Stockholms stad

Bilaga 1

GDPR årsrapport

År 2025

AB Stockholmshem

GDPR årsrapport
Januari 2026

Dnr: YYYY
Utgivningsdatum: 2025-12-30
Kontaktperson: Johan Åhs

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 AB Stockholmshems dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

Draftit ska utgöra ett centralt nav i Stockholmshems dataskyddsarbete och är av grundläggande betydelse för att skapa struktur, spårbarhet och efterlevnad av GDPR. Arbetet med Draftit behöver prioriteras för att hantera risken att Stockholmshems registrerade behandlingar inte hålls uppdaterade med fullständig och korrekt information vilket i så fall kan försvåra överblicken och styrningen i dataskyddsarbetet och få följdeffekter på arbetet med tröskelanalyser, konsekvensbedömningar och dokumentation av tredjelandsöverföringar.

Avsaknad av genomförda tröskelanalyser för behandlingar som bedömts ha en medelhög risk medför att potentiella integritetsrisker inte identifieras och hanteras på ett sätt som GDPR föreskriver.

Avslutningsvis kan ett fördröjt arbete med konsekvensbedömningar för högriskbehandlingar innebära en förhöjd risk för bristande lagefterlevnad och otillräckligt dataskydd vilket sammantaget kan leda till relativt allvarliga konsekvenser för både de registrerade och verksamheten.

De tre största riskerna enligt dataskyddsombudets bedömning är följande.

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Komplett registerförteckning i Draftit		Prioritera arbetet med Draftit och säkerställ att alla registrerade behandlingar är uppdaterade med all relevant information. Särskilt prioritet bör läggas på högriskbehandlingar men för att säkerställa en enkel överblick över lågriskbehandlingar bör det arbetet inte heller åsidosättas.
Genomförda tröskelanalyser för alla behandlingar i gråzonen		Säkerställ att tröskelanalyser är gjorda för alla behandlingar som bedöms ha en medelhög risk.
Genomförda konsekvensbedömningar för alla högriskbehandlingar		Gör en handlingsplan och påbörja arbetet med konsekvensbedömningar för alla högriskbehandlingar. Utarbeta även en prioritetsordning för dessa behandlingar som sedermera dokumenteras.

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

Sammanfattningsvis rekommenderas att Stockholmshem prioriterar arbetet med att kontrollera och uppdatera samtliga registrerade behandlingar i Draftit så att informationen är korrekt, fullständig och aktuell. Särskilt bör fokus läggas på att komplettera saknade uppgifter om ändamål och tidsfrister för radering samt all information beträffande identifierade högriskbehandlingar.

De etablerade rutinerna för det löpande dataskyddsarbetet samt uppföljning genom punktinsatser enligt årshjulet bör även fortsättningsvis utföras och följas upp. Vidare bör migreringen till Draftit slutföras under första halvåret i 2026 för att säkerställa att systemet fullt ut kan fungera som ett samlat stöd och styrverktyg för organisationens dataskyddsarbete.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade? 52 st.		Fortsätt att kontrollera och uppdatera alla registrerade behandlingar i Drafit med korrekt information i enlighet med de rutiner som finns.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar? Ja.		Fortsätt följa de rutinerna finns dels avseende det löpande dataskyddsarbetet, dels avseende kontroll genom punktinsatser i årshjulet.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför? Ja.		Se ovanstående svar.
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna? Delvis.		Migreringen till Draftit är ännu inte fullständig men arbetet fortlöper. Det saknas information om bl.a. ändamål och tidsfrister för radering för många registrerade behandlingar varför detta arbete behöver prioriteras.

Säkerhet i samband med behandlingen

Dataskyddskommittén utför organisatoriska uppgifter för att säkerställa en hög nivå av säkerhet i samband med personuppgiftsbehandling enligt GDPR. Arbetet omfattar dokumentation av känsliga personuppgifter och högriskbehandlingar i Draftit, vilket ska ske löpande i enlighet med fastställda rutiner. Verksamheten har i stor utsträckning styrande dokument som vid behov ska uppdateras och revideras, och dataskyddskommittén bör fortsatt utveckla och implementera rutiner där ytterligare behov identifieras.

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? Ja.		Känsliga personuppgifter och högriskbehandlingar är dokumenterade i Draftit och detta arbete för fortsatt ske löpande genom de rutiner som finns.
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd? Ja.		Verksamheten har styrande dokument i hög utsträckning som ska uppdateras och revideras vid behov.
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända? Ja.		Dataskyddskommittén bör fortsätta med att utveckla och implementera rutiner där behov finns.

Konsekvensbedömning avseende dataskydd

Genom Draftit tydliggörs vilken risknivå respektive behandling har och därmed även när det behöver göras tröskelanalyser och konsekvensbedömningar. Tröskelanalyser och konsekvensbedömningar genomförs i högre grad vid införandet av nya system (t.ex. ImBox).

Verksamheten behöver även säkerställa att konsekvensbedömningar görs för existerande behandlingar som vid en tröskelanalys visar att behandlingarna leder till en hög risk för de registrerade. Eftersom detta arbete kan vara omfattande behöver verksamheten först dokumentera tröskelanalyserna och därefter dokumentera en prioritetsordning för de konsekvensbedömningar som ska genomföras. En handlingsplan som kontinuerligt följs upp bör därefter upprättas.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys? Ja.		Fortsätta arbeta med Draftit som tydliggör vilken risknivå respektive behandling har och om behov finns för en tröskelanalys och/eller konsekvensbedömning.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar? Ja.		Fortsätta uppdatera Draftit och därmed identifiera vilka behandlingar som utgör högriskbehandlingar.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd? Ja.		Stockholmshem har en mall för konsekvensbedömningar avseende dataskydd som svarar mot kraven i artikel 35 vilken ska användas för konsekvensbedömningar avseende dataskydd. Mallen bör fortsatt revideras vid behov.
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs? Delvis.		Verksamheten bör delegera ansvar avseende konsekvensbedömningar och ta fram en prioritetslista över i vilken ordning dessa ska utföras.

Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta? Delvis.		Verksamheten behöver fortsätta detta arbete och säkerställa att det genomförs.

Den registrerades rättigheter

Stockholmshems hantering av de registrerades rättigheter föranleder inga specifika rekommendationer. DSO noterar att arbetet med att hantera de registrerades rättigheter följer etablerade rutiner och processer som säkerställer lagefterlevnad i enlighet med GDPR.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade? Ja.		Begäran från de registrerade bör även fortsättningsvis hanteras genom en central funktion som hanterar begäran på ett sätt som svarar mot dataskyddsförordningens krav.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade? 7		Se ovanstående svar.
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad? 7		Se ovanstående svar.
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven? Ja.		Stickprovet har visat att begäran om tillgång (registerutdrag) enligt artikel 15 har hanterats på ett sätt som tyder på god lagefterlevnad.

Personuppgiftsincidenter

Stockholmshems årshjul föreskriver att dataskyddskommittén utbildas i hantering av personuppgiftsincidenter genom praktiska övningar en gång per tillsammans med DSO. Vidare finns etablerade rutiner och information till medarbetare om hur personuppgiftsincidenter ska hanteras. Dokumenterade personuppgiftsincidenter som skett hos verksamheten under året har hanterats på ett sätt som svarar mot GDPR:s krav. Det kan även tilläggas att Stockholmshem inte omfattades av personuppgiftsincidenten hos Miljödata.

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? Utbildningar och praktiska övningar.		Regelbundna utbildningar och praktiska övningar i personuppgiftsincidenter samt rutiner och information på intranätet säkerställer organisatoriska skyddsåtgärder som skapar en process för hantering av personuppgiftsincidenter som svarar mot dataskyddsförordningens krav och bör fortsätta användas.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa? Ja.		Se ovanstående svar.
Hur många personuppgiftsincidenter har dokumenterats under året? 4 st.		Se ovanstående svar.
Hur många personuppgiftsincidenter har anmälts till IMY under året? 1 st.		Se ovanstående svar.

Överföring till tredje land

Drafit möjliggör för verksamheten att få en överblick av vilka registrerade behandlingar som omfattas av eventuella tredjelandsöverföringar. Av de kartlagda faktiska tredjelandsöverföringar som sker till USA tillämpas EU-kommissionens adekvansbeslut i kombination med att säkerställa att mottagaren är certifierad mot Data Privacy Framework En TIA som svarar mot dataskyddsförordningens krav har bl.a. gjorts för användandet av ”ImBox” i enlighet med verksamhetens rutiner.

Det rekommenderas att verksamheten håller sig fortsatt uppdaterade på att adekvansbeslutet för tredjelandsöverföringar till USA (DPF) är fortsatt giltigt och inte ogiltigförklaras av EU-domstolen. DSO kommer att säkerställa att detta i så fall uppmärksammas inom ramen för bl.a. ”DSO-informerar”.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs? Ja.		Säkerställ att behandlingsaktiviteter i Draftit är uppdaterat så att alla eventuella tredjelandsöverföringar framgår.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs? Ja.		Det rekommenderas att verksamheten håller sig fortsatt uppdaterade på att adekvansbeslutet för tredjelandsöverföringar till USA (DPF) är fortsatt giltigt och inte ogiltigförklaras av EU-domstolen.
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar? Ja.		Detta behöver säkerställas genom att uppdatera Draftit och kontrollera att eventuella ytterligare tredjelandsöverföringar.

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?

Stockholmshems registerförteckning används genom processtödet Visma Drafit. I dagsläget finns 52 personuppgiftsbehandlingar registrerade som är utspridda på enheterna Utveckling & Marknad, HR, Förvaltning, Underhåll, Ekonomi – Inköp, Bygg & Teknik och VD-stab.

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

Ja. Dels genom dokumentet ”Arbetssätt för dataskyddsorganisationen vid Stockholmshem”, dels genom årliga punktinsatser som framkommer av årshjulet.

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

Ja.

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

Delvis. Migreringen till Draftit är ännu inte fullständig men arbetet fortlöper. Det saknas information om bl.a. ändamål och tidsfrister för radering för många registrerade behandlingar.

Dataskyddsombudets jämförelse med föregående års resultat

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

Registerförteckningen var fullständig under föregående år men arbetet till att migrera behandlingsaktiviteterna till Draftit har kommit längre under detta år.

Dataskyddsombudets bedömning samt rekommendationer

Säkerställ att migreringen till Draftit färdigställs under våren 2026 och att alla registrerade behandlingar innehåller komplett information i syfte att få en bra överblick över verksamhetens behandlingar.

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?

Ja.

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

Ja.

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

Ja.

Dataskyddsombudets jämförelse med föregående års resultat

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

Nej.

Dataskyddsombudets bedömning samt rekommendationer

Dataskyddskommittén bör fortsätta med att utveckla och implementera rutiner där behov finns.

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?

Ja.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Ja.

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

Ja.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Delvis.

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

Delvis.

Dataskyddsombudets jämförelse med föregående års resultat

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

Nej.

Dataskyddsombudets bedömning samt rekommendationer

Verksamheten bör delegera ansvar avseende konsekvensbedömningar och ta fram en prioritetslista över i vilken ordning dessa ska utföras. Verksamheten behöver fortsätta detta arbete och säkerställa att det genomförs.

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?

Ja.

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

7 st.

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

7 st.

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?

Ja, i antalet begäran från de registrerade. Förra året dokumenterades 9 st. begärande varav alla hanterades inom en månad.

Dataskyddsombudets bedömning samt rekommendationer

Eftersom begäran från de registrerade har hanterats på ett sätt som svarar mot dataskyddsförordningens krav föranleder granskningen inga ytterligare rekommendationer.

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?

Genom utbildning och tillgänglig information på intranätet.

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

Ja.

Hur många personuppgiftsincidenter har dokumenterats under året?

4 st.

Hur många personuppgiftsincidenter har anmälts till IMY under året?

1 st.

Dataskyddsombudets jämförelse med föregående års resultat

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

Ja, i antalet personuppgiftsincidenter. Förra året dokumenterades 3 st. personuppgiftsincidenter varav inga rapporterades till IMY.

Dataskyddsombudets bedömning samt rekommendationer

Eftersom de uppkomna personuppgiftsincidenterna har hanterats på ett sätt som svarar mot dataskyddsförordningens krav föranleder granskningen inga ytterligare rekommendationer än att verksamheten bör fortsätta att utbilda medarbetare i upptäckt och hantering av personuppgiftsincidenter samt medvetandegöra var informationen om personuppgiftsincidenter finns på intranätet.

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?

Ja.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

Ja.

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

Ja.

Dataskyddsombudets jämförelse med föregående års resultat

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

Nej.

Dataskyddsombudets bedömning samt rekommendationer

Verksamheten bör inom ramen för migreringen till systemstödet Draftit säkerställa att alla registerade behandlingar innehåller information om tredjelandsöverföringar. DSO anser dock att nuvarande eventuella brister i detta arbete är en låg risk eftersom denna information endast saknas om ett ytterst fåtal behandlingar.

---

[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.

Bilaga 2 – Andra genomförda granskningar och omvärldsbevakning

Andra granskningar som dataskyddsombudet har genomfört under året

Under våren 2025 granskade DSO Stockholmshems webbplats i syfte att undersöka om det sätt som Stockholmshem informerar om användning av cookies och inhämtar samtycke för användning av cookies svarar mot kraven som framkommer av LEK och dataskyddsförordningen. Granskningen föranledde en mängd rekommendationer som därefter följdes upp och åtgärdades.

Det planerade dataskyddsarbetet inom Stockholmshem utförs efter ett ”årshjul” med återkommande aktiviteter. Årshjulet ger Stockholmshem möjlighet att på ett förutsägbart sätt regelbundet göra dataskyddsrelaterade granskningar, revisioner och uppdateringar i syfte att säkerställa lagefterlevnad.

Under våren 2025 granskade DSO vidare årshjulet eftersom det dåvarande årshjulet togs fram i samband med att Stockholmshems dataskyddsorganisation utarbetades våren år 2024 och därför var i behov av en revision. Efter att DSO granskat årshjulet och därefter inkom med rekommendationer har årshjulet justerats för att vara bättre anpassat till Stockholmshems dataskyddsorganisation.

Aktiviteterna i årshjulet är framtagna i syfte att verksamheten regelbundet ska uppdatera och revidera befintliga dokument, rutiner och policies, att granska behovet för ytterligare aktiviteter (t.ex. konsekvensbedömningar och riskanalyser) samt att genomföra granskningar och kontroller.

Under våren 2025 granskade DSO även hur Stockholmshem informerar om behandling av personuppgifter på webbplatsen. Granskningen ledde till en rapport med rekommendationer om förändringar i informationen vilket följdes upp och åtgärdades omedelbart.

Dataskyddsombudets rekommendationer baserat på iakttagelserna ovan var följande och har omhändertagits av Stockholmshem under året.

Dataskyddsombudets rekommendationer
1. Uppdatera informationen om webbplatskakor (färdigt) 2. Revidera och uppdatera årshjulet för det planerade dataskyddsarbetet (färdigt) 3. Uppdatera informationen på webbplatsen (färdigt)

Omvärldsbevakning

DSO är ansvarig för omvärldsbevakning och kompetensöverföring till dataskyddskommittén avseende det senaste inom dataskydd vilket genomförs en gång i månaden i ett informationsmöte som heter ”DSO informerar”. Under mötet gör DSO en presentation av dennes omvärldsbevakning vilket inkluderar genomgång av ny praxis, relevanta beslut från IMY och andra tillsynsmyndigheter avseende dataskydd inom EU samt ny vägledning från EDPB.

Underskriftens äkthet valideras här: https://underskriftpas.stockholm.se/validera

Signerad av
Sofia Forsman

Signaturdatum
2026-03-11 17:10:05

Elektronisk underskrift

underskrift.stockholm.se

Signerad av
Åsa Wigfeldt

Signaturdatum
2026-03-12 14:20:57

Elektronisk underskrift

underskrift.stockholm.se