Stockholms stad

Bilaga 3:4

GDPR årsrapport

2025

Skarpnäcks stadsdelsnämnd

GDPR årsrapport
Januari 2026

Dnr: SKA 2026/22
Utgivningsdatum: 2026-02-19
Kontaktperson: Julia Ögren, dataskyddsombud

Sammanfattning

GDPR, eller dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten. Ett dataskyddsombud har i uppdrag att oberoende granska verksamhetens efterlevnad av dataskyddsförordningen. I denna rapport redovisar dataskyddsombudet årets granskning av Skarpnäcks stadsdelsnämnds dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

År 2025 har rollen som dataskyddsombud fram till den 8 september varit tillsatt av vikarie under ordinarie dataskyddsombuds frånvaro. Majoriteten av de granskningar som ligger till grund för de bedömningar som framgår i rapporten har därför genomförts under perioden september-december, där en prioritering har behövt ske med avsteg från årshjulet. Underlaget utgörs av bland annat av observationer och dialoger, enkät till cheferna om dataskyddsåret 2025, stickprov av ett antal sociala medier-konton, en fördjupad granskning av hela registerförteckningen samt granskning av deltagandet i den obligatoriska utbildningen.

Ett annat perspektiv som bör lyftas inledningsvis är att dataskyddsarbetet följer principen det som inte är skrivet finns inte, vilket direkt relaterar till en av dataskyddsförordningens sju grundprinciper om ansvarsskyldighet. Det innebär att resultaten från den här granskningen enbart kan baseras på de dokumenterade åtgärderna och vad cheferna har rapporterat. Det utesluter alltså inte att det finns bra idéer och initiativ och att arbete ibland inletts, men arbetet behöver formaliseras och dokumenteras för att vara åtgärder i dataskyddsrättslig mening.

Dataskyddsombudet ser fortfarande att förvaltningen ligger efter i flera aspekter av dataskyddsarbetet. I denna rapport blir det synligt framförallt när det kommer till genomförande av moment som relaterar till säkerhet för personuppgifter, såsom informationsklassningar och konsekvensbedömningar. Det finns också ett behov av att stärka kvalitén när det kommer till dokumentationen av personuppgiftsincidenter. Ett grundläggande problem som även pekades ut i förra årets GDPR-rapport är den fortsatta avsaknaden av tydligare styrning för verksamheterna när det kommer till att leva upp till de krav som ställs i dataskyddsförordningen.

Under 2025 har ett stort antal aktörer, många offentliga och däribland Stockholms stad fått erfara en stor och allvarlig personuppgiftsincident när Miljödata drabbades av en dataläcka orsakad av en antagonist. Händelsen ledde till ett intensivt arbete inom staden med tät samordning. Händelsen satte starkt ljus på behovet av en robust informationssäkerhetskultur och hur viktigt skyddet av personuppgifter är.

Dataskyddsombudet ser positivt på de insatser som görs gemensamt i staden kring dataskydd såsom referenskonsekvensbedömningar, erfarenhetsutbyten och normerande klassningar. Staden är en stor och komplex organisation där varje enskild nämnd är personuppgiftsansvarig, men där vi sannolikt har mycket att tjäna på att samarbeta då vi alla har begränsningar i resurser, och för att likforma processer för en säkrare, effektivare och bättre hantering.

Förvaltningen har idag ett ökat antal dataskyddssamordnare, en resurs som dataskyddsombudet ser som mycket positiv och vars roll och ansvarsområde med fördel kan utvecklas och utökas. Gruppen består av personer med olika kompetenser i grunden men som på olika sätt har god insikt i och förståelse för sin verksamhets personuppgiftsbehandlingar.

De tre största riskerna enligt dataskyddsombudets bedömning

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Kunskap i dataskyddsfrågor		Rekommenderad åtgärd: fortsatta utbildningsinsatser för chefer, både övergripande och fördjupande utifrån behov. Öka andelen medarbetare som genomför de obligatoriska grundutbildningarna i dataskydd och informationssäkerhet. Ökad kunskap innebär bl.a. ökad medvetenhet om och efterfrågan av åtgärder som behöver vidtas för en korrekt och säker personuppgiftshantering.
Styrning och systematik		Dataskydd behöver vara en integrerad del av det dagliga arbetet för att PUA ska leva upp till kraven i lagstiftningen och stadens riktlinjer. Rekommenderad åtgärd att öka styrningen på området för att uppnå kontinuerlig uppföljning av linjeansvaret för dataskyddsfrågorna, vilket också leder till ökad systematik i arbetet.
Säkerhet i samband med behandling av personuppgifter		Rekommenderad åtgärd att styra och resurssätta verksamheter och stödfunktioner så att informationsklassningar, riskanalyser och konsekvensbedömningar genomförs och se till att resultaten av dessa omsätts i praktiken.

Innehållsförteckning

Inledning

GDPR, eller dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. Dataskyddsreglerna (*kallas GDPR fortsättningsvis*) sätter tydliga ramar för hur personuppgifter får behandlas för att minimera risken för skada och säkerställa att hanteringen sker ansvarsfullt och rättvist. GDPR har sin grund i de mänskliga rättigheterna, där varje individ har rätt till respekt för sitt privat- och familjeliv samt skydd av sina personuppgifter.

I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten.

Dataskyddsombudets uppgift

Varje personuppgiftsansvarig (nämnd eller styrelse) ska utse ett dataskyddsombud. Dataskyddsombudets uppgifter framgår direkt av lagstiftningen. Ombudets roll är att kontrollera att GDPR följs inom organisationen. Det innebär bland annat att ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. Dataskyddsombudet har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs. DSO ska rapportera direkt till högsta förvaltnings-/bolagsnivå. I Stockholms stad innebär det att dataskyddsombudet rapporterar till nämnder och styrelser.

Dataskyddsombudet lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och styrelse. Genom rapporten kan nämnd och styrelse ta emot de råd och rekommendationer som dataskyddsombudet lämnar. Årsrapporten syftar till att nämnd/styrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Årsrapporten är ett medel för nämnds/styrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Granskning av dataskyddsarbetet 2025

Kontroll av obligatoriska områden

Dataskyddsombudet har granskat verksamhetens dataskyddsarbete utifrån sex obligatoriska områden. De sex områdena har identifierats genom en analys av kraven i GDPR om hur verksamheter bör arbeta systematiskt med dataskydd. Varje område innehåller ett antal kontrollfrågor som ger en bild av verksamhetens dataskyddsarbete. Dessa områden överensstämmer med de delar som enligt Integritetsskyddsmyndigheten (IMY) utgör grunden för en verksamhets systematiska och rättssäkra hantering av personuppgifter.

I rapporten används en riskmodell med fyra nivåer av risk. Modellen hjälper dataskyddsombudet att visa vilken bedömning hen gör av verksamhetens dataskyddsrisker utifrån de iakttagelser som gjorts i granskningen.

Risknivå	Beskrivning
Hög risk 	Iakttagelsen avser en brist som kan leda till betydande risker för de registrerades rättigheter och friheter. Bristen kräver omgående åtgärd och korrigering.
Medelhög risk 	Iakttagelsen avser en brist som kan leda till risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas skyndsamt, men kräver inte omedelbar korrigering.
Låg risk 	Iakttagelsen avser en brist som kan leda till mindre risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas, men kräver inte omedelbar korrigering.
Inget att anmärka 	Dataskyddsombudet har inga brister att rapportera avseende denna del.

Notera att risken för att tilldelas en sanktion vid tillsyn är större desto högre risken är.

Resultatsammanställning och centrala iakttagelser inom dataskyddsarbetet

I detta avsnitt presenteras en sammanställning av den bedömda risknivån för verksamhetens dataskyddsarbete, grundat på kontrollfrågorna inom de sex obligatoriska områdena. Vidare redovisas dataskyddsombudets centrala iakttagelser, inklusive områden där verksamheten uppvisar goda resultat och bör upprätthålla sitt arbete, samt identifierade brister som kan utgöra dataskyddsrisker. Avsnittet innehåller även dataskyddsombudets rekommenderade åtgärder för att hantera dessa risker och stärka dataskyddsarbetet.

En fullständig redovisning av dataskyddsombudets underlag och resultat från granskningen av de sex obligatoriska områdena finns att läsa i bilaga 1. Bilagan innehåller även en beskrivning av syftet och bakgrunden för varje område.

Register över personuppgiftsbehandlingar

Sammanfattning

Förvaltningens arbete med registerförteckningen har i huvudsak gått framåt de senaste åren men avstannat något under 2025. Det finns goda exempel på flera verksamheter som kommit långt i sitt arbete. Dock finns även verksamheter, som behandlar stora mängder känsliga personuppgifter som inte förtecknat dessa på ett korrekt och fullständigt sätt enligt kraven i artikel 30. Det är även ett fåtal verksamheter som fortfarande inte finns representerade i registerförteckningen trots att de behandlar personuppgifter. Dataskyddsombudet stöttar dessa verksamheter att påbörja sitt arbete under senhösten 2025.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		151 behandlingar är registrerade till dags dato. Gällande antalet har risk har identifierats kopplat till de verksamheter som ännu inte finns representerade. Risken bedöms dock inte som omfattande då arbetet pågår. Rekommendationen är att samtliga enhetschefer ska säkerställa att de personuppgiftsbehandlingar som sker inom ramen för verksamheten finns registrerade.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		Det finns i dagsläget en förvaltningsgemensam rutin för inventering och registrering av nya/förändrade behandlingar. Behov har lyfts från chefer av att upprätta egna, lokala rutiner för att arbetet med registerförteckningen ska fungera bättre.

		Verksamheterna rekommenderas därför att se över det egna behovet av mer lokala rutiner, samt att ta stöd av befintliga förvaltningsgemensamma rutiner.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		Utifrån resultatet av höstens granskning bedöms risken vara omfattande eftersom det saknas kravställd information i registreringar som berör personuppgiftsbehandlingar av känslig natur i stora volymer. Rekommenderad åtgärd är att samtliga enhetschefer ser över sina personuppgiftsbehandlingar och huruvida dessa finns upptagna i registerförteckningen.
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		I majoriteten av registreringarna har de obligatoriska uppgifterna angetts, men eftersom framförallt socialtjänstens och delar av äldreomsorgens verksamheter inte har besvarat dessa anges risken på totalen som medelhög. Se även ovan kontrollfråga. Rekommenderad åtgärd är samma som ovan kontrollfråga men med särskilt fokus på den kravställda informationen i artikel 30.

Säkerhet i samband med behandlingen

Sammanfattning

I likhet med tidigare årsrapporter så har omfattande brister fortsatt identifierats på detta område. I huvudsak handlar det om att förvaltningen ännu inte kommit igång med att kontinuerligt och systematiskt arbeta med att minimera risker kring personuppgiftsbehandlingar, vilket i huvudsak sker genom att genomföra informationsklassningar, riskanalyser, tröskelanalyser och i förevarande fall konsekvensbedömningar. Andra åtgärder för att minska risker är att etablera rutiner i verksamheterna som gör att personuppgifter skyddas, exempelvis för att undvika personuppgiftsincidenter. Detta sker redan idag i vissa verksamheter vilket ska anses som positivt och steg i rätt riktning.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?		Urvalet av befintliga informationsklassningar är för litet för att genomföra stickprov. Det kan därför inte anges någon risk för denna kontroll. Att kategorin markeras med röd risk förklaras med avsaknaden av fastställda och omsatta informationsklassningar. Den kartläggning av risker kopplat till personuppgiftsbehandlingar och åtgärder för att minimera dessa som dokumenteras i en informationsklassning sker alltså inte i den omfattning som krävs. *För kännedom tas tillräcklig hänsyn till olika kategorier av personuppgifter i de pågående men ännu inte fastställda informationsklassningarna.*
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		De existerande förvaltningsgemensamma styrande dokumenten och rutinerna om dataskydd bedöms utgöra ett bra underlag för de grundläggande processerna som rör verksamheternas uppdrag kopplade till dataskydd. Stadsgemensamt stöd finns även att tillgå kopplat till genomförande av konsekvensbedömning, både rutin samt mall. Styrdokument på lokal nivå gällande informationssäkerhet är under färdigställande, Även om den inte specifikt riktar in sig på dataskydd så utgör den en viktig del i hur väl personuppgifter skyddas genom exempelvis utpekande av ansvar och roller, processbeskrivningar och behörighetshanering. Rekommenderade åtgärder är fastställda och sprida styrning på området informationssäkerhet.

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		Bedömningen är att de existerande styr- och stöddokumenten avseende dataskydd inte är tillräckligt implementerade och kända. Rekommendation att tydligare sprida kunskap om dessa, exempelvis på APT eller i chefsbrev.

Konsekvensbedömning avseende dataskydd

Sammanfattning

Dataskyddsombudet bedömer i likhet med tidigare årsrapporter att detta är ett område som behöver prioriteras då det fortsatt omgärdas av stora brister eftersom konsekvensbedömningar i regel inte genomförts trots pågående högriskbehandlingar. Kunskaperna kring processen behöver öka och verksamheterna behöver få stöd i hur de ska ta sig an metoden och prioritera bland sina personuppgiftsbehandlingar. Metoden är viktig och dessutom specifikt kravställd i GDPR. Konsekvensbedömningar utgör ett effektivt sätt att upptäcka, åtgärda och förebygga risker kopplat till personuppgiftsbehandlingar som innebär hög risk för registrerades integritet.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		Det finns ingen specifik förvaltningsspecifik rutin för tröskelanalys. Dock finns det en välarbetad stadsgemensam mall för tröskelanalys tillgängligt på intranätet. Risk kan dock kopplas till hur känd och tillämpad denna är, varför rekommenderad åtgärd är att sprida kunskapen om vart den finns och när den ska användas.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		Under året har en form av tröskelanalys skett från avdelningarna där de fick uppdrag att välja ut en högriskbehandling att konsekvensbedöma. Detta ledde till att en konsekvensbedömning genomfördes.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		Ja, det finns ändamålsenligt stadsgemensamt metodstöd samt mall för genomförande av konsekvensbedömning.

		En möjlig åtgärd är dock att bättre sprida kunskapen om vart detta stöd kan hittas.
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		Arbetet har inte kommit igång på så sätt att det går att säga att de genomförs när det krävs. Två har fastställts under året. Förslag på åtgärder är: Att erbjuda utbildning ledd av DSO med medverkan av dataskyddssamordnare som specifikt riktar i sig på att komma igång med tröskelanalys och konsekvensbedömning. Att chefer genomför utbildningen på utbildningsplattformen om konsekvensbedömning. Att överväga möjligheten att lägga in genomförande av konsekvensbedömning i styrningen för verksamheterna.
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		Nej, se även ovan kontrollfråga. Se föreslagna åtgärder i ovan kontrollfråga.

Den registrerades rättigheter

Sammanfattning

Dataskyddsombudets uppfattning är att de begäranden som inkommit under året har hanterats i enlighet med både dataskyddsförordningens krav och stadens och förvaltningens riktlinjer. Dock bör dataskyddsombudet ta ett kliv tillbaka i denna hantering under nästkommande år och överlämna hanteringen helt till verksamheterna och enbart agera råd och stöd vid behov.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	**Risk**	**Rekommendationer**
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		Revidering pågår med förtydliganden men grundläggande information finns i nuvarande rutiner. Mallar är också under framtagande och väntar på godkännande från ansvariga chefer. I huvudsak är utvecklingsområdet i denna fråga att få bättre spridning på de stöddokument som finns.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		Under året har tre begäran hanterats. De begäranden som inkommit har hanterats i tid och på ett adekvat sätt. Det samordnande arbetet kring en begäran bör på ett tydligare sätt övergå till chef under nästkommande år för att
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		Samtliga begäranden har besvarats inom en månad.
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		I en genomgång av de besvaranden som ännu inte gallrats av integritetsskäl så uppfyller dessa lagkraven.

Personuppgiftsincidenter

Sammanfattning

Resultatet av granskningen på detta område skiljer sig inte på något betydande sätt från föregående år. Dokumentationen av incidenterna omgärdas fortsatt av en del brister, Dataskyddsförordningen ställer specifika krav på vilken information som ska dokumenteras och i förevarande fall delas med de registrerade. Antalet som rapporteras i tid bör också öka då det är en relativt stor andel som anmälts senare än gränsen på 72 timmar efter upptäckt.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?		Till dataskyddsombudets kännedom är den enda återkommande åtgärden som når samtliga medarbetare den obligatoriska grundutbildningen som ska genomföras varje år. Den 3 november 2025 hade enbart ca 11 % av förvaltningens medarbetare genomfört utbildningen (216 av 2028 medarbetare). Rekommenderad åtgärd är därför att cheferna följer upp att samtliga medarbetare genomfört utbildningen. Medarbetare bör också få information om var man hittar kunskapsstöd och rutiner när det kommer till personuppgiftsincidenter, exempelvis på APT.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter?		Ja, det finns ändamålsenlig rutin samt tillhörande checklista och mallar för olika typer av beslut.
Följs dessa?		Granskning visar att en stor andel av inrapporterade incidenter brister i dokumentationen. Detta innebär att förvaltningen inte lever upp till kravet på dokumentation ställs i dataskyddsförordningens artikel 33.
Hur många personuppgiftsincidenter har dokumenterats under året?		30 incidenter har rapporterats under året.

Hur många personuppgiftsincidenter har anmälts till IMY under året?		20 incidenter har anmälts till IMY.

Överföring till tredje land

Sammanfattning

I genomgången av förvaltningens registerförteckning, PUB-avtal, konsekvensbedömningar samt påbörjade och avslutade informationsklassningar kan det konstateras att förvaltningen har rapporterat en personuppgiftsbehandling som innebär tredjelandsöverföring, vilket rör konton i sociala medier.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		En personuppgiftsbehandling har identifierats. Avsaknaden av informationsklassningar gör att det inte går att utesluta att tredjelandsöverföringar finns som inte identifierats och bedömts. Därav bedöms risken som möjlig. Risken avhjälps bland annat genom genomförande av informationsklassningar och konsekvensbedömningar.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		För den identifierade personuppgiftsbehandlingen gäller EU-kommissionens adekvansbeslut från 10 juli 2023
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?	N/A	N/A

Bilagor

Bilaga 1: Detaljerad redovisning av dataskyddsombudets granskning

Bilaga 2: Andra genomförda granskningar och omvärldsbevakning

Bilaga 1 - Detaljerad redovisning av dataskyddsombudets granskning

Denna bilaga innehåller en beskrivning av syftet med respektive obligatoriskt område samt en mer detaljerad redovisning av dataskyddsombudets granskning och slutsatser. Här framgår vilka iakttagelser som gjorts och vilken information som samlats in under granskningsarbetet av de sex obligatoriska rapporteringsområdena. För varje område redovisas de underlag som har använts, de iakttagelser som har gjorts samt hur dessa har utgjort grunden för dataskyddsombudets riskbedömning och rekommenderade åtgärder.

1. Register över personuppgiftsbehandlingar

Syftet med området

I GDPR framkommer det att personuppgiftsansvariga (och personuppgiftsbiträden) ska föra ett register över sina personuppgiftsbehandlingar. Registret brukar benämnas ”behandlingsregister” eller ”registerförteckning”. Registret ska finnas tillgängligt i elektronisk form och ska omfatta samtliga personuppgiftsbehandlingar som personuppgiftsansvarig utför. Det ska hållas uppdaterat vilket innebär att det ska uppdateras vid nya eller förändrade personuppgiftsbehandlingar.

Syftet med detta rapporteringsområde är att rapportera om verksamheten har ändamålsenliga rutiner som möjliggör att nya/förändrade personuppgiftsbehandlingar registreras, huruvida personuppgiftsbehandlingar registreras/uppdateras såsom det krävs samt huruvida de uppgifter som är obligatoriska har besvarats kopplat till de registrerade personuppgiftsbehandlingarna.

Kontroller och iakttagelser gjord av dataskyddsombudet

Antal behandlingar som är registrerade?

150

Har verksamheten ändamålsenliga rutiner som möjliggör att nya/förändrade behandlingar registreras?

Förvaltningen har en gemensam rutin för alla verksamheter som beskriver hur inventering och registrering kan ske. Dataskyddsombudet skickar även ut påminnelser två gånger per år om att verksamheterna bör se över sina registreringar för att säkerställa att de är korrekta och aktuella.

Inom exempelvis socialtjänstområdet och inom förskola har man valt att samarbeta kring registreringen av personuppgiftsbehandlingar. Detta kräver samordning för att fungera, och det kan innebära att vissa områden eller verksamheter kan behöva ta fram egna rutiner för att komplettera den gemensamma för att se till att nödvändiga uppdateringar görs.

Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?

Nej, det behöver ske registreringar och uppdateringar i en högre omfattning än idag för att registret ska anses korrekt återspegla de personuppgiftsbehandlingar som sker. Detta gäller för majoriteten av verksamheterna, enbart en mindre andel av dessa hade arbetat aktivt med registerförteckningen under perioden januari till september då ordinarie dataskyddsombud var åter i tjänst och påbörjade granskning.

Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?

Ja, till största del har de obligatoriska uppgifterna besvarats. Dock finns det en relativt stor mängd personuppgiftsbehandlingar som innefattar behandling av känsliga personuppgifter i stor omfattning där dessa uppgifter saknas, särskilt inom socialtjänstområdet. Detta är något som omgående behöver åtgärdas, se mer under rubriken dataskyddsombudets bedömning samt rekommendationer.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Resultatet kan inte jämföras helt eftersom årsrapportens utformning var annorlunda, men resultatet blir att avsaknaden av kravställd information avseende personuppgiftsbehandlingar som rör känsliga personuppgifter i stor omfattning får ett genomslag i bedömningen. Bristerna anses därmed i delar vara allvarligare i år eftersom detta inte åtgärdats.

Dataskyddsombudets bedömning samt rekommendationer

Nödvändiga uppdateringar har gjorts i delar av registerförteckningen. Vissa enheter har kommit långt i sitt arbete och bör ses som goda exempel. En fullständig genomgång av registerförteckningen visade dock att verksamheter som behandlar stora mängder av känsliga personuppgifter ännu inte dokumenterat dem på ett korrekt sätt där de uppgifter som är obligatoriska enligt artikel 30 inte besvarats. Detta gäller i huvudsak enheterna inom socialtjänsten. Registreringar har påbörjats men den kravställda informationen har inte angivits. Detta behöver åtgärdas omgående eftersom förvaltningen inte lever upp till kravet som ställs i artikel 30 och heller inte lever upp till principen om ansvarsskyldighet. För de få verksamheter som idag saknas helt i registerförteckningen har uppstartsmöten skett där ett grundläggande arbete för att skapa registreringar har påbörjats vilket är positivt. Samtliga verksamheter som behandlar personuppgifter bör finnas i registerförteckningen under nästkommande år.

Den sammantagna bilden är att arbetet har avstannat något och att det nu krävs åtgärder för att komma till bukt med avsaknaden av registreringar som svarar på de obligatoriska frågorna, samt till del avsaknaden av vissa verksamheter.

Rekommendationer som lämnas utifrån detta resultat är:

- att varje enhetschef behöver tillse, oavsett hur avdelningar eller områden organiserat sig i arbetet kring registerförteckningen, att de personuppgiftsbehandlingar som sker inom ramen för den egna verksamheten finns i registerförteckningen
- dra nytta av dataskyddsombudets granskningsresultat med kommentarer och råd kring registreringar
- följ anvisningarna som kommer två gånger per om att kontrollera aktualiteten för verksamhetens registreringar

2. Säkerhet i samband med behandlingen

Bakgrund och syfte

Personuppgiftsansvarig ska tillse att personuppgifter skyddas med lämpliga säkerhetsåtgärder, detta för att till exempel undvika att obehöriga får tillgång till uppgifterna eller att uppgifterna förloras.

Personuppgiftsansvarig behöver bedöma vilka tekniska- och organisatoriska säkerhetsåtgärder som ska vidtas för de behandlingar som utförs. Till tekniska säkerhetsåtgärder räknas till exempel kryptering, pseudonymisering och säkerhetskopiering. Organisatoriska säkerhetsåtgärder avser till exempel interna riktlinjer och rutiner.

För att skapa förutsättningar för att skydda information (inklusive personuppgifter) med rätt slags skydd ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. Genom riskanalyser identifierar informationsägaren risker och väljer åtgärder för att minska riskerna. Risker i samband med personuppgiftsbehandling är en typ av risk som informationsägaren behöver omhänderta i riskanalyser.

Att det finns skriftliga, beslutade och kommunicerade styrdokument samt kända rutiner medför att medarbetarna vet hur de ska agera avseende frågor som rör dataskydd. Den personuppgiftsansvariga måste kunna *visa* hur GDPR efterlevs och att det finns styrdokument och rutiner är en viktig del i detta.

Syftet med detta rapporteringsområde är därmed att rapportera huruvida DSO bedömer att det tas hänsyn till risker för den registrerade och om dessa beaktas i tillräcklig mån i genomförda informationsklassningar och riskanalyser. Vidare bedömer DSO huruvida det finns tillräckligt mycket reglerat om dataskydd i styrdokument och rutiner samt om dessa är tillräckligt implementerade och kända.

Kontroller och iakttagelser gjord av dataskyddsombudet

Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?

Eftersom det saknas fastställda informationsklassningar i diariet kan stickprov inte genomföras. I de pågående informationsklassningarna som ännu en fastställts är dataskyddsombudets bedömning att det tas adekvat hänsyn till de olika kategorierna av personuppgifter.

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?

Det finns ett omfattande stadsgemensamt stöd när det kommer till informationsklassningar. Detta behöver kompletteras med lokal anvisning för informationssäkerhet som bland annat tydliggör roller och ansvar, anvisningen är under framtagande men ännu inte fastställd. När det kommer till säker informationshantering i frågor om lagring och handlingarnas livscykel finns stadsdelarnas hanteringsanvisningar, framtagna och kvalitetssäkrade av stadsarkivet. Förutom stadens riktlinje för informationssäkerhet och tillhörande tillämpningsanvisningar finns även exempelvis stadens regler för e-post, obligatorisk utbildning i informationssäkerhet och ett antal rutiner och stöddokument lokalt framtagna avseende dataskydd.

Bedömningen är att det finns ett gediget kunskapsstöd och reglemente som utgörs av både stadsövergripande samt lokalt fastställda dokument när det kommer till säker hantering av personuppgifter, men den nuvarande avsaknaden av lokal anvisning för informationssäkerhet innebär att det inte finns en lokalt fastställd ordning när det kommer till exempelvis roller och ansvar inom informationssäkerhetsarbetet eller processbeskrivning för behörighetsstyrning.

I dataskyddsombudets enkät till enhetscheferna framkom även önskemål om framtagande av verksamhetsspecifika, lokala rutiner. Det rekommenderas därför att de verksamheter som ser behov av detta påbörjar arbetet med att upprätta rutiner och att de i samband med detta tar stöd av de befintliga stöddokument som finns.

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?

Bedömningen är att rutinerna behöver bättre spridning än de har i dagsläget.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Ja, bristerna bedöms vara allvarligare i år jämfört med omfattande föregående år. Detta är mot bakgrund av att det under året inte genererats några tydliga resultat på området trots de bedömningar som gjorts under 2023 och 2024 års rapporter samt den åtgärdsplan som togs fram.

Dataskyddsombudets bedömning samt rekommendationer

Utöver de kontrollfrågor som ställs i denna rapport baserar sig bedömningen av detta rapporteringsområde på hur väl förvaltningen förmår informationsklassa de processer och system som behandlar personuppgifter, samt vilka organisatoriska eller tekniska säkerhetsåtgärder som verksamheterna själva rapporterat om att de implementerat eller avser att implementera under 2025.

Det kan konstateras att förvaltningen inte har genomfört några informationsklassningar i sin helhet under året (fastställt och omsatt i verksamhet). Ett antal informationsklassningar har påbörjats vilket får anses som positivt och steg i rätt riktning, och att en av dessa inte fastställts beror till del på att processen i den normerande klassningen i staden dragit ut på tiden. Dataskyddsombudets enkät till enhetscheferna om dataskyddsarbetet 2025 visade att majoriteten av de svarande cheferna meddelade att de inte planerat eller genomfört några organisatoriska eller tekniska säkerhetsåtgärder. En verksamhet rapporterade att detta sker varje gång det sker en incident, vilket bör ses som positivt.

Att tillägga är att ett grundläggande problem som identifierades i förra årets GDPR- rapport är avsaknaden av styrning och organisation kring informationssäkerhetsarbetet. Det finns till dataskyddsombudets kännedom i dagsläget heller ingen styrning på området för nästkommande år som på ett tydligt sätt förändrar de rådande förutsättningarna, där bland annat resurser i form av tid har rapporterats till dataskyddsombudet som orsaker till varför arbetet inte gått framåt. Ledningens genomgång är det verktyg som tydligast fastslår riktningen för informationssäkerhetsarbetet, men utgör i sig en rapport till ledningen/nämnden om vad ISAM anser bör prioriteras, och inte styrning för förvaltningen.

I styrningen inför nästa år framgår dock att man ska utreda förutsättningarna för ett införande av styr- och samverkansmodellen Pm3. Detta får ses som ett steg i en positiv riktning då ett

införande av Pm3 skulle ge en tydlig struktur med utpekade ansvar, något som är avgörande för att informationssäkerhetsarbetet ska kunna fungera i praktiken.

3. Konsekvensbedömning avseende dataskydd

Bakgrund och syfte

En konsekvensbedömning avseende dataskydd krävs när personuppgiftsansvarig planerar att inleda en personuppgiftsbehandling som innebär hög risk för de registrerade. Huruvida en behandling innebär hög risk eller inte behöver personuppgiftsansvarig avgöra genom att genomföra en s.k. tröskelanalys.

En konsekvensbedömning ska vara genomförd för samtliga behandlingar som innebär hög risk, vilket innebär att personuppgiftsansvarig även behöver kontrollera huruvida denne utför befintliga behandlingar som innebär hög risk. Om högriskbehandlingar utförs för vilka en konsekvensbedömning inte har gjorts, behöver personuppgiftsansvarig genomföra en sådan.

Genom att genomföra en konsekvensbedömning kan personuppgiftsansvarig identifiera risker med en personuppgiftsbehandling, hantera riskerna genom åtgärder och rutiner samt påvisa ansvarsskyldighet. Genom konsekvensbedömningar kan risker identifieras och förebyggas.

Syftet med detta rapporteringsområde är att rapportera huruvida verksamheten har ändamålsenliga rutiner som möjliggör att tröskelanalyser och konsekvensbedömningar genomförs, huruvida sådana genomförs när det krävs samt huruvida personuppgiftsansvarig har genomfört konsekvensbedömningar för de behandlingar som kräver det.

Kontroller och iakttagelser gjord av dataskyddsombudet

Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?

Det finns väl utformade stadsgemensamma rutiner och mallar för tröskelanalys (bedömning av behov av konsekvensbedömning) tillgängliga på intranätet. Det finns ingen lokal rutin för denna process, något som sannolikt vore bra att ta fram för att ytterligare stötta verksamheterna i sitt arbete.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Enligt dataskyddsombudets observationer och kontroller sker detta inte på något systematiskt sätt. I dataskyddsombudets enkät till enhetscheferna rapporterade ingen specifikt angående detta.

Under året har en form av tröskelanalys skett från avdelningarna där de fick uppdrag att välja ut en högriskbehandling att konsekvensbedöma. Detta ledde till att en konsekvensbedömning genomfördes.

Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?

Ja, det finns bra och uppdaterade stadsgemensamma resurser att tillgå när det kommer till konsekvensbedömning avseende dataskydd i form av utbildning på utbildningsplattformen samt mall för själva bedömningen. Mallen är framtagen av juridiska avdelningen och är kvalitetssäkrad. Det finns inte några lokalt framtagna rutiner eller mallar för detta ändamål, men det är dataskyddsombudets uppfattning inte ändamålsenligt att ta fram. Däremot kan en

kompletterande lokal rutin för tröskelanalys tas fram, den analys som leder fram till huruvida en konsekvensbedömning behöver göras.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Det finns en positiv rörelse framåt i år jämfört med föregående år då ett antal konsekvensbedömningar är pågående och en har fastställts under året. Dock kan det fortsatt inte sägas att konsekvensbedömning avseende dataskydd genomförs när så krävs. Den stora majoriteten av de högriskbehandlingar som finns listade i registerförteckningen har inte konsekvensbedömts. Det innebär att risker kopplat till personuppgiftsbehandling inte identifieras och åtgärdas på det sätt som krävs enligt dataskyddsförordningen vilket i sig innebär en hög risk.

Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?

Nej, personuppgiftsansvarig har inte identifierat samtliga personuppgiftsbehandlingar som kräver konsekvensbedömning och genomfört dessa. Detta behöver ske genom att samtliga enheter, enskilt eller i samordning med varandra, genomför tröskelanalyser utifrån de personuppgiftsbehandlingar som finns registrerade i registerförteckningen. Här bör samordning ske för att arbeta på ett effektivt sätt då varje enskild behandling inte bör bedömas för sig, utan snarare bör sikte tas på processer och att likartade behandlingar bedöms tillsammans.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Eftersom resultaten från föregående år var att inga konsekvensbedömningar fastställts, skiljer sig årets resultat på så vis att två fastställts och två till är nära ett fastställande vilket ska ses som en positiv riktning och i jämförelse ett bättre resultat. Dock utgör frånvaron av fler konsekvensbedömningar och till viss del en bristande kunskap om behovet av att genomföra konsekvensbedömning en fortsatt omfattande brist.

Dataskyddsombudets bedömning samt rekommendationer

Bedömningen på området konsekvensbedömning avseende dataskydd är att bristerna är allvarliga eftersom avsaknaden av konsekvensbedömningar innebär att majoriteten av högriskbehandlingarna fortgår utan att verksamheterna på ett adekvat sätt dokumenterat ställningstaganden och åtgärder för att mildra riskerna som personuppgiftsbehandlingen innebär. Att inte genomföra konsekvensbedömningar när så är nödvändigt leder dels till att personuppgiftsansvarig inte lever upp till kraven som ställs specifikt i artikel 35, men heller inte till principen om integritet och konfidentialitet, och brister även i efterlevnaden av ansvarsskyldigheten i att visa hur man lever upp till säkerhetskraven i artikel 32.

Åtgärder som föreslås för att läka bristerna på detta område är:

- en tydligare och mer aktiv styrning på området
- utbildningstillfällen ledda av exempelvis DSO och ISAM för att hjälpa verksamheterna att komma igång med processen
- samordning mellan enheter för att möjliggöra gemensamma konsekvensbedömningar för liknande personuppgiftsbehandlingar

- chefer kan med fördel begära om att ta del av motsvarande verksamheters konsekvensbedömningar från andra förvaltningar som lärande exempel

4. Den registrerades rättigheter

Bakgrund och syfte

Den registrerade har ett antal rättigheter enligt GDPR. Den registrerade kan bland annat begära tillgång (registerutdrag), rättelse eller radering. Den som är personuppgiftsansvarig har att tillmötesgå en begäran enligt de krav som finns.

Syftet med detta rapporteringsområde är att kontrollera huruvida det finns ändamålsenliga mallar samt rutiner för besvarande av rättighetsbegäran, huruvida inkomna begäranden har hanterats inom den tidsram som finns att förhålla sig till samt huruvida svaren till de registrerade, baserat på ett antal stickprov, uppfyller lagkraven.

Kontroller och iakttagelser gjord av dataskyddsombudet

Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?

Rutin för hanteringen av registrerades rättigheter finns och har också reviderats under hösten för att kvalitetssäkra innehållet. Mallar är framtagna men ännu inte publicerade och ligger för godkännande hos ansvarig chef, men kommer inom kort att tillgängliggöras för hela förvaltningen.

Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?

Tre begäranden har kommit in och behandlats under året. Två gällande rätten till tillgång (registerutdrag) och en begäran som avsåg rätten att invända mot behandling.

Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?

Samtliga.

Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?

Av de två begäranden som ännu inte gallrats av integritetsskäl så har svaren levt upp till de lagkrav som finns.

Dataskyddsombudets jämförelse med föregående års resultat

Skiljer sig resultatet åt från föregående år och hur i så fall?

Nej, resultatet skiljer sig inte från föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Antalet inkomna begäranden har varit få till antalet men har hanterats på ett korrekt sätt. En av dem innebar behov av samordning inom hela socialtjänsten vilket genomfördes på ett bra sätt med kommunikation mellan cheferna, dataskyddssamordnare och medarbetare. Dataskyddssamordnare utvecklade under processen ett verktyg för att på ett effektivt sätt följa upp de informationsmängder som kontrollerats.

Rekommenderad åtgärd inför nästa år är att hanteringen på ett tydligare sätt övergår från DSO till verksamheterna och ansvariga chefer,

5. Personuppgiftsincidenter

Bakgrund och syfte

Med begreppet personuppgiftsincident avses 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.

Om en inträffad personuppgiftsincident medför en risk för fysiska personers rättigheter och friheter ska den anmälas till Integritetsskyddsmyndigheten (IMY) inom 72 timmar från upptäckt. Om personuppgiftsincidenten sannolikt leder till hög risk för de registrerade måste de informeras utan onödigt dröjsmål.

Om en personuppgiftsincident inte bedöms vara anmälningspliktig ska den dokumenteras.

Syftet med detta rapporteringsområde är att kontrollera huruvida det säkerställs att samtliga medarbetare har den kunskap som krävs om personuppgiftsincidenter, huruvida det finns ändamålsenliga rutiner för att hantera händelser som kan utgöra personuppgiftsincidenter och huruvida dessa rutiner följs.

Kontroller och iakttagelser gjord av dataskyddsombudet

Antalet inrapporterade personuppgiftsincidenter skiljer sig inte på något betydande sätt från tidigare år. Resultatet av granskningen av dokumentationen kring personuppgiftsincidenter skiljer sig inte heller på något betydande sätt, vilket innebär att det fortsatt finns brister på området. För varje inrapporterad incident kontrolleras kvalitén på rapportering, huruvida den rapporterats i tid, om den anmälts till IMY och om det överlag hanterats på ett korrekt sätt. Tidigare år skickades en enkät ut till cheferna med syfte att genomföra en kvalitativ granskning av dokumentationen av personuppgiftsincidenter. Svarsfrekvensen var dock för låg för att resultaten skulle kunna användas.

Påminnelse behöver gå ut till samtliga chefer att dataskyddsombudet alltid ska kontaktas i händelse av en personuppgiftsincident då detta brister i många fall vilket leder till merarbete.

Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?

Den enda återkommande åtgärden för att säkerställa att samtliga medarbetare har den kunskapen är genom den obligatoriska grundutbildningen i dataskydd som ska genomföras årligen. I en granskning av hur många som genomfört utbildningen visade det sig att vid datumet 3 november 2025 hade ca 11 % av stadsdelens medarbetare och chefer genomfört utbildningen. Även om det under granskningsdatumet fortsatt fanns utrymme att genomföra utbildningen under året, och att vissa verksamheter väljer att genomföra det gemensamt på exempelvis APT anser dataskyddsombudet att slutsatsen kan dras att deltagandet är för lågt och utgör en risk för att hanteringen av exempelvis personuppgiftsincidenter inte sker på korrekt sätt, eller ens uppmärksammas.

Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?

Denna kontrollfråga har delats upp i två i riskmatrisen som återfinns tidigare i rapporten. På frågan huruvida det finns ändamålsenliga rutiner är dataskyddsombudets uppfattning att så är fallet – dessa utgörs av ett rutindokument, en checklista och mallar för olika typer av beslut kopplat till personuppgiftsincidenter samt en mall för information till registrerade. Även detta vore bra att visa och gå igenom med chefer, inte minst för att det sedan den nya chefsorganisationen tillsattes har tillkommit nya chefer och ändring har också gjorts i delegationsordningen som gör att även områdeschefer har mandat att besluta om och anmäla incidenter.

Det som utgör brist på detta område är fortsatt kvalitén på dokumentationen av personuppgiftsincidenter. GDPR ställer specifika krav på vilka frågor som behöver besvaras för att underlaget ska anses vara komplett.

Hur många personuppgiftsincidenter har dokumenterats under året?

30

Hur många personuppgiftsincidenter har anmälts till IMY under året?

20

Dataskyddsombudets jämförelse med föregående års resultat

Resultatet vad gäller antalet incidenter, antal incidenter som rapporterats i tid, antalet som rapporterats till IMY eller dokumentationens kvalitet skiljer sig inte avsevärt från föregående år. Siffrorna visar fortsatt ett behov av förbättring i de flesta avseenden av hanteringen.

Dataskyddsombudets bedömning samt rekommendationer

Sammanfattningsvis kan sägas att dokumentationen av en personuppgiftsincident bland annat ska innehålla information om vad som har hänt, varför det har hänt och vilka personuppgifter som är påverkade. Den ska även innehålla konsekvenser för de registrerade och de åtgärder som förvaltningen har vidtagit för ett minska konsekvenserna. Förvaltningen bör även dokumentera skälen för de beslut som fattats med anledning av personuppgiftsincidenten. Det bör framgå varför man bedömt att en incident inte ska anmälas eller varför registrerade inte ska informeras.

Allt detta är krav som ställs i lagstiftningen. Av de beskrivna åtgärderna ovan så görs bedömningen att förbättringar behöver ske på alla områden för att nämnden ska anses uppfylla kraven i Dataskyddsförordningen.

För att det ska ske rekommenderas följande:

- Cheferna följer upp att alla medarbetare genomgått grundutbildningen i dataskydd (oavsett om det sker enskilt eller i grupp)
- Utbildningstillfälle lett av DSO med genomgång av tillgängliga stöddokument
- Fortsatt feedback till rapportörer och chefer vid tillfället för rapporteringen de gånger som dokumentationen inte är fullständig

6. Överföring till tredje land

Bakgrund och syfte

För att säkerställa att den nivå av skydd för personuppgifter som ställs i GDPR inte undergrävs får överföringar av personuppgifter till länder utanför EU/EES (tredje land) endast ske under särskilda förutsättningar. Det innebär att sådan överföring måste stödjas på antingen ett beslut från EU-kommissionen om att landet ifråga upprätthåller en adekvat skyddsnivå, att överföringen omfattas av en lämplig skyddsåtgärd eller i särskilda undantagsfall. Vidare behöver även kompletterade skyddsåtgärder, utöver de lämpliga skyddsåtgärderna, vidtas i vissa fall.[1]

Syftet med detta rapporteringsområde är att rapportera huruvida personuppgiftsansvarig har identifierat de tredjelandsöverföringar som utförs, huruvida personuppgiftsansvarig tillämpar överföringsverktyg på de tredjelandsöverföringar som utförs och om nödvändiga bedömningar har gjorts avseende tredjelandsöverföringarna.

Kontroller och iakttagelser gjord av dataskyddsombudet

Kontroller om huruvida det förekommer tredjelandsöverföringar har gjorts genom att söka igenom registerförteckningen, genomförda samt pågående konsekvensbedömningar och PUB-avtal.

Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?

Eftersom förvaltningen ännu inte genomfört informationsklassningar för de system som används är det svårt att utesluta att tredjelandsöverföringar skulle kunna förekomma som ännu inte identifierats.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

Överföringen som sker kopplat till Meta-företagen grundar sig på adekvansbeslut från 2023.

Har nödvändig bedömning, ”Transfer Impact Assessment” (TIA), gjorts avseende tredjelandsöverföringarna?

Ingen TIA har genomförts av stadsdelsförvaltningen, den överföring som sker grundar sig på adekvansbeslutet från 2023.

Dataskyddsombudets jämförelse med föregående års resultat

Detta rapporteringsområde är nytt för i år och det finns därför inget resultat från föregående år att jämföra med.

Dataskyddsombudets bedömning samt rekommendationer

Många av de verksamhetssystem som används inom förvaltningen har upphandlats och förvaltas centralt i staden. Exempel finns på system där tredjelandsöverföring förekommer, där man gjort nödvändiga bedömningar i form av Transfer Impact Assessment.

Staden har tidigare, genom juridiska avdelningen, trots adekvansbeslutet 2023 kommunicerat en restriktiv hållning när det kommer till tredjelandsöverföringar även där detta beslut är gällande. Stadsdelsförvaltningen kan i linje med detta fortsätta ställa krav på att

[1] Europeiska dataskyddsstyrelsens (EDPB) Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överenstämmelsen med EU-nivån för skydd av personuppgifter, Version 2.0, Antagna den 18 juni 2021.

personuppgifter ska lagras och behandlas inom EU/EES, och i de fall detta inte är möjligt behöver leverantören visa på adekvata skyddsåtgärder

Rekommendationen på detta område är att fortsatt alltid beakta frågan om tredjelandsöverföring vid upphandlingar och val av IT-system, samt att tidigt inkludera dataskyddsombudet i alla processer som kan innebära att övervägningar kring tredjelandsöverföring kan behöva ske.

Bilaga 2 – Andra genomförda granskningar och omvärldsbevakning

Andra granskningar som dataskyddsombudet har genomfört under året

Mot bakgrund av ordinarie dataskyddsombuds frånvaro mellan januari-september har huvuddelen av de granskningar som genomförts skett mellan september-december. Prioriteringar har behövt ske vilket inneburit vissa avsteg från årshjulet. De granskningar som har prioriterats och genomförts under hösten har bland andra varit följande.

1. Dataskyddsombudets enkät till enhetschefer om dataskyddsarbetet 2025

Enkäten bestod av två frågor:

1. Har din enhet genomfört eller planerar att genomföra några av följande åtgärder under 2025:

   - Uppdatering eller kontroll av befintliga registreringar i Draftit Privacy Records (registerförteckningen)

   - konsekvensbedömning av högriskbehandlingar

   - tekniska eller organisatoriska åtgärder för att öka säkerheten kring personuppgiftsbehandlingar (t.ex. upprätta/uppdatera lokala rutiner, genomföra informationsklassningar, se över fysisk säkerhet kring hantering av handlingar, genomföra utbildningar etc.)

2. Upplever du att du idag har tillräcklig kunskap om dataskydd/GDPR för att göra bedömningar och/eller vid behov stötta medarbetare i frågor om att behandla personuppgifter i det dagliga arbetet?

   Om nej, vilken typ av stöd skulle du önska mer av? T ex utbildningar, stöd från dataskyddsombud/dataskyddssamordnare, tydligare rutiner/checklistor m.m.

Svarsfrekvensen bland svarande chefer var omkring 40 %.

Resultatet av fråga ett visade att majoriteten av de svarande inte genomfört eller planerade att genomföra någon av åtgärderna som framgår av fråga ett. Övriga beskrev att åtgärder planerades samt var under genomförande, samt att rutiner uppdateras kontinuerligt utifrån uppkomna händelser såsom personuppgiftsincidenter.

Resultatet av fråga två var att en majoritet önskade mer stöd från DSO, tydligare rutiner och önskemål kom även kring förtydliganden gällande dataskyddssamordnarnas roll. Ett antal svarande uppgav att de hade tillräcklig kunskap om dataskydd för det dagliga arbetet.

2. Fördjupad granskning av registerförteckningen

I genomgången av registerförteckningens nästan samtliga registreringar visade resultatet på både många goda exempel där verksamheterna kommit långt och svarat på alla obligatoriska frågor. Dock visade granskningen även på att det finns en ansenlig mängd registreringar som

avser högriskbehandlingar där arbetet inte kommit tillräckligt långt och man inte har svarat på de obligatoriska frågorna. Detta behöver åtgärdas omgående. Att förvaltningen inte dokumenterat kring vare sig ändamål, hur personuppgiftsbehandlingarna behandlas, vilket lagstöd man har eller vilka säkerhetsåtgärder som behandlingarna omgärdas av blir extra bekymmersamt när det just handlar om behandlingar som avser stora mängder känsliga personuppgifter. Behandlingarna avser även personer som befinner sig i särskilt utsatta positioner såsom barn, funktionsvarierade, äldre och i övrigt sårbara positioner. Ansvariga chefer har under hösten fått feedback från dataskyddsombudet på sina registreringar

3. Antal som genomfört den obligatoriska utbildningen i dataskydd och informationssäkerhet

Kontroll har genomförts av hur många som genomgått den obligatoriska grundutbildningen i dataskydd som ska genomföras årligen. Resultatet från slutet av november visade på att enbart 11 % av förvaltningens medarbetare genomfört utbildningen.

4. Granskning sociala medier-konton

Två av förvaltningens sociala medier-konton granskades för att se huruvida profilerna innehöll länkar till den nödvändiga informationen till registrerade om personuppgiftsbehandling. De granskade kontona som inte innehöll rätt information fick återkoppling och åtgärdade.

Dataskyddsombudets rekommendationer baserat på iakttagelserna ovan

Dataskyddsombudets rekommendationer
1. Utbildning ledd av DSO med genomgång av tillgängligt stödmaterial för att säkerställa att alla känner till de rutiner och riktlinjer som redan finns upprättade. Fortsätt vidareutveckla befintliga stöd och styrdokument, samt stötta i utveckling och framtagande av mer verksamhetsspecifika rutiner utefter behov. **2.** Uppföljning under 2026 av de åtgärder som vidtagits efter återkopplingen som gavs till verksamheterna efter höstens granskning. **3.** Rekommendation att chefer ser över hur de kan säkerställa att alla medarbetare genomför den obligatoriska grundutbildningen.

Omvärldsbevakning

Resultatet av dataskyddsombudets omvärldsbevakning i korthet

- Integritetsskyddsmyndigheten (IMY) har inlett en tillsyn mot Miljödata i Karlskrona AB. Tillsynen pågår. IMY har även inlett tillsyn mot Region Västmanland, Älmhults kommun och Göteborgs stad. Tillsynerna mot Region Västmanland, Älmhults kommun och Göteborgs stad granskar huruvida de vidtagit lämpliga tekniska och organisatoriska åtgärder enligt dataskyddsförordningen, GDPR. Granskningen avser åtgärder för att säkerställa en lämplig säkerhetsnivå i förhållande till riskerna med den behandling av personuppgifter som skett i Miljödatas system. Det blir mycket viktigt för nämnden och staden i sin helhet att ta del av resultaten i dessa tillsyner.

- Den 1 april 2025 började nya kameraregler att gälla. De innebär att ingen längre behöver söka tillstånd hos Integritetsskyddsmyndigheten (IMY) för sin bevakning. Istället införs nya krav på framför allt offentlig verksamhet som kamerabevakar eller planerar att bevaka. Enligt IMY innebär reglerna nya krav på bland annat kommuner, regioner och myndigheter att själva säkerställa att deras bevakning är tillåten. De behöver nu upprätta dokumenterade intresseavvägningar för all sin bevakning och registrera sin bevakning i en förteckning.

- NIS2, EU:s nya direktiv för att höja cybersäkerheten ersätter det äldre NIS-direktivet, med syfte att stärka skyddet för samhällsviktiga tjänster genom tydligare krav på riskhantering, incidentrapportering och utökad omfattning till fler sektorer, implementeras i Sverige som cybersäkerhetslagen och träder i kraft 15 januari 2026. Lagen omfattar fler typer av organisationer än tidigare lagstiftning, däribland kommuner och ställer högre krav på informationssäkerhet.

Övrigt att rapportera/övriga observationer

I dataskyddsombudets mening är ett ökat samarbete mellan förvaltningar och bolag och staden i stort att anse som positivt för kvalitet, likvärdighet och effektivitet när det kommer till arbetet med personuppgiftshantering. Att vi idag i hög utsträckning arbetar separat i vad som torde vara mycket liknande processer över staden på grund av vårt egna personuppgiftsansvar är att inte ta tillvara på resurserna på bästa sätt. Det sker redan ett gott samarbete i många processer, men samarbetsformer och gemensam styrning bör kunna utvecklas än mer.

Något som bör lyftas är behovet av en säkrare lösning för e-postanvändning när det kommer till känsliga personuppgifter och sekretesskyddad information. Det finns bestämmelser i staden som är tydliga med att denna typ av information inte ska skickas med vanlig e-post (orkypterad), men erfarenhet och observationer gör tydligt att så sker över förvaltningen. Det är starkt efterfrågat från chefshåll att få tillgång till en säker (krypterad) e-posttjänst för att på ett bättre sätt kunna skydda informationen. Rekommendationen är därför att prioritera detta under 2026.

Det är viktigt att dataskyddsombudet blir involverad tidigt i alla processer såsom upphandlingar, införande av IT-system eller andra förändringar som innebär att personuppgifter ska behandlas, särskilt om det handlar personuppgiftsbehandlingar i stor omfattning. Detta för att dataskyddsombudet ska kunna stötta i de bedömningar som behöver göras och ge rekommendationer när det behövs. Det är också viktigt att det alltid upprättas PUB-avtal i de fall det finns behov av detta, men att det också föregås av en grundlig genomgång av vilka personuppgifter som ska behandlas, med vilka syften och uppdelningen mellan parterna vilket bör ske i samråd med dataskyddsombudet.

Rekommenderas att granska följande under nästkommande år, baserat på årets resultat samt vad som inte hunnit prioriteras:

- Hur arbetet framskrider med tröskelanalyser och konsekvensbedömningar
- Information till registrerade
- Personuppgiftsincidenter – fortsatt granskning av dokumentationen kring incidenter
- Stickprov i verksamhetssystem utifrån uppgifts- och lagringsminimering