Stockholms stad

Bilaga 9

GDPR årsrapport

År 2025

Stockholms Stadshus AB

GDPR årsrapport
Mars 2026

Dnr: SSAB 2026/51
Utgivningsdatum: 2026-03-10
Kontaktperson: Simon Jernelöv

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 Stockholms stadshus AB:s dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

Dataskyddsombudet har under 2025 inte involverats löpande i bolagets dataskyddsarbete i någon större omfattning, utan har i huvudsak skapat sig en bild av förhållandena i bolaget genom dokumentgranskning och intervjuer i samband med denna årsrapport.

De tre största riskerna enligt dataskyddsombudets bedömning

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?	🟡	Det saknas dokumenterade rutiner för detta, vilket innebär att principen om ansvarsskyldighet inte efterlevs. Ta fram och implementera rutiner för detta.
Hur många personuppgiftsincidenter har dokumenterats under året?	🟡	Inga personuppgiftsincidenter har dokumenterats under året. Bolaget bör försöka utröna om här finns ett mörkertal och om utbildningsinsatser för personalen därmed kan vara nödvändiga.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?	🟡	Ja, dessa dokumenteras dock inte, vilket innebär att principen om ansvarsskyldighet inte efterlevs. Dokumentera era överväganden i samband med tröskelanalys.

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

Register över personuppgiftsbehandlingar

Sammanfattning

DSO konstaterar att den senast uppdaterade versionen av registerförteckningen som tillhandahållits till DSO är daterad 12 januari 2026, vilket indikerar att registerförteckningen hålls uppdaterad och levande. Bedömningen att registerförteckningen hålls uppdaterad understöds av bolagets internkontrollplan och av uppgifter från de intervjuer som hållits i samband med tillsynsarbetet.

DSO rekommenderar att verksamheten fortsätter att arbeta löpande med registerförteckningen utifrån att nya behandlingar införs eller att gällande behandlingar förändras. DSO rekommenderar att de anställda får information om vad en personuppgiftsbehandling är och hur de ska gå tillväga vid en ny eller förändrad personuppgiftsbehandling, för att säkerställa att registerförteckningen återspeglar bolagets aktuella behandlingar.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		52 stycken.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		Verksamheten har nedtecknade rutiner som anger att registerförteckningen ska överses årligen. Det innebär att verksamheten arbetar med registerförteckningen som ett levande dokument på ett löpande sätt. Det finns även ett utpekat ansvar för uppdatering och översyn av registerförteckningen.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		Med hänsyn till verksamhetens storlek bedömer DSO det som sannolikt att samtliga behandlingar fångas upp med de nuvarande rutinerna för registrering och uppdatering.
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		Behandlingarna i registerförteckningen innehåller de uppgifter som är obligatoriska enligt artikel 30 GDPR.

Säkerhet i samband med behandlingen

Sammanfattning

Dataskyddsombudet upplever att verksamheten har en hög nivå av säkerhetstänk överlag, vilket påverkar även personuppgiftshanteringen i bolaget. Stockholms stadshus tar del av och följer de dokument och rutiner för riskklassificering som Stadsledningskontoret tagit fram inom dataskyddsområdet, vilka i viss utsträckning anpassas utifrån bolagets verksamhet.

DSO bedömer att de skriftliga styrande dokumenten och rutinerna är tillräckligt implementerade och kända inom organisationen. De anställda uppger att de har god kännedom om styrdokumenten och att dessa efterlevs i praktiken. Nyanställda får information om styrdokumenten och var dessa kan hittas.

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 – DSO bedömer att de granskade informationsklassningarna tar sådan hänsyn i tillräcklig utsträckning.
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		Ja – DSO bedömer att de granskade dokumenten erbjuder tillräckligt stöd och innebär en tillräcklig reglering.
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		Ja – DSO bedömer att dokument och rutiner gällande säkerhet i behandlingen är tillräckligt kända bland personalen.

Konsekvensbedömning avseende dataskydd

Sammanfattning

Bolaget har kunskap om vad en konsekvensbedömning är och när den ska göras. Verksamheten har gjort en kartläggning över aktuella personuppgiftsbehandlingar och vid inventering har inga behandlingar hittills bedömts som högriskbehandlingar.

Verksamheten genomför tröskelanalyser men dokumenterar inte dessa. DSO rekommenderar att verksamheten dokumenterar tröskelanalyser för att säkerställa att principen om ansvarsskyldighet uppfylls. Enligt principen är det inte tillräckligt att följa GDPR, man behöver även kunna visa att man följer GDPR, ofta genom dokumentation.

Det saknas rutiner för att vid nya eller förändrade personuppgiftsbehandlingar genomföra tröskelanalyser, det finns dock ett inarbetat arbetssätt för att hantera detta. Med hänsyn till verksamhetens storlek bedömer DSO att det är osannolikt att det uppstår högriskbehandlingar som inte fångas upp av de som är ansvariga för arbetet med konsekvensbedömningar.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		Det saknas dokumenterade rutiner för detta. Ta fram sådana rutiner.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		Ja, dessa dokumenteras dock inte, vilket innebär att principen om ansvarsskyldighet inte efterlevs. Dokumentera era överväganden i samband med tröskelanalys.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		Det finns utpekade ansvariga för genomförandet av konsekvensbedömningar och verksamheten har tillgång till stadens mallar och metodstöd för genomförande av konsekvensbedömning.
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		Inte aktuellt i nuläget.

Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		Hittills har bolaget inte identifierat några högriskbehandlingar i sin verksamhet.

Den registrerades rättigheter

Sammanfattning

Under 2025 har ingen begäran om att utöva registrerades rättigheter inkommit till bolaget, DSO kan därmed inte fullt ut uttala sig om bolagets förmåga att hantera dessa. Verksamheten har dock tidigare år visat god förmåga att hantera dessa inom föreskriven tidsfrist. DSO har tagit del av verksamhetens svar från det senaste begärandet om utövande av registrerades rättigheter, vilket var en begäran om registerutdrag som inkom 2023. I det aktuella fallet förekom inte den registrerades personuppgifter hos bolaget, vilket innebär att saknas formkrav för vad svaret ska innehålla. DSO konstaterar dock att svaret innehöll tydlig information och att begäran hanterades inom föreskriven tidsfrist.

DSO konstaterar att verksamheten har goda förutsättningar att hantera registrerades rättigheter på ett mycket gott sätt. Rutinen för hantering av dessa ärenden tycks vara fullt ut förankrad i verksamheten. Det är väl känt för medarbetarna vem de ska kontakta om en begäran från en registrerad inkommer till bolaget. DSO bedömer att de rutiner som finns nedtecknade för att tillvarata de registrerades rättigheter är väl utformade.

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. Dokumenten har tagits fram i samarbete med DSO tidigare år.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		Inga begäranden har inkommit under året.
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		Inte aktuellt.
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		Ja. DSO har dock bara granskat svar till de registrerade (från 2023) för fall där de registrerades uppgifter inte förekom hos bolaget. Notera att det finns formkrav för vad ett registerutdrag ska innehålla när det förekommer uppgifter om den registrerade hos bolaget.

Personuppgiftsincidenter

Sammanfattning

Bolaget uppger att inga personuppgiftsincidenter har inträffat under året. DSO kan därför inte fullt ut uttala sig om bolagets förmåga att hantera personuppgiftsincidenter.

Vid föregående tillsyn rekommenderade DSO att bolaget skulle anpassa rutinen för personuppgiftsincidenthantering, som då utgick från den rutin som stadsledningskontoret tagit fram och därmed var inte anpassad för bolaget. Bolaget har under året åtgärdat detta och rutinen är numera anpassad för bolagets storlek och typ av verksamhet.

Verksamheten uppger att det finns kunskap om när en incident ska anmälas till IMY samt när de registrerade ska informeras om en incident. Detta säkerställs bland annat genom utbildningar, särskilt till nyanställda.

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?		Detta säkerställs genom utbildning, dokumenterade rutiner och kontinuerliga påminnelser.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		Bolaget har utifrån stadens mall tagit fram en rutin anpassad utifrån bolagets storlek och typ av verksamhet.
Hur många personuppgiftsincidenter har dokumenterats under året?		Inga personuppgiftsincidenter har dokumenterats under året. Bolaget bör försöka utröna om här finns ett mörkertal och om utbildningsinsatser därmed kan vara nödvändiga.
Hur många personuppgiftsincidenter har anmälts till IMY under året?		Inga personuppgiftsincidenter har anmälts till IMY under året.

Överföring till tredje land

Sammanfattning

Bolaget har kunskap om vad en tredjelandsöverföring är och vad detta innebär. Verksamheten har gjort en kartläggning över aktuella personuppgiftsbehandlingar och har bedömt att inga tredjelandsöverföringar hittills sker. Därmed har inga nödvändiga åtgärder identifierats.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		Verksamheten har gjort en kartläggning över aktuella personuppgiftsbehandlingar och har bedömt att inga tredjelandsöverföringar hittills sker.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		Inte aktuellt i nuläget.
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		Inte aktuellt i nuläget.

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

DSO konstaterar att den senast uppdaterade versionen av registerförteckningen som tillhandahållits till DSO är daterad 12 januari 2026, vilket indikerar att registerförteckningen hålls uppdaterad och levande. Bedömningen att registerförteckningen hålls uppdaterad understöds av bolagets internkontrollplan och av uppgifter från de intervjuer som hållits i samband med tillsynsarbetet.

DSO rekommenderar att verksamheten fortsätter att arbeta löpande med registerförteckningen utifrån att nya behandlingar införs eller att gällande behandlingar förändras. DSO rekommenderar att de anställda får information om vad en personuppgiftsbehandling är och hur de ska gå tillväga vid en ny eller förändrad personuppgiftsbehandling, för att säkerställa att registerförteckningen återspeglar bolagets aktuella behandlingar.

Antal behandlingar som är registrerade?

52 stycken.

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

Verksamheten har nedtecknade rutiner som anger att registerförteckningen ska överses årligen. Det innebär att verksamheten arbetar med registerförteckningen som ett levande

dokument på ett löpande sätt. Det finns även ett utpekat ansvar för uppdatering och översyn av registerförteckningen.

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

Ja. Med hänsyn till verksamhetens storlek bedömer DSO det som sannolikt att samtliga behandlingar fångas upp med de nuvarande rutinerna för registrering och uppdatering.

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

Ja. Behandlingarna i registerförteckningen innehåller de uppgifter som är obligatoriska enligt artikel 30 GDPR.

Dataskyddsombudets jämförelse med föregående års resultat

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

Föregående år rekommenderade DSO att de anställda skulle få information om vad en personuppgiftsbehandling är och hur de ska gå tillväga vid en ny eller förändrad personuppgiftsbehandling, för att säkerställa att registerförteckningen återspeglar bolagets aktuella behandlingar. Under året har de anställda fått utbildningar och påminnelser om detta med jämna mellanrum.

Dataskyddsombudets bedömning samt rekommendationer

DSO rekommenderar att verksamheten fortsätter att arbeta löpande med registerförteckningen utifrån att nya behandlingar införs eller att gällande behandlingar förändras. DSO rekommenderar även att bolaget fortsätter arbetet med att kontinuerligt informera de anställda om vad en personuppgiftsbehandling är och hur anställda ska gå tillväga vid en ny eller förändrad personuppgiftsbehandling, för att säkerställa att registerförteckningen återspeglar bolagets aktuella 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 även 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 – DSO bedömer att de granskade informationsklassningarna tar sådan hänsyn i tillräcklig utsträckning.

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

Ja – DSO bedömer att de granskade dokumenten erbjuder tillräckligt stöd och innebär en tillräcklig reglering.

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

Ja – DSO bedömer att dokument och rutiner gällande säkerhet i behandlingen är tillräckligt kända bland personalen.

Dataskyddsombudets jämförelse med föregående års resultat

Stockholm stads mall för 2024 års rapport var annorlunda utformad och frågorna formulerade på ett annat sätt. DSO rekommenderade detta år att bolaget skulle slutföra arbetet med att kontrollera att samtliga genomförda informationsklassningar var aktuella, relevanta och att bolaget vid behov reviderar klassningarna.

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

DSO:s bedömning är att bolagets arbete med säkerhet kring behandlingen har förbättrats. Man uppger att förra årets rekommenderade åtgärd har genomförts och att informationsklassningarna nu har inventerats och bedömts vara relevanta. DSO har också granskat bolagets uppdaterade anvisning för informationssäkerhet och rutin för hantering av behörigheter och bedömer att de organisatoriska säkerhetsåtgärder som anges i dessa dokument är tillfredsställande.

Dataskyddsombudets bedömning samt rekommendationer

Fortsätt arbetet i enlighet med inarbetade rutiner.

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?

Det saknas dokumenterade rutiner för detta.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Ja, dessa dokumenteras dock inte.

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

Det finns utpekade ansvariga för genomförandet av konsekvensbedömningar och verksamheten har tillgång till stadens mallar och metodstöd för genomförande av konsekvensbedömning.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Inte aktuellt i nuläget.

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

Hittills har bolaget inte identifierat några högriskbehandlingar i sin verksamhet.

Dataskyddsombudets jämförelse med föregående års resultat

[Se dokument ”Instruktion för dataskyddsombudets årsrapport” för vägledning.]

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

Föregående tillsyn gav DSO rådet att verksamheten skulle värdera och identifiera de personuppgiftsbehandlingar som kan tänkas utgöra hög risk och kräva konsekvensbedömning. Bolaget har gjort en övergripande kartläggning över aktuella personuppgiftsbehandlingar och vid inventering har inga behandlingar hittills bedömts som högriskbehandlingar.

Dataskyddsombudets bedömning samt rekommendationer

Verksamheten genomför tröskelanalyser men dokumenterar inte dessa. DSO rekommenderar att verksamheten dokumenterar tröskelanalyser för att säkerställa att principen om ansvarsskyldighet uppfylls. Enligt principen är det inte tillräckligt att följa GDPR, man behöver även kunna visa att man följer GDPR, ofta genom dokumentation. Därefter rekommenderar DSO att bolaget säkerställer att alla nödvändiga konsekvensbedömningar genomförts av antingen bolaget, av stadsledningskontoret eller annat organ inom staden.

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

Under 2025 har ingen begäran om att utöva registrerades rättigheter inkommit till bolaget, DSO kan därmed inte fullt ut uttala sig om bolagets förmåga att hantera dessa. Verksamheten har dock tidigare år visat god förmåga att hantera dessa inom föreskriven tidsfrist. DSO har tagit del av verksamhetens svar från det senaste begärandet om utövande av registrerades rättigheter, vilket var en begäran om registerutdrag som inkom 2023. I det aktuella fallet förekom inte den registrerades personuppgifter hos bolaget, vilket innebär att saknas formkrav för vad svaret ska innehålla. DSO konstaterar dock att svaret innehöll tydlig information och att begäran hanterades inom föreskriven tidsfrist.

DSO konstaterar att verksamheten har goda förutsättningar att hantera registrerades rättigheter på ett mycket gott sätt. Rutinen för hantering av dessa ärenden tycks vara fullt ut förankrad i verksamheten. Det är väl känt för medarbetarna vem de ska kontakta om en begäran från en registrerad inkommer till bolaget. DSO bedömer att de rutiner som finns nedtecknade för att tillvarata de registrerades rättigheter är väl utformade.

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

Ja. Dokumenten har tagits fram i samarbete med DSO tidigare år.

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

Inga begäranden om utövande av registrerades rättigheter har inkommit under året.

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

Inte aktuellt.

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

Ja. Eftersom ingen begäran om utövande av registrerades rättigheter inkommit under året har DSO istället tagit del av verksamhetens svar från det senaste begärandet, vilket var en begäran om registerutdrag som inkom 2023. I det aktuella fallet förekom inte den registrerades personuppgifter hos bolaget, vilket innebär att saknas formkrav för vad svaret ska innehålla. DSO konstaterar dock att svaret innehöll tydlig information och att begäran hanterades inom föreskriven tidsfrist.

Dataskyddsombudets jämförelse med föregående års resultat

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

Nej.

Dataskyddsombudets bedömning samt rekommendationer

Eftersom ingen begäran om att utöva de registrerades rättigheter har inkommit under tillsynsåret så kan inte DSO fullt ut uttala sig om bolagets förmåga att hantera dessa. Verksamheten har dock tidigare år visat god förmåga att kunna hantera dessa inom föreskriven tidsfrist. DSO uppmuntrar verksamheten att fortsättningsvis tillmötesgå begäran om att utöva registrerades rättigheter på en sådan god nivå som de hittills har gjort.

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

Bolaget uppger att inga personuppgiftsincidenter har inträffat under året. DSO kan därför inte fullt ut uttala sig om bolagets förmåga att hantera personuppgiftsincidenter.

Verksamheten uppger att det finns kunskap om när en incident ska anmälas till IMY samt när de registrerade ska informeras om en incident. Detta säkerställs bland annat genom utbildningar, särskilt till nyanställda.

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

Detta säkerställs genom utbildning, dokumenterade rutiner och kontinuerliga påminnelser.

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

Bolaget har utifrån stadens mall tagit fram en rutin anpassad utifrån bolagets storlek och typ av verksamhet.

Hur många personuppgiftsincidenter har dokumenterats under året?

Inga personuppgiftsincidenter har dokumenterats under året. Bolaget bör försöka utröna om här finns ett mörkertal och om utbildningsinsatser därmed kan vara nödvändiga.

Hur många personuppgiftsincidenter har anmälts till IMY under året?

Inga personuppgiftsincidenter har anmälts till IMY under året.

Dataskyddsombudets jämförelse med föregående års resultat

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

Vid föregående tillsyn rekommenderade DSO att bolaget skulle anpassa rutinen för personuppgiftsincidenthantering, som då utgick från den rutin som stadsledningskontoret tagit fram och därmed var inte anpassad för bolaget. Bolaget har under året åtgärdat detta och rutinen är numera anpassad för bolagets storlek och typ av verksamhet.

Dataskyddsombudets bedömning samt rekommendationer

DSO rekommenderar bolaget att bibehålla den interna kunskapen om personuppgiftsincidenter genom kontinuerliga utbildningar och påminnelser till anställda. Bolaget bör försöka utröna om här finns ett mörkertal och om ytterligare utbildningsinsatser därmed kan vara nödvändiga.

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

Bolaget har kunskap om vad en tredjelandsöverföring är och vad detta innebär. Verksamheten har gjort en kartläggning över aktuella personuppgiftsbehandlingar och har bedömt att inga tredjelandsöverföringar hittills sker. Därmed har inga nödvändiga åtgärder identifierats.

Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?

Verksamheten har gjort en kartläggning över aktuella personuppgiftsbehandlingar och har bedömt att inga tredjelandsöverföringar hittills sker.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

Inte aktuellt.

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

Inte aktuellt.

Dataskyddsombudets jämförelse med föregående års resultat

[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.

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

Det här området granskades inte föregående tillsyn.

Dataskyddsombudets bedömning samt rekommendationer

DSO rekommenderar att bolaget fortsätter kartlägga aktuella och nya personuppgiftsbehandlingar för att identifiera eventuella tredjelandsöverföringar. Om tredjelandsöverföringar sker ska dessa ske med stöd av ett överföringsverktyg samt föregås av en TIA.

Se även under omvärldsanalys nedan.

Bilaga 2 – Omvärldsbevakning

Omvärldsbevakning

Resultatet av dataskyddsombudets omvärldsbevakning

Oroligt omvärldsläge

Enligt Säpo är den samlade hotbilden mot Sverige allvarlig och det är främst ryska målsättningar och säkerhetshotande verksamhet i närområdet som bidrar till detta. Även om Ryssland således utgör det största övergripande hotet mot Sverige bedriver även andra stater som Iran, Kina och Nordkorea säkerhetshotande verksamhet i vårt land. Det finns enligt Säpo även ett attentatshot från våldsbejakande islamism respektive högerextremism som utgörs av ensamagerande individer eller mindre celler som agerar mot tillgängliga mål med enklare medel. Till detta kan läggas ett hot i form av cyberattacker som enligt Säpo är allvarligt och ökande mot svenska myndigheter - liksom mot företag och privatpersoner. Förövarna kan vara fientliga nationer men även mer eller mindre fristående kriminella nätverk. Sverige utsätts dagligen för IT-attacker, främst med syfte att stjäla data, orsaka driftstopp eller utkräva pengar (ransomware) – i närtid kan nämnas attackerna mot Miljödata och Tietoevry som drabbat många kommuner hårt. Säpo uppger att intensiteten i attacker varit hög så här långt under 2026, med över 2100 attacker per vecka mot svenska verksamheter.

Enligt rapporten ”Det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen” från MSB (2024) har 69 % av myndigheter och organ inom offentlig förvaltning allvarliga brister i sitt cybersäkerhetsarbete. Rapporten konstaterar att det i dessa fall handlar om brister på den mest grundläggande nivån och att kommunerna är den del av offentlig förvaltning som genomgående har svagast resultat. Parallellt med detta oroande resultat har alltså hotbilden mot kritiska samhällssektorer inom både statlig och kommunal förvaltning ökat kraftigt på senare år. FRA med flera myndigheter betonar vikten av att möta de ökande hoten mot cybermiljön, inklusive riktade angrepp mot kritisk infrastruktur, med ökad resiliens.

I början av 2026 trädde Cybersäkerhetslagen i kraft som en implementering av EU:s NIS2-direktiv. SKR kommer med anledning av detta att under våren 2026 bjuda in till en kraftsamling, syftande till att gemensamt stärka kommunsektorns förmåga att förebygga, upptäcka och hantera cyberangrepp. Genom att samla arbetet nationellt är deras syfte att skapa en mer likvärdig, robust och uthållig cybersäkerhetsförmåga än vad enskilda kommuner kan förväntas åstadkomma var för sig.

Även om det finns skäl att hålla isär begreppen ”dataskydd” som har fokus på data i form av personuppgifter, och ”cybersäkerhet” som omfattar elektroniskt behandlad information i vidare mening, kan även konstateras att säkerhetsarbetet på dessa båda områden ofta kan och bör samordnas.

Risker i samband med tredjelandsöverföring

Frågan om s.k. tredjelandsöverföring av personuppgifter till USA har tidigare varit aktuell, inte minst genom de två ”Schrems-domarna” från EU-domstolen där två tidigare adekvansbeslut från EU-kommissionen gentemot USA har upphävts. I juli 2023 fattade EU-kommissionen ett nytt beslut om adekvat skyddsnivå för USA. Beslutet innebär att det i nuläget är möjligt för företag och organisationer, att på ett lagligt sätt överföra alla typer av

personuppgifter till företag och organisationer i USA, som är certifierade enligt ett ramverk för dataskydd, ”EU-US Data Privacy Framework” (DPF).

Den nuvarande amerikanska presidentadministrationen har emellertid vidtagit ett antal åtgärder, bl.a. genom att avskeda majoriteten av ledamöterna i den oberoende styrelse (PCLOB) som skulle övervaka att DPF följs, vilka föranlett de svenska och norska tillsynsmyndigheterna att komma med uttalanden. IMY påtalar att ifall det finns information som visar att ett adekvat skydd inte längre kan säkerställas kan EU-kommissionen återkalla, ändra eller upphäva ett beslut om adekvat skyddsnivå. Dessutom har EU-domstolen möjlighet att ogiltigförklara ett beslut om adekvat skyddsnivå (vilket som sagt skett tidigare).

Den norska tillsynsmyndigheten Datatilsynet anger i information på sin hemsida att även om vi för närvarande har ett adekvansbeslut som gör att det är tillåtet att överföra personuppgifter till USA, förväntar man sig att adekvansbeslutet förr eller senare kommer att ifrågasättas i EU-domstolen. Man skriver vidare att verksamheter, när de köper amerikanska data-tjänster, behöver vara medvetna om att situationen i USA även har bidragit till osäkerhet. Det är därför viktigt att personuppgiftsansvariga som genomför tredjelandsöverföringar skaffar en exitstrategi för hur man ska agera om det inte längre är tillåtet att överföra personuppgifter till USA på samma sätt som idag. Datatilsynet menar att även användningen av amerikanska molntjänster på europeisk mark skulle påverkas negativt om adekvansbeslutet upphävs.