Stockholms stad

Bilaga 9

GDPR årsrapport

2025

Kungsholmens stadsdelsnämnd

GDPR årsrapport 2025

Dnr: KUNG 2025/556

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

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

Se bilaga 1.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade? *209*		Se rekommendation nedan.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		Att dataskyddshandläggare utses i enlighet med den lokala anvisningen för informationssäkerhet.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		Att se över behovet av en övergripande rutin för hur registerförteckningen ska samordnas och hållas aktuell.
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		Se ovan rekommendationer.

Säkerhet i samband med behandlingen

Se bilaga 1.

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?		
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		

Konsekvensbedömning avseende dataskydd

Se bilaga 1.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		Förtydliga lokal anvisning för informationssäkerhet avseende ansvar för tröskelanalys och konsekvensbedömning.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		Se rekommendation ovan.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		Se rekommendation ovan.
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		Se rekommendation ovan.

Den registrerades rättigheter

Se bilaga 1.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade? En (1) begäran.		
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		

Personuppgiftsincidenter

Se bilaga 1.

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?		
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		
Hur många personuppgiftsincidenter har dokumenterats under året? 21 incidenter har rapporterats.		
Hur många personuppgiftsincidenter har anmälts till IMY under året? 3		

Överföring till tredje land

Se bilaga 1.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		

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

Antal behandlingar som är registrerade?

I registerförteckningen finns 209 stycken behandlingar registrerade.

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

I den lokala anvisningen för informationssäkerhet (KUNG 2023/163) anges roller och organisation för förvaltningens informationssäkerhetsarbete inklusive dataskydd. I anvisningen framkommer att chef har ansvar för att säkerställa att registervård görs inom sitt verksamhetsområde samt att uppdatera och följa upp stadsdelsförvaltningens registerförteckning. Vidare anges att det ska finnas dataskyddshandläggare som bland annat har till uppgift att ansvara för att samordna och sammanställa avdelningens och verksamheternas registerförteckning. [1]

Delar av förvaltningen har en utsedd funktion som har ansvar för att samordna arbetet med att hålla registerförteckningen aktuell och uppdaterad. Funktionen dataskyddshandläggare är inte fullt ut införd. Därmed kan det finnas en risk för att registerförteckningen inte hålls aktuell. Därtill beskriver inte den lokala anvisningen arbetsgången i praktiken avseende hur nya eller förändrade personuppgiftsbehandlingar ska registreras.

[1] Lokal anvisning för informationssäkerhet KUNG 2023/163 s. 7,11.

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

Förvaltningens registerförteckning förs i ett Exceldokument per avdelning, eller tillsammans med en annan avdelning, som förvaras lokalt. Delar av registerförteckningen har under året uppdaterats. Delar av förvaltningen anger att en översyn eller uppdatering kommer att göras.

I och med att registerförteckningen inte har setts över i sin helhet kan det finnas risk för att nya eller förändrade behandlingar av personuppgifter inte har dokumenterats.

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

Det finns behandlingar där samtliga obligatoriska områden inte är besvarade. Kraven enligt artikel 30 är inte fullt ut uppfyllda.

Dataskyddsombudets jämförelse med föregående års resultat

Det har under året tillkommit några fler behandlingar jämfört med föregående år (200 behandlingar registrerade 2024) men det är marginellt. Förvaltningen har under året sett över möjligheten att införa ett system för att samla registerförteckningen. Förvaltningen inväntar det arbete som pågår för staden gemensamt.

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

Hela registerförteckningen har inte setts över under året och det skiljer sig mot föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Registerförteckningen är ett centralt dokument för förvaltningens dataskyddsarbete, för att ha uppsikt över de personuppgiftsbehandlingar som personuppgiftsansvarig utför. Det är därför av vikt att registerförteckningen hålls aktuell.

Det är positivt att förvaltningen under året har sett över möjligheten att samla registerförteckningen i ett system, då det kan underlätta dataskyddsarbetet och skapa en bättre överblick över de behandlingar som görs.

Dataskyddsombudets rekommendation:

- Att dataskyddshandläggare utses i enlighet med den lokala anvisningen för informationssäkerhet.
- Att se över behovet av en övergripande rutin för hur registerförteckningen ska samordnas och hållas aktuell.

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?

Stickprov har genomförts. Stickproven har visat att informationsklassningarna tar hänsyn till olika kategorier av personuppgifter.

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

Stadens mall för klassningsprotokoll utgör ett gott stöd. Det finns därutöver information på intranätet om ställningstagande om personuppgifter i samband med klassningar, såsom exempelvis gällande konsekvensbedömning.

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

Information finns tillgänglig på intranätet och används inom förvaltningen vid informationsklassningar.

Dataskyddsombudets jämförelse med föregående års resultat

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

Resultatet skiljer sig inte nämnvärt åt från föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Stadens mallar utgör ett gott stöd i arbetet med informationsklassningar avseende personuppgifter.

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 en mall som är gemensam för staden. Mallen finns tillgänglig på intranätet.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Det förefaller vara ett område att utveckla, då dataskyddsombudet inte har fått tillräckligt underlag. För att säkerställa att tröskelanalyser dokumenteras bör den lokala anvisningen för informationssäkerhet förtydligas gällande ansvar för tröskelanalyser.

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

Det finns en mall som är gemensam för staden. Mallen finns tillgänglig på intranätet. Den lokala anvisningen för informationssäkerhet skulle behöva förtydligas gällande ansvar för konsekvensbedömning.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Det har genomförts konsekvensbedömning inom exempelvis förskola och äldreomsorg. Det är oklart om konsekvensbedömningar har gjorts i samtliga berörda klassningar.

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

Se kommentarer ovan.

Dataskyddsombudets jämförelse med föregående års resultat

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

Resultatet skiljer sig inte nämnvärt åt från föregående år. Konsekvensbedömningar har genomförts för system inom förskola och äldreomsorgen.

Dataskyddsombudets bedömning samt rekommendationer

Konsekvensbedömning är ett område som fortsatt behöver prioriteras.

Dataskyddsombudets rekommendation:

- Förtydliga lokal anvisning för informationssäkerhet avseende ansvar för tröskelanalys och konsekvensbedömning.

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?

Det finns vägledning och rutiner till stöd för att på ett säkert sätt efterleva kravet på enskildas rättigheter.

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

Under 2025 har en begäran om registerutdrag inkommit.

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

Begäran har hanterats inom en månad.

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

Ja.

Dataskyddsombudets jämförelse med föregående års resultat

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

Det är försumbart färre begäran om registerutdrag mot föregående år (tre).

Dataskyddsombudets bedömning samt rekommendationer

Kunskapen om rättigheterna och befintliga rutiner säkerställs bland berörda medarbetare.

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

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

Stadens obligatoriska utbildning om dataskydd ska säkerställa att samtliga medarbetare har information. Därtill har varje chef möjlighet att följa upp att medarbetare genomgår utbildning.

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

Personuppgiftsincidenter rapporteras i incidentrapporteringssystemet IA. På intranätet finns information om hur personuppgiftsincidenter ska hanteras.

Hur många personuppgiftsincidenter har dokumenterats under året?

Under 2025 har 21 personuppgiftsincidenter rapporterats.

Hur många personuppgiftsincidenter har anmälts till IMY under året?

Under 2025 har tre personuppgiftsincidenter rapporterats utav de 21 rapporterade incidenterna.

Dataskyddsombudets jämförelse med föregående års resultat

Från föregående år har fler incidenter rapporterats, utfallet 2024 var 13 anmälda incidenter mot 21 under 2025. Därmed har fler incidenter rapporterats under verksamhetsåret.

Dataskyddsombudets bedömning samt rekommendationer

Kompetensen inom dataskydd behöver fortsatt säkerställas bland samtliga användare.

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.[2]

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

Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?

Det förekommer system som medför tredjelandsöverföring. Förhållningsättet är restriktivt till tredjelandsöverföring. Registerförteckningen behöver förtydligas i detta avseende.

Dataskyddsombudets bedömning samt rekommendationer

Kompetensen inom tredjelandsöverföring behöver säkerställas bland berörda medarbetare.

[2] 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.