Stockholms stad

Bilaga 7
till VB 2025

GDPR årsrapport

År 2025

Farsta stadsdelsnämnd

GDPR årsrapport
Januari 2026

Dnr: FAR 2026/10
Kontaktperson: Christer Bergman

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 Farsta stadsdelsnämnds dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

Under 2025 har rollen som dataskyddsombud hanterats av tre olika personer där ingen överlämning skett mellan byte av dataskyddsombud. Det gör det svårt för DSO att få en helhet av vad som skett under året. DSO rekommenderar att PuA ska sträva efter att kontinuitet i rollen och få en stabilitet i arbetet.

DSO rekommenderar PuA att alltid involvera DSO vid personuppgiftsincidenter. DSO besitter specialkunskap och kan komma med värdefulla rekommendationer vilket bör tas till vara på.

DSO skulle starkt rekommendera att det utsågs en dataskyddshandläggare på förvaltningen som kan samordna och genomföra det arbetet som krävs med registerförteckningen och framtagandet av rutiner.

De tre största riskerna enligt dataskyddsombudets bedömning

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?	🟡	*En fullständig registerförteckning är inte bara ett krav utan utgör också grunden för resten av dataskyddsarbetet. DSO rekommenderar PuA att utse en dataskyddshandläggare som färdigställer registerförteckningen.*
Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?	🟠	*Information om att hantera personuppgiftsincidenter har gått ut till chefer som ansvarar för att föra informationen vidare till sina medarbetare. Ingen uppföljning sker. DSO rekommenderar PuA att utöka informationsinsatser för att säkerställa kunskapen om vad som är en personuppgiftsincident och hur den ska hanteras.*
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning	🟠	Behovet av konsekvensbedömningar för personuppgiftsbehandlingar med stora mängder känsliga personuppgifter är fortsatt stort. DSO rekommenderar PuA att färdigställa arbetet med

avseende dataskydd görs samt genomfört detta?		registerförteckningen och identifierar alla behandlingar som kräver en konsekvensbedömningar.

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

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

Registerförteckningen innehåller poster från olika verksamhetsområden och en stor anledning till att en stor del av registerförteckningen fortfarande är ofullständig är personalrelaterat. Under 2025 har tre olika personer varit dataskyddsombud och en stor del av året har ingen dataskyddshandläggare funnits på plats. Det är ingen som har kunna genomföra det fysiska arbete som registerförteckningen kräver, till exempel att granska och begära in kompletteringar. Rutiner för att föra och uppdatera registerförteckningen finns på plats men då inga poster tillkommit på över ett år finns det stor risk att rutinerna inte följs.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?	🟡	*Det finns 96 registerposter i Draftit varav 65 är markerade som godkänd. 31 behandlingar är alltså under arbete.*
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?	🟢	*Rutiner för registrering i Draftit finns.*
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?	🟡	*Under 2025 har ingen ny post i registerförteckningen tillkommit. Det är osannolikt att ingen ny behandling har tillkommit under året. Förvaltningen behöver bli bättre på att föra in nya personuppgiftsbehandlingar i registerförteckningen. Det är också 31 behandlingar som är under arbete och behöver antingen kompletteras eller färdigställas.*

Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		*Ett antal poster är fortfarande under bearbetning och är inte fullständiga.*

Säkerhet i samband med behandlingen

Sammanfattning

Dataskyddsombudet deltar vid samtliga informationsklassningar och anser att det finns tillräckligt med dokumentation.

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?		*Dataskyddsombudet närvarar vid samtliga informationsklassningar*
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		*DSO bedömer att det finns tillräkligt med stöd.*
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		*Ja*

Konsekvensbedömning avseende dataskydd

Sammanfattning

Rutiner för att genomföra en konsekvensbedömning finns från staden. Vid granskning av registerförteckningen konstaterar DSO att ingen behandling någon risk angiven.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		*Nej*
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		*Nej*
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		*Ja*
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		*Ja*
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		*Delvis*

Den registrerades rättigheter

Sammanfattning

Det saknas rutiner för att hantera begäran om registerutdrag. Dock finns en mall för att svara på begäran. Den begäran som inkommit till förvaltningen under året har kunnat hanteras korrekt.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		*Det finns en mall för att besvara en begäran. Det finns dock ingen rutin för att hantera en begäran.*
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		*Under 2025 kom det in en begäran om registerutdrag.*
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		*Samtliga begäran besvarades inom en månad*
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		*Ja*

Personuppgiftsincidenter

Sammanfattning

Förvaltningen är relativt bra på att rapportera incidenter. Det tyder på att rutinerna för att rapportera personuppgiftsincidenter är åtminstone relativt spridda på förvaltningen. Dock är det vissa verksamheter som är bättre på att rapportera incidenter vilket kommer att kräva en utbildningsinsats. DSO gissar att antal incidenter ute på förvaltningen är större och att fler incidenter borde anmälas till IMY.

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?		*Information om att hantera personuppgiftsincidenter har gått ut till chefer som ansvarar för att föra informationen vidare till sina medarbetare. Ingen uppföljning sker.*
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		*Nej*
Hur många personuppgiftsincidenter har dokumenterats under året?		*44 personuppgiftsincidenter har rapporterats under2025*
Hur många personuppgiftsincidenter har anmälts till IMY under året?		*6 incidenter rapporterades till IMY enligt vad DSO kan se i diariet. Det borde vara fler.*

Överföring till tredje land

Sammanfattning

En tredjelandöverföring till Storbritannien har identifierats under året vilket omfattas av beslut om adekvat skyddsnivå.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		*Ja, en tredjelandöverföring har identifierats*
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		*Nej*
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		*Nej då överföringen omfattas av ett adekvansbeslut*

Bilagor

Bilaga 1: Detaljerad redovisning av dataskyddsombudets granskning

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

Under 2025 fanns 96 behandlingar registrerade och det finns rutiner på plats för nya eller förändrade behandlingar. Registerförteckningen uppdateras inte i den omfattning som krävs. Under året har inga nya behandlingar tillkommit. När registerposten markeras som godkänd i registerförteckningen har alla obligatoriska frågor besvarats. Det finns dock ett flertal poster som fortfarande är under arbete.

Dataskyddsombudets jämförelse med föregående års resultat

Förra årets rapport identifierade några brister och förbättringar från året innan. Årets granskning visar att det fortfarande krävs en del arbete med registerförteckningen. Antalet konsekvensbedömningar har ökat under året men behovet av konsekvensbedömningar för personuppgiftsbehandlingar med stora mängder känsliga personuppgifter är fortsatt stort.

Dataskyddsombudets bedömning samt rekommendationer

Många av de brister som har identifierats vid granskningen har att göra med brist på ansvariga. Under året har det funnits tre dataskyddsombud och även om det fanns en dataskyddshandläggare under en del av året har den rollen saknats under en del av året. DSO rekommenderar PuA att få en kontinuitet i rollerna och snarast ser till att det finns en dataskyddshandläggare på plats för färdigställa arbetet med registerförteckningen.

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. DSO har deltagit på stadsgemensamma klassningar där diskussionerna har påvisat svårigheter med stadens interna hantering av pub-avtal.

Dataskyddsombudets jämförelse med föregående års resultat

Granskningen visar att flera av de system som är informationsklassade saknar svar på flera organisatoriska eller tekniska säkerhetsåtgärder, alternativt att informationsklassning som pågår fastnad på samma grunder och att detta beror på bristande information från systemägare/leverantör. Ofta handlar det om system som staden, genom ansvarig facknämnd, tagit in och implementerat och där stadsdelarna förväntas börja använda systemet utan att en lokal klassning har hunnit genomföras. När de lokala klassningarna påbörjas är systemet ofta

redan infört och det PuA beskriver är att det har varit svårt att få svar på de frågor som ställs i klassningen. Det försvårar PuAs möjligheter att vidta lämpliga organisatoriska och tekniska skyddsåtgärder för att skydda personuppgifter.

Dataskyddsombudets bedömning samt rekommendationer

DSO rekommenderar PUA att initiera och föra dialog med facknämnderna när det gäller informationsklassningar (och vidta rätt tekniska och organisatoriska säkerhetsåtgärder) för att säkerställa att PUA lokalt kan säkerställa att rätt åtgärder har vidtagits för att skydda personuppgifter i enlighet med befintlig lagstiftning. DSO rekommenderar även PUA att höja tempot i informationsklassningar av de verksamhetssystem/processer som finns i organisationen. Prioriteringen bör utgå från parametrar som känsliga personuppgifter, mängd personuppgifter och eventuell tredjelandsöverföring. Därefter bör klassningarna påbörjas och organisatoriska och tekniska skyddsåtgärder vidtas i syfte att leva upp till kraven i Dataskyddsförordningen avseende skydd för personuppgifter. DSO rekommenderas att under året inventera behovet av pub-avtal i alla behandlingar som görs. DSO rekommenderar även PUA att fortsätta ligga på stadsledningskontoret kring behovet av att tydliggöra hur stadens nämnder och bolag ska förhålla sig till frågor om interna pub-avtal (alternativt PUA-PUA situationer).

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 utfös 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

Dataskyddsombudets jämförelse med föregående års resultat

Antalet konsekvensbedömningar har ökat under året men behovet av konsekvensbedömningar för personuppgiftsbehandlingar med stora mängder känsliga personuppgifter är fortsatt stort.

Dataskyddsombudets bedömning samt rekommendationer

DSO rekommenderar PuA att få en kontinuitet i rollerna och snarast ser till att det finns en dataskyddshandläggare på plats för att komplettera med nödvändiga rutiner och nödvändig inventering.

DSO rekommenderar PUA att omedelbart initiera ett arbete med att identifiera och genomföra konsekvensbedömningar för de behandlingar som bedöms behöva det.

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

Det saknas rutiner för att hantera en begäran av registerutdrag.

Dataskyddsombudets jämförelse med föregående års resultat

DSO kan inte se någon förändring från föregående år.

Dataskyddsombudets bedömning samt rekommendationer

DSO rekommenderar PuA att snarast se till att det finns en dataskyddshandläggare på plats för att färdigställa nödvändiga rutiner.

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

DSO kan konstatera att det rapporterats 44 incidenter under 2025. Dock har bara sex av dem rapporterats till IMY vilket är orimligt. Det noteras att det fortsatt är vissa enheter som rapporterar mycket medan andra verksamheter knappt rapporterat något. Det finns anledning att tro att det beror på en okunskap i de verksamheter som rapporterar färre incidenter snarare än en bristfällig hantering i de verksamheter som rapporterar många. Det saknas idag också en systematik i hur man ska följa upp rapporterade incidenter. Det är viktigt att verksamheten ser incidenter som ett tillfälle att identifiera och åtgärda eventuella brister i verksamheter för att säkerställa att det finns ett lärande i detta.

Dataskyddsombudets jämförelse med föregående års resultat

Förra året rapporterades 43 incidenter och i år rapporterade 44 incidenter. Dock anmäldes 20 färre till IMY jämfört med förra året.

Dataskyddsombudets bedömning samt rekommendationer

Antal incidenter som rapporterats det här året var ungefär samma som förra året dock anmäldes 20 färre till IMY. Det skulle kunna tyda på att förvaltningen behöver förnyad information om personuppgiftsincidenter och rutinen för att hantera dem. I rutinen framgår även att incidenterna ska skickas till förvaltningens registratur. Det skulle kunna vara att antal anmälda incidenter under året är större än sex, men inte har diarieförts.

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

Under året har en tredjelandsöverföring identifierats. Den skedde till Storbritannien och omfattas av adekvansbeslut.

Dataskyddsombudets bedömning samt rekommendationer

Det är av stor vikt att DSO underrättas om eventuella upphandlingar, rådfrågas vid framtagande av PUB-avtal och deltar vid klassningar för att säkerställa att eventuella tredjelandsöverföringar sker säkert.

[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.