Stockholms stad

GDPR Årsrapport

2023

Valnämnden

GDPR årsrapport
Januari 2024

Dnr: YYYY
Utgivningsdatum: 202X-MM-DD
Kontaktperson: Namn Namn

1 Bakgrund

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 nämnd och bolagsstyrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett Dataskyddsombud (”DSO”). DSO:n har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

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

Innehåll

2 Sammanfattning

I egenskap av Dataskyddsombud i Stockholms stads Valnämnd lämnar jag följande årsrapport.

Under tillsynsåret har Valnämndens verksamhet varit på en förhållandevis nedskalad nivå, med anledning av den karaktär på uppgifter som åligger Valnämnden mellan valår. DSO konstaterar att verksamhetens dataskyddsarbete håller en hög nivå i relation till den begränsade omfattning som det dagliga arbetet legat på under tillsynsåret. Även DSO:s tillsynsarbete påverkas av nämndens begränsade verksamhet, varför DSO valt att hålla anmärkningar och granskningar i årets rapport på en mer övergripande nivå.

DSO har granskat de sex obligatoriska granskningsområdena, samt utfört tre granskningar utöver de obligatoriska. Inledningsvis konstaterar DSO att verksamheten i stor utsträckning uppfyller de krav som ställs enligt dataskyddsförordningen och Stockholms stads interna målsättningar. Nedan sammanfattas ändå de områden där vissa brister förekommer.

- DSO rekommenderar att Valnämnden anpassar de styrdokument som stadsledningskontoret tagit fram och som nämnden använder sig av, för att säkerställa att innehållet är relevant för nämndens verksamhet.
- DSO rekommenderar att Valnämnden ser över användandet av och besökares möjlighet att godkänna cookies vid besök på Kaskelots webbplats.

3 Obligatoriska rapporteringsområden

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

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

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

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	36
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

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

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

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

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

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

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

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

Valnämndens registerförteckning har för närvarande 36 registrerade behandlingar.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Valnämnden har genomfört uppdateringar i registerförteckningen under tillsynsåret. Uppdateringarna avsåg ett nytt rekryteringssystem, förändrade behörighetsrutiner och en ny modul i systemet Kaskelot. DSO konstaterar att den senast uppdaterade versionen av registerförteckningen som tillhandahållits till DSO är daterad 3 maj 2023, vilket indikerar att registerförteckningen hålls uppdaterad och levande i förhållande till Valnämndens verksamhet. Bedömningen att registerförteckningen hålls uppdaterad understöds av uppgifter från den intervju som hållits i samband med tillsynsarbetet.

DSO bedömer hur fullständig registerförteckningen är

DSO noterar att registerförteckningen är mer behandlingsorienterad än systemorienterad och att det talar för en god fullständighet. DSO konstaterar att verksamhetens samtliga personuppgiftsbehandlingar tycks ingå i registerförteckningen. Det finns definitivt en sådan ambition i verksamheten.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Registerförteckningen har tagits fram i samråd med DSO. DSO konstaterade vid tillsynen 2021 att verksamheten saknade nedtecknade rutiner för arbetet med registerförteckningen. På grund av Valnämndens periodiska arbetssätt bedömer DSO att en utförlig nedtecknad rutin inte är nödvändig med beaktande av verksamhetens omfång, men att exempelvis det systematiska kvalitetsarbetets årshjul kan påminna om att återkommande översyn bör göras.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

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

3.1.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att verksamheten fortsätter arbeta löpande med registerförteckningen utifrån att nya behandlingar förs in eller att gällande behandlingar förändras. Vidare bör nämnden granska registerförteckningen årsvis för att säkerställa att den återspeglar nämndens personuppgiftsbehandlingar.

3.2 Styrdokument

3.2.1 Sammanfattning

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

3.2.2 Syfte

Området syftar till att personuppgiftsansvarige genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar personuppgiftsansvarige till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna, när de hanterar personuppgifter. 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). 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.

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

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

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?

DSO konstaterar att med beaktande av Valnämndens periodiska arbetssätt så är behovet av unik upprättad styrande dokumentation förhållandevis lågt, inte minst mellan valåren. Valnämnden tar del och följer de av stadsledningskontorets skapade dokument och rutiner inom dataskyddsområdet. Valnämnden har under tillsynsåret även uppdaterat rutinen för hantering av personer med skyddad identitet. All personal genomgår de obligatoriska dataskyddsutbildningar som staden publicerar. Av den anledningen bedömer DSO att lämplig styrande dokumentation finns på plats.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

Valnämnden tar del och följer de av Stadsledningskontorets skapade dokument och rutiner inom dataskyddsområdet. Dokumenten antas och används av Valnämnden utan att anpassas utifrån nämndens verksamhet.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

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

3.2.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att Valnämnden anpassar de styrdokument som Stadsledningskontoret tagit fram och som nämnden använder sig av, för att säkerställa att innehållet är relevant för nämndens

verksamhet. Framöver rekommenderar DSO även att verksamheten successivt upprättar sådana rutiner och riktlinjer som är av särskilt intresse för Valnämnden, i de fall ett sådant behov skulle uppstå. I övrigt bedömer DSO att med beaktande av Valnämndens periodiska arbetssätt så är verksamhetens arbete med styrande dokumentation på en lämplig nivå.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

3.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	Internt system ”Kaskelot” och ”Rösta i Stockholm” har aktuell informationssäkerhetsklassning. De centrala systemen t.ex. mailsystem, Lisa, Agresso mm. litar man på det arbete systemägare gör.
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

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

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 uppdraget, minskar sannolikheten avsevärt att en klassning faktiskt initieras.

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

3.3.3 Resultat

Personuppgifter för icke anställda behandlas i det valadministrativa systemet Kaskelot. Kaskelot är informationssäkerhetsklassad i KLASSA den 25 augusti 2020 i nivåerna: Konfidentialitet 2, Riktighet 2 och Tillgänglighet 2. Systemet innehåller personuppgifter såsom personnummer, adress och kontaktuppgifter. Inga särskilt skyddsvärda personuppgifter registreras. Personer med skyddade uppgifter hanteras särskilt. Systemet har nyligen förändrats vilket innebär att en ny informationsklassning kommer genomföras. De övriga IT-system som ingår i Valnämndens verksamhet är beslutade om från SLK:s håll. Valnämnden har en utpekad ansvarig person för informationsklassning; Roger Wihlborg.

3.3.4 DSO anger hur allvarliga bristerna är på en skala

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

3.3.5 DSO ger råd och rekommendationer till PUA

DSO ger rådet att informationsklassa eventuell framtida användning av nya IT-system och att fortsättningsvis bibehålla en god nivå av informationssäkerhetskunskap inom verksamheten. DSO rekommenderar även att nämnden med anledning av förändringen i systemet Kaskelot genomför den planerade informationsklassningen så snart som möjligt.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Ja
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Ja, hittills har Valnämnden inte identifierat några högriskbehandlingar i sin verksamhet
Är de genomförda bedömningarna aktuella?	-

3.4.2 Syfte

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

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

3.4.3 Resultat

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

I dataskyddsarbetet och vid inventering har inga behandlingar hittills bedömts som högriskbehandlingar. Vid föregående tillsyn diskuterades en ny förändring i systemet Kaskelot avseende personer med skyddad identitet, som har genomförts under detta år. Valnämnden har bedömt att förändringen inte innebär en hög risk för de registrerade och att en konsekvensbedömning därmed inte är nödvändig. DSO instämmer i denna bedömning.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

-

Är de genomförda konsekvensbedömningarna aktuella?

-

3.4.4 DSO anger hur allvarliga bristerna är på en skala

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

3.4.5 DSO ger råd och rekommendationer till PUA

DSO ger rådet att Valnämnden fortsättningsvis kontinuerligt värderar och identifierar de personuppgiftsbehandlingar som kan tänkas utgöra hög risk och kräva konsekvensbedömning.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	1
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	1

3.5.2 Syfte

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

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

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

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

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

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Under 2023 har en begäran om registerutdrag inkommit. Begäran hanterades inom föreskriven tidsfrist på 30 dagar. I systemet Kaskelot finns sedan 2019 en enkel funktion för att kunna ta bort en person helt ur registret. Personer som begär att bli glömda och som haft förordnande som röstmottagare tas bort ur systemet, men person och uppdrag levereras till stadens E-arkiv för bevarande enligt gällande regler. DSO bedömer att verksamheten har goda förutsättningar för att hantera registrerades rättigheter inom föreskriven tidsfrist.

3.5.4 DSO anger hur allvarliga bristerna är på en skala

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

3.5.5 DSO ger råd och rekommendationer till PUA

DSO uppmuntrar verksamheten att fortsättningsvis tillmötesgå begäran om att utöva registrerades rättigheter på en sådan god nivå som de i dagsläget gör.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Valnämnden har inte haft någon personuppgiftsincident under 2023.
Hur många personuppgiftsincidenter har dokumenterats?	Ingen
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Ingen
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	-

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen (artikel 4.12) ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

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

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att flera personuppgiftsincidenter ska rapporteras till IMY, och då inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om

personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, ska rapportering även ske till de berörda registrerade personerna, utan dröjsmål. Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering även till de berörda personerna.

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

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

3.6.3 Resultat

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

Eftersom inga personuppgiftsincidenter har skett under tillsynsåret så kan inte DSO uttala sig om Valnämndens förmåga att rapportera personuppgiftsincidenter i tid till IMY.

3.6.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten

	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
x	Inga brister av nämnvärd betydelse identifierade

3.6.5 DSO ger råd och rekommendationer till PUA

I föregående årsrapport rekommenderade DSO Valnämnden att sprida kunskap och information internt om personuppgiftsincidenter och hur de ska hanteras, inte minst bland tillfälligt engagerad personal. Detta har åtgärdats genom utbildning till de anställda. DSO uppmuntrar Valnämnden att bibehålla den interna kunskapen om personuppgiftsincidenter genom kontinuerliga utbildningar.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- *Granskning 1 – Implementering av åtgärder från förra årets tillsynsrapport*
- *Granskning 2 – Arbetet med dataskydd vid upphandling*
- *Granskning 3 – De anställdas användning av e-post på arbetet*

4.2 Syfte

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

4.3 Genomförda granskningar och deras resultat

Granskning 1 - Implementering av åtgärder från förra årets tillsynsrapport

- I föregående årsrapport föreslog DSO ett antal åtgärder:
- att Valnämnden skulle sprida kunskap och information internt om personuppgiftsincidenter och hur de ska hanteras,
- att Valnämnden särskilt skulle granska förändringen i systemet Kaskelot och besluta om riskvärderingen var korrekt och om en ny konsekvensbedömning annars behövde genomföras, samt
- att verksamheten skulle se över användandet av och besökares möjlighet att godkänna cookies vid besök på Kaskelots webbplats.

DSO konstaterar att majoriteten av de tidigare rekommenderade åtgärderna har implementerats av Valnämnden. Den åtgärd som ännu inte implementerats fullt ut enligt den information som tillhandahållits till DSO är:

- att verksamheten skulle se över användandet av och besökares möjlighet att godkänna cookies vid besök på Kaskelots webbplats.

DSO rekommenderar att Valnämnden implementerar åtgärden så snart som möjligt.

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

Granskning 2 – Arbetet med dataskydd vid upphandling

Dataskyddsförordningen gäller för behandling av personuppgifter i olika it-system som den personuppgiftsansvarige använder. Den personuppgiftsansvarige har ansvar för att säkerställa att all behandling som sker av den personuppgiftsansvarige eller på den personuppgiftsansvariges uppdrag uppfyller kraven på teknisk och organisatorisk säkerhet som uppställs i dataskyddsförordningen. Tekniska och organisatoriska säkerhetsåtgärder kan vara åtgärder som den personuppgiftsansvarige själv vidtar eller kan det vara krav som ställs på en systemleverantör som är personuppgiftsbiträde. För att säkerställa att lämpliga tekniska och organisatoriska säkerhetsåtgärder vidtas behöver den personuppgiftsansvarige analysera informationen och personuppgiftsbehandlingen. I de flesta fall behöver en riskanalys och informationsklassning göras och i vissa fall behöver en konsekvensbedömning enligt dataskyddsförordningen göras.

Den personuppgiftsansvariges ansvar för att vidta säkerhetsåtgärder för att säkerställa och visa att personuppgiftsansvarige följer dataskyddsförordningen regleras i artikel 24 och artikel 25 dataskyddsförordningen. Den personuppgiftsansvariges ansvar för

personuppgiftsbiträden regleras i artikel 28 dataskyddsförordningen. Den personuppgiftsansvariges och personuppgiftsbiträdens ansvar för att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att säkerställa en lämplig säkerhetsnivå i förhållande till risken regleras i artikel 32 dataskyddsförordningen.

Valnämnden genomför sällan upphandlingar och om en upphandling ska genomföras stöttas nämnden av Serviceförvaltningen. Verksamheten använder Stadens mall för PUB-avtal vid upphandling och inköp som omfattar personuppgiftsbehandling av personuppgiftsbiträden. Analys av hur personuppgiftsansvaret ska se ut inför nya upphandlingar och inköp av system genomförs centralt. Inga nödvändiga åtgärder har identifierats av DSO.

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

Granskning 3 – De anställdas användning av e-post på arbetet

Den behandling av personuppgifter som sker i anställdas e-post på arbetet omfattas av dataskyddsförordningen. Precis som all behandling av personuppgifter behöver den personuppgiftsbehandling som sker i e-posten ha en rättslig grund. Behandlingen behöver även vara förenlig med de grundläggande principer som finns i dataskyddsförordningen, såsom att enbart samla in personuppgifter för specifika ändamål, att radera personuppgifterna när de inte längre behövs och att skydda uppgifterna från spridning eller från att obehöriga får tillgång till dem.

För att säkerställa att hanteringen av personuppgifter i e-posten är laglig och sker på ett korrekt sätt måste organisationen ta fram rutiner eller andra riktlinjer som anger hur e-posten ska hanteras.

Därefter behöver informationen spridas till dem som berörs inom organisationen och även tillämpas av dessa.

Skyldigheten att behandla personuppgifter korrekt i e-posten följer av de grundläggande principerna i artikel 5 dataskyddsförordningen. Principerna innebär bland annat att personuppgiftsansvariga:

• måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter
• bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål
• inte ska behandla fler personuppgifter än vad som behövs för ändamålen
• ska säkerställa att personuppgifterna är riktiga
• ska radera personuppgifterna när de inte längre behövs
• ska skydda personuppgifterna, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs
• ska kunna visa att ni lever upp till dataskyddsförordningen och hur ni gör det.

De grundläggande principerna i artikel 5 ska genomsyra all personuppgiftsbehandling.

DSO konstaterar inledningsvis att verksamheten uppvisar god kunskap avseende hur dataskydd ska beaktas vid användning av e-post. Det finns en medvenhet om vilka uppgifter som inte ska behandlas i e-post. Verksamheten använder sig av eDok vilket minskar risken för att anställda använder e-posten som lagringsyta. DSO har fått information om att det finns en rutin för användning av e-post som hittills inte implementerats fullt ut i verksamheten.

	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

4.4 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att verksamheten säkerställer att samtliga åtgärder från tidigare årsrapport implementeras fullt ut i verksamheten. DSO rekommenderar även att en rutin avseende anställdas användning av e-post implementeras i verksamheten.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- *Känsliga personuppgifter*

5.2 Syfte

Med anledning av Valnämndens nedskalade verksamhet mellan valår, så bedömer DSO att verksamhetens dagliga arbete inte innehåller några nämnvärda risker ur dataskyddssynpunkt. Däremot menar DSO att det är viktigt att ändå lyfta de aspekter av verksamhetens natur som medför särskild aktsamhet.

5.3 Resultatet av riskkartläggningen

Risk 1 – Känsliga personuppgifter

Enligt art. 9.1 i dataskyddsförordningen så utgör *politiska åsikter* känsliga personuppgifter. Valnämndens personuppgiftshantering har ett tätt naturligt samband med sådana personuppgifter. Av den anledningen vill DSO lyfta Valnämndens skyldighet att vidta särskild aktsamhet för sin personuppgiftsbehandling vad gäller uppgifter om registrerades politiska åsikter.

	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

5.4 DSO ger råd och rekommendationer till PUA

DSO uppmuntrar verksamheten att fortsättningsvis hålla en god kunskapsnivå om den aktsamhet som följer av Valnämndens

befattning med känsliga personuppgifter. DSO vill rikta ett särskilt fokus på att verksamheten påtalar den aktsamheten för nyanställda.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Dataskyddsarbete i relation till uppskalad verksamhet*
- *Hantering av personuppgiftsincidenter*

6.2 Syfte

Det granskande arbetet är en av dataskyddsombudets viktigaste uppgifter. Granskningsområdena har valts utifrån ett riskbaserat synsätt, det vill säga att fokus läggs på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister.

6.3 Planerade granskningar

Granskning 1 – Dataskyddsarbete i relation till uppskalad verksamhet

DSO har i avsnitt 4 granskat hur väl verksamheten är rustad för en uppskalning av verksamheten och bedömt att Valnämnden är väl rustade i sitt dataskyddsarbete.

Med anledning av Valnämndens uppskalade verksamhet till följd av det förestående EU-valet 2024, så väljer DSO att till nästa tillsynsår granska hur verksamhetens dataskyddsarbete i realiteten följt den uppskalade verksamheten. DSO kommer att lägga fokus på vilket stöd nyanställda fått i dataskyddsfrågor, inbegripet utbildning, lättillgängliga rutiner och riktlinjer samt vilken nivå på generell dataskyddskultur som förekommer i det dagliga arbetet.

Granskning 2 – Hantering av personuppgiftsincidenter

I takt med den uppskalade verksamheten så ökar även risken för att personuppgiftsincidenter sker. Verksamhetens hantering av personuppgiftsincidenter är en grundläggande del av dataskyddsarbetet och skyddet för de registrerades fri- och rättigheter. DSO väljer därför att granska hur verksamheten hanterar personuppgiftsincidenter, samt hur väl rustad verksamheten är för att hantera sådana. DSO uppmuntrar Valnämnden att lägga särskilt fokus på att utbilda verksamheten på vad en personuppgiftsincident

är och hur de ska hanteras, särskilt inbegripet den tidsfrist som finns för att anmäla vissa personuppgiftsincidenter till IMY.

Stockholm 2023-01-25

Simon Jernelöv, Externt DSO för Valnämnden, Stockholms stad,
och Ebba Holm, dataskyddsjurist.