Stockholms stad

Bilaga 11

DSO GDPR
Årsrapport

År 2024

SISAB Skolfastigheter i Stockholm AB

GDPR årsrapport
Januari 2025

Dnr: SISAB 2025/38
Utgivningsdatum: 2025-01-10
Kontaktperson: Annette Bengtsson

1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen är att skapa enhetliga dataskydds-regler 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 SISAB:s bolagsstyrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av person-uppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett dataskyddsombud (DSO). DSO 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 SISAB:s bolagsstyrelse att ta emot de råd och rekommendationer som DSO är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:s granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att bolagsstyrelsen ska kunna fatta beslut om prioriteringar, resurser och aktiviteter framåt. Detta samspel resulterar vidare i att det blir enklare för ansvarig styrelse att visa hur de som personuppgifts-ansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är *ansvarsskyldigheten*. Den innebär att bolags-styrelsen ska kunna *visa* att verksamheten efterlever dataskydds-förordningen. Årsrapporten är en mycket viktig del av denna dokumenteringsskyldighet. Årsrapporten är även ett medel för bolagsstyrelsens uppföljning och styrning av verksamhetens syste-matiska integritets- och dataskyddsarbete.

I egenskap av ert dataskyddsombud lämnar jag härmed följande årsrapport.

Innehåll

1 Bakgrund ... 3

2 Omvärldsbevakning ... 5

3 Obligatoriska rapporteringsområden ... 6

3.1 Register över behandling, registerförteckning ... 7

3.2 Styrdokument ... 8

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar ... 10

3.4 Konsekvensbedömning dataskydd ... 11

3.5 Individens rättigheter ... 13

3.6 Personuppgiftsincidenter ... 14

4 Genomförda granskningar under året ... 16

4.1 DSO ger råd och rekommendationer till PUA ... 16

5 Risker inom dataskydd ... 16

5.1 DSO ger råd och rekommendationer till PUA ... 17

6 Planerade granskningar under det nya verksamhetsåret ... 18

7 Övrigt att rapportera ... 18

2 Omvärldsbevakning

Nedan följer en kort beskrivning av omvärldsbevakningen på integritetsskyddsområdet.

Dataskyddsförordningen har förändrat svensk praxis avseende klagomålshantering avseende dataskydd och utökat tillsynsmyndigheten Integritetsskyddsmyndighetens, nedan IMY, skyldighet att utreda inkomna individuella klagomål.[1]

Detta har fått till följd att IMY under 2024 har utrett fler klagomål från de registrerade [2]och inlett fler tillsynsärenden utifrån enskilda inkomna klagomål än under tidigare år.

I avgöranden har Högsta förvaltningsdomstolen fastställt att Integritetsskyddsmyndighetens beslut att inte utreda ett klagomål vidare respektive att avsluta ett tillsynsärende utan åtgärd är överklagbara. Detta innebär att den registrerade har rätt att överklaga IMY:s beslut till förvaltningsdomstol och att de blir part i ett tillsynsärende[3]. De registrerade har således fått en bättre möjlighet att få sina rättigheter enligt dataskyddsförordningen tillgodosedda.

Ett omfattande klagomålsinitierat tillsynsärende i domstol under 2024 avser rätten till tillgång till personuppgifter och rätten att erhålla klar och tydlig information samt all information som specificeras i dataskyddsförordningen.[4]

Företag får inte längre under utgivningsbevis tillhandahålla sökmöjligheter på individnivå för att få ta del av domstolsavgöranden i mål om LPT och LVM, då de innehåller känsliga uppgifter om hälsa.[5] Prövningstillstånd har meddelats i Högsta förvaltningsdomstolen, vilket innebär att den rättsliga prövningen fortsätter.

Begäran om tillgång till allmänna handlingar från domstolar innehållande uppgifter om brott kopplade till en specifik individ har

---

[1] EU-domstolens dom i mål C-311/18, Facebook Ireland och Schrems, punkt 109 och EU-domstolens dom i de förenade målen nr C-26/22 och C-64/22, UF och AB mot Land Hessen och SCHUFA Holding AG, punkt 57 och 68–69

[2] Fysisk person (levande) vars personuppgifter behandlas.

[3] HFD mål nr 6193–22 och 3691–22

[4] Mål nr 13539-23, IMY/Spotify

[5] Mål nr 1128-23 IMY/Verifiera. Med LPT avses lagen (1991:1128) om psykiatrisk tvångsvård och med LVM avses lagen (1988:870) om vård av missbrukare i vissa fall.

nekats. Dataskyddsförordningen får även konsekvenser för andra personuppgiftsansvariga i förhållande till hur de får behandla uppgift om brott vid en bakgrundkontroll inför exempelvis en anställning.

Den ökade användningen av AI, AI förordningen[6] samt att dataskyddsförordningen ska tillämpas fullt ut vid nyttjande av AI-tjänster, om personuppgifter behandlas, innebär att komplexiteten av att praktiskt efterleva dataskyddsregelverket har ökat.

Avslutningsvis är det viktigt att framhålla att dataskydds-förordningen i grunden avser att harmonisera skyddet för den personliga integriteten inom EU. Det är därför särskilt viktigt att omvärldsbevaka vad som sker utifrån EU-domstolens praxis och i andra EU länder. Även Europeiska dataskyddstyrelsen riktlinjer, vägledningar och rekommendationer behöver inhämtas för att identifiera dataskyddsrisker. Europeiska dataskyddsstyrelsen har bland annat till uppgift att harmonisera tillämpningen av dataskyddslagstiftningen.

Om omvärldsbevakning görs samt tillsyn och praxis analyseras kan faktiska dataskyddsrisker omhändertas tidigt i den egna verksamheten. Utifrån omvärldsbevakningen kunde man redan tidigt se att andra EU-länders tillsynsmyndigheter tilldelade sanktionsavgift gällande felaktig användning av Facebooks metapixel, där IMY först fattade beslut 2023 om att utfärda sanktionsavgift.

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporterings-områden som SISAB 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, konsekvensbedömning avseende dataskydd, individens rättigheter och personuppgiftsincidenter*.

[6] Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förord-ningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (*förordning om artificiell intelligens*)

Nedan redogörs för SISAB:s status och DSO slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO genomförda uppföljning och granskning.

3.1 Register över behandling, registerförteckning

3.1.1 Årets arbete med registerförteckning och DSO rekommendation

I samband med tillträde såsom dataskyddsombud för SISAB 2024 framförde ledning behov av översyn och utveckling av befintlig registerförteckning.

Dataskyddsombudet har granskat befintlig registerförteckning 2024 och lämnat rekommendation om fortsatt arbete. Lämnad rekommendation baseras på stadens vägledning om att arbeta processbaserat utifrån fastställda verksamhetsprocesser i hanteringsanvisningarna. Att arbeta processbaserat utifrån verksamhetsprocesser underlättar bland annat att fastställa korrekt laglig grund.

Att samma processer som används för att efterleva arkivlagstiftningen och dess behov av informationskartläggning bidrar även till att skapa synergier i de olika informationskartläggningar som behöver utföras med anledning av lagkrav.

Registret över behandlingar, registerförteckningen, har uppdaterats med de verksamhetsprocesser som behöver förtecknas. Ett antal förteckningar har även kunnat färdigställas 2024.

Arbete pågår med HR-avdelningen, där samtidigt hanteringsanvisningarnas innehåll har uppdaterats. Arbete för att registerförteckna processen Upphandling förbereds tillsammans med verksamheten.

Arbetet med att utveckla registerförteckningen till ett processbaserat behandlingsregister utifrån verksamhetsprocesserna i hanteringsanvisningarna behöver fortsätta under 2025. Påbörjat arbete avser att resultera i en mer fullständig registerförteckning utifrån ett personuppgiftsbehandlingsperspektiv.

Under 2025 bör även arbetet fortsätta med att implementera roller utifrån ett dataskyddsperspektiv i verksamhetsprocesserna. När

roller implementeras bör instruktion för hantering av register-förteckning spegla detta.

Fråga/kontroll	Svar
Har nödvändiga uppdateringar gjorts i registerförteckningen?	Arbete behöver fortsätta under 2025 för att säkerställa att detta om-händertas.
Bedöms registerförteckningen vara fullständig?	Arbete behöver fortsätta under 2025 för att säkerställa att detta om-händertas.
Har verksamheten lämpliga rutiner för registerföring?	Arbete behöver fortsätta under 2025 för att säkerställa att detta om-händertas.

3.1.2 Sammanfattning av rekommenderade aktiviteter för 2025

- Arbetet med att uppdatera och förteckna personuppgifts-behandlingar processbaserat i ett behandlingsregister behöver fortsätta under 2025 för att bland annat säkerställa laglig grund för hantering av personuppgifter.
- Att samtliga avdelningar avsätter resurs för att upprätta och säkerställa att deras verksamhetsprocess är fullständigt registerförtecknad i systemstödet tillsammans med dataskyddsombudet.
- Dataskyddsombudet rådger och vägleder verksamheten i aktiviteten för registerförteckning för att underlätta genom-förandet och samtidigt utbilda i praktiskt integritets-skyddsarbete.
- Framtagande av instruktion för registerföring utifrån 2025 års arbete.

Om ovan aktiviteter utförs åtgärdas brister, och dataskyddsrisker minimeras.

3.2 Styrdokument

3.2.1 Årets arbete med styrdokument och DSO rekommendation

SISAB tillämpar stadens riktlinje för informationssäkerhet och tillhörande tillämpningsanvisning. SISAB tar även systematiskt

fram lokala styrdokument för informationssäkerhet. Informationssäkerhetssamordnare, ISAM, redogör för det arbete som gjorts under 2024 och planering för 2025 i upprättat dokument, Ledningens genomgång Informationssäkerhet SISAB 2024. Dataskyddsombudet ser det som positivt att rutiner, instruktioner och interna processer för att SISAB skall kunna bedriva ett systematiskt och fungerande informationssäkerhetsarbete håller på att etableras och systematiseras.

I egenskap av dataskyddsombud har jag varit behjälplig med att ta fram en instruktion för hantering av rätten till tillgång, ett så kallat registerutdrag. Instruktionen har sin grund i den rättspraxis som utvecklats på området. Dataskyddsombudet har även varit behjälplig med uppdatering och strukturering av metodstöd för tröskelanalys och mall för konsekvensbedömning avseende dataskydd.

SISAB behöver fortsätta att ta fram ytterligare instruktioner för dataskydd under 2025, då stadens övergripande styrdokument inte innefattar dataskydd fullt ut, då varje nämnd/bolagsstyrelse är eget personuppgiftsansvariga. Rekommendationen har sin grund i den dataskyddspraxis som utvecklas utifrån de grundläggande dataskyddsprinciperna och organisatoriska åtgärder för säkerhet avseende personuppgiftsbehandling.

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

3.2.2 Sammanfattning av rekommenderade aktiviteter för 2025

- Dataskyddsombudet ska fortsätta sitt rådgivande och stödjande arbeta vid framtagande och uppdatering av styrdokument, strategier samt instruktioner avseende dataskydd under 2025.

Dataskyddsombudets prioriteringar avseende styrdokument 2025 baseras på dataskyddsförordningens generella krav om att *dataskyddsombudet vid utförandet av sina uppgifter ska ta vederbörlig hänsyn till de risker som är förknippade med behandling, med beaktande av behandlingens art, omfattning, sammanhang och syften*. Den legala omvärldsbevakningen kommer även att ligga till grund för prioriterat arbete för styrdokument under 2025.

Om ovan aktivitet utförs löpande hanteras dataskyddsrisker systematiskt, och minimeras.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

3.3.1 Årets arbete med informationsklassning och DSO rekommendation

I årets Ledningens genomgång Informationssäkerhet SISAB 2024 har ISAM redogjort för årets arbete med informationsklassning. ISAM har även lämnat rekommendationer för 2025.

ISAM har i nära samarbete arbetat med DSO både gällande Ledningens genomgång och i genomförandet av faktiska informationsklassningar under året. På så vis vävs även dataskyddsperspektivet in i informationssäkerhetsarbetet med att hantera tekniska och organisatoriska åtgärder.

Rättspraxis avseende dataskydd finns idag som har direkt påverkan på tekniska och organisatoriska åtgärder. De tekniska och organisatoriska åtgärderna behöver vara implementerade i enlighet med praxis vid personuppgiftsbehandling. DSO ska under 2025 vara behjälplig med att dokumentera praxis i en instruktion.

DSO instämmer i ISAM:s bedömning att informationsklassningsarbetet behöver fortgå under 2025. Fler verksamhetsprocessers och

objekts informationstillgångar behöver således informationsklassas och hållas aktuella.

Fråga/kontroll	Svar
Hur många av personuppgifts-behandlingarna som finns i verksamheten har informations-klassats?	Informationsklassning utförs utifrån ett objekts informations-tillgångar, vilket gör att antal klassade personuppgifts-behandlingar inte redogörs för under 2024. Ny bedömning angående antal görs efter ytterligare arbete med registerförteckning 2025.
Är klassade personuppgiftsbehandlingar aktuella?	Arbete med att informations-klassa och hålla dessa klassningar aktuella behöver fortsätta under 2025

3.3.2 Sammanfattning av rekommenderade aktiviteter för 2025

- Informationsklassningsarbetet behöver fortgå under 2025. Både till antal och för att hålla informationsklassningarna aktuella.
- Fortsätta att implementera tekniska och organisatoriska åtgärder i enligt med dataskyddspraxis.
- DSO ska stödja med att upprätta en instruktion avseende legal dataskyddspraxis att beakta vid informationsklassning.

3.4 Konsekvensbedömning dataskydd

3.4.1 Årets arbete med konsekvensbedömning och DSO rekommendation

Under 2024 har dataskyddsombudet varit behjälplig med strukturering och uppdatering av metodstöd för tröskelanalys och mall för konsekvensbedömning avseende dataskydd.

Under 2025 bör den nya mallen för konsekvensbedömning avseende dataskydd införlivas i verksamheten.

Konsekvensbedömning avseende dataskydds syfte är att förebygga dataskyddsrisker. Målet är att värna integritetsskyddet och minimera integritetsrisker. Metodstödet är således användbart för att omhänderta dataskyddsfrågor vid anskaffning av en tjänst.

En konsekvensbedömning avseende dataskydd ska enligt IMY exempelvis utföras när verksamheten utför bakgrundskontroller inför anställning, arbetsgivare inrättar kandidat- och kompetens-databas eller visselblåsarsystem.

Dataskyddspraxis visar även att sanktionsavgift tilldelas när personuppgiftsansvarig inte utfört en konsekvensbedömning avseende dataskydd. Ett exempel på när sanktionsavgift utfärdats är när kommunal nämnd inte genomfört en konsekvensbedömning innan den digitala skolplattformen Google Workspace infördes.

Metodstödet för konsekvensbedömning avseende dataskydd behöver således införlivas som arbetsverktyg. Metodstödet behöver vidare ingå vid framtagande av övergripande strategier för att operativt implementera dataskydd, hantera dataskyddsrisker och minimera dessa risker.

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Arbete behöver påbörjas med att identifiera och börja använda metodstöd för konsekvens-bedömning avseende dataskydd
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Arbete behöver påbörjas med att identifiera och börja använda metodstöd för konsekvens-bedömning avseende dataskydd
Är de genomförda bedömningarna aktuella?	Arbete behöver påbörjas med att identifiera och börja använda metodstöd för konsekvens-bedömning avseende dataskydd

3.4.2 Sammanfattning av rekommenderade aktiviteter för 2025

- Införliva den nya mallen för konsekvensbedömning avseende dataskydd i verksamheten.

- Metodstödet bör ingå i strategidokument för att operativt användas för att hantera och minimera integritetsrisker.

Om ovan aktiviteter utförs hanteras integritetsbrister operativt och dataskyddsrisker minimeras.

3.5 Individens rättigheter

3.5.1 Årets arbete med den registrerades rättigheter och DSO rekommendation

DSO har tillgång till kommunikationskanaler för den registrerade och kan kommunicera direkt med den registrerade. SISAB uppfyller således att DSO kan fullgöra sin lagstadgade uppgift att vara kontaktpunkt gentemot den registrerade.[7]

Under 2024 har dataskyddsombudet involverats i hanteringen av ärende, där den registrerade begärt radering av dennes person-uppgifter. Dataskyddsombudet har även varit behjälpligt med att ta fram en uppdaterad Instruktion avseende rätten till tillgång enligt dataskyddsförordningen med anledning av ny rättspraxis. Europeiska dataskyddsstyrelsen har även aviserat att rätten till tillgång är en fråga som kommer att samordnat granskas inom EU genom att samtliga tillsynsmyndigheter, även IMY, deltar.[8]

Det återstår att fastställa roller och ansvar för dataskydd i verksamhetsprocesserna, utifrån hanteringsanvisningarna, för att systematiskt kunna hantera t.ex. en begäran om tillgång till personuppgifter, ett registerutdrag.

Dataskyddsombudet fortsätter under 2025 att prioritera instruktioner avseende den registrerades rättigheter.

En översyn av SISAB:s integritetspolicy, de registrerades rätt till information, har planerats för 2025. Översynen kommer att beakta rättspraxis[9] på området och utföras tillsammans med verksamheten.

---

[7] Artikel 38.4 ”Den registrerade får kontakta dataskyddsombudet med avseende på alla frågor som rör behandlingen av dennes personuppgifter och utövandet av dennes rättigheter enligt denna förordning.”
[8] CEF 2024: Launch of coordinated enforcement on the right of access | European Data Protection Board
[9] Mål nr 2829-23 IMY/Klarna

Fråga/kontroll	Svar
Hur många begäranden (om register-utdrag, begränsning, radering etc.) har inkommit från registrerade personer?	Sedan mitt tillträde har 1 begäran om radering inkommit.
Hur många av dessa begäranden har hanterats av verksamheten inom 30 dagar?	Begäran om radering har hanterats inom lagstadgad tidsram.

3.5.2 Sammanfattning av rekommenderade aktiviteter för 2025

- Roll och ansvar för dataskydd i verksamhetsprocesserna, utifrån hanteringsanvisningarna, behöver sättas för att kunna systematiskt hantera t.ex. en begäran om tillgång till personuppgifter, ett registerutdrag
- Fortsätta att ta fram instruktioner avseende den registrerades rättigheter.
- Översyn av integritetspolicy för att säkerställa att den är i överenstämmelse med gällande rättspraxis.

3.6 Personuppgiftsincidenter

3.6.1 Årets arbete med personuppgiftsincidenter och DSO rekommendation

SISAB:s verksamhet har stämt av sina informationssäkerhets-händelser innefattande personuppgifter under 2024 med sin ISAM och DSO.

DSO har kunnat rådge verksamheten avseende hantering av person-uppgiftsincidenter. DSO har även fått rådge om incident ska an-mälas till IMY och om den berörde registrerade behöver informeras. DSO har vidare informerat om skyldigheten att dokumentera enligt dataskyddsförordningen och vad dokumentationen måste innehålla. IMY har rätt att begära ut dokumenteringen avseende personuppgiftsincidenter för att kontrollera efterlevnaden.[10]

[10] Artikel 33.5 dataskyddsförordningen

Verksamhetens transparens avseende informationsäkerhets-händelser innefattande incidenter bidrar till att personuppgifts-incidenter kan hanteras enligt gällande lagkrav.

Ett medskick avseende personuppgiftsincidenter är att följa IMY:s årliga rapportering avseende personuppgiftsincidenter.[11] IMY:s rapportering har även innefattat personuppgiftsincidenter med anledning av antagonistiska angrepp. I den rapporteringen lyfter IMY att offentlig sektor bör säkerställa sin förmåga att upptäcka

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	• Av verksamheten. • Rapportering inom staden
Hur många personuppgiftsincidenter har dokumenterats?	Årets informationssäkerhets-incidenter inklusive personuppgiftsincidenter har rapporterats i dokumentet Ledningens genomgång Informationssäkerhet SISAB 2024
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	• Ingen av personuppgifts-incidenterna har efter bedömning och samråd med DSO rapporteras till IMY. • Efter bedömning har heller inte registrerad infor-merats om incident. • Annan personuppgifts-ansvarig har dock informerats om en personuppgiftsincident för att kunna utföra bedöm-ningar enligt lagkrav.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Tidsaspekten har inte granskats under 2024, då ingen incident rapporterats till IMY.

och anmäla it-angrepp som berör personuppgifter.

[11] Ex.: IMY rapport 2023:2 Anmälda personuppgiftsincidenter 2022 & rapport 2020:3 Personuppgiftsincidenter som beror på antagonistiska angrepp 2019

3.6.2 Sammanfattning av rekommenderade aktiviteter för 2025

- DSO väljer att lyfta fram IMY:s råd om att offentlig sektor bör säkerställa sin förmåga att upptäcka och anmäla it-angrepp som berör personuppgifter.
- Att se över dokumentering så att det är möjligt för IMY att kontrollera efterlevnaden av hantering av personuppgifts-incidenter.

4 Genomförda granskningar under året

I och med att dataskyddsombudet tillträdde 2024 har prioriteringen varit att rådge och stödja verksamheten avseende dataskydds-lagstiftningen. I och med rådgivning har granskning utförts av aktuellt område. Granskning har även skett och avrapporteras i denna rapport avseende de obligatoriska områdena ovan.

Granskningen har även identifierat dataskyddsrisk som redogörs för nedan i avsnitt 6 Risker inom dataskydd.

4.1 DSO ger råd och rekommendationer till PUA

DSO ger råd och rekommendation om att fortsätta arbeta med integritetsskydd och informationssäkerhet i enlighet med aktiviteterna ovan.

En del i skyddet för individens personliga integritet är att PUA ska ge DSO insyn och tillse att dataskyddsombudet kan utföra sina lagstadgade uppgifter. Detta omhändertas mycket väl av SISAB.

5 Risker inom dataskydd

Rättspraxis utvecklas löpande avseende dataskydd, vilket gör att operativa anpassningar behöver utföras i enlighet med den legala utvecklingen. Det är således en risk att inte omvärldsbevaka den legala utvecklingen på området.

Det finns även risk utifrån informationssäkerhet, dvs att inte korrekta eller tillräckligt robusta tekniska och organisatoriska åtgärder implementeras för att skydda personuppgifter och behandlingen av dem.

Nu tas instruktioner fram för att hantera dessa risker. Riskanalys utförs även i nära anslutning till informationsklassningen av informationstillgångar. Annan metod för att hantera och minimera integritetsrisker är att utföra den lagstadgade bedömningen, konsekvensbedömning avseende dataskydd.

Utifrån att leverantörer idag använder sig av underleverantörer, underbiträden, är det även viktigt att identifiera och analysera om tredjelandsöverföring sker. Dessa bedömningar ska ske i enlighet med EU-domstolens praxis och Europeiska dataskyddsstyrelsen rekommendationer. Stockholms stads juridiska avdelning har tagit fram ett metodstöd för att hantera dessa bedömningar. En ytterligare dataskyddsrisk att hantera är således potentiella tredjelandsöverföringar.

5.1 DSO ger råd och rekommendationer till PUA

SISAB rekommenderas att fortsätta att arbeta systematiskt med informationssäkerhet och dataskydd. Att operativt arbeta utifrån verksamhetsprocesserna förenklar implementeringen av lagkrav och att personuppgifterna erhåller korrekta tekniska och organisatoriska skyddsåtgärder (informationssäkerhet).

I det fortsatta arbetet bör prioritering ske utifrån integritetsrisk. Av dataskyddslagstiftningen framgår vad som är risk inom integritetsskyddet. Således bör dataskyddsombudet involveras i riskstrategier för att säkerställa att lagkrav om integritetsskydd kan vävas samman med verksamhetsrisk alternativt separeras.

Att omsätta dataskyddsombudets rekommendationer ovan bidrar till att hantera och minimera integritetsrisker.

6 Planerade granskningar under det nya verksamhetsåret

Planerade granskningar under 2025 kommer att utföras i samråd med verksamheten. Dataskyddsombudets huvudsakliga prioritering avseende granskning 2025 är att följa upp hur väl samtliga rekommenderade aktiviteter i denna rapport genomförts.

7 Övrigt att rapportera

I övrigt att rapportera återknyter dataskyddsombudet till Ledningens genomgång Informationssäkerhet SISAB 2024 och rekommenderar att svarsfrekvensen för dataskydds- och informationssäkerhets-utbildningarna ses över 2025 för att få till en mycket hög svars-frekvens. Dessa utbildningar är enligt stadens styrning obligatoriska och är viktiga för att främja en informationssäkerhets- och dataskyddskultur inom stadens verksamheter.

Attesterat av

Detta dokument har godkänts digitalt av följande personer:

Namn	Datum
Ebba Agerman, VD	2025-01-21
Anders Lundbeck, Avdelningschef Ekonomi	2025-01-21