Bilaga 5

Stockholms stad

GDPR årsrapport

År 2025

SISAB

GDPR årsrapport
Januari 2026

Dnr: 2026/26
Utgivningsdatum: 2026-01-20
Kontaktpersoner: Peter Sundström, Nils Lundborg

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 SISAB:s dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

De viktigast rekommendationerna sammanfattas i nedanstående tabell.

De fyra största riskerna enligt dataskyddsombudets bedömning:

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Registerförteckningen		Bolaget behöver prioritera att säkerställa en aktuell registerförteckning för att kunna identifiera eventuella högriskbehandlingar och vilken tredjelandsöverföring som sker vid anlitande av underleverantör/underbiträde. Att området lämnats ohanterat en längre period ökar risken för brister i efterlevnaden av skyddet för den registrerade. En organisation med tydlighet vem som ansvarar för respektive personuppgiftsbehandling behöver sättas.
Säkerhet vid behandling		Kunskap om dataskyddspraxis angående säkerhet för integritetskänsliga personuppgifter såsom personnummer och lön behöver öka genom utbildning. Bolaget behöver även börja använda krypterad mejl och funktioner såsom säkra meddelanden. Hög risk för sanktionsavgift vid granskning av tillsynsmyndighet om kryptering ej används.
Tredjelandsöverföring och AI		Kontroll över faktisk och potentiell tredjelandsöverföring vid anlitande av underleverantörer. Fortsätta använda stadens pub-avtal med instruktion och uppdatera registerförteckningen. Dokumentera underleverantörs användning av AI i HR-tjänster för att säkerställa efterlevnad av AI-förordningen och GDPR.
Att operativt ansvariga för integritetsarbetet inte utsetts		Integritetsskydd måste integreras i ledningens genomgång och få resurssatta aktiviteter utifrån årets DSO-årsrapport för att få styrfart.

		Framtagna metodstöd såsom att bedöma behov av konsekvensbedömning och tredjelandsöverförings-bedömning ska kunna användas.

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 (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 bolagsnivå. I Stockholms stad innebär det att dataskyddsombudet rapporterar till styrelsen.

Dataskyddsombudet lämnar årligen en rapport om verksamhetens dataskyddsarbete till styrelsen. Genom rapporten kan styrelsen ta emot de råd och rekommendationer som dataskyddsombudet lämnar. Årsrapporten syftar till att styrelsen ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Årsrapporten är ett medel för styrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Granskning av dataskyddsarbetet 2025

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 denne 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.

Resultat från granskningen av de sex obligatoriska områdena

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

Granskningen visar att bolaget i huvudsak har etablerade strukturer för hantering av personuppgiftsbehandlingar, men att flera brister och förbättringsbehov kvarstår från föregående år. Det finns i dagsläget 58 registrerade personuppgiftsbehandlingar, vilka behöver ses över för att säkerställa att samtliga följer stadens mall, är korrekt kopplade till relevanta processer och har utsedda ansvariga som löpande upprätthåller kvaliteten i registerförteckningen. Utan en sådan översyn finns en risk att högriskbehandlingar förbises.

Rutinerna för att identifiera nya personuppgiftsbehandlingar bedöms fungera relativt väl genom koppling till informationsklassning, medan ansvaret för att fånga upp och registrera förändringar i befintliga behandlingar behöver tydliggöras. Om detta inte sker finns en risk att ändrade behandlingar inte registreras eller uppdateras i tid. Vidare rekommenderas en samlad genomgång under 2026 för att säkerställa att registret fullt ut speglar samtliga personuppgiftsbehandlingar som den personuppgiftsansvarige utför.

Slutligen konstateras att de obligatoriska uppgifterna enligt artikel 30 i dataskyddsförordningen finns med i den mall som används, men att äldre registreringar behöver kontrolleras och uppdateras för att säkerställa fullständighet och aktualitet. Om detta inte genomförs finns en risk att väsentlig information saknas, vilket kan påverka både regelefterlevnad och styrning negativt

Bedömning av risknivå och rekommendationer från dataskyddsombudet:

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		Det finns idag 58 registrerade personuppgiftsbehandlingar hos bolaget. En översyn behöver göras så att samtliga följer stadens mall, är kopplade till en process och har en ansvarig person som upprätthåller kvaliteten i registerförteckningen. Risk om inget görs är att någon högriskbehandling missas.

Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		Nya behandlingar fångas upp i samband med informationsklassningar, vid nyanskaffning av system eller årlig omklassning av system/informationsmängder. För förändrade behandlingar behöver ansvaret tydliggöras. Risk om inget görs är att förändringar inte fångas upp.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		En genomgång behöver utföras under 2026 för att säkerställa att inga personuppgiftsbehandlingar missas.
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		Ja, finns med i stadens mall men behöver säkerställas att äldre registreringar följer den och är uppdaterade. Risk om inget görs är att viktiga frågor missas.

Säkerhet i samband med behandlingen

Årets genomgång visar att dataskyddsarbetet i verksamheten i huvudsak är väl integrerat i befintliga processer och styrning. Efter genomförda stickprov bedömer dataskyddsombudet att informationsklassningarna i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter, vilket bedöms vara en naturlig och etablerad del av klassningsarbetet som bör fortsätta.

Vidare konstateras att det finns ändamålsenliga styrande dokument och rutiner inom informationssäkerhet där dataskydd är inkluderat. Dessa ger tillräckligt stöd för verksamheten och kompletteras av etablerade rutiner för årlig revidering, vilket säkerställer att dokumentationen hålls aktuell.

Slutligen bedöms de skriftliga styrande dokumenten och rutinerna vara tillräckligt implementerade och kända i organisationen, bland annat genom att de regelbundet uppmärksammas och följs upp i samband med den årliga revisionen.

Bedömning av risknivå och rekommendationer från dataskyddsombudet:

Fråga/kontroll	Risk	Rekommendationer
Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att resultatet i		Är en naturlig del i klassningsarbetet och ska fortsätta vara så.

genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?		
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		Det finns bra styrdokument kring informationssäkerhet där dataskydd är inkluderat. Rutiner för revidering av styrande dokument finns som säkerställer årlig översyn.
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		De styrande dokumenten uppmärksammas vid den årliga revisionen.

Konsekvensbedömning avseende dataskydd

Genomgången visar att det i huvudsak finns ändamålsenliga rutiner och stöd för att hantera tröskelanalyser och konsekvensbedömningar avseende dataskydd. Rutiner för att genomföra tröskelanalyser vid nya eller förändrade personuppgiftsbehandlingar är integrerade i arbetet med registerförteckningen och tillämpas i samband med registrering och uppdatering av behandlingar.

Vidare konstateras att det finns väl utformade mallar och metodstöd för genomförande av konsekvensbedömningar avseende dataskydd, framtagna under 2024 och 2025. Dessa används i de fall där en konsekvensbedömning krävs. Samtidigt rekommenderas att registerförteckningen genomlyses för att säkerställa att samtliga personuppgiftsbehandlingar som kan omfattas av krav på konsekvensbedömning har identifierats och att behovet av sådan bedömning korrekt har prövats för respektive behandling.

Bedömning av risknivå och rekommendationer från dataskyddsombudet:

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		Följer av rutinen för registerförteckningen av personuppgiftsbehandlingar.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		Följer av rutinen för registerförteckningen av personuppgiftsbehandlingar.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		Bra mallar och metodstöd har tagits fram under 2024 och 2025.
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		Mall finns framtagen och används i de fall det krävs.
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		Vid genomlysning av registerförteckningen bör det säkerställas att konsekvensbedömning inte behöver göras för någon av de berörda behandlingarna.

Den registrerades rättigheter

Verksamheten har ändamålsenliga mallar och rutiner för att hantera och besvara begäranden från registrerade enligt dataskyddsregelverket. Under året har dock inga begäranden om exempelvis registerutdrag, begränsning eller radering inkommit, vilket innebär att frågor om handläggningstider och kvalitet i svaren inte har varit aktuella att pröva. Därmed har heller inga stickprov kunnat genomföras för att bedöma om svaren uppfyller lagkraven.

Bedömning av risknivå och rekommendationer från dataskyddsombudet:

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		Mallar och rutiner finns framtagna.
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?		Ej aktuellt.
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		Ej aktuellt.

Personuppgiftsincidenter

SISAB arbetar aktivt med att säkerställa medarbetarnas kunskap om hantering av personuppgiftsincidenter, bland annat genom årlig uppföljning av stadens utbildning i dataskydd. Ändamålsenliga rutiner för hantering av potentiella personuppgiftsincidenter finns på plats, men dessa har ännu inte behövt testas i praktiken. Under året har inga incidenter dokumenterats, och därför har heller inga anmälningar till IMY varit aktuella.

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?		Genomförande av stadens utbildning i Dataskydd följs årligen upp.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		Rutiner finns. Har ej behövt testas skarpt ännu.
Hur många personuppgiftsincidenter har dokumenterats under året?		En, enligt ledningens genomgång.
Hur många personuppgiftsincidenter har anmälts till IMY under året?		Inga incidenter har anmälts till IMY.

Överföring till tredje land

Årets granskning visar att arbetet med tredjelandsöverföringar av personuppgifter pågår och behöver fortsätta under 2026 för att säkerställa att samtliga överföringar har identifierats. För de överföringar som redan har identifierats tillämpar personuppgiftsansvarig stadens mallar baserade på standardavtalsklausuler (SCC) för att säkerställa laglig och säker överföring. Dessutom genomförs en nödvändig bedömning, så kallad Transfer Impact Assessment (TIA), för de tredjelandsöverföringar som identifierats, vilket säkerställer att eventuella risker i mottagarlandet bedöms och hanteras.

Bedömning av risknivå och rekommendationer från dataskyddsombudet:

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		Arbete pågår men behöver fortsätta under 2026 för att säkerställa att samtliga tredjelandsöverföringar har fångats upp.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		SISAB använder stadens mallar som är anpassade utifrån standardavtalsklausuler (SCC).
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		Genomförs på de tredjelandsöverföringar som har identifierats.

Bilagor

Bilaga 1: Detaljerad redovisning av dataskyddsombudets granskning

Bilaga 2: Rekommendationer 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?

Det finns idag 58 registrerade personuppgiftsbehandlingar hos bolaget. En översyn behöver enligt verksamheten göras så att samtliga följer stadens mall, är kopplade till en process och har en ansvarig person som upprätthåller kvaliteten i registerförteckningen. Risk om inget görs är att någon högriskbehandling missas.

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

Nya behandlingar fångas enligt verksamheten upp i samband med informationsklassningar, vid nyanskaffning av system eller årlig omklassning av system/informationsmängder. För förändrade behandlingar behöver ansvaret tydliggöras. Risk om inget görs är enligt verksamheten att förändringar inte fångas upp.

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

En genomgång behöver enligt verksamheten utföras under 2026 för att säkerställa att inga personuppgiftsbehandlingar missas.

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

Verksamheten uppger att det finns med i stadens mall men behöver säkerställas att äldre registreringar följer den och är uppdaterade. Man uppger vidare att det föreligger en risk att viktiga frågor missas om inget görs.

Dataskyddsombudets jämförelse med föregående års resultat

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

Verksamheten har tillsammans med dataskyddsombudet genom rådgivning och utbildning 2025 registerförtecknat ett antal personuppgiftsbehandlingar i registerförteckningsverktyget Visma Draftit Records. Dessa är följande;

- Planera verksamheten,
- Följa upp verksamheten
- Bedriva verksamhetsutveckling
- Handlägga remisser
- Hantera arbetsmiljö och gemensamma personalfrågor
- Att upphandla,
- Att informera, marknadsföra, kommunicera och dokumentera
- Att informera och marknadsföra - extern & intern webb
- Kamerabevakning
- Utföra byggprojekt

Ovanstående processer har utpekad ansvarig i verksamheten och den utpekade ansvarige har tillgång till behandlingsprocessen i registerförteckningsverktyget för att uppdatera informationen vid förändringar. Den utpekade ansvarige har även utbildats i dataskydd av dataskyddsombudet.

Behandlingsprocesser avseende anställda, såsom, rekrytera, hantera anställning & avsluta/förändrade anställningsförhållanden, beräkna och betala ut löner och arvoden, hantera personalsociala frågor och hantera rehabilitering och arbetsskada, har utpekade ansvariga, men är kvar att registerförteckna med nödvändig information.

Dataskyddsombudets bedömning samt rekommendationer

Bolaget behöver prioritera att säkerställa en aktuell registerförteckning för att kunna identifiera eventuella högriskbehandlingar och vilken tredjelandsöverföring som sker vid anlitande av underleverantör/underbiträde.

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?

Verksamheten uppger att detta är en naturlig del i klassningsarbetet och att det ska fortsätta vara så.

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

Verksamheten uppger att det finns bra styrdokument kring informationssäkerhet där dataskydd är inkluderat. Likaså att rutiner för revidering av styrande dokument finns, som säkerställer årlig översyn.

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

Verksamheten uppger att de styrande dokumenten uppmärksammas vid den årliga revisionen.

Dataskyddsombudets jämförelse med föregående års resultat

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

Dataskyddsombudet har i varierande omfattning under 2025 deltagit vid faktiska informationsklassningar och delat tillsynspraxis i form av tillsynsbeslut avseende vilka tekniska och organisatoriska säkerhetsåtgärder som behöver implementeras.

Då SISAB till stor del upphandlar leverantörer som behandlar personuppgifter för SISAB:s räkning har övervägande fokus 2025 varit att tillsammans med verksamheten att ställa krav

om inbyggt dataskydd och dataskydd som standard i upphandling samt att stadens mall för personuppgiftsbiträdesavtal används vid anlitande av leverantör i egenskap såsom personuppgiftsbiträde.

SISAB har under 2025 utfört ett mycket omfattande arbete med att införliva stadens personuppgiftsbiträdesavtalsmall vid tecknande av personuppgiftsbiträdesavtal. Dataskyddsombudet har bistått med omfattande råd och vid avtalsförhandling med leverantör.

Dataskyddsombudets bedömning samt rekommendationer

Kunskap om dataskyddspraxis angående säkerhet för integritetskänsliga personuppgifter såsom personnummer och lön behöver öka genom utbildning. Bolaget behöver även börja använda krypterad mejl och funktioner såsom säkra meddelanden.

3. Konsekvensbedömning avseende dataskydd

Bakgrund och syfte

En konsekvensbedömning avseende dataskydd krävs när personuppgiftsansvarig planerar att inleda en personuppgiftsbehandling som innebär hög risk för de registrerade. Huruvida en behandling innebär hög risk eller inte behöver personuppgiftsansvarig avgöra genom att genomföra en s.k. tröskelanalys.

En konsekvensbedömning ska vara genomförd för samtliga behandlingar som innebär hög risk, vilket innebär att personuppgiftsansvarig även behöver kontrollera huruvida denne utför befintliga behandlingar som innebär hög risk. Om högriskbehandlingar utförs för vilka en konsekvensbedömning inte har gjorts, behöver personuppgiftsansvarig genomföra en sådan.

Genom att genomföra en konsekvensbedömning kan personuppgiftsansvarig identifiera risker med en personuppgiftsbehandling, hantera riskerna genom åtgärder och rutiner samt påvisa ansvarsskyldighet. Genom konsekvensbedömningar kan risker identifieras och förebyggas.

Syftet med detta rapporteringsområde är att rapportera huruvida verksamheten har ändamålsenliga rutiner som möjliggör att tröskelanalyser och konsekvensbedömningar genomförs, huruvida sådana genomförs när det krävs samt huruvida personuppgiftsansvarig har genomfört konsekvensbedömningar för de behandlingar som kräver det.

Kontroller och iakttagelser gjord av dataskyddsombudet

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

Följer av rutinen för registerförteckningen av personuppgiftsbehandlingar enligt verksamheten.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Följer av rutinen för registerförteckningen av personuppgiftsbehandlingar enligt verksamheten.

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

Ändamålsenliga mallar och metodstöd har tagits fram under 2024 och 2025 enligt verksamheten.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Mall finns framtagen och används i de fall det krävs enligt verksamheten.

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

Vid genomlysning av registerförteckningen behöver det säkerställas huruvida konsekvensbedömning behöver göras för någon av de berörda behandlingarna enligt verksamheten.

Dataskyddsombudets jämförelse med föregående års resultat

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

Dataskyddsombudet har under 2025 tagit fram en ny mall för tröskelanalys och konsekvensbedömning avseende dataskydd som följer tillsynsmyndighetens metodstöd och vägledning. Att välja att implementera tillsynsmyndighetens metodstöd och vägledningar skapar en effektivitet, då själva metodstödets innehåll är i linje med tillsynsmyndighetens krav och underlättar vid en granskning eller när behov av förhandssamråd med tillsynsmyndigheten inför en förestående personuppgiftsbehandling föreligger.

Dataskyddsombudets bedömning samt rekommendationer

Registerförteckningen behöver färdigställas och vid genomlysning av registerförteckningen behöver det återigen säkerställas huruvida konsekvensbedömning behöver göras för någon av de berörda behandlingarna enligt verksamheten.

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?

Mallar och rutiner finns framtagna enligt verksamheten.

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?

Såvitt känt har inga begäranden inkommit under granskningsperioden.

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

Se ovan.

Dataskyddsombudets jämförelse med föregående års resultat

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

Under 2024/2025 har dataskyddsombudet tagit fram en rutin för tillgång till personuppgifter ett s.k. registerutdrag och tillhörande svarsmall för registerutdrag till den registrerade med användande av SISAB:s grafiska profil. Rutinen bygger på vägledning från Europeiska dataskyddstyrelsen vägledning om rätt till tillgång och hur tillsynsmyndigheten svarar den registrerade vid en faktisk begäran om registerutdrag. Under 2025 har ingen förfrågan om rätt till tillgång inkommit till SISAB och rutinen och svarsmallen har således inte testats och använts av verksamheten. Dataskyddsombudet har haft tillgång till SISAB:s dataskyddsmejl och har under året gett råd i samband med en begäran om radering avseende en rekrytering. Denna har hanterats i tid och korrekt av verksamheten.

Informationstexter till registrerade

Under 2025 har en separat integritetspolicy tagits fram för kamerabevakning och verksamheten har satt sig in i de nya reglerna för kamerabevakning. Verksamheten har även deltagit vid tillsynsmyndighetens informationsseminarium om de nya reglerna. Dataskyddsombudet har även delat information om stadens interna rutiner avseende hantering av utlämnande av kameramaterial.

Dataskyddsombudets bedömning samt rekommendationer

SISAB har årligen, så även 2025, sett över den övergripande integritetspolicyn och inhämtat dataskyddsombudets råd avseende behov av uppdatering med anledning av ny tillsynspraxis gällande innehåll och utformning. Dataskyddsombudet anser att motsvarande översyn med fördel kan genomföras även under 2026.

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?

Genomförande av stadens utbildning i Dataskydd följs årligen upp enligt verksamheten.

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

Ja, såvitt är känt.

Hur många personuppgiftsincidenter har dokumenterats under året?

En, enligt ledningens genomgång, se nedan.

Hur många personuppgiftsincidenter har anmälts till IMY under året?

Under 2025 har inga incidenter anmälts till IMY.

Dataskyddsombudets jämförelse med föregående års resultat

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

Från ledningens genomgång 2025: ”Under perioden 3 november 2024 tom 3 november 2025 har 8 stycken informationssäkerhetsincidenter rapporterats i IA-systemet, en minskning jämfört med föregående år.

Av dessa 8 incidenter var endast en verksamhetspåverkande, detta var nätverksproblem i stadens nät, och en personuppgiftsrelaterad, SISAB-filmer med personuppgifter var uppladdade på Youtube. Resterande var rapporterade i informerande syfte så som borttappade mobiler, kort och phishing-mail.”

Dataskyddsombudets bedömning samt rekommendationer

SISAB rekommenderas att fortsätta sprida kunskap i verksamheten om hur personuppgiftsincidenter upptäcks och hanteras, exempelvis på APT möten.

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?

Arbete pågår enligt verksamheten men behöver fortsätta under 2026 för att säkerställa att samtliga tredjelandsöverföringar har fångats upp.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

SISAB använder stadens mallar som är anpassade utifrån standardavtalsklausuler (SCC).

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

Genomförs enligt verksamheten på de tredjelandsöverföringar som har identifierats.

Dataskyddsombudets jämförelse med föregående års resultat

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

En tredjelandsöverföringsbedömning har gjorts för twoday INSIKT och den begränsade användningen av molntjänsten JIRA i anslutning till twoday INSIKT.

Vid avtalstecknande 2025 har även leverantörs tredjelandsöverföringsbedömningar, TIA, granskats av dataskyddsombudet och rådgivning har getts till ansvarig i verksamheten.

SISAB har även tidigt involverat dataskyddsombudet i arbetet med att utländsk leverantör flaggar för utbyte från befintlig on-prem-lösning till molnlösning som genererar behov av fördjupad tredjelandsöverföringsbedömning.

---

[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.

Dataskyddsombudets bedömning samt rekommendationer

Genomföra kontroll över faktisk och potentiell tredjelandsöverföring vid anlitande av underleverantörer. Fortsätta använda stadens pub-avtal med instruktion och uppdatera registerförteckningen. Dokumentera underleverantörs användning av AI i HR-tjänster för att säkerställa efterlevnad av AI-förordningen och GDPR.

Bilaga 2 – Rekommendationer och omvärldsbevakning

Dataskyddsombudets rekommendationer baserat på iakttagelserna ovan

Dataskyddsombudets rekommendationer
1. Bolaget behöver prioritera att säkerställa en aktuell registerförteckning för att kunna identifiera eventuella högriskbehandlingar och vilken tredjelandsöverföring som sker vid anlitande av underleverantör/underbiträde. Att området lämnats ohanterad en längre period ökar risken för brister i efterlevnaden av skyddet för den registrerade. En organisation med tydlighet vem som ansvarar för respektive personuppgiftsbehandling behöver sättas. 2. Kunskap om dataskyddspraxis angående säkerhet för integritetskänsliga personuppgifter såsom personnummer och lön behöver öka genom utbildning. Bolaget behöver även börja använda krypterad mejl och funktioner såsom säkra meddelanden. Hög risk för sanktionsavgift vid granskning av tillsynsmyndighet om kryptering ej används. 3. Kontroll över faktisk och potentiell tredjelandsöverföring vid anlitande av underleverantörer. Fortsätta använda stadens pub-avtal med instruktion och uppdatera registerförteckningen. Dokumentera underleverantörs användning av AI i HR-tjänster för att säkerställa efterlevnad av AI-förordningen och GDPR.

Omvärldsbevakning

Resultatet av dataskyddsombudets omvärldsbevakning

EU-kommissionens adekvansbeslut gällande tredjelandsöverföringar av personuppgifter mellan EU/EES och USA överprövades efter att en fransk parlamentariker påtalat vad han ansåg var fundamentala brister i skyddet för de registrerade och som inte i tillräcklig utsträckning hade beaktats vid beslutet. EU-domstolen meddelade dock sommaren 2025 att beslutet skulle stå fast. I och med detta har förvaltningar och kommunala bolag kunnat fortsätta med vissa behandlingar som innebär överföring av personuppgifter till USA.

Övrigt att rapportera

Precis som tidigare dataskyddsombud har påtalat måste integritetsskydd integreras i ledningens genomgång och få resurssatta aktiviteter utifrån årets DSO-årsrapport för att få styrfart.

Framtagna metodstöd såsom att bedöma behov av konsekvensbedömning och tredjelandsöverförings-bedömning ska kunna användas.

Övriga observationer

SISAB:s cookiehantering har även granskats och uppdateringsbehov har lyfts avseende ”Mina sidors” cookiehantering. Granskningen har gjorts i samband med att tillsynsmyndigheten publicerat sina tillsynsbeslut avseende kakbanners.[2]

[2] Beslut efter tillsyn enligt dataskyddsförordningen – Aktiebolaget Trav och Galopp, Beslut efter tillsyn enligt dataskyddsförordningen – Aller Media AB och Beslut efter tillsyn – Warner Music Sweden AB

Attesterat av

Detta dokument har godkänts digitalt av följande personer:

Namn	Datum
Ebba Bock Agerman, VD	2026-01-21
Anders Lundbeck, Ekonomichef	2026-01-21