Stockholms stad

GDPR årsrapport

År 2025

Micasa Fastigheter

GDPR årsrapport
Januari 2026

Dnr: MIC 2026/21
Utgivningsdatum: 2026-01-15
Kontaktperson: Dejana Cecez

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 Micasa Fastigheter i Stockholm AB:s dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

Årets granskning visar att Micasa Fastigheter i Stockholm AB har etablerade grundläggande förutsättningar för att bedriva ett systematiskt dataskyddsarbete. Flera centrala komponenter finns på plats, såsom registerförteckning, informationsklassning, rutiner för personuppgiftsincidenter samt stöd för konsekvensbedömningar. Verksamheten uppvisar även en grundläggande medvetenhet om dataskyddsfrågor hos medarbetare.

Samtidigt visar granskningen att det finns utvecklingsbehov kopplade till systematik, helhetsöverblick och dokumentation, snarare än till enskilda brister i efterlevnaden. I flera delar är dataskyddsarbetet beroende av manuella moment eller enskilda funktioner, vilket innebär att risker kan uppstå vid förändrade förutsättningar, ökad komplexitet eller ny systemanvändning.

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?		*För att säkerställa att registret på ett heltäckande sätt speglar verksamhetens personuppgiftsbehandlingar rekommenderas en strukturerad översyn av befintliga registreringar samt löpande uppföljning av att förändringar i verksamheten återspeglas i registret.*
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		*Genomför en samlad kartläggning i syfte att identifiera samtliga personuppgiftsbehandlingar som kan kräva konsekvensbedömning avseende dataskydd.*
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		*Klargör om och hur överföringsverktyg tillämpas vid eventuella tredjelandsöverföringar, för att säkerställa ett tillräckligt skydd för personuppgifter.*

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

Verksamheten har ett etablerat register över personuppgiftsbehandlingar som används aktivt. Nya behandlingar har registrerats och befintliga behandlingar har reviderats under året, vilket är ett arbete som bör fortsätta och upprätthållas.

Granskningen visar samtidigt brister i hur registerföringen styrs och följs upp. Rutinerna för att säkerställa att nya och förändrade personuppgiftsbehandlingar identifieras och registreras är inte tillräckligt ändamålsenliga, och registret speglar inte fullt ut verksamhetens faktiska behandlingar. Vidare finns behov av att komplettera vissa uppgifter i registret för att säkerställa fullständighet enligt artikel 30 i dataskyddsförordningen.

För att stärka dataskyddsarbetet rekommenderas att verksamheten tydliggör och formaliserar arbetssättet för registrering av nya och förändrade personuppgiftsbehandlingar samt genomför en strukturerad översyn av befintliga registreringar i syfte att säkerställa ett heltäckande och aktuellt register.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		*Verksamheten bör fortsätta att löpande registrera personuppgiftsbehandlingar för att möjliggöra uppföljning över tid.*
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		*För att säkerställa att nya och förändrade personuppgiftsbehandlingar identifieras och registreras rekommenderas att rutinerna för registrering tydliggörs och integreras i verksamhetens ordinarie styr- och beslutsprocesser.*

Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		*För att säkerställa att registret på ett heltäckande sätt speglar verksamhetens personuppgiftsbehandlingar rekommenderas en strukturerad översyn av befintliga registreringar samt löpande uppföljning av att förändringar i verksamheten återspeglas i registret.*
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		*För att säkerställa fullständiga och enhetliga uppgifter i registret rekommenderas en strukturerad komplettering av vissa uppgifter enligt artikel 30 i dataskyddsförordningen.*

Säkerhet i samband med behandlingen

Sammanfattning

Verksamheten har ett etablerat grundarbete avseende säkerhet i samband med personuppgiftsbehandlingar, inklusive informationsklassning, styrande dokument och återkommande utbildningsinsatser.

Samtidigt visar granskningen att informationsklassningens kategorisering av personuppgifter behöver tillämpas mer enhetligt, samt att styrande dataskyddsrutiner inte är fullt ut konsekvent implementerade i praktiken. För att stärka säkerhetsarbetet rekommenderas att tillämpningen av informationsklassning förtydligas och att styrande dataskyddsrutiner används mer enhetligt i verksamheten.

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?		*Se över hur kategorisering av personuppgifter tillämpas i informationsklassningar, inklusive bedömning av om uppgifter kan vara känsliga eller integritetskänsliga, i syfte att stärka informationsklassningens stöd för fortsatt risk- och säkerhetsarbete.*
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		*Se över styrande dokument och rutiner för dataskydd i syfte att tydliggöra ansvarsfördelning och stärka det praktiska stödet till verksamheten vid tillämpning av befintliga rutiner.*
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		*Tydliggör när och av vem styrande dataskyddsrutiner ska tillämpas, exempelvis genom att integrera dem i ordinarie arbetsmoment och forum i verksamheten, för att säkerställa att dataskyddsåtgärder initieras på ett systematiskt sätt.*

Konsekvensbedömning avseende dataskydd

Sammanfattning

Verksamheten har etablerade rutiner och systemstöd för tröskelanalys och konsekvensbedömning avseende dataskydd, vilket ger förutsättningar för att identifiera och hantera behandlingar som kan innebära förhöjda risker.

Samtidigt framgår att genomförandet av tröskelanalyser och konsekvensbedömningar inte sker fullt ut systematiskt i praktiken och att det saknas en samlad säkerhet kring att samtliga personuppgiftsbehandlingar som kräver konsekvensbedömning har identifierats. För att stärka dataskyddsarbetet rekommenderas att tillämpningen av tröskelanalyser och konsekvensbedömningar integreras tydligare i verksamhetens ordinarie arbetssätt.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		*Inget att anmärka.*
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		*Integrera genomförandet av tröskelanalyser i verksamhetens befintliga arbetsprocesser så att bedömningar initieras systematiskt vid nya eller förändrade personuppgiftsbehandlingar.*
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		*Inget att anmärka.*
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		*Säkerställ att resultatet av genomförda tröskelanalyser leder till att konsekvensbedömningar initieras och genomförs när behov identifieras, exempelvis genom att detta följs upp som ett obligatoriskt steg i verksamhetens befintliga besluts- eller förändringsarbete.*
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende		*Genomför en samlad kartläggning i syfte att identifiera samtliga personuppgiftsbehandlingar som kan kräva konsekvensbedömning avseende dataskydd.*

dataskydd görs samt genomfört detta?		

Den registrerades rättigheter

Sammanfattning

Under året har inga begäranden från registrerade avseende rättigheter enligt dataskyddsförordningen inkommit till verksamheten. Hantering av rättighetsförfrågningar sker centralt via Dataskyddsgruppen och tidigare ärenden har hanterats inom föreskriven tid.

Samtidigt framgår att det saknas dokumenterade rutiner för hantering av registrerades rättigheter. Mot bakgrund av den låga ärendemängden bedöms risken i nuläget som låg, men dokumentation av befintligt arbetssätt kan bidra till ökad tydlighet och kontinuitet vid förändrade förutsättningar.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	**Risk**	**Rekommendationer**
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		*Dokumentera befintligt arbetssätt för hantering av registrerades rättighetsförfrågningar, i syfte att säkerställa kontinuitet och tydlighet vid förändrade förutsättningar.*
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		*Det har inte inkommit några begäranden under året.*
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		*Ej tillämplig, se ovan.*
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		*Ej tillämplig, se ovan.*

Personuppgiftsincidenter

Sammanfattning

Verksamheten har etablerade rutiner och genomför utbildningsinsatser för att säkerställa att medarbetare har grundläggande kunskap om hur personuppgiftsincidenter ska hanteras. Under året har inga personuppgiftsincidenter dokumenterats eller anmälts till Integritetsskyddsmyndigheten.

Samtidigt framgår att det finns behov av att säkerställa en enhetlig tillämpning av när inträffade säkerhetshändelser ska registreras och hanteras som personuppgiftsincidenter. För att stärka incidenthanteringen rekommenderas att tillämpningen förtydligas för att säkerställa konsekvens och tydlighet i verksamheten.

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?		*Fortsätt att stärka informations- och utbildningsinsatser kring personuppgiftsincidenter för att säkerställa en enhetlig medvetenhet i organisationen.*
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		*Tydliggör och följ upp hur rutiner för hantering av potentiella personuppgiftsincidenter ska tillämpas i verksamheten, så att incidenthantering initieras konsekvent när händelser uppstår.*
Hur många personuppgiftsincidenter har dokumenterats under året?		*Se över och tydliggör tillämpningen av när säkerhetshändelser ska registreras och hanteras som personuppgiftsincidenter för att säkerställa en enhetlig bedömning i verksamheten.*
Hur många personuppgiftsincidenter har anmälts till IMY under året?		*Inget att anmärka.*

Överföring till tredje land

Sammanfattning

Verksamheten utgår från stadens övergripande krav om att undvika tredjelandsöverföringar och sådana överföringar bedöms i huvudsak vara identifierade i de behandlingar som används i praktiken.

Samtidigt framgår att det finns osäkerhet kring hur tredjelandsöverföringar hanteras i vissa delar av använda tjänster, samt att nödvändiga bedömningar i form av Transfer Impact Assessment ännu inte har genomförts. För att stärka efterlevnaden rekommenderas att bedömning och dokumentation av tredjelandsöverföringar säkerställs i de fall sådana överföringar kan förekomma.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		*Se över registerförteckningens detaljeringsnivå så att den i tillräcklig utsträckning speglar hur olika delar av använda tjänster förhåller sig till tredjelandsöverföring.*
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		*Klargör om och hur överföringsverktyg tillämpas vid eventuella tredjelandsöverföringar, för att säkerställa ett tillräckligt skydd för personuppgifter.*
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		*Säkerställ att nödvändiga bedömningar av tredjelandsöverföringar, inklusive Transfer Impact Assessment (TIA), genomförs i de fall sådana överföringar kan förekomma.*

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?

Vid verksamhetsårets utgång fanns totalt 29 registrerade personuppgiftsbehandlingar i verksamhetens registerförteckning. Under 2025 registrerades fyra nya behandlingar och 22 befintliga behandlingar reviderades.

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

Dataskyddsombudet har granskat huruvida verksamheten har ändamålsenliga rutiner som möjliggör att nya eller förändrade personuppgiftsbehandlingar registreras i registerförteckningen.

Granskningen visar att det saknas tillräckligt etablerade och kända rutiner för hur nya eller förändrade personuppgiftsbehandlingar ska identifieras och anmälas för registrering. Information från verksamhetens dataskyddsarbete indikerar att processägare och andra berörda roller inte i tillräcklig utsträckning vänder sig till Dataskyddsgruppen eller dataskyddsombudet vid införande eller förändring av personuppgiftsbehandlingar.

Avsaknaden av ändamålsenliga rutiner innebär att identifiering och registrering av nya eller förändrade behandlingar i stor utsträckning riskerar att bli personberoende och osystematisk. Detta ökar risken för att personuppgiftsbehandlingar inte fångas upp i ett tidigt skede, vilket kan medföra att nödvändiga bedömningar och skyddsåtgärder inte genomförs i tid och därmed innebära risker för de registrerades rättigheter och friheter.

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

Dataskyddsombudet har granskat huruvida personuppgiftsbehandlingar registreras och uppdateras i den omfattning som krävs för att registret ska omfatta samtliga behandlingar som verksamheten utför.

Granskningen visar att befintliga personuppgiftsbehandlingar inte uppdateras konsekvent vid förändringar i verksamheten. Det förekommer att flera olika behandlingar är samlade i en och samma registrering, vilket medför att det blir otydligt vilka ändamål, lagliga grunder, system och mottagare som är kopplade till respektive behandling.

Vidare framgår att viss information i registret är ofullständig eller inte tillräckligt uppdaterad, vilket indikerar att registret inte fullt ut speglar verksamhetens faktiska personuppgiftsbehandlingar.

När personuppgiftsbehandlingar inte uppdateras konsekvent och flera behandlingar sammanförs i samma registrering finns risk för otydlighet kring hur och varför personuppgifter behandlas. Detta kan försvåra verksamhetens möjlighet att agera korrekt vid förändringar eller vid begäranden från registrerade och därigenom medföra risker för de registrerades rättigheter och friheter.

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

Dataskyddsombudet har granskat huruvida de uppgifter som är obligatoriska enligt artikel 30 i dataskyddsförordningen är besvarade för de registrerade personuppgiftsbehandlingarna.

Granskningen visar att registret i huvudsak innehåller de uppgifter som krävs enligt artikel 30. Samtidigt framgår att vissa registreringar saknar fullständig information, exempelvis avseende mottagare och gallring.

Brister i fullständigheten av registret innebär att överblicken över personuppgiftsbehandlingarna kan bli begränsad och att registret därmed inte fullt ut ger det stöd som krävs för styrning och uppföljning av dataskyddsarbetet. Sammantaget bedöms detta kunna medföra mindre risker för de registrerades rättigheter och friheter.

Dataskyddsombudets jämförelse med föregående års resultat

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

I föregående årsrapport bedömdes verksamheten ha en etablerad registerförteckning där samtliga kända personuppgiftsbehandlingar var identifierade och dokumenterade i Draftit. Samtidigt identifierades behov av kontinuerlig uppföljning, förbättrad kommunikation av rutiner och fortsatt kvalitetsutveckling.

Årets granskning bekräftar att registret fortsatt används och uppdateras, men visar att flera av de tidigare identifierade förbättringsbehoven kvarstår och i viss utsträckning påverkar hur registret kan användas som stöd för styrning och uppföljning samt hur efterlevnaden säkerställs i praktiken. Bedömningen har därför fördjupats med ökat fokus på hur rutinerna fungerar i praktiken och i vilken grad registret speglar verksamhetens faktiska personuppgiftsbehandlingar.

Dataskyddsombudets bedömning samt rekommendationer

Dataskyddsombudet bedömer att verksamheten har ett register över personuppgiftsbehandlingar som är upprättat och används, men att styrning och tillämpning av registerföringen behöver stärkas för att registret fullt ut ska spegla verksamhetens faktiska personuppgiftsbehandlingar.

Rekommendationer:

- Genomför en samlad gapanalys i syfte att identifiera eventuella personuppgiftsbehandlingar som ännu inte finns dokumenterade i registerförteckningen, så att registret i sin helhet speglar verksamhetens faktiska behandlingar.
- Kvalitetssäkra befintliga registreringar genom en strukturerad genomgång av hur personuppgiftsbehandlingar dokumenteras, inklusive hur behandlingar avgränsas och delas upp, för att säkerställa konsekvens, tydlighet och ändamålsenlighet i registerföringen.
- Integrera identifiering av nya och förändrade personuppgiftsbehandlingar i verksamhetens ordinarie arbetsflöden, exempelvis genom återkommande avstämning i relevanta forum, för att säkerställa att registerförteckningen hålls aktuell över tid.

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?

Dataskyddsombudet har genomfört stickprov på tre genomförda informationsklassningar av system som behandlar personuppgifter om kunder och/eller anställda.

Granskningen visar att informationsklassningarna beaktar kategorisering av personuppgifter (känsliga respektive icke-känsliga). I ett av stickproven har personuppgifter klassificerats som icke-känsliga trots att uppgifterna kan vara att betrakta som känsliga eller i vart fall integritetskänsliga.

Sammantaget bedömer dataskyddsombudet att hänsyn till olika kategorier av personuppgifter beaktas i informationsklassningsarbetet, men endast delvis.

En sådan osäkerhet i kategoriseringen kan leda till att personuppgifter inte bedöms utifrån rätt skyddsbehov. Detta kan i sin tur innebära att risker i behandlingen inte identifieras eller hanteras på ett tillräckligt ändamålsenligt sätt, vilket kan påverka skyddet av de registrerades personuppgifter.

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

Dataskyddsombudet har granskat om det finns skriftligt styrande dokument och rutiner som i tillräcklig omfattning reglerar verksamhetens dataskyddsarbete och ger stöd i den praktiska tillämpningen.

Granskningen visar att det finns flera centrala styrdokument och rutiner på plats, bland annat avseende övergripande dataskydd, informationsklassning, personuppgiftsincidenter samt risk-

och konsekvensbedömningar. Sammantaget finns därmed en dokumenterad grund för dataskyddsarbetet.

Samtidigt framgår att delar av styrningen inte är fullt ut anpassad till nuvarande organisation och arbetssätt. I flera rutiner är ansvarsfördelningen mellan verksamheten och dataskyddsombudet otydlig, och stödet till verksamheten i hur rutinerna ska tillämpas i praktiken är begränsat.

Osäkerhet kring ansvarsfördelningen innebär en risk för att dataskyddsuppgifter inte utförs av rätt funktion eller i rätt tid. Detta kan leda till att uppgifter faller mellan stolarna eller onödigt fördröjs, vilket i sin tur kan påverka de registrerades möjligheter att få sina rättigheter tillgodosedda inom föreskriven tid.

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

Dataskyddsombudet har granskat om de skriftligt styrande dokument och rutiner som finns är tillräckligt implementerade och kända i verksamheten.

Granskningen visar att verksamheten genomför återkommande utbildnings- och informationsinsatser inom dataskydd och informationssäkerhet. Medarbetare inom kundnära verksamhet och verksamhetsstöd erbjuds riktade utbildningar, obligatoriska utbildningar finns tillgängliga och kompletterande informationsinsatser genomförs löpande, vilket bidrar till en grundläggande medvetenhet om dataskyddsfrågor i verksamheten.

Samtidigt framgår att denna medvetenhet inte fullt ut omsätts i praktisk tillämpning av styrande dokument och rutiner. Processägare och verksamheten i stort uppvisar begränsad kännedom om när och hur Dataskyddsgruppen eller dataskyddsombudet ska involveras, och i praktiken behöver Dataskyddsgruppen ofta efterfråga information för att initiera nödvändiga dataskyddsåtgärder.

Bristande kännedom och implementering innebär en risk för att styrande dokument och rutiner inte tillämpas konsekvent i verksamheten, utan i stället aktiveras reaktivt. Detta kan leda till att dataskyddsarbetet bedrivs ojämlikt mellan olika delar av verksamheten och att skyddet av personuppgifter inte upprätthålls med tillräcklig konsekvens.

Dataskyddsombudets jämförelse med föregående års resultat

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

I föregående års granskning bedömdes verksamheten ha ändamålsenliga styrdokument och rutiner för dataskydd och informationssäkerhet, inklusive genomförd informationsklassning och dokumentation av tekniska och organisatoriska åtgärder. Fokus låg i huvudsak på förekomsten och kvaliteten i styrdokumenten samt deras tillgänglighet i organisationen.

Årets granskning har haft ett tydligare fokus på hur säkerhetsarbetet fungerar i praktiken, inklusive hur informationsklassning tillämpas och hur styrande dataskyddsrutiner omsätts i verksamhetens arbetssätt. Bedömningen påverkas även av förändrade organisatoriska förutsättningar, vilket har synliggjort behov av ökad tydlighet och konsekvens i tillämpningen.

Dataskyddsombudets bedömning samt rekommendationer

Dataskyddsombudet bedömer att grundläggande säkerhetsarbete är etablerat i verksamheten, inklusive informationsklassning, styrande dokument och återkommande utbildningsinsatser. Dessa utgör en stabil grund för skydd av personuppgifter.

Samtidigt visar granskningen att säkerhetsarbetet påverkas av förändrade organisatoriska förutsättningar och att tillämpningen av informationsklassning och styrande dataskyddsrutiner inte är fullt ut konsekvent i praktiken.

Dataskyddsombudet rekommenderar därför att:

- tillämpningen av informationsklassning förtydligas för att säkerställa en enhetlig bedömning av personuppgifter,
- styrande dataskyddsrutiner används mer konsekvent i verksamheten genom tydligare koppling till ordinarie arbetssätt.

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

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

Dataskyddsombudet har granskat om det finns ändamålsenliga rutiner för att genomföra tröskelanalys vid nya eller förändrade personuppgiftsbehandlingar.

Granskningen visar att det finns stöd för genomförande av tröskelanalys beskrivet i verksamhetens systemstöd. Rutinen ger vägledning för hur tröskelanalys ska genomföras och utgör därmed en grund för att identifiera när en konsekvensbedömning avseende dataskydd kan behöva genomföras.

Dataskyddsombudet bedömer att rutinen i sig är ändamålsenlig och ger tillräckligt stöd för att genomföra tröskelanalys vid nya eller förändrade personuppgiftsbehandlingar.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Dataskyddsombudet har granskat om tröskelanalyser genomförs vid nya eller förändrade personuppgiftsbehandlingar.

Granskningen visar att nya personuppgiftsbehandlingar har identifierats och lagts in i systemstödet under året. Samtidigt framgår att genomförande av tröskelanalyser och konsekvensbedömningar i stor utsträckning initieras efter påminnelse eller efterfrågan från Dataskyddsgruppen snarare än som en etablerad del av verksamhetens ordinarie processer.

Vidare framkommer att det finns indikationer på att ytterligare personuppgiftsbehandlingar kan kräva tröskelanalys eller konsekvensbedömning, men ännu inte har identifierats eller dokumenterats. Detta innebär en risk för att tröskelanalyser inte genomförs konsekvent vid nya eller förändrade behandlingar, vilket kan leda till att behov av konsekvensbedömning identifieras sent eller uteblir.

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

Dataskyddsombudet har granskat om det finns en ändamålsenlig mall och rutiner för genomförande av konsekvensbedömning avseende dataskydd.

Granskningen visar att det finns systemstöd i verksamheten som ger vägledning för hur konsekvensbedömningar ska genomföras. Den nuvarande versionen av systemstödet innehåller tydligare och mer strukturerade frågor än tidigare, vilket ger förbättrade förutsättningar för att genomföra konsekvensbedömningar på ett enhetligt och ändamålsenligt sätt.

Dataskyddsombudet bedömer att befintlig mall och vägledning ger tillräckligt stöd för genomförande av konsekvensbedömning avseende dataskydd.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Dataskyddsombudet har granskat om konsekvensbedömning avseende dataskydd genomförs i de fall det krävs.

Granskningen visar att konsekvensbedömningar genomförs i vissa fall. Samtidigt framgår att genomförandet inte sker konsekvent, utan att konsekvensbedömningar i vissa fall initieras först efter dialog eller påminnelse från Dataskyddsgruppen.

Detta innebär en risk för att konsekvensbedömning inte genomförs i alla fall där det krävs, eller att den genomförs sent i processen. Om behovet av konsekvensbedömning inte identifieras och hanteras i rätt tid kan risker för de registrerades rättigheter och friheter förbises eller inte hanteras på ett ändamålsenligt sätt. Vidare framkommer att Dataskyddsgruppen bedömer att det finns behov av att identifiera och kartlägga ytterligare processer där konsekvensbedömning kan vara aktuell.

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

Dataskyddsombudet har granskat om personuppgiftsansvarig har identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd genomförs samt genomfört detta.

Granskningen, baserad på uppgifter från Dataskyddsgruppen, visar att det inte finns en samlad säkerhet kring att samtliga personuppgiftsbehandlingar som kräver konsekvensbedömning har identifierats och bedömts. Samtidigt framgår att konsekvensbedömningar genomförs för vissa behandlingar, men att helhetsbilden av vilka behandlingar som omfattas är oklar.

Detta innebär en risk för att personuppgiftsbehandlingar som kan medföra förhöjda risker för de registrerades rättigheter och friheter inte identifieras och bedöms i tid. Om konsekvensbedömning inte genomförs där det krävs finns risk för att skyddsåtgärder inte utformas eller anpassas på ett tillräckligt ändamålsenligt sätt.

Dataskyddsombudets jämförelse med föregående års resultat

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

I föregående års granskning bedömdes verksamheten ha etablerade rutiner och systemstöd för konsekvensbedömning avseende dataskydd, och de genomförda konsekvensbedömningarna bedömdes vara aktuella. Fokus låg på att säkerställa att verktyg och dokumentation fanns på plats samt att inga högriskbehandlingar hade identifierats.

Årets granskning har i större utsträckning fokuserat på hur tröskelanalyser och konsekvensbedömningar initieras och genomförs i praktiken samt om samtliga personuppgiftsbehandlingar som kan kräva konsekvensbedömning har identifierats. Denna fördjupning har synliggjort behov av ökad systematik och helhetsöverblick i arbetet med konsekvensbedömningar.

Dataskyddsombudets bedömning samt rekommendationer

Dataskyddsombudet bedömer att verksamheten har etablerade rutiner och systemstöd för tröskelanalys och konsekvensbedömning avseende dataskydd. Dessa ger en god grund för att identifiera och hantera personuppgiftsbehandlingar som kan innebära förhöjda risker för de registrerades rättigheter och friheter.

Samtidigt visar granskningen att arbetet med tröskelanalyser och konsekvensbedömningar inte är fullt ut systematiskt i praktiken och att det saknas en samlad säkerhet kring att samtliga

personuppgiftsbehandlingar som kan kräva konsekvensbedömning har identifierats. Detta innebär att behov av konsekvensbedömning riskerar att identifieras sent eller utebli.

Dataskyddsombudet rekommenderar därför att:

- genomförandet av tröskelanalyser integreras tydligare i verksamhetens befintliga arbetsprocesser,
- säkerställs att identifierade behov av konsekvensbedömning konsekvent leder till genomförda bedömningar,
- en samlad översyn genomförs i syfte att identifiera ytterligare personuppgiftsbehandlingar där konsekvensbedömning kan vara aktuell.

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?

Dataskyddsombudet har granskat om det finns ändamålsenliga rutiner för att ta emot och hantera registrerades rättighetsförfrågningar.

Granskningen visar att personal får grundläggande information om vad en rättighetsförfrågan är och vart de ska vända sig vid mottagande av en sådan förfrågan, bland annat inom ramen för introduktionsutbildning för nyanställda. Det finns även information tillgänglig på intranätet om hur anställda ska agera när de tar emot en rättighetsförfrågan.

Vidare framgår att rättighetsförfrågningar hanteras centralt av Dataskyddsgruppen. Under det senaste året har inga rättighetsförfrågningar inkommit, och de få förfrågningar som tidigare har mottagits har hanterats manuellt och besvarats inom föreskriven tid. Samtidigt saknas skriftligt dokumenterade rutiner för hur rättighetsförfrågningar ska hanteras.

Avsaknaden av dokumenterade rutiner innebär i nuläget en begränsad risk, då ärendemängden är låg och hanteringen sker centralt. Vid förändrade förutsättningar, såsom ökad ärendemängd eller organisatoriska förändringar, kan dock behov uppstå av tydligare dokumentation för att säkerställa kontinuitet och enhetlighet i hanteringen.

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

Under året har inga begäranden från registrerade avseende rättigheter enligt dataskyddsförordningen, såsom registerutdrag, rättelse, radering eller begränsning av behandling, inkommit till verksamheten.

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

Under året har inga begäranden från registrerade inkommit. Det finns därför inga ärenden att bedöma avseende svarstid inom föreskriven tidsfrist.

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

Eftersom inga begäranden från registrerade har inkommit under året har dataskyddsombudet inte genomfört några stickprov av svar till registrerade.

Dataskyddsombudets jämförelse med föregående års resultat

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

I föregående års granskning konstaterades att verksamheten hade förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist, men att hanteringen i praktiken var manuell och i hög grad personberoende. Samtidigt noterades att inga brister av nämnvärd betydelse hade identifierats.

Årets granskning visar ingen förändring i bedömningen. Inga rättighetsförfrågningar har inkommit under året, och hantering av sådana förfrågningar sker fortsatt centralt via Dataskyddsgruppen. Avsaknaden av dokumenterade rutiner kvarstår, men givet den låga ärendemängden har detta inte medfört några identifierade brister i hanteringen.

Dataskyddsombudets bedömning samt rekommendationer

Dataskyddsombudet bedömer att verksamheten har grundläggande förutsättningar för att ta emot och hantera registrerades rättighetsförfrågningar. Information om hur rättighetsförfrågningar ska hanteras ges till personal och hanteringen sker centralt via Dataskyddsgruppen. Under året har inga rättighetsförfrågningar inkommit.

Samtidigt saknas dokumenterade rutiner för hantering av registrerades rättigheter. Mot bakgrund av den låga ärendemängden bedöms risken i nuläget som låg, men avsaknaden av dokumentation innebär att hanteringen är personberoende och kan påverka kontinuitet och enhetlighet vid förändrade förutsättningar.

Dataskyddsombudet rekommenderar därför att befintligt arbetssätt för hantering av registrerades rättighetsförfrågningar dokumenteras, i syfte att säkerställa tydlighet och kontinuitet vid behov.

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?

Kunskap om hur personuppgiftsincidenter ska hanteras säkerställs genom utbildningsinsatser, inklusive obligatoriska digitala utbildningar för medarbetare.

Dataskyddsgruppen upplever att det finns viss medvetenhet bland personalen om vad som kan utgöra en personuppgiftsincident och hur man ska agera vid osäkerhet. Medarbetare hör i praktiken av sig för att stämma av om en viss händelse, exempelvis e-post som innehåller personuppgifter, ska betraktas som en incident.

Samtidigt framgår att medvetenheten inte är helt enhetlig och att kommunikation och information kring personuppgiftsincidenter kan förbättras. Detta innebär en risk för att incidenter inte alltid identifieras eller hanteras på ett konsekvent sätt, vilket kan påverka verksamhetens möjlighet att vidta rätt åtgärder i tid.

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

Det finns dokumenterade rutiner för hur händelser som kan utgöra personuppgiftsincidenter ska hanteras, och dessa är tillgängliga för verksamheten.

I praktiken följs rutinerna i huvudsak, men granskningen visar att Dataskyddsgruppen i vissa fall har behövt initiera eller uppmärksamma incidenthantering efter att händelser blivit kända på annat sätt. Detta indikerar att rutinerna inte alltid tillämpas helt enhetligt i samtliga delar av verksamheten.

Mot bakgrund av att rutiner finns och används bedöms detta i nuläget inte utgöra en betydande risk, men det finns ett behov av att säkerställa en mer konsekvent tillämpning för att undvika personberoende hantering.

Hur många personuppgiftsincidenter har dokumenterats under året?

Under året har inga personuppgiftsincidenter dokumenterats i verksamhetens systemstöd.

Det finns ett behov av att säkerställa en gemensam och tydlig tillämpning av när inträffade säkerhetshändelser ska registreras och hanteras som personuppgiftsincidenter, i syfte att uppnå en enhetlig bedömning i verksamheten.

Hur många personuppgiftsincidenter har anmälts till IMY under året?

Under året har inga personuppgiftsincidenter anmälts till Integritetsskyddsmyndigheten (IMY).

Dataskyddsombudets jämförelse med föregående års resultat

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

I föregående års granskning konstaterades att verksamheten hade fungerande rutiner för hantering av personuppgiftsincidenter. Incidenter som blev kända dokumenterades i systemstödet, inga incidenter bedömdes behöva anmälas till Integritetsskyddsmyndigheten och inga brister av nämnvärd betydelse identifierades. Det noterades även ett högt incidentmedvetande bland medarbetare samt att utbildning genomfördes löpande.

Årets granskning visar att inga personuppgiftsincidenter har dokumenterats eller anmälts under året. Samtidigt har granskningen haft ett tydligare fokus på tillämpningen av när inträffade säkerhetshändelser ska registreras och hanteras som personuppgiftsincidenter. Bedömningen av området är i huvudsak oförändrad jämfört med föregående år, men granskningen har synliggjort ett behov av ökad tydlighet för att säkerställa en enhetlig tillämpning över tid.

Dataskyddsombudets bedömning samt rekommendationer

Dataskyddsombudet bedömer att verksamheten har etablerade förutsättningar för att hantera personuppgiftsincidenter. Granskningen visar samtidigt att det finns behov av att säkerställa en enhetlig tillämpning av när inträffade säkerhetshändelser ska registreras och hanteras som personuppgiftsincidenter. Mot bakgrund av detta bedöms risken i nuläget som låg.

Dataskyddsombudet rekommenderar därför att:

- tillämpningen av när säkerhetshändelser ska registreras och hanteras som personuppgiftsincidenter tydliggörs, i syfte att säkerställa konsekvens och kontinuitet i incidenthanteringen.

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

Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?

Dataskyddsombudet har granskat om personuppgiftsansvarig har identifierat de tredjelandsöverföringar som utförs.

Granskningen visar att verksamheten utgår från stadens övergripande krav om att undvika tredjelandsöverföringar vid användning av IT-tjänster. I de granskade behandlingarna har tredjelandsöverföring i huvudsak inte identifierats utifrån de funktioner och tjänster som används i praktiken.

Samtidigt framkommer att vissa tjänster kan ha en struktur där begränsade delar av hanteringen sker hos leverantörer med hemvist utanför EU/EES. Sammantaget bedöms tredjelandsöverföringar i nuläget vara i huvudsak identifierade, men granskningen visar att registerförteckningens nuvarande nivå av detaljer inte fullt ut speglar hur olika delar av använda tjänster förhåller sig till tredjelandsöverföring.

Detta innebär en risk för att tredjelandsöverföringar inte identifieras eller bedöms konsekvent i de fall där olika delar av en tjänst hanteras på olika sätt, vilket kan försvåra verksamhetens möjlighet att säkerställa korrekt efterlevnad av dataskyddsregelverket över tid.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

Dataskyddsombudet har granskat om personuppgiftsansvarig tillämpar ett överföringsverktyg på de tredjelandsöverföringar som utförs.

---

[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.

Granskningen, baserad på uppgifter från Dataskyddsgruppen, visar att det i nuläget är oklart om överföringsverktyg tillämpas vid de delar av använda tjänster där tredjelandsöverföring kan förekomma. Detta innebär att tillämpningen av överföringsverktyg inte är fullt ut klarlagd.

Detta innebär en risk för att tredjelandsöverföringar, i de fall de förekommer, inte omfattas av ett tillämpligt överföringsverktyg enligt dataskyddsregelverket, vilket kan påverka möjligheten att säkerställa ett tillräckligt skydd för personuppgifter vid överföring till tredje land.

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

Dataskyddsombudet har granskat om nödvändig bedömning, Transfer Impact Assessment (TIA), har genomförts avseende tredjelandsöverföringar.

Granskningen visar att några TIA inte har genomförts. Bedömningar har i stället gjorts på en övergripande nivå utifrån vilken typ av personuppgifter som behandlas och var data lagras, men utan att en formell TIA har dokumenterats.

Avsaknaden av dokumenterad TIA innebär en risk för att tredjelandsöverföringar, i de fall de förekommer, inte bedöms tillräckligt systematiskt i förhållande till gällande krav i dataskyddsregelverket. Detta kan påverka verksamhetens möjlighet att visa att tillräckliga skyddsåtgärder vidtas vid överföring till tredje land.

Dataskyddsombudets jämförelse med föregående års resultat

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

Granskningsområdet tredjelandsöverföringar omfattades inte av föregående års årsrapportmall och har därför inte tidigare granskats som ett eget område inom ramen för dataskyddsombudets årsrapport.

Årets granskning utgör därmed en första samlad genomgång av hur tredjelandsöverföringar identifieras, bedöms och dokumenteras i verksamheten.

Dataskyddsombudets bedömning samt rekommendationer

Dataskyddsombudets bedömning baseras på uppgifter från Dataskyddsgruppen. Granskningen visar att verksamheten utgår från stadens övergripande krav om att undvika tredjelandsöverföringar och att sådana överföringar, enligt tillgänglig information, i huvudsak inte förekommer i de tjänster som används i praktiken. Samtidigt framgår att dokumentation och bedömning av tredjelandsöverföringar inte är fullt ut etablerad för samtliga delar av använda tjänster, och att nödvändiga bedömningar i form av Transfer Impact Assessment ännu inte har genomförts.

Dataskyddsombudet rekommenderar därför att:

- registerförteckningens detaljeringsnivå ses över så att den i tillräcklig utsträckning speglar hur olika delar av använda tjänster förhåller sig till tredjelandsöverföring,
- det klargörs om och hur överföringsverktyg tillämpas vid tredjelandsöverföringar,
- nödvändiga bedömningar i form av Transfer Impact Assessment genomförs i de fall tredjelandsöverföringar kan förekomma.

Bilaga 2 – Andra genomförda granskningar och omvärldsbevakning

Andra granskningar som dataskyddsombudet har genomfört under året

Genomförda granskningar och deras resultat

Granskning 1 – Information till registrerade på webbplatsen (micasa.se)

Dataskyddsombudet har granskat den information om behandling av personuppgifter som tillhandahålls via webbplatsen micasa.se (”Information om behandling av personuppgifter”) mot bakgrund av dataskyddsförordningens krav på transparens och information.

Granskningen visar att informationen ger en övergripande beskrivning av hur personuppgifter behandlas i verksamheten samt innehåller generell information om registrerades rättigheter och kontaktvägar. Samtidigt framgår att informationen i flera avseenden inte är tillräckligt specificerad för att uppfylla kraven på tydlig, fullständig och lättillgänglig information enligt dataskyddsförordningen. Informationen saknar i delar den struktur och detaljnivå som krävs för att registrerade på ett enkelt sätt ska kunna förstå vilka personuppgifter som behandlas, för vilka ändamål och på vilka rättsliga grunder.

Sammantaget bedöms integritetsinformationen i sin nuvarande form inte ge registrerade en tillräckligt klar och transparent bild av bolagets personuppgiftsbehandlingar.

Bristande transparens kan leda till att registrerade inte får den information de har rätt till enligt dataskyddsförordningen, vilket kan försvåra möjligheten att utöva sina rättigheter och minska förtroendet för hur personuppgifter hanteras. Mot denna bakgrund bedöms risken som medelhög.

Granskning 2 – Hantering av tjänstekort

Dataskyddsombudet har granskat hanteringen av tjänstekort inom verksamheten, med fokus på hur tjänstekort används och förvaras i det dagliga arbetet. Granskningen har genomförts genom intervju med tidigare dataskyddsombud samt genom information från Dataskyddsgruppen.

Granskningen visar att tjänstekort i praktiken ofta lämnas utan uppsyn i verksamhetens lokaler. Detta sker trots att det finns fastställda rutiner för hur tjänstekort ska hanteras och trots återkommande påminnelser till medarbetare om gällande krav.

Eftersom tjänstekort används för inloggning till IT-system, innebär bristande efterlevnad av rutinerna en ökad risk för obehörig åtkomst. Sammantaget bedöms hanteringen av tjänstekort i sin nuvarande form innebära en förhöjd risk kopplad till skyddet av personuppgifter. Mot denna bakgrund bedöms risken som medelhög.

Dataskyddsombudets rekommendationer baserat på iakttagelserna ovan

Dataskyddsombudets rekommendationer

1. *Prioritera att i närtid omarbeta och uppdatera informationen till registrerade på webbplatsen så att den uppfyller dataskyddsförordningens krav på tydlig, fullständig och lättillgänglig information.*
2. *Utred om nuvarande säkerhetsåtgärder för hantering av tjänstekort behöver kompletteras för att minska risken för obehörig åtkomst till system samt vilka åtgärder som är ändamålsenliga med beaktande av hur tjänstekort hanteras i praktiken.*

Omvärldsbevakning

Resultatet av dataskyddsombudets omvärldsbevakning

IMY:s vägledning om konsekvensbedömningar (DPIA)

IMY har publicerat vägledning som förtydligar när konsekvensbedömning ska genomföras, hur arbetet bör struktureras och vikten av att DPIA hålls uppdaterad över tid. Vägledningen är praktiskt användbar för att stärka systematik och dokumentation i arbetet med högriskbehandlingar.

Länk:

https://www.imy.se/nyheter/imy-publicerar-vagledning-vid-konsekvensbedomning/

Pseudonymisering

EDPB:s riktlinjer om pseudonymisering

EDPB har antagit riktlinjer som klargör hur pseudonymisering ska förstås och tillämpas enligt GDPR samt att pseudonymiserade uppgifter fortsatt är personuppgifter. Riktlinjerna är relevanta vid informationsklassning, riskbedömning och som skyddsåtgärd i konsekvensbedömningar.

Länkar:

https://www.edpb.europa.eu/news/news/2025/edpb-adopts-pseudonymisation-guidelines-and-paves-way-improve-cooperation_sv

https://www.edpb.europa.eu/system/files/2025-02/edpb_summary_202501_pseudonymisation_en.pdf

SRB-målet

EU-domstolen har i det s.k. SRB-målet klargjort att bedömningen av om uppgifter utgör personuppgifter ska göras utifrån mottagarens faktiska möjlighet att identifiera en person, även när uppgifterna är pseudonymiserade. Domen tydliggör hur pseudonymisering ska bedömas i administrativa processer och vid delning av uppgifter inom och mellan organisationer.

Länk:

https://curia.europa.eu/site/upload/docs/application/pdf/2025-09/cp250107en.pdf

Nationella riktlinjer för användning av generativ AI i offentlig sektor

Nationella riktlinjer för generativ AI inom offentlig förvaltning har lanserats och betonar krav på riskbedömning, transparens och ansvar när personuppgifter behandlas. Riktlinjerna är strategiskt relevanta även för verksamheter med begränsad AI-användning i nuläget.

Länk:

https://www.imy.se/nyheter/nu-lanseras-nationella-riktlinjer-for-anvandningen-av-generativ-ai-inom-offentlig-forvaltning/

Nya regler och vägledning om kamerabevakning

Nya regler för kamerabevakning har trätt i kraft och IMY har publicerat vägledning om hur regelverket ska tillämpas. EU-domstolen har även klargjort kraven på information till registrerade vid kamerabevakning, vilket påverkar offentlig verksamhet där kameror används.

Länkar:

https://www.imy.se/nyheter/fran-1-april-galler-nya-regler-for-verksamheter-som-kamerabevakar/

https://www.imy.se/nyheter/imy-vagleder-om-nya-kameraregler/

https://www.imy.se/nyheter/klargorande-fran-eu-domstolen-om-information-vid-kamerabevakning/

Samordnad EU-tillsyn 2026 – transparens och information till registrerade

EDPB har beslutat att temat för det samordnade tillsynsramverket (Coordinated Enforcement Framework) 2026 ska vara organisationers efterlevnad av transparens- och informationskraven i GDPR, särskilt enligt artiklarna 12–14. Det innebär att tillsynsmyndigheter i flera EU-länder parallellt kommer att granska hur väl registrerade informeras om personuppgiftsbehandlingar, inklusive tydlighet, fullständighet och tillgänglighet i informationen.

Länk:

https://www.edpb.europa.eu/news/news/2025/coordinated-enforcement-framework-edpb-selects-topic-2026_sv

EDPS om användning av Microsoft 365 i EU:s institutioner

EDPS meddelar att Europeiska kommissionen, efter ett tillsynsärende, har genomfört åtgärder som innebär att tidigare identifierade brister i användningen av Microsoft 365 bedöms vara åtgärdade och att ärendet därmed har avslutats. Ärendet illustrerar vilka krav som kan ställas på styrning, ansvarsfördelning och skyddsåtgärder vid användning av molntjänster i offentlig verksamhet.

Länk:

https://www.edps.europa.eu/press-publications/press-news/press-releases/2025/european-commission-brings-use-microsoft-365-compliance-data-protection-rules-eu-institutions-and-bodies_en

Förslag om förenklingar i GDPR – Digital Omnibus

EU-kommissionen har presenterat ett förslag till Digital Omnibus som bland annat omfattar förenklingar och förtydliganden i GDPR, exempelvis kring dokumentationskrav och samordnad incidentrapportering. Förslaget är ännu under beredning men visar riktningen för kommande utveckling av regelverket.

Länk:

https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

Tredjelandsöverföringar – USA, Storbritannien och Brasilien

EU-domstolen har bekräftat att EU-US Data Privacy Framework fortsatt innebär ett giltigt adekvansstöd för överföring av personuppgifter till certifierade mottagare i USA. Europeiska kommissionen har beslutat att förlänga EU:s adekvansbeslut för Storbritannien, vilket innebär att personuppgifter fortsatt kan överföras utan kompletterande skyddsåtgärder. EDPB har dessutom antagit ett yttrande om ett förslag till adekvansbeslut för Brasilien och bedömt att landets dataskyddsramverk i huvudsak ger en adekvat skyddsnivå, med vissa rekommenderade förtydliganden inför ett slutligt beslut.

Länkar:

https://curia.europa.eu/site/upload/docs/application/pdf/2025-09/cp250106en.pdf

https://europa.eu/newsroom/ecpc-failover/pdf/ip-25-3059_en.pdf

https://www.edpb.europa.eu/news/news/2025/draft-adequacy-decision-brazil-edpb-adopts-opinion_en