Stockholms stad

Dataskyddsombudets GDPR årsrapport

2025

Stockholm Business Region AB

GDPR årsrapport
Januari 2026

Dnr: SBR 2026/10
Utgivningsdatum: 2026-01-16
Kontaktperson: Annette Bengtsson

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 (DSO) har i uppdrag att oberoende granska verksamhetens efterlevnad av dataskyddsförordningen. I denna rapport redovisar dataskyddsombudet årets granskning av Stockholm Business Region AB:s (nedan benämnd SBR) dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

SBR har under 2025 systematiskt och riskbaserat arbetat med att införliva de rekommendationer som DSO lämnat i sin årsrapport för 2024. ISAM har varit operativt ansvarig och DSO:s kontaktpunkt. DSO har i veckovisa avstämningar kunnat lämna oberoende råd utifrån de personuppgiftsbehandlingar som SBR utför. I den transparenta kommunikationen har även DSO kunnat granska aktiviteter och löpande kunnat ge råd avseende personuppgiftsbehandling.

SBR är stadens näringslivs- och destinationsbolag med uppgift att utveckla och marknadsföra Stockholm som etablerings- och besöksdestination internationellt och nationellt. Detta innebär att SBR behöver befinna sig i tidsenliga och ibland internationella kanaler. Detta ställer krav på att förstå regelverket för tredjelandsöverföring och hur det ska hanteras.

Dataskyddsregelverket är under ständig uppdatering genom tillsyns- och domstolspraxis, vilket gör att regelverkets detaljnivå kan upplevas som komplex och kräver utbildningsinsatser och omvärldsbevakning. Det innebär att vissa bedömningar i nedan rapport har definierats med en mindre dataskyddsrisk, då det är viktigt att SBR fortsätter de aktiviteter som genomförts och påbörjats under 2025, såsom tredjelandsöverföringsbedömningar och vid behov konsekvensbedömning avseende dataskydd. Val av risknivå som mindre risk har sin grund i SBR:s kärnuppgift att utveckla och marknadsföra Stockholm som etablerings- och besöksdestination internationellt och nationellt.

För att hantera dataskyddsrisk rekommenderas SBR även i dialog med verksamheten och genom utbildning att kontrollera hur verksamheten faktiskt använder AI och personuppgifter för att säkerställa att framtagna styrdokument efterlevs.

EU-kommissionen har lämnat förslag om uppdateringar i dataskyddsförordningen som avser att förenkla regelverket. Detta förslag ska nu behandlas av rådet och Europaparlamentet. Om förenklingar kommer att genomföras i regelverket påverkar det de aktiviteter som SBR behöver genomföra framgent, vilket gör att även detta behöver omvärldsbevakas.

De tre största riskerna enligt dataskyddsombudets bedömning

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Tredjelandsöverförings-bedömningar	Risken påverkas av vilka tjänster som används.	Vid förändrade/nya tjänster där SBR ska behandla personuppgifter behöver tredjelandsöverföringsbedömningar fortsätta utföras.

		Användande av AI och tjänster med ägandeskap utanför EU/EES generar ofta tredjelandsöverföring.
Omhändertagande av ny praxis och omvärldsbevakning	Dataskyddsrisken påverkas av vilken omvärldsbevakning och utbildnings-insats som utförs.	Denna aktivitet har stor påverkan på dataskyddsrisk. Att regelverket är under ständig utveckling kräver utbildnings-insatser.
Användande av ny teknik och verksamhetens användande av personuppgifter	Dataskyddsrisken påverkas av vilka utbildningsinsatser och kontroller i dialog med verksamheten som utförs.	Omfattande EU-regelverk kräver kunskap om regelverken och att kontroll av verksamhetens användning av tjänsterna, i dialog med verksamheten, utförs.

Innehållsförteckning

Sammanfattning 1
Inledning 4
Dataskyddsombudets uppgift 4
Granskning av dataskyddsarbetet 2025 4
Kontroll av obligatoriska områden 4
Resultatsammanställning och centrala iakttagelser inom dataskyddsarbetet 5
Register över personuppgiftsbehandlingar 5
Säkerhet i samband med behandlingen 7
Konsekvensbedömning avseende dataskydd 8
Den registrerades rättigheter 9
Personuppgiftsincidenter 10
Överföring till tredje land 11
Övrigt att rapportera 12
Bilagor 12
Bilaga 1 - Redovisning av dataskyddsombudets granskning 13
Bilaga 2 – Andra genomförda granskningar och omvärldsbevakning 20

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 person-uppgifter 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 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 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

SBR:s personuppgiftsbehandlingar är processbaserade utifrån stadens arkivprocesser som återfinns i stadens hanteringsanvisningar med tillägg för SBR:s kärnområden. Det innebär att SBR har en god helhetsgrund för sin informationsförvaltning och de personuppgifts-behandlingar som faktiskt sker. Ett ambitiöst arbete har utförts med att erhålla en fullständig registerförteckning

Med förflyttningen och användande av nya externa tjänster som tillhandahålls av bolag med utländskt ägandeskap är det emellertid viktigt att registerförteckningen hålls *uppdaterad* avseende vilka tjänster som faktiskt används av verksamheten och i vilka arkiv- och behandlingsprocesser tjänsterna används så att exponeringen är väl synlig i registerförteckningen. Detta för att ledningen ska ha fullständig kontroll över möjlig exponering och effektivt kunna utföra stadens exit-strategi vid behov. Vid användande av stadens mall för personuppgiftsbiträdesavtal med instruktion finns goda förutsättningar att hantera om EU-kommissionens adekvansbeslut ogiltigförklaras eller inte förlängs avseende

exempelvis USA och Storbritannien. Mall för personuppgiftsbiträdesavtal omhändertar även om leverantör uppvisar brott mot EU:s dataskyddsregelverk.

Utifrån hur verksamheten arbetar idag rekommenderas att en arbetsordning skapas mellan arkivfunktion och registerförteckningsfunktion så att förändringar av hanteringsanvisningarna effektivt och systematiskt omhändertas i registerförteckningen. Vidare rekommenderas att ansvarig i den faktiska verksamheten får ett större inflytande i registerförteckningen över sin process så att den löpande hålls uppdaterad. Detta effektiviserar arbetet och säkerställer att förteckningen är korrekt.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?	Inget att anmärka 	SBR har registerförtecknat 65 stycken personuppgiftsbehandlingar ur ett processperspektiv utifrån stadens arkivprocesser.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?	Låg risk 	SBR rekommenderas att i rutiner sammanhålla arkiv- och registerförteckningsfunktionen. Detta underlättar att förändringar i arkivprocesserna effektivt omhändertas i registerförteckningsprocesserna.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?	Låg risk 	Behandlingar är registerförtecknade men behöver uppdateras när nya tjänster används som särskilt generar dokumentering avseende tredjelandsöverföring. Avsaknaden av dokumentering av tredjelandsöverföring kan i förlängning påverka och öka dataskyddsrisk.
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?	Inget att anmärka 	SBR:s registerförteckning innehåller svar avseende obligatoriska uppgifter enligt artikel 30 i GDPR. Uppdateringsbehov, se ovan.

Säkerhet i samband med behandlingen

SBR:s informationssäkerhetssamordnare (nedan ISAM) arbetar riskbaserat med informationsklassning i enlighet med stadens riktlinje för informationssäkerhet och tillhörande tillämpningsanvisning. Informationsklassning utförs utifrån SKR:s verktyg KLASSA och SBR har tagit del av SLK:s kravmall för informationsklassning, där GDPR-frågorna har, enligt DSO:s egen synpunkt, förbättrats i jämförelse med GDPR-kraven i KLASSA.

ISAM är av DSO informerad om att tillsynspraxis kräver att vissa personuppgifter behöver hanteras krypterat, såsom lön och personnummer även om dessa kan få förekomma i en offentlig handling. Integritetskänsliga uppgifter är vidare uppgift om t.ex. brott och resultat avseende personlighetstester. Känsliga personuppgifter, definierade i dataskyddsförordningen, kräver även en högre nivå av säkerhet. [1]

Dagens omvärldsbevakning och faktiska händelser avseende cyberangrepp visar att det föreligger en dataskyddsrisk vid utkontraktering av IT-drift om personuppgifter behandlas.

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?	Inget att anmärka 	ISAM har under 2025 regelbundet stämt av genomförda informationsklassningar med DSO. Vid dessa tillfällen har DSO bland annat påtalat behov av kryptering och behov av utbildning. SBR använder även personuppgiftsbiträden, dvs. underleverantörer, där deras IT-policys och informationssäkerhet har granskats av ISAM och DSO under 2025. Utifrån omvärldsbevakning och de cyberattacker som externa leverantörer idag utsätts för finns det alltid en ökad dataskyddsrisk vid utkontraktering.
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?	Inget att anmärka 	SBR följer det regelverk för informationssäkerhet som staden implementerat.

[1] Känsliga personuppgifter | IMY (2026-01-11). I länken behandlas även extra skyddsvärda personuppgifter (integritetskänsliga personuppgifter)

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?	Inget att anmärka 	DSO bedömer att skriftligt styrande dokument och rutiner som finns är implementerade och kända. Rutiner och checklistor finns även publicerade på SBR:s intranätet.

Konsekvensbedömning avseende dataskydd

SBR har under 2025 implementerat och tillämpat tillsynsmyndighetens (IMY) metodstöd och vägledning för tröskelanalys och konsekvensbedömning avseende dataskydd. DSO:s råd från GDPR-årsrapport 2024 har således omhändertagits. Att genomföra konsekvensbedömning avseende dataskydd är ett effektivt sätt att identifiera, dokumentera och åtgärda integritets-/dataskyddsrisker.

DSO rekommenderar att metodstöden fortsatt används när behov föreligger. För att identifiera behov, följ tillsynsmyndighetens vägledning[2] och ny DSO-funktions rådgivning under 2026.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys och konsekvensbedömning?	Låg risk 	SBR har på sitt intranät lagt till information om tröskelanalys och konsekvensbedömning avseende dataskydd. En intern rutin bör tas fram för att säkerställa att tröskelanalyser faktiskt genomförs av verksamheten
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?	Inget att anmärka 	SBR har under 2025 genomfört tröskel-analys vid ny personuppgiftsbehandling. Arbetet behöver emellertid, när behov föreligger, fortgå för att hantera integritetsrisker.
Finns det en ändamålsenlig mall för genomförande av konsekvensbedömning avseende dataskydd?	Inget att anmärka 	SBR tillämpar av tillsynsmyndigheten (IMY) publicerade metodstöd, mall och vägledning.

[2] Konsekvensbedömning enligt GDPR | IMY (2026-01-11)

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?	Låg risk 	Utifrån SBR:s verksamhet att marknadsföra Stockholm och att främja företags-verksamhet behandlas huvudsakligen personuppgifter som inte generar hög risk. Hög risk kan emellertid uppkomma när anställdas personuppgifter behandlas i ny teknik. En kontroll behöver därför utföras under 2026 om ny teknik implementeras av SBR.
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?	Låg risk 	Ett arbete pågår med att kartlägga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd behöver utföras. Kartläggningsbehov föreligger med anledning av till exempel användande av ny teknik.

Den registrerades rättigheter

SBR erhåller sällan en begäran från den registrerade. När en begäran väl inkommer gäller det rätten till tillgång. Det finns en genomarbetad rutin och svarsmall för att hantera rätten till tillgång. Den har även testas och använts. Vid begäran om radering hanterar verksamheten denna fråga och några frågor eller klagomål har aldrig inkommit från den registrerade till DSO under 2025 eller 2024.

Bedömning av risknivå och rekommendationer från dataskyddsombudet.

Fråga/kontroll	**Risk**	**Rekommendationer**
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?	Inget att anmärka 	Rutin och mall finns för att hantera en begäran om rätten till tillgång. Då ingen annan begäran om övriga rättigheter inkommit under 2024–2025 har mall och rutin för övriga rättigheter inte hanterats. SBR har heller aldrig valt att inte tillmötesgå en registrerads begäran, därav finns ingen hänvisning till rätt att överklaga beslut.

Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?	Inget att anmärka 	Inga begäranden har inkommit under 2025.
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?	Inget att anmärka 	Om begäranden inkommit har de hanterats i samråd med DSO och inom en månad.
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?	Inget att anmärka 	Om begäranden inkommit har de stämts av med DSO och svaren uppfyller lagkraven.

Personuppgiftsincidenter

DSO har endast kännedom om borttappad/stulen telefon och dator, men inga andra personuppgiftsincidenter under 2025 som berört SBR. Omvärldsbevakning har utförts av SBR och leverantörer har tillfrågats avseende publicerade informationssäkerhetshändelser. Vad det beror på att inga andra personuppgiftsincidenter har kommit till DSO:s kännedom är svårt att svara på och kan ha olika förklaringar. Insyn och transpararens mellan DSO och ISAM har varit mycket god. DSO rekommenderar därför att ISAM och nya DSO-funktionen under 2026 genomför kunskapshöjande insatser gentemot den operativa verksamheten.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	**Risk**	**Rekommendationer**
Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?	Låg risk 	Frånvaro av rapportering avseende potentiella personuppgiftsincidenter kan ha sin grund i att mer kunskap behövs hos medarbetarna. DSO rekommenderar utbildningsinsats.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?	Inget att anmärka 	Rutin finns för att hantera händelser som kan utgöra potentiell personuppgiftsincident och medarbetare tar del av information på intranätet, t.ex. Stöld och förlust av dator och telefon.

Hur många personuppgiftsincidenter har dokumenterats under året?	Låg risk 	DSO har kännedom om att borttappad/stulen telefon har dokumenterats och i övrigt hanterats enligt stadens riktlinjer. Fortsätt att säkerställa att personuppgiftsincidenter upptäcks och dokumenteras enligt lagkrav i artikel 33.5 i GDPR.
Hur många personuppgiftsincidenter har anmälts till IMY under året?	Inget att anmärka 	Inga personuppgiftsincidenter har anmälts till IMY 2025.

Överföring till tredje land

SBR:s ISAM har tillsammans med DSO genomfört tredjelandsöverföringsbedömningar, TIA under 2025. Behov av tredjelandsöverföringsbedömning har förelegat när personuppgifts-biträdet i sin tur anlitat amerikanskt ägda molntjänstleverantör såsom underbiträde och när australiensk och amerikanskt ägd molntjänst använts av verksamheten i den operativa verksamheten att marknadsföra Stockholm och interagera med näringslivet.

SBR har även under 2025 börjat använda AI-verktyg på prov vilket kan generera tredjelands-överföring.

Då SBR utkontrakterar viss IT-drift är det viktigt att även de svenska leverantörernas underleverantörer blir kända för SBR. Detta säkerställs vid användande av stadens mall för personuppgiftsbiträdesavtal med instruktion. I denna ska alla underleverantörer specificeras, i GDPR omnämnda såsom underbiträden. Utifrån DSO:s erfarenhet kan i detta led en mängd tredjelandsöverföring förekomma.

Bedömning av risknivå och rekommendationer från dataskyddsombudet.

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelands-överföringar som utförs?	Låg risk 	Ett systematiskt arbete har pågått under 2025 med att identifiera de tredjelands-överföringar som utförs. Detta behöver fortgå under 2026. Dataskyddsrisken påverkas från låg till hög om arbetet avstannar. Viktigt att tredjelands-överföringen dokumenteras i register-förteckningen. Behöver även använda stadens mall för personuppgifts-biträdesavtal med instruktion.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?	Inget att anmärka 	Vid tredjelandsöverföring tillämpas ett överföringsverktyg, såsom exempelvis SCC:s eller EU-kommissionens adekvansbeslut, antingen direkt i avtal med den utländska leverantören eller så har personuppgiftsbiträdet till SBR säkerställt detta med sina underbiträden.
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?	Låg risk 	SBR har under 2025 genomfört Transfer Impact Assessment (TIA) i enlighet med stadens mall för tredjelandsöverförings-bedömning, Arbete med dessa bedömningar behöver fortgå under 2026.

Övrigt att rapportera

Även i år har samtliga anställda certifierat sig och genomgått stadens obligatoriska kurser i dataskydd och informationssäkerhet. Detta är ett mycket positivt resultat som främjar ett integritetsskydd i den operativa verksamheten.

SBR har även utbildningar avseende AI:

- Stärka din kompetens och trygghet i hur du använder AI som ett professionellt verktyg i ditt arbete. Ansvarsfull användning av generativ AI på SBR.

Bilagor

Bilaga 1: Detaljerad redovisning av dataskyddsombudets granskning

Bilaga 2: Andra genomförda granskningar och omvärldsbevakning

Bilaga 1 - Redovisning av dataskyddsombudets granskning

SBR:s dataskyddsarbete har integrerats med SBR:s informationssäkerhetsarbete. SBR:s informationssäkerhetssamordnare, ISAM, har varit dataskyddsombudets centrala kontaktpunkt. ISAM och DSO har haft veckovisa avstämningar, där dataskyddsombudet involverats i personuppgiftsfrågor och systematiskt fått lämna råd i aktuella frågor som kopplar mot grundläggande integritetsskydd och säkerhet avseende personuppgiftsbehandling.

I och med att dataskyddsombudet involverats systematiskt i det faktiska integritetsarbetet för rådgivning innebär att uppgifterna i dataskyddsombudets årsrapport ovan är en analys av SBR:s faktiska dataskyddsarbete 2025. SBR arbetar riskbaserat utifrån antal anställda och de huvuduppdrag som åligger SBR det vill säga att främja näringsliv och att marknadsföra Stockholm som stad både inom Sverige och internationellt. Detta innebär att SBR huvudsakligen i sitt kärnuppdrag inte behandlar känsliga personuppgifter eller integritetskänsliga uppgifter i sin verksamhetsutövning. Däremot behandlas känsliga och integritetskänsliga personuppgifter när anställdas uppgifter behandlas av SBR i egenskap av arbetsgivare.

Att samarbeta med näringslivet och marknadsföra Stockholm internationellt innebär att SBR kan ha ett behov av att använda och befinna sig i tjänster som innebär tredjelandsöverföring. Detta får till följd att fler arbetsuppgifter tillkommer för att tillförsäkra ett lagenligt integritetsskydd.

Dataskyddslagstiftningen kan även vara komplex att efterleva för en mindre verksamhet, då lagstiftningen ständigt utvecklas i tillsyns- och domstolspraxis. Detta har uppmärksammats av EU-kommission som nu lagt fram ett förslag avseende bland annat uppdatering av dataskyddsförordningen och cookiereglerna. Att dataskyddslagstiftningen ständigt utvecklas och praxis kommer på detaljnivå är förklaringen till varför jag lagt vissa gula punkter, mindre risk, i rapporten ovan, då det arbete som idag utförs faktiskt behöver fortgå under 2026. På så vis tar SBR även del av dataskyddsombudets rådgivning om prioriterade uppgifter att utföra utifrån dataskyddsrisk även för 2026.

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 ”behandlings-register” 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 personuppgifts-behandlingarna.

Kontroller, iakttagelser och bedömning gjord av dataskyddsombudet

Antal behandlingar som är registrerade?

SBR har en fyllig registerförteckning med 65 stycken personuppgiftsbehandlingar dokumenterade i verktyget Visma Draftit Records. Registerförteckningen är processbaserad och utgår från stadens gemensamma arkivprocesser. SBR har även registerförtecknat sina kärnområden.

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

Idag är det SBR:s ISAM som har det operativa ansvaret att uppdatera registerförteckningen alternativt att tillse att ansvarig chef tillser att registerförteckningen uppdateras.

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

Det operativa genomförandet av uppdatering bör utökas till att omfatta även arkivfunktionen och till den verksamhet som hanterar själva personuppgiftsbehandlingen. Visma Records har tekniska funktioner att vidarebefordra separata behandlingar.

Dataskyddsombudet kommer i samband med överlämning till ny DSO-funktion dela hur andra verksamheter utanför Stockholm stad arbetar med denna fråga.

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

SBR:s registerförteckning innehåller alla obligatorisk uppgifter enligt artikel 30. SBR behöver dock hålla registerförteckningen uppdaterad om exempelvis obligatorisk områden såsom tredjelandsöverföring och personuppgiftsbiträdesavtal. Då nya avtal träffas regelbundet med leverantör om användande av digitala tjänster behöver dessa frågor hanteras och samtidigt uppdateras i registerförteckningen. Detta är förklaringen till varför DSO påtalar en dataskyddsrisk om registerförteckningen inte hålls uppdaterad och föreslår en utökning eller i vart fall ett aktivitetshjul vid förändrad hanteringsanvisning ska generera uppdatering av registerförteckning.

Dataskyddsombudets jämförelse med föregående års resultat

SBR har fortfarande en väl genomarbetad registerförteckning. Registerförteckningen har emellertid systematiska behov av uppdatering, då den ska spegla de tjänster som faktiskt används, vilka personuppgiftsbiträden det genererar och om val av personuppgiftsbiträde genererar tredjelandsöverföring. Därför kvarstår rekommendationen från 2024. Utifrån lagkrav om innehåll finns här alltid en risk, då behov av uppdatering ingår i uppfyllande av lagkrav.

2024 års rekommendationer kvarstår:

- Utvärdera arbetet med hur registerförteckningen ska hållas aktuell. Väv in de tekniska möjligheterna i systemstödet.
- Framtagande av checklista för registerföring utifrån utvärdering.

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, iakttagelser och bedömning gjord av dataskyddsombudet

Det är idag viktigt att arbeta riskbaserat med dataskydd. I det riskbaserade synsättet behöver emellertid tillsyns- och domstolspraxis avseende säkerhet för personuppgiftsbehandling vävas in. Verksamheten kan idag inte informationsklassa och riskvärda personuppgifter utan att ta hänsyn till att vissa kategorier av personuppgifter och personuppgifter i sitt sammanhang kan kräva en högre säkerhetsnivå. Tillsynsmyndigheten Integritetsskyddsmyndigheten IMY har publicerat information om detta, se Känsliga personuppgifter | IMY (extra skyddsvärda personuppgifter längre ned på sidan).

Att personuppgifter kan efter en sekretessprövning lämnas ut i en offentlig handling innebär inte att de inte är särskilt skyddsvärda såsom exempelvis lön och personnummer. Personuppgifter ska heller inte vara åtkomliga för obehöriga genom internet, om inte en medveten publicering har gjorts, se t.ex. Tillsyn: Trygg-Hansa | IMY.

Att som DSO få dela information om säkerhetsåtgärder i tillsynspraxis, såsom om kryptering och pseudonymisering vid tredjelandsöverföring och se att dessa åtgärder faktiskt implementeras i verksamheten värnar individens skydd.

Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?

DSO har informerat ISAM om att säkerställa säkerhetsåtgärder såsom kryptering och även pseudonymisering vid tredjelandsöverföring av personuppgifter. KLASSA 4 kraven är inte riktigt tydliga här och DSO rekommenderar därför att SBR arbetar efter av SLK:s framtagna kravmall som informerades om i nyhetsbrev till stadens samtliga ISAM i mars 2025.

När DSO gett råd har ISAM varit lyhörd avseende rådgivning om pseudonymisering och kryptering och dessa säkerhetsåtgärder har implementerats regelbundet i informationssäkerhetsarbetet under 2025.

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

SBR arbetar i enlighet med stadens framtagna riktlinjer för informationssäkerhet och tillhörande tillämpningsanvisning för informationssäkerhet. Staden har även en handbok för informationsklassning som används i arbetet. DSO har fått lämna råd och synpunkter vid framtagande av ledningens genomgång för informationssäkerhet och dataskydd. DSO har även fått delta vid ISAM:s dragning inför ledningsgruppen av rapporten och delat information avseende dataskydd.

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

De skriftligt styrande dokumenten och handböcker är implementerade och kända. ISAM har även tagit fram information på intranätet med hänvisning till styrande dokument och rutiner. Vid behov har ISAM även tagit fram checklistor till verksamheten.

Dataskyddsombudets jämförelse med föregående års resultat

I 2024 års DSO-årsrapport lyftes att dataskyddsombudet ser det som positivt att SBR följer stadens metodik avseende implementeringen av ett systematiskt informationssäkerhetsarbete.

Dataskyddsombudet rekommenderade även att det systematiska informationsklassningsarbetet skulle fortgå med implementering av tekniska och organisatoriska åtgärder i enligt med dataskyddspraxis.

Det systematiska riskbaserade informationssäkerhetsarbetet har fortgått under 2025 i enlighet med DSO-rekommendationerna. Dataskyddsombudet ser gärna att den nya DSO-funktionen fortsätter att informera om den dataskyddspraxis som gäller säkerhet vid personuppgiftsbehandling. Det är en viktig insats för att värna integritetsskydd inom stadens nämnder och bolag.

Dataskyddsombudets råd avseende framtida aktivitet

Att granska anlitade externa leverantörers säkerhet för personuppgiftsbehandling är särskilt viktigt idag utifrån omvärldsbevakning och de cyberangrepp som faktiskt har inträffat under 2025. Att informationsklassa information är viktigt, men det är än viktigare att säkerställa att de tekniska och organisatoriska åtgärderna faktiskt blir implementerade. Vid utkontraktering av IT-drift behöver idag faktiska granskningar av informationssäkerheten utföras.

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, bedömningar och iakttagelser gjord av dataskyddsombudet, samt dataskyddsombudets jämförelse med föregående års resultat

I DSO-årsrapport 2024 rekommenderade dataskyddsombudet att arbete behöver påbörjas med att identifiera och börja använda metodstöd för tröskelanalys och mall för konsekvens-bedömning avseende dataskydd.

Detta arbete har påbörjats under 2025 och behöver fortgå under 2026, En tröskelanalys vid ny personuppgiftsbehandling har genomförts under 2025, likaså en konsekvensbedömning avseende dataskydd. Under 2025 har även SBR implementerat och använt tillsyns-myndighetens, Integritetsskyddsmyndigheten IMY, metodstöd för tröskelanalys och mall för konsekvensbedömning avseende dataskydd. Detta innebär att dataskyddsombudet bedömer att det finns en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Här ser dataskyddsombudet positivt på att SBR har börjat genomföra konsekvensbedömning avseende dataskydd under 2025. Utifrån SBR:s kärnuppdrag att vara stadens näringslivs- och

destinationsbolag med uppgift att utveckla och marknadsföra Stockholm som etablerings- och besöksdestination internationellt och nationellt i sig inte genererar hög risk behandling av personuppgifter är det viktigt att SBR väljer att utföra konsekvensbedömningar när det föreligger hög risk vid personuppgiftsbehandling, dvs hög integritetsrisk. Här rekommenderas att avstämning görs med ny DSO-funktion för 2026.

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

SBR har börjat identifiera behandlingar och genomfört konsekvensbedömning avseende dataskydd under 2025. Arbete behöver fortsätta med att identifiera samtliga personuppgifts-behandlingar som kräver en konsekvensbedömning avseende dataskydd. Detta kan med fördel göras med DSO-funktionen under 2026. Utifrån SBR:s verksamhet har DSO valt låg dataskyddsrisk även om aktivitet kvarstår, i linje med det riskbaserade synsättet.

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, iakttagelser och bedömning gjord av dataskyddsombudet

År 2024 inkom endast en begäran om tillgång till personuppgifter som behandlas (registerutdrag). Denna begäran hanterades korrekt och i enlighet med dataskydds-förordningen och kompletterande svensk dataskyddslag. Då rätten till tillgång är en central rättighet har en rutin tagits fram under 2024 avseende denna rättighet och en svarsmall.

Under 2025 har ingen registrerad, den vars uppgifter som behandlas, inkommit med en begäran till SBR. Utifrån det låga inflödet och frånvaron av begäranden 2025 har inte ytterligare framtagande av rutiner och mallar prioriterats under året.

SBR:s informationstexter avseende personuppgiftsbehandling har granskats och uppdaterats under 2025. Uppdatering har även gjorts i SBR:s integritetspolicy under 2025/2026.

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, iakttagelser och bedömning gjord av dataskyddsombudet

Dataskyddsombudet har endast kännedom om personuppgiftsincident kopplad till borttappad/stulen telefon och dator. Hur det kommer sig att personuppgiftsincidenter inte kommer till DSO:s kännedom är svårt att svara på. Utifrån omvärldsbevakning idag är det ovanligt att en verksamhet inte berörs av informationssäkerhetshändelser som kan resultera i en personuppgiftsincident, därför är det viktigt att utbilda medarbetarna under 2026 avseende personuppgiftsincidenter. Detta kan med fördel göras av ISAM och den nya DSO-funktionen. Inga personuppgiftsincidenter har anmälts till IMY under året.

SBR har information om hantering av personuppgiftsincidenter på sitt intranät.

Dataskyddsombudets jämförelse med föregående års resultat och dataskyddsrisk

År 2024 rekommenderade dataskyddsombudet att verksamheten behöver involvera ISAM och DSO vid informationssäkerhetshändelser. Denna rekommendation kvarstår. Att inte upptäcka, rapportera och dokumentera personuppgiftsincidenter kan leda till dataskyddsrisker för individen. Integritetsrisken kan i förlängningen bli hög därför rekommenderas att en utbildningsinsats genomförs under 2026.

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.[3]

[3] 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.

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, iakttagelser och bedömning gjord av dataskyddsombudet

Ett omfattande arbete har gjorts under 2025 med att tredjelandsöverföringsbedöma tjänster i enligt med stadens mall som följer Europeiska dataskyddsstyrelsen rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, version 2.0, antagna den 18 juni 2021, se Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter | European Data Protection Board. Även kallad Transfer Impact Assessment" (TIA).

När tredjelandsöverföringsbedömning genomförts har överföringsverktyg säkerställts. Aktuellt överföringsverktyg säkerställs vidare i avtal och i stadens mall för personuppgiftsbiträdesavtal med instruktion.

Digitalisering och utkontraktering av IT-drift samt AI-användning genererar ofta tredjelandsöverföring. SBR behöver därför fortsätta att identifiera tredjelandsöverföring. I detta sammanhang är det viktigt att inte glömma att anlitade svenska leverantörer i sin tur kan använda underleverantörer, underbiträden, som genererar tredjelandsöverföring av SBR:s personuppgifter. Vilka underbiträden som används ska dokumenteras i instruktionen till stadens personuppgiftsbiträdesavtal.

SBR behöver således fortsätta identifiera de tredjelandsöverföringar som kan uppkomma och genomföra tredjelandsöverföringsbedömningar i stadens mall för dessa bedömningar. Hög dataskyddsrisk kan uppkomma om dessa bedömningar inte görs eller inte görs korrekt, därför är det viktigt att arbetet fortsätter och att råd inhämtas av ny dataskyddsombudsorganisation.

Bilaga 2 – Andra genomförda granskningar och omvärldsbevakning

Dataskyddsombudet utgår från tillsyns- och domstolspraxis i sin rådgivning. Dataskyddslagstiftningen är i ständig utveckling genom tillsynsbeslut och domstolspraxis. Detta skiljer EU-rätten från svensk lag. Lagstiftningsprocessen i Sverige baseras på utredning och väl genomarbetade förarbeten. Hur lagen ska tolkas framkommer till stor del i dessa förarbeten. Detta gör att ett väl underbyggt dataskyddsarbete behöver innehålla systematisk omvärldsbevakning. Här har dataskyddsombudet en viktig roll att fylla i sin rådgivande roll för att t.ex. ett mindre bolag ska kunna arbeta riskbaserat med informationssäkerhet och samtidigt iaktta lagstiftningen om integritetsskydd.

Dataskyddsombudet har löpande granskat det som varit aktuellt för företaget under 2025. Någon större granskning utanför de obligatoriska områdena ovan har inte prioriterats. Övervägande fokus under 2025 har varit att tillsammans med ISAM utveckla arbetet avseende tredjelandsöverföringsbedömningar i enlighet med stadens metodstöd. ISAM och DSO har även tillsammans utvecklat förståelse och användning av tröskelanalys och konsekvensbedömning avseende dataskydd. Att använda de dataskyddsverktyg som finns främjar en förståelse för integritetsrisk och hur den kan sänkas och hanteras.

2025 har även innehållit rådgivning avseende AI och delning av omvärldsbevakning avseende integritetsskydd och AI.

Ett granskningsområde som emellertid har prioriterats är integritetspolicyn och uppdateringar har utförts i och med granskningen.

Omvärldsbevakning

I årets årsrapport väljs att rapportera om några förändringar som framkommer i omvärlds-bevakningen. Den 1 januari 2026 inrättade tillsynsmyndigheten Integritetsskyddsmyndigheten (IMY) en ny organisation för den operativa verksamheten.

Organisationsförändringen avser att stärka myndighetens förmåga att genomföra riskbaserad tillsyn och att ge tydlig och effektiv vägledning, samt effektivisera myndighetens hantering av klagomål.

Dataskyddsombudet välkomnar organisationsförändringen, då tydlig och effektiv vägledning till personuppgiftsansvariga verksamheter efterfrågas av alla som arbetar med integritets-skydd. Förändringen innebär även att tillsyns- och klagomålshanteringen förbättras, vilket i förlängningen stärker individens integritetsskydd. Integritetsskydd är en mänsklig rättighet och är ett rättighetsskydd som ska värnas alla individer. Ett påtryckningsmedel är att klagomål och (efterföljande) tillsyn kan leda till administrativa sanktionsavgifter. Resursfrågan för det operativa dataskyddet bör därför finnas i den kommunala budgeten.

EU-kommissionen har även lämnat ett förslag till ändringar i dataskyddsförordningen. Tillsynsmyndigheten Integritetsskyddsmyndigheten (IMY) har i ett pressmeddelande uttalat att det är substantiella förändringar som föreslås och de behöver analyseras av myndigheten. IMY ser emellertid också ett behov av att regelverket blir tydligare och i högre grad utgår från ett riskbaserat synsätt. Rådet och Europaparlamentet ska nu ta ställning till EU-kommissionens förslag.

I IMY:s pressmeddelande lyfts även att dataskyddsförordningen är ett centralt regelverk som skyddar vår personliga integritet, men också grundläggande europeiska värden. Att värna dataskyddsförordningen bör därför enligt DSO vara viktigt och som IMY skriver en självklarhet.