbedömningen som stöd vid upphandling för att få fram rätt kravmassa parallellt med informationssäkerhetsverktyget KLASSA.

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

Dataskyddsombudets råd är att sprida kunskapen om konsekvensbedömningen som verktyg till upphandling och de roller som har informationsägarskap.

Ökar förståelsen för konsekvensbedömningen som verktyg skapar det bättre kravställningar redan i designstadiet och förenklar/förtydligar i avtal och kommunikation med leverantörer.

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 Intetgritetsskyddsmyndighetens, 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 personal upptäcker incidenten.
Hur många personuppgiftsincidenter har dokumenterats?	3
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

Tre personuppgiftsincidenter har upptäckts inom organisationen fr.o.m. 220501 t.o.m. 221231.

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.

Under 2023 behöver instruktionen som förklarar hur man agerar vid en personuppgiftsincident kommuniceras igen för att upprätthålla kunskapen. I dag finns troligen ett mörkertal som inte anmäls.

3 Genomförda granskningar under året

3.1 SAMMANFATTNING

Genomförda granskningar:

- *Kamerabevakning*
- *Arbetsmetodik för tecknande av personuppgiftsbiträdesavtal*

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 Kamerabevakning

Våren 2022 kontaktades Dataskyddsombudet av säkerhetsansvarig för att se över kamerabevakningen och att den var lagenlig med GDPR. Tillsammans med Familjebostäders informationssäkerhetssamordnare granskades dokumentation och rutiner. Efter granskningen uppdaterades dokumentationen något. Nya informationsskyltar har också tagits fram med tydligare kontaktuppgifter.

	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

3.3.2 Arbetsmetodik för tecknande av personuppgiftsbiträdesavtal

Under våren 2022 tog Stadsledningskontoret fram en ny mall för personuppgiftsbiträdesavtal. Den har sedan anpassats till Familjebostäders egen layout. Under de första månaderna efter tillträdet som DSO, uppmärksammades också att det framkom ofta frågor just om biträdesavtalet och hur det ska tecknas och när. Resultatet blev en utbildning med de medarbetare som arbetar med

upphandling under hösten 2022. Detta för att skapa en förståelse för när i processen kravmassan för att uppfylla dataskyddslagstiftningen ska tas fram. Vidare kommer samma utbildning hållas under 2023 för bland annat personal inom IT.

	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 DSO GER RÅD OCH REKOMMENDATIONER TILL PUA

3.4.1 Kamerabevakning

För området kamerabevakning finns idag tydliga instruktioner och informationstexter. Att ha en årlig översyn av detta är en bra systematisk åtgärd och som jag som dataskyddsombud uppskattade att bli involverad i på ett tidigt stadium.

3.4.2 Arbetsmetodik för tecknande av personuppgiftsbiträdesavtal

Metodik för framtagning och tecknande av personuppgiftsbiträdesavtal behöver skrivas in i tillämpningsanvisningens kapitel för rollbeskrivning. Detta för att synlig- och tydliggöra ansvarsfördelningen. Vidare behöver också ansvariga få ta del av utbildningen om personuppgiftsbiträdesavtal.

4 Risker inom dataskydd

4.1 SAMMANFATTNING

Relevanta risker inom verksamheten:

- *Brist på kunskap om dataskyddsförordningen*
- *Problematik kring Azure*

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

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 Problematik kring Azure

Enligt stadens beslut finns en stor problematik att använda molntjänster då risk för tredjelandsöverföringar kan ske. Gränsdragningen för personuppgift är också om det endast gäller en inloggningsuppgift likt en e-postadress via en molntjänst.

I flertalet av de projekt som Familjebostäder ska delta i med entreprenörer, krävs inloggningar till olika tjänster. Ett av de verktyg som behöver användas är Byggvarubedömningen[1] vilket kräver en inloggning via Azure, Microsofts molntjänst och den personuppgift som behöver delas är endast e-post och IP-adress.

Under hösten 2022 har också flertalet möjligheter undersökts för att införskaffa ett nytt HR-verktyg. Bland annat flaggar också nuvarande leverantör av löneadministrationsverktyget, att de kommer bli molnbaserade inom snar framtid. Vid en större granskning av marknaden för HR-verktyg framkommer det att de flesta verktygen har lagringsplats i Sverige eller Norden, men kräver inloggning via Azure eller Amazons motsvarighet.

De exempel som anges ovan skapar risker som kan påverka organisationen ur olika aspekter. En risk kan vara att projekten blir kostsammare då entreprenörer måste lägga mer tid på administrationslösningar. En annan är att den enskilde medarbetaren måste skapa egna genvägar för att kunna lösa sina arbetsuppgifter, vilket i sin tur bygger in risker när organisationen tappar kontrollen och spårbarheten.

	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

[1] Byggvarubedömningens syfte: *”Vi bedömer byggrelaterade produkter utifrån dess kemiska innehåll, miljöpåverkan under livscykeln och i förlängningen även social påverkan i leverantörsledet. Detta gör vi för att främja produktutvecklingen mot en giftfri och god bebyggd miljö samt ansvarsfulla leverantörsled.”* https://byggvarubedomningen.se/ (230105)

4.4 DSO GER RÅD OCH REKOMMENDATIONER TILL PUA

4.4.1 Risk 1- Brist på kunskap om dataskyddsförordningen

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.

Inom Familjebostäder har i dagsläget ingen chef genomgått utbildningen.

4.4.2 Risk 2- Problematik kring Azure

Den identifierade risken med att inte få använda Azure och för egna lösningar/ work-arounds har framstått som att vara stor. Rekommendationen från DSO är att göra en fördjupad analys om riskerna och se vilken typ av information som kan användas för molntjänster och vilka gränser som finns.

Personuppgiftsansvarig behöver också sätta tydlig vilja för vilken riskaptit man har i frågan.

Ett förhandssamråd med IMY, Integritetsskyddsmyndigheten, är ett verktyg att ta till för att avgöra om överföringen är legal via Azure/liknande men till andra lagringsplatser ex. i norden.

5 Planerade granskningar under det nya verksamhetsåret

5.1 SAMMANFATTNING

Relevanta granskningsområden inom verksamheten:

- Problem uppkomna vid tredjelandsöverföringar
- 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 Problem uppkomna vid tredjelandsöverföringar

Då verksamheten har stort behov av att använda molntjänster behöver detta område granskas extra under det kommande året. Detta kommer ske genom samarbetsgrupper mellan olika bolag inom Stockholm stad samt internt inom organisationen.

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 SAMMANFATTNING

Familjebostäders informationssäkerhetssamordnare, DSO och f.d. DSO har sett över organisationen för dataskyddsarbetet. Nytt förslag har framtagits för att starta om den interna gruppen med dataskyddssamordnare. Detta då bland annat Stadsrevisionens rapport 2021 påvisade en rekommendation att:

- *Säkerställa utveckling av styrning och uppföljning av arbetet med att efterleva dataskyddsförordningen, så som dataskyddsombudets oberoende samt arbetet med personuppgiftsbiträdesavtal och konsekvensbedömningar.*

För att minska detta operativa beroende har ett externt dataskyddsombud engagerats i form av en konsult. Det operativa arbetet ska flyttas till verksamheten på sikt och dataskyddsorganisationen utvecklas under 2023.

6.2 ÖVRIGT

Vid uppdragets start 2022 inleddes detta med en så kallad GAP-analys för att se hur efterlevnaden var inom organisationen. Detta med hjälp av verktyget DraftIT Evaluation.

Resultatet var 63p jämfört med benchmark 51p[2]. De områden som det kvarstår åtgärder är desamma som DSO identifierat i årsrapporten.

[2] *Definition och syfte med benchmarking handlar om att förbättra en organisations verksamhet genom att jämföra sig med andra liknade organisationer. Med hjälp av benchmarking går det tydligt att visa och få information om hur ex. ett företag presterar mot sina konkurrenter.*