Stockholms stad

Bilaga 9

GDPR årsrapport

År 2025

Norra innerstadens stadsdelsnämnd

GDPR årsrapport
Januari 2026

Dnr: NI 2025/1934
Utgivningsdatum: 2026-01-16
Kontaktperson: Marju Stenudd

Sammanfattning

GDPR syftar till att skydda individers rättigheter och friheter med 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 Norra innerstadens stadsdelsförvaltnings dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet:

Förvaltningens dataskyddsarbete har utvecklats i positiv riktning: De viktigaste styrdokumenten i form av rutiner, processbeskrivningar och mallar har formulerats, antalet anmälda personuppgiftsincidenter har dubblerats och kunskapshöjande insatser har skett. Konsekvensbedömningar sker systematiskt för att identifiera och förebygga riskfyllda personuppgiftsbehandlingar.

Kommande arbete bör fokuseras på att: skapa en tydlig årsplanering för informationsklassningar där risker för de registrerade är en parameter för prioritering, fortsatt säkerställa att PUB-avtal finns upprättade som innebär tillräckliga skyddsåtgärder och att inga tredjelandsöverföringar sker. Riktade insatser bör också ske i syfte att upptäcka personuppgiftsbehandlingar som saknas i förvaltningens registerförteckning och säkerställa att dessa antingen sker i enlighet med GDPR eller upphör.

De tre största riskerna enligt dataskyddsombudets bedömning

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		*De årliga revideringarna bör kompletteras med stickkontroller för att upptäcka eventuella personuppgiftsbehandlingar som saknas i registerförteckningen.* *Kunskapshöjande insatser bör göras så varje medarbetare förstår risker för de registrerade när personuppgiftsbehandlingar sker i strid mot GDPR.*
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		*Personuppgiftsbehandlingar som kan innebära hög risk för de registrerade och som saknar aktuell informationsklassning bör prioriteras för kommande informationsklassningar.*
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		*Det saknas kunskap i ett flertal personuppgiftsbehandlingar om tredjelandsöverföringar sker då aktuell informationsklassning saknas.* *Årsplan för informationsklassningar bör prioritera personuppgiftsbehandlingar där aktuell informationsklassning saknas.*

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 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

Sammanfattning

Utformning av registerförteckningen samt instruktioner för hur den ska fyllas i reviderades i början av året för att tydliggöra syftet med förteckningens beståndsdelar samt skapa bättre förutsättningar för en komplett och korrekt information om de personuppgiftsbehandlingar som sker inom förvaltningen. Registerförteckningens utformning uppfyller kraven i GDPR.

Granskning visar på en kvalitetsförbättring i jämförelse med föregående år genom att behandlingar som inte var relevanta för förvaltningen uppmärksammats och raderats och enhetligheten av den information som förts in om behandlingarna har ökat.

Ett förbättringsområde är hur ändamål med personuppgiftsbehandlingar formuleras för att de ska vara tillräckligt specifika och inte vara för allmänt och brett formulerade. Vidare behöver uppgifter om det finns befintliga gallringsrutiner kompletteras för ett flertal behandlingar för att säkerställa att förvaltningen följer principen om lagringsminimering i samtliga behandlingar som sker.

Ett arbete bör göras med att granska om det sker personuppgiftsbehandlingar som inte ingår i ordinarie processer och därmed kan saknas i registerförteckningen. Förslagsvis görs detta i form av stickkontroller av enskilda medarbetares hantering av personuppgifter.

Vidare bör interna utbildningar tydligare belysa konsekvenser för de registrerade vid felaktig behandling av personuppgifter samt vikten av att ta del av och följa förvaltningens lokala rutiner kopplade till området.

Bedömning av risknivå och rekommendationer från dataskyddsombudet:

Fråga/kontroll	Risk	Kommentarer och rekommendationer
Antal behandlingar som är registrerade?		*Registerförteckningen innehåller efter årets revidering 332 behandlingar vilket är i nivå med föregående år.*
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		*Rutin finns som steg för steg beskriver tillvägagångssätt för att säkerställa att nya personuppgiftsbehandlingar sker i enlighet med GDPR samt vilka uppgifter om behandlingen som behöver föras in i registerförteckningen.*
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		*De årliga revideringarna bör kompletteras med stickkontroller för att upptäcka eventuella personuppgiftsbehandlingar som saknas i registerförteckningen.* *Kunskapshöjande insatser bör göras så varje medarbetare förstår risker för de registrerade när personuppgiftsbehandlingar sker i strid mot GDPR.*
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		*Formuleringar av ändamål med personuppgiftsbehandlingar behöver bli mer specifika.* *Uppgifter om gallringsrutiner behöver kompletteras för att säkerställa att princip om lagringsminimering efterlevs.* *Strukturen i registerförteckningen möjliggör att samtliga obligatoriska uppgifter förs in om behandlingarna.*

Säkerhet i samband med behandlingen

Sammanfattning

Verktyget KLASSA används för de olika momenten i informationsklassningsarbetet. När objektet omfattar personuppgifter skickas mall för tröskelanalys till berörd verksamhet i samband med att första klassningstillfället bokas in för att bedöma behovet av konsekvensbedömning. Konsekvensbedömning av riskfyllda personuppgiftsbehandlingar sker parallellt med informationsklassningsarbetet med stöd av DSO. För tröskelanalyser och konsekvensbedömningar används IMY:s mallar framtagna i februari 2025.

DSO deltar som regel i informationsklassningsarbetet i syfte att bevaka att risker med personuppgiftsbehandlingar uppmärksammas samt för att stötta i att utreda personuppgiftsansvar och eventuella biträdesförhållanden. Representanter från verksamheter som kommer nyttja/nyttjar tjänsten eller verktyget är alltid delaktiga i informationsklassning och konsekvensbedömning samt för att identifiera risker samt åtgärder för att minska risker med behandlingen.

Det bör inför varje nytt år göras en preliminär helårsplan som sätter ramarna för vilka informationsklassningar som ska genomföras och vad som ligger till grund för prioritering. Antal registrerade och kategorier av personuppgifter som behandlas ska vara centrala faktorer vid bedömning av prioritering. När prioriteringsgrunderna är tydligt formulerade är det lättare att fatta beslut om behov av förändringar i årsplanen på grund av nya förfrågningar om informationsklassningar som inkommer.

Bedömning av risknivå och rekommendationer från dataskyddsombudet:

Fråga/kontroll	Risk	Kommentarer och 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?		*DSO och verksamhetsrepresentanter deltar i alla informationsklassningar som omfattar personuppgiftsbehandlingar.* *Tröskelanalyser och konsekvensbedömningar av riskfyllda personuppgiftsbehandlingar genomförs systematiskt med stöd av DSO.*
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		*Skriftliga rutiner med tillhörande mallar och processbeskrivningar finns för hantering av personuppgiftsincidenter, registrerades rättigheter samt inför behandling av nya personuppgifter och uppdatering av registerförteckning.* *Rutin för att initiera tröskelanalys och konsekvensbedömning sker strukturerat men muntligt och bör kompletteras med skriftlig rutin.*

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		*Rutin för hantering av personuppgiftsincidenter upplevs kända och implementerade till stor del. Riktade utbildningsinsatser bör göras till verksamheter som sällan anmäler incidenter.* *Rutin för registrerades rättigheter görs kända och implementeras löpande med översyn av DSO när förfrågningar inkommer.* *Rutin för vad som behöver klargöras inför ny behandling av personuppgifter samt vilka uppgifter som ska föras in i förvaltningens registerförteckning behöver göras mer kända.*

Konsekvensbedömning avseende dataskydd

Sammanfattning

Sedan våren genomförs tröskelanalyser systematiskt i samband med att informationsklassning bokas om det inte redan är känt att konsekvensbedömning behöver göras. Konsekvensbedömningar och tillhörande riskanalyser genomförs med stöd av DSO för samtliga personuppgiftsbehandlingar som uppfyller kriterier enligt tröskelanalys.

Förvaltningen använder IMY:s mallar och vägledningar för konsekvensbedömning som publicerades i februari 2025.

Resultat av konsekvensbedömning där redogörelse görs av de främsta riskerna samt förebyggande åtgärder med utpekat aktivitetsansvar delges berörda avdelningschefer för eventuella synpunkter innan detta skickas för information till och godkännande av stadsdelsdirektör.

Redan pågående behandlingar som saknar aktuell informationsklassning behöver prioriteras i årsplanering över kommande informationsklassningar för att säkerställa en högre säkerhetsnivå avseende behandling av personuppgifter.

Bedömning av risknivå och rekommendationer från dataskyddsombudet:

Fråga/kontroll	Risk	Kommentarer och rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		*Underlag för tröskelanalys skickas till verksamheten när informationsklassning bokas in.*
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		*Tröskelanalyser genomförs alltid när informationsklassning bokas in såvida det inte redan är känt att konsekvensbedömning behöver genomföras.*
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		*Förvaltningen använder IMY:s mallar för konsekvensbedömning och riskanalys.* *ISAM och DSO stämmer av med varandra när i processen för informationsklassning som konsekvensbedömning ska genomföras.*
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		*Konsekvensbedömning genomförs alltid när personuppgiftsbehandling som kan innebära hög risk för registrerad har identifierats.*

Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		*Personuppgiftsbehandlingar som kan innebära hög risk för de registrerade och som saknar aktuell informationsklassning bör prioriteras för kommande informationsklassningar.*

Den registrerades rättigheter

Sammanfattning

Det är fortsatt få personer som utövar sina rättigheter i enlighet med GDPR.

I början av året reviderades rutinen för hantering av begäran och kompletterades med processbeskrivning som förtydligar ansvarsfördelning vid en förfrågan. Mallar togs fram för att säkerställa att förvaltningen besvarar förfrågan med kompletta uppgifter.

Rutinen har utvärderats och reviderats efter varje förfrågan då förbättringar identifierats i samband med hantering.

Syftet med och vikten av att tillgodose de registrerades rättigheter samt kännedom om förvaltningens lokala rutiner för att hantera begäran behöver spridas i högre grad för att säkerställa att förvaltningen uppfyller lagkrav.

Bedömning av risknivå och rekommendationer från dataskyddsombudet:

Fråga/kontroll	**Risk**	**Kommentarer och rekommendationer**
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		*Rutin har reviderats samt kompletterats med processbeskrivning och mallar.* *Rutinen har utvärderats och reviderats efter varje förfrågan då förbättringsområden identifierats.*
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		*Fyra begäranden av registerutdrag har inkommit. I ett fall har även underlag på personuppgiftsbehandlingarna begärts.*
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		*Samtliga begäranden har besvarats inom en månad.*
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		*Då det är så få inkomna begäranden har samtliga granskats.* *Samtliga svar uppfyller lagkrav.*

Personuppgiftsincidenter

Sammanfattning

Antalet rapporterade personuppgiftsincidenter har fördubblats i jämförelse med föregående år. Detta kan vara ett positivt resultat av att det under året genomförts tretton utbildningstillfällen avseende dataskydd för olika medarbetar- och chefsgrupper. Under 2024 genomfördes ett fåtal utbildningsinsatser då DSO var ny i sin roll.

Den enskilt mest omfattande personuppgiftsincidenten skedde i samband med cyberattack hos leverantören Miljödata där personuppgifter röjdes avseende nuvarande och tidigare anställda medarbetare. Incidenten hanterades enligt lokala rutiner, i linje med GDPR samt instruktioner från Stadsledningskontoret som var samordnande kontakt gentemot leverantör. Information till de drabbade skedde i enlighet med GDPR och målgruppsanpassat initierat både av förvaltningen samt Stadsledningskontoret.

Resultat av IMY:s tillsyn av Miljödata samt tre av deras kunder med anledning av incidenten samt förvaltningens egna erfarenheter bör analyseras och förbättringsområden identifieras och tas om hand.

Utbildning i vad som utgör en personuppgiftsincident behöver fortsatt prioriteras för att säkerställa att alla incidenter anmäls och förebyggande åtgärder hanteras. Särskilt fokus bör läggas på verksamheter som sällan anmäler incidenter.

Den övergripande incidentprocess som tagits fram behöver kompletteras med rutiner och implementeras för att säkerställa att potentiella personuppgiftsincidenter upptäcks i ett tidigt skede samt även när de inte är orsakade av enskild medarbetare.

Bedömning av risknivå och rekommendationer från dataskyddsombudet:

Fråga/kontroll	**Risk**	**Kommentarer och rekommendationer**
Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?		*DSO har hållit tretton utbildningstillfällen om dataskydd under året för olika medarbetar- och chefsgrupper.* *Rutin för personuppgiftsincidentshantering nås via stadsdelsförvaltningens samarbetsyta samt intranätet.* *DSO mailar länk till rutin när person gjort anmälan i IA.* *Kunskapshöjande insatser bör fokuseras på verksamheter som sällan eller aldrig anmäler incidenter.*
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella		*Rutiner finns för hantering av personuppgiftsincidenter.* *Övergripande incidentrutin har tagits fram i syfte att exempelvis upptäcka potentiella*

personuppgiftsincidenter? Följs dessa?		*personuppgiftsincidenter. Denna behöver kompletteras med rutiner samt implementeras.*
Hur många personuppgiftsincidenter har dokumenterats under året?		*48 personuppgiftsincidenter har anmälts i år vilket är en dubblering från föregående år.*
Hur många personuppgiftsincidenter har anmälts till IMY under året?		*20 av totalt 48 personuppgiftsincidenter har anmälts till IMY. 16 av dessa har anmälts inom 72 timmar.* *DSO erbjuder stöd i hur allvarlighetsgrad av en incident ska bedömas.*

Överföring till tredje land

Sammanfattning

I förvaltningens registerförteckning uppges att inga tredjelandsöverföringar sker.

I samband med informationsklassningar utreds personuppgiftsansvaret och om behandlingen innebär ett personuppgiftsbiträdesförhållande (PUB). Befintliga eller upprättade PUB-avtal där eventuella underbiträden framkommer granskas. Inga tredjelandsöverföringar har framkommit i de behandlingar där informationsklassning genomförts under året.

Då det finns personuppgiftsbehandlingar där det saknas aktuell informationsklassning går det inte att utesluta att det sker tredjelandsöverföringar.

Förvaltningen är ansvarig för konton i sociala medier. Förvaltningen har beslutat att inga personuppgifter får förekomma i sociala medier då detta innebär tredjelandsöverföring. DSO har inte granskat om detta efterlevs.

Årsplanering för informationsklassningar bör prioritera personuppgiftsbehandlingar där aktuell informationsklassning saknas för att få en aktuell bild av befintliga leverantörer och underleverantörer och att tillräckliga skyddsåtgärder har formulerats i PUB-avtal.

Bedömning av risknivå och rekommendationer från dataskyddsombudet:

Fråga/kontroll	Risk	Kommentarer och rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		*Det saknas kunskap i ett flertal personuppgiftsbehandlingar om tredjelandsöverföringar sker då aktuell informationsklassning saknas.* *Årsplan för informationsklassningar bör prioritera personuppgiftsbehandlingar där aktuell informationsklassning saknas.*
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		*Förvaltningen innehar konton för sociala medier. Dessa omfattas av adekvansbeslut.* *Förvaltningen har beslutat att inga personuppgifter får förekomma i sociala medier. DSO har inte granskat om detta efterlevs.*
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		*Detta har hittills ej varit av relevans.* *Det behöver fastställas rutiner för att genomföra TIA om behovet skulle uppstå.*

Bilagor

Bilaga 1: Detaljerad redovisning av dataskyddsombudets granskning

Bilaga 2: 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

Bakgrund och syfte

I GDPR framkommer det att personuppgiftsansvariga 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.

Resultat

Kontroller och iakttagelser gjord av dataskyddsombudet

Antal behandlingar som är registrerade?

Förvaltningen har sin registerförteckning över behandlade personuppgifter i en excelfil. Varje avdelning har en flik för behandlingar som sker inom processer som är unika för sin avdelning, behandlingar som sker inom förvaltningsövergripande processer som omfattar fler eller alla avdelningar ligger i en separat flik. Förteckningen följer samma processtruktur som stadsdelsförvaltningarnas hanteringsanvisningar.

Registerförteckningen innehåller efter årlig revidering och granskning 332 behandlingar vilket är i nivå med föregående år (329). Korrigeringar har skett både genom att inaktuella behandlingar tagits bort likväl som att kompletteringar har skett av behandlingar som tidigare saknats i förteckningen.

Revidering av registerförteckningen initieras av DSO och görs av avdelningarnas dataskyddshandläggare som kontrollerar och justerar uppgifterna med stöd av medarbetare med kunskap om respektive behandling.

DSO genomför sin granskning när dataskyddshandläggare inkommer med reviderat underlag och återkopplar med förbättringsområden eller där uppgifter saknats eller varit otydliga. Resultatet ovan baseras på förteckningens utformning efter en korrigeringsomgång.

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

Förvaltningen har en lokal rutin som beskriver steg för steg vilka överväganden som behöver göras inför att en ny behandling av personuppgifter ska påbörjas för att säkerställa att bestämmelserna i GDPR följs. Rutinen beskriver vidare vilka uppgifter om behandlingen som behöver föras in i registerförteckningen samt under vilken kolumn i förteckningen.

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

Avdelningarnas dataskyddshandläggare gör en årlig revidering av registerförteckningen. I arbetet görs avstämningar med medarbetare som har kunskap om behandlingarna. Däremellan ska uppdateringar ske när förändringar avseende personuppgiftsbehandlingar sker.

Frågor om uppdatering av registerförteckningen inkommer sällan till DSO vilket kan tyda på att kunskapen om behovet av löpande uppdatering av denna är begränsad. Vissa löpande uppdateringar sker i samband med informationsklassningar då avdelningarnas dataskyddshandläggare deltar i dessa.

Det saknas kunskap i dagsläget om det sker personuppgiftsbehandlingar som inte är en del i verksamheternas ordinarie processer på enskilda medarbetares eget initiativ. Detta kan innebära att det sker personuppgiftsbehandlingar som inte är upptagna i registerförteckningen.

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

Registerförteckningen är utformad så att alla obligatoriska uppgifter enligt artikel 30 ska kunna besvaras. Utformning av och instruktionerna för hur registerförteckningen ska fyllas i har förtydligats för att göra det lättare att förstå vilka uppgifter som efterfrågas samt för att skapa en tydligare logik i den ordning som uppgifterna fylls i.

Granskning visar att det i ett flertal fall finns brister i hur ändamål med behandlingarna formuleras. Dessa tenderar att bli för generellt och brett beskrivna vilket gör att GDPR:s bestämmelse om uttryckligt och specifikt angivna ändamål med behandlingen inte uppfylls. Vidare saknas uppgifter om det finns befintliga gallringsrutiner för ett flertal behandlingar.

Dataskyddsombudets jämförelse med föregående års resultat

Identifierade brister redovisade i årsrapport för 2024 har hanterats enligt följande:

Styrdokument och mallar

I början av året reviderades strukturen i registerförteckningen med utgångspunkt från resultat av granskning redovisade i Årsrapport GDPR 2024. Kolumnerna sorterades i en mer logisk ordning och rullister med svarsalternativ skapades där det var ändamålsenligt för att skapa en enhetlighet i svarsformuleringar eller för att tydligare synliggöra var det saknas uppgifter. Vidare kompletterades den med kolumner för att fylla i förekomst av gallringsrutiner kopplade till varje behandling för att uppmärksamma om förvaltningen inte uppfyller principen om lagringsminimering.

Den årliga revideringen av registerförteckningen genomfördes under vår och sommar av avdelningarnas dataskyddshandläggare. Inför revideringsarbetet formulerades och presenterades nya styrdokument i form av processbeskrivning och rutin över hur revidering av

registerförteckningen ska ske och hur ansvarsfördelningen ser ut för roller involverade i detta arbete.

I rutinen beskrivs steg för steg vilka överväganden som behöver göras innan en ny personuppgiftsbehandling påbörjas och vilka uppgifter som behöver föras in i registerförteckningen avseende behandlingen.

Kompetenshöjning

Kompetenshöjning avseende innebörden av GDPR:s artiklar har varit en återkommande punkt på agendan för årets dataskyddsnätverksmöten. För att skapa bättre förståelse inför årets revidering av registerförteckningen genomfördes därför gemensamt fem av IMY:s kunskapsfilmer om grundläggande principer i personuppgiftsbehandling i enlighet med GDPR.

Inbjudningar till webbinarier avseende olika områden inom GDPR har även delats till dataskyddsnätverket för att möjliggöra fördjupade kunskaper.

DSO har under året hållit tretton utbildningar för förvaltningens medarbetare och chefer om dataskydd samt förvaltningens lokala rutiner och arbetssätt.

Utforska möjlighet till digitalt verktyg som inkluderar registerförteckning

DSO har sett två presentationer avseende stödsystem för arbete med dataskydd inklusive underhåll av registerförteckning.

Då det under hösten framkom att stadsledningskontoret påbörjat en förstudie kring att införa ett systemstöd för informationssäkerhet och dataskydd för hela staden inväntas resultat av detta. DSO har ingått som referensintervjuperson i kartläggningen av behov av systemstöd.

Dataskyddsombudets bedömning samt rekommendationer

Det finns goda förutsättningar för förvaltningen att ha ett systematiskt arbetssätt för att upprätthålla en korrekt och aktuell registerförteckning över behandlade personuppgifter som uppfyller samtliga krav i GDPR. Styrdokument i form av rutiner, mallar och processdokument som tidigare saknats har formulerats och presenterats och finns tillgängliga för samtliga medarbetare och chefer via samarbetsytan för informationssäkerhet och dataskydd.

Mallen för registerförteckningen har struktur utifrån GDPR:s krav och rutinbeskrivning inför hantering av personuppgifter beskriver vilka principer som behöver uppfyllas och varför och hur arbetet ska genomföras steg för steg.

Granskning av registerförteckning efter revidering visar på en kvalitetsförbättring i jämförelse med föregående år med större enhetlighet i hur den fyllts i samt att inaktuella behandlingar tagits bort. Information har även kompletterats som tidigare har saknats.

Om möjligheten till ett systemstöd ges bör detta prioriteras då ett mer användarvänligt sätt att hålla registerförteckningen uppdaterad förmodligen skulle resultera i ett mer korrekt register över personuppgiftsbehandlingar.

Under året har flera kunskapshöjande insatser skett för de som ingår i förvaltningens dataskyddsnätverk: gemensamt har nätverket genomfört fem av IMY:s kunskapsfilmer om grundläggande principer i GDPR.

DSO har förutom detta hållit tretton enskilda utbildningstillfällen om dataskydd för förvaltningens medarbetare och chefer.

Kunskaperna behöver dock fördjupas ytterligare och medarbetare behöver få en större förståelse för konsekvenser för klienter, brukare och invånare av en bristande personuppgiftsbehandling.

Ett större fokus bör läggas på att sprida och implementera rutinen för löpande uppdatering av registerförteckningen och att upptäcka eventuella personuppgiftsbehandlingar som sker hos enskilda medarbetare utanför verksamheternas ordinarie processer. Detta för att säkerställa att förvaltningen uppfyller sitt ansvar avseende samtliga personuppgiftsbehandlingar som sker.

DSO:s rekommendationer på aktiviteter för 2026:

- I utbildningar i dataskydd för medarbetare och chefer bör information om rutin för behandling av personuppgifter och uppdatering av registerförteckning få större utrymme
- En workshop med avdelningens dataskyddshandläggare bör genomföras i syfte att öka kunskapen i hur ändamål med personuppgiftsbehandling ska formuleras för att bli tillräckligt avgränsade och specifika
- Med stöd av avdelningarnas dataskyddshandläggare bör stickprov genomföras av ett antal medarbetares personuppgiftsbehandlingar för att upptäcka behandlingar som inte finns upptagna i registerförteckningen

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?

DSO gör bedömningen att olika kategorier av personuppgifter beaktas och att riskerna i personuppgiftsbehandlingen hanteras i klassningsprocessen genom nuvarande arbetssätt:

DSO deltar som regel i samtliga informationsklassningar där informationsklassning inte tidigare genomförts, och även i vissa fall i uppföljande informationsklassningar, i syfte att bevaka vilka personuppgifter som behandlas, eventuellt behov av att genomföra konsekvensbedömning samt om behandlingen innebär ett biträdesförhållande och om det då finns ett befintligt PUB-avtal som reglerar hantering av personuppgifter mellan parterna eller om detta behöver upprättas.

DSO deltar även regelbundet i normerande klassningsarbete och konsekvensbedömningar då detta tillför en mer nyanserad bild av förutsättningar och konsekvenser av personuppgiftsbehandlingar och bidrar till en större likställighet över staden samt ger ett värdefullt underlag och bättre helhetsbild att utgå ifrån till förvaltningens eget klassningsarbete.

Klassninsgsledare använder verktyget KLASSA i samtliga moment i informationsklassningen och DSO stöttar genom att leda verksamheternas representanter genom materialet för konsekvensbedömningarna. För konsekvensbedömningar används IMY:s mallar och vägledningar.

Representanter från berörda verksamheter med praktisk kunskap av den specifika personuppgiftsbehandlingen deltar alltid i informationsklassningarnas olika moment för att säkerställa en rättvis bedömning av risker och konsekvenser och en korrekt bild av hur behandlingen sker.

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

DSO bedömer att det finns tillräckligt reglerat och stöd avseende styrande dokument och rutiner.

Tydligt formulerade rutiner med tillhörande mallar och processbeskrivningar finns för hantering av personuppgiftsincidenter, registrerades rättigheter samt inför behandling av nya personuppgifter och uppdatering av registerförteckning.

För att genomföra tröskelanalys, konsekvensbedömning samt riskanalys av personuppgiftsbehandlingar används stödmaterial från IMY som publicerades i februari 2025.

Rutin för att initiera tröskelanalys och konsekvensbedömning sker i samråd mellan klassningsledare och DSO. Detta har hittills skett muntligt då det är ett för året nytt arbetssätt och en logisk och ändamålsenlig följd i de olika momenten har prövats fram. En skriftlig rutin med processbeskrivning över klassningsarbetets olika delmoment bör tas fram och

kommuniceras till verksamheterna för att ytterligare förtydliga de olika delar verksamheterna behöver ha i beaktande när nya personuppgiftsbehandlingar ska införas.

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

DSO:s bedömning är att skriftligt styrande dokument och rutiner är till viss del implementerade och kända.

Under 2025 formulerades eller reviderades skriftliga rutinbeskrivningar, tillhörande mallar samt processbeskrivningar som förtydligar processflöde och ansvarsfördelning för:

- Hantering av personuppgiftsincidenter
- Begäran om tillgång till personuppgifter och registrerades övriga rättigheter enligt GDPR
- Revidering av registerförteckning i enlighet med GDPR

Rutinerna finns tillgängliga för samtliga medarbetare via samarbetsytan för informationssäkerhet och dataskydd som nås via Norra innerstadens samarbetsyta eller intranätets sidor för informationssäkerhet och dataskydd.

Information om vilka lokala rutiner som finns samt var de finns tillgängliga har presenterats i samband med de utbildningstillfällen DSO hållit för verksamheterna samt i samband med utskick i chefsbrev.

Länk till aktuell rutin har även bifogats i kommunikation med medarbetare och chefer när det uppstått situation där rutinen ska följas.

Rutin för hantering av personuppgiftsincidenter upplevs till stor del känd och implementerad. Vissa verksamheter anmäler fortsatt få incidenter vilket kan tyda på att kunskaperna är bristfälliga avseende vad som utgör en personuppgiftsincident och vikten av att anmäla dessa.

Rutin för uppdatering av registerförteckningen och grund för de uppgifter som behöver föras in i registerförteckningen är främst känd av dataskyddshandläggare och behöver spridas till övriga medarbetare och chefer.

Begäran om tillgång till personuppgifter ska hanteras via registraturet. En tät kommunikation vid de fåtal begäranden som inkommit har säkerställt att de som berörs fått tydliga instruktioner om hur rutinen är formulerad. Rutinen har utvärderats efter varje enskild förfrågan och förfinats efter varje tillfälle för att säkerställa en rutin som är hållbar och uppfyller GDPR även om antalet förfrågningar skulle öka kraftigt.

Dataskyddsombudets jämförelse med föregående års resultat

Identifierade brister i årsrapport 2024 har hanterats enligt följande:

Tydligare och mer överblickbar uppföljning av informationsklassningar

Registerförteckningen har uppdaterats med information om för vilka personuppgiftsbehandlingar det genomförts informationsklassningar samt vilka moment inom klassningsarbetet som gjorts samt när.

Det saknas fortsatt en tydlighet hur prioritering av informationsklassningar planeras in och genomförs vilket kan innebära risker för de registrerade.

Övrigt utvecklingsarbete kopplat till säkerhet i samband med behandling av personuppgifter

Under våren infördes ett systematiskt arbetssätt med att genomföra tröskelanalyser samt konsekvensbedömningar som en del av informationsklassningsarbetet. Detta har gjort att risker med personuppgiftsbehandlingar uppmärksammats i högre grad och att verksamhetens representanter engagerats i vilka förebyggande åtgärder de bör genomföra för att minska riskerna samt att ansvariga för att genomföra åtgärderna har utsetts.

Kunskap om syfte med informationsklassningar samt varje medarbetares ansvar i behandlingen av personuppgifter är fortsatt begränsad då det ofta är samma medarbetare som deltar i informationsklassningarna som representanter för sin verksamhet.

Ett flertal grundläggande rutindokument, mallar och processbeskrivningar för att uppfylla GDPR har upprättats eller reviderats under året vilket är en tydlig kvalitetshöjning sedan föregående år. Frekventa utbildningstillfällen under året för att sprida kunskap och innebörden av rutinerna har gjort att fler vänt sig till DSO för att få råd avseende behandling av personuppgifter vilket skapat tillfällen till fördjupande kunskapsspridning.

Dataskyddsombudets bedömning samt rekommendationer

De informationsklassningar som genomförs följer strukturen i verktyget KLASSA. För att säkerställa att riskfyllda personuppgiftsbehandlingar identifieras och förebyggs genomförs tröskelanalyser, konsekvensbedömningar och riskanalyser. Under informationsklassningarna deltar ISAM, DSO, representant från IT samt medarbetare från berörda verksamheter samt deras dataskyddshandläggare.

Förvaltningens informationshantering är omfattande och trots att det genomförts ett antal informationsklassningar under året saknas det aktuella informationsklassningar i ett flertal system och tjänster. Det framgår inte vilka parametrar som ligger till grund för vilka informationsklassningar som prioriteras före andra vilket kan resultera i risker för de registrerade i de behandlingar där aktuell informationsklassning saknas.

För att säkerställa att personuppgiftsbehandlingar sker på ett säkert sätt bör det inför varje nytt år tas fram en preliminär årsplanering av informationsklassningar som ska genomföras.

I planeringen bör det tydligt framgå vilka parametrar som ligger till grund för de prioriteringar som görs för att enklare kunna ta ställning till eventuella behov av ändringar i årsplanen. Förekomst av personuppgifter ska vara en viktig parameter och då främst när det förekommer känsliga personuppgifter, en stor mängd personuppgifter och när många registrerade omfattas av behandlingen.

Fler medarbetare bör inkluderas i arbetet med informationsklassningar för att bredda kunskaperna inom förvaltningen om syfte och mål med dessa. Detta kan med fördel ske genom att variera vilka verksamhetsrepresentanter som bjuds med till informationsklassningarna när verksamhetskompetensen innehas av flera personer.

DSO:s rekommendationer på aktiviteter för 2026:

- Inför nytt verksamhetsår ska årsplanering för informationsklassningar tas fram där parametrar för prioritet framgår. Förekomst av personuppgifter ska vara en tungt vägande parameter

- Verksamheterna bör variera vilka medarbetare som bjuds in till informationsklassningar för att sprida kompetens om syfte och mål med dessa till fler inom förvaltningen
- Dataskyddshandläggares ansvar i att sprida kunskaper till sina kollegor bör förtydligas för att få fler aktiva ambassadörer som hjälper till med att bredda kompetensen inom förvaltningen

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 så kallad 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?

Sedan våren genomförs tröskelanalyser systematiskt i samband med att informationsklassning bokas om det inte redan är känt att konsekvensbedömning behöver göras.

Detta har skett genom muntlig avstämning mellan ISAM och DSO och behöver formuleras till en skriftlig rutin som en del i informationsklassningsprocessen.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Tröskelanalyser genomförs alltid när informationsklassning bokats avseende objekt som innebär personuppgiftsbehandling såvida det inte redan är känt att konsekvensbedömning behöver genomföras.

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

Förvaltningen använder IMY:s mallar och vägledningsdokument för konsekvensbedömningar med tillhörande riskanalys.

Då det systematiska arbetet med konsekvensbedömningar är nytt för året, samt behöver ske delvis parallellt med informationsklassningsarbetet, har ISAM och DSO valt att stämma av med varandra i varje enskilt fall var i processen det är lämpligt att genomföra konsekvensbedömningen. Detta behöver dock formaliseras i en skriftlig rutin nu när arbetssättet har satt sig.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Konsekvensbedömning genomförs alltid när resultat av tröskelanalys visar på att detta bör göras eller om det även utan tröskelanalys bedömts att behandlingen uppfyller kriterierna för att konsekvensbedömning behöver göras.

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

Behovet av att genomföra en konsekvensbedömning kontrolleras i samband med att en informationsklassning bokats in.

Förvaltningen har en omfattande informationshantering och det saknas aktuella informationsklassningar i ett flertal av dessa. Detta gör att det saknas information om i vilken omfattning det saknas konsekvensbedömningar som borde ha genomförts.

Dataskyddsombudets jämförelse med föregående års resultat

Identifierade brister i årsrapport 2024 har hanterats enligt följande:

Prioritera att genomföra konsekvensbedömningar

Det systematiska arbetet med tröskelanalyser och konsekvensbedömningar infördes under våren. Från att inte ha genomfört några konsekvensbedömningar alls under 2024 har förvaltningen sedan april, när arbetssättet infördes, genomfört nio konsekvensbedömningar. Detta resulterar i en högre medvetenhet i vilka risker en personuppgiftsbehandling kan innebära och vilka förebyggande insatser verksamheten behöver genomföra för att minska riskerna och vilken funktion som är ansvarig för att aktiviteterna genomförs.

DSO har agerat stöd genom att leda verksamheterna genom materialet i konsekvensbedömningarna och hjälpa verksamheterna att förstå vilken information som efterfrågas och ligger till grund för att bedöma om riskerna med personuppgiftsbehandlingen är godtagbara.

Färdigt material har skickats till ansvariga avdelningschefer som information och eventuella synpunkter men även för att skapa en medvetenhet om vilka risker som behöver omhändertas av verksamheterna.

Prioritera informationsklassningar utifrån konsekvenser för de registrerade

Ett flertal informationsklassningar har genomförts under året och då det bedömts behövas har konsekvensbedömningar genomförts för att belysa risker för de registrerade och hur dessa kan förebyggas.

För att säkerställa en högre säkerhetsnivå avseende behandling av personuppgifter krävs att en analys görs av vilka riskfyllda personuppgiftsbehandlingar som redan sker inom förvaltningen och prioritera dessa i en årsplan för kommande informationsklassningar.

Dataskyddsombudets bedömning samt rekommendationer

Förvaltningens systematiska arbetssätt med tröskelanalyser och konsekvensbedömningar är ett stort steg i rätt riktning för att öka medvetenheten om vilka risker personuppgiftsbehandlingar kan innebära och göra verksamheterna aktiva i att förebygga identifierade risker.

En årsplanering för informationsklassningar bör tas fram där det framgår vad som ligger till grund för prioriteringar. I detta bör en vägande parameter vara kategorier och omfattning av personuppgifter som behandlas samt antal registrerade som berörs av behandlingen. Detta skulle innebära att fler personuppgiftsbehandlingar som innebär en hög risk skulle uppmärksammas och att adekvata skyddsåtgärder som förebygger dessa risker skulle identifieras.

För att synliggöra för vilka behandlingar det saknas konsekvensbedömning har ett tillägg gjorts i registerförteckningen där det för varje behandling behöver uppges om konsekvensbedömning genomförts eller om det gjorts en bedömning att detta inte behövs.

DSO:s rekommendationer på aktiviteter för 2026:

- Inför nytt verksamhetsår bör årsplanering för informationsklassningar tas fram där parametrar för prioritet framgår. Behandlingar som kan innebära hög risk för de registrerade där aktuell informationsklassning saknas ska ha en hög prioritet.
- Skriftlig processbeskrivning över samtliga steg i informationsklassning bör formuleras och implementeras

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?

I början av året reviderades rutin för begäranden som kompletterades med processbeskrivning samt mallar för att specificera avgränsat område för den registrerades förfrågan samt ge ett sammanställt svar till den registrerade.

Rutin och arbetssätt har utvärderats efter varje enskild begäran och därefter reviderats för att steg för steg skapa en hållbar rutin som uppfyller de registrerades rättigheter enligt GDPR även om förfrågan är komplex och/eller om antalet förfrågningar ökar kraftigt i antal.

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

Fyra begäranden av registerutdrag har inkommit. I ett fall har även underlag på personuppgiftsbehandlingarna begärts ut.

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

Samtliga begäranden har besvarats inom en månad.

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

Då det är så få inkomna förfrågningar har samtliga begäranden granskats.

Samtliga svar uppfyller lagkrav.

Dataskyddsombudets jämförelse med föregående års resultat

Identifierade brister i årsrapport 2024 har hanterats enligt följande:

Formulera process samt utveckla rutin för att hantera begäran från den registrerade enligt artikel 15-22

I början av året formulerades en reviderad rutin, processbeskrivning med ansvarsfördelning och mallar för en strukturerad hantering när en registrerad vill utöva sina rättigheter i enlighet med GDPR.

Utformning och utvärdering av det nya arbetssättet har skett i nära dialog med kanslichef och registratur som är den funktion som är första mottagare av registrerads begäran.

Det är fortsatt få personer som utövar sina rättigheter. Det har gjort det möjligt att efter varje begäran systematiskt utvärdera arbetssättet och genomföra justeringar för att skapa en långsiktigt hållbar rutin även om antalet begäranden ökar kraftigt och för att säkerställa att förvaltningen hanterar begäran utifrån sitt personuppgiftsansvar.

Dataskyddsombudets bedömning samt rekommendationer

Behandling av personuppgifter ska ske med hänsyn tagen till mänskliga fri- och rättigheter. För att uppfylla detta behöver man som personuppgiftsansvarig kunna uppfylla de registrerades rättigheter genom att exempelvis kunna redogöra för vilka personuppgifter som behandlas och i vilket syfte.

Den rutin och de mallar som i början av året formulerades och implementerades är en viktig del för att uppnå detta och gör att förvaltningen genomfört en kvalitetshöjning inom detta område i jämförelse med föregående år.

Registerförteckningen ska fungera som ett uppslagsverk för verksamheten när en enskild inkommer med en begäran om registerutdrag. En väl underhållen registerförteckning är därför till stor hjälp för verksamheterna för att veta vilka behandlingar som behandlas inom vilka processer och var de förvaras. En löpande uppdatering av denna bör därför prioriteras.

Ett fortsatt arbete med att utvärdera rutinen när förfrågningar inkommer, en kontinuerlig uppdatering av registerförteckningen samt att säkerställa att inga personuppgiftsbehandlingar sker som inte finns i registerförteckningen är delar som kombinerat skapar en respektfull behandling av personuppgifter och säkerställer att ett komplett underlag kan lämnas till den som efterfrågar detta.

Hittills är det få som inkommer med förfrågan om vilka personuppgiftsbehandlingar som sker. Det går dock att anta att medvetenheten om vilka konsekvenser det kan innebära att ens personuppgifter behandlas av andra ökat generellt bland invånare med tanke på ökat antal incidenter och dataläckor som bevakas i media. Detta kan komma att resultera i att intresset av att begäran om registerutdrag och även prövningar av radering av personuppgifter kan komma att öka. Med ett krav att besvara dessa frågor inom 30 dagar är det viktigt att ha fungerande rutiner och processer och en bra ordning på de personuppgifter som behandlas.

DSO:s rekommendationer på aktiviteter för 2026:

- Fortsatt utvärdera rutin och styrdokument kopplat till rutinen när begäranden inkommer för att säkerställa att arbetssätt håller lagkrav även vid hög belastning
- Fortsatt sprida kunskap om lagkrav och arbetssätt till förvaltningens medarbetare och chefer och koppla detta till vikten av en aktuell registerförteckning som omfattar samtliga personuppgiftsbehandlingar

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?

DSO har hållit tretton utbildningstillfällen om dataskydd under året för olika medarbetar- och chefsgrupper främst i samband med APT.

När en anmälan av personuppgiftsincident görs i IA skapas automatiskt ett mail till DSO med information om detta. När incidentrutinen var nyligen reviderad skickade DSO ett mail till anmälare samt händelseansvarig med länk till incidentrutinen samt påtalade tidsgräns för anmälan till IMY. Detta görs fortsatt när det inkommer anmälan från person som inte anmält tidigare för att säkerställa att rätt rutin följs.

Rutin för personuppgiftsincidentshantering nås via samarbetsytan för informationssäkerhet och dataskydd som hittas via stadsdelsförvaltningens samarbetsyta.

Avdelningarnas dataskyddshandläggare fungerar som ytterligare stöd när medarbetare eller chefer behöver stöd i hur personuppgiftsincidenter ska anmälas.

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

Rutiner finns för hantering av personuppgiftsincidenter. Efterlevnad av dessa följs löpande upp av DSO vid varje incidentanmälan som sker.

Det finns en övergripande incidentprocess framtagen för samtliga typer av incidenter som kan inkomma till IT-enhet och ISAM som kan innebära att även en personuppgiftsincident skett. Denna behöver kompletteras med rutiner.

Hur många personuppgiftsincidenter har dokumenterats under året?

48 personuppgiftsincidenter har anmälts och dokumenterats under året.

Hur många personuppgiftsincidenter har anmälts till IMY under året?

20 av totalt 48 personuppgiftsincidenter har anmälts till IMY. 16 av dessa har anmälts inom 72 timmar.

Dataskyddsombudets jämförelse med föregående års resultat

Identifierade brister i årsrapport 2024 har hanterats enligt följande:

Öka kunskaperna om vad som utgör personuppgiftsincidenter för att fler incidenter ska anmälas

48 personuppgiftsincidenter har anmälts under året vilket är en tydlig ökning från föregående år då 24 incidenter anmäldes. Detta tyder på att kunskaperna om vad som utgör en incident och när en incident behöver anmälas har ökat.

DSO var ny i sin roll 2024 och höll då inga utbildningstillfällen. Under 2025 har DSO hållit tretton utbildningstillfällen för chefer och medarbetare avseende dataskyddsfrågor. Detta kan vara en bidragande orsak till det ökade antalet anmälda incidenter då det skapats forum för kunskapshöjning och tillfällen att ställa direkta frågor. Det har också gjort DSO synlig i organisationen vilket märkts genom att många medarbetare vänt sig direkt för att få råd i frågor kopplade till hantering av personuppgifter generellt men även om incidenter specifikt.

Den obligatoriska utbildningen i dataskydd som finns tillgänglig på utbildningsplattformen ska genomföras av samtliga medarbetare årligen. Uthämtning av statistik av hur många som genomfört utbildning upplevs bristfällig. Medarbetare ha lyft att det inte registrerats som att de utfört utbildningen fast de genomfört samtliga moment och chefer har inte kunnat lägga in uppgifter på medarbetare som genomfört utbildningen om den genomförts gemensamt under exempelvis APT. Den uppgift som visar på att 16,5 % av medarbetarna genomfört utbildningen känns därför högst osäker.

Öka det aktiva upptäckandet av incidenter genom att implementera en övergripande incidentprocess som inkluderar alla typer av incidenter som även kan resultera i en personuppgiftsincident

En incidentprocess har formulerats. Denna behöver kompletteras med rutiner för att fungera i praktiken.

Dataskyddsombudets bedömning samt rekommendationer

Förvaltningen har fungerande rutiner för anmälan och uppföljning av personuppgiftsincidenter. DSO följer löpande upp att anmälningar slutförs och klarmarkeras i IA och ger verksamheterna stöd i vad som ligger till grund för att göra bedömning av om anmälan även bör göras till tillsynsmyndigheten IMY. I de fall verksamhet gör bedömningen att anmälan till IMY inte behöver göras dokumenteras motiveringen antingen i IA-anmälan eller i den sammanställning DSO för över anmälda incidenter. DSO följer även upp IMY:s beslut av anmälda ärenden för att säkerställa om ytterligare åtgärder behövs. Inga ytterligare åtgärder har krävts av IMY i de beslut som inkommit vid skrivande av denna rapport.

Antalet anmälda personuppgiftsincidenter har ökat tydligt i jämförelse med föregående år vilket tyder på att kunskaperna om vad som utgör en incident och vikten av att anmäla har ökat. Fortsatt är det dock verksamheter som sällan anmäler incidenter vilket tyder på att det finns kunskapsbrister i delar av förvaltningen.

Perioden efter sommaren präglades av cybersäkerhetsincidenten hos Miljödata som drabbade anställda och till viss del personer som avslutat sin anställning. Utredning av omfattning av incidenten, information och instruktioner från Stadsledningskontoret följdes löpande och agerades på skyndsamt. DSO resonerade även i Stadens DSO-nätverk med kollegor om hur de hanterat instruktioner och eventuella frågor som uppstått för att gemensamt kunna återkoppla eventuella oklarheter till Stadsledningskontoret.

När IMY slutfört sin tillsyn av Miljödata samt tre av deras kunder med anledning av incidenten bör resultatet tillsammans med förvaltningens erfarenheter av konsekvenser av incidenten analyseras och beslut fattas om aktiviteter som fungerar förebyggande vid eventuell liknande incident.

DSO:s rekommendationer på aktiviteter för 2026:

- Utbildningsinsatser i dataskydd bör riktas till de verksamheter som sällan anmäler incidenter
- Rutiner bör formuleras och implementeras kopplat till övergripande incidentprocess för en mer proaktiv incidenthantering inom förvaltningen

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

[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.

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?

I förvaltningens registerförteckning finns möjlighet att för varje personuppgiftsbehandling uppge om tredjelandsöverföring sker. Inga tredjelandsöverföringar har uppgivits.

Dock går det inte att säkert veta att detta är helt överensstämmande med verkligheten då det kräver en fullständig inventering av vilka personuppgiftsbiträden och eventuella underbiträden som finns och var de behandlar personuppgifter åt förvaltningen.

För att skapa en systematik i att inventera och granska förekomst och utformning av befintliga PUB-avtal, samt behov av att upprätta PUB-avtal som saknas, görs detta i samband med informationsklassning. Som ett stöd har DSO upprättat ett separat dokument som utgår från ISAM:s lista över förvaltningens system och tjänster. Utifrån denna inventering saknas det kunskap om det finns eller behöver upprättas PUB-avtal på 82 system/tjänster av 159.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

Förvaltningen har konton i sociala medier. Beslut finns dock att inga personuppgifter får förekomma i de konton som förvaltningen ansvarar för. Samtliga typer av sociala medier som nyttjas omfattas av gällande adekvansbeslut.

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

Inga bedömningar enligt TIA har behövt genomföras under året.

Dataskyddsombudets jämförelse med föregående års resultat

Identifierade brister i årsrapport 2024 har hanterats enligt följande:

Granskning av PUB-avtal för att inventera vilka underleverantörer som anlitas

Helhetsbild av om tredjelandsöverföringar sker samt om adekvata skyddsåtgärder finns för dessa växer i samma takt som informationsklassningsarbetet fortskrider. Nulägesbilden har därmed ökat i jämförelse med föregående år men det saknas fortsatt information i huvudparten av de personuppgiftsbehandlingar som sker. Inga tredjelandsöverföringar har hittills identifierats.

För de PUB-avtal som upprättats under året har stadens reviderade mall för PUB-avtal använts där vikten av att ha en exit-strategi för tredjelandsöverföringar påtalas.

Utan en heltäckande inventering av i vilka behandlingar det råder personuppgiftsbiträdesförhållande och var behandlingar sker hos leverantör går det inte att med säkerhet påstå att uppgifterna i registerförteckningen om att det inte sker tredjelandsöverföringar stämmer.

Dataskyddsombudets bedömning samt rekommendationer

Även om bilden av hur aktuella leverantörsförhållanden och därmed eventuella tredjelandsöverföringar klarnar allteftersom informationsklassningar sker finns det fortsatt brister då det saknas aktuella informationsklassningar i ett flertal personuppgiftsbehandlingar. Detta kan innebära att tredjelandsöverföringar sker som inte finns upptagna i registerförteckningen.

Med en tydlig årsplanering av informationsklassningar där prioriteringarna utgår från omfattning och kategorier av personuppgiftsbehandlingar säkerställs att eventuella riskfyllda behandlingar identifieras och att åtgärder för att förebygga risker hanteras.

DSO:s rekommendationer på aktiviteter för 2026:

- Inför nytt verksamhetsår bör årsplanering för informationsklassningar tas fram där parametrar för prioritet framgår. Behandlingar som kan innebära hög risk för de registrerade där aktuell informationsklassning saknas bör ha en hög prioritet.

Bilaga 2 – Omvärldsbevakning

Nedan följer resultatet av delar av den omvärldsbevakning som dataskyddsombudet genomfört under året. DSO bevakar fortsatt de delar som påverkar förvaltningens arbete med dataskydd och eventuella förändringar som behöver göras i arbetssätt och rutiner:

EU-kommissionen föreslår ändringar i GDPR:

EU-kommissionen presenterade i november 2025 förslag på ändringar i GDPR. Förändringarna motiveras med att de ska innebära förenklingar i att följa GDPR och avser bland annat:

- Tydliggöra innebörden av olika begrepp såsom *personuppgifter* och *särskilda kategorier av personuppgifter*
- Underlätta efterlevnad i form av informationskrav och anmälningar av personuppgiftsincidenter:
    - Höja tröskeln för anmälan till IMY
    - Höja tidsgränsen från 72 till 96 timmar vid anmälan till IMY
    - Samma tillsynsmyndighet för anmälan av olika typer av incidenter som exempelvis personuppgiftsincidenter och NIS-incidenter

Förslaget behandlas av europeiska rådet och Europaparlamentet. EDPB (Europeiska dataskyddstyrelsen) kommer tillsammans med EDPS (Europeiska datatillsynsmannen) att yttra sig över förslaget.

Adekvansbeslut vid överföring av personuppgifter till USA

Nuvarande adekvansbeslut som gör det möjligt att överföra personuppgifter till USA beslutades 2023. I beslutet om adekvat skyddsnivå för USA lyfter EU-kommissionen särskilt fram PCLOB (Privacy and Civil Liberties Oversight Board). PCLOB övervakar bland annat amerikansk underrättelsetjänst för att säkerställa att individers rättigheter inte kränks när personuppgifter samlas in.

Då president Trump avskedat ett flertal av ledamöterna i PCLOB och det därmed finns en osäkerhet i hur detta kan komma att påverka adekvansbeslutet är det än mer viktigt att ha kontroll över personuppgiftsbehandlingar som kan innebära överföring till USA samt en exitstrategi i händelse av att adekvansbeslutet upphävs.

Registerkontroller vid anställning

Regeringen har publicerat en lagrådsremiss i oktober 2025 om bland annat ökade möjligheter att göra registerkontroller av personer som ska arbeta inom kommunen i syfte att hindra personer med skadliga och brottsliga intentioner att ingå anställning:

- Kommunen får ta del av utdrag av belastnings- och misstankeregister för hemtjänstpersonal
- Kontroll av personer som ska arbeta med barn utökas med misstankeregister
- Utdrag ur belastningsregister får tas för anställning i ledande befattningar.

Lagändringarna föreslås träda i kraft 1 mars 2026.

Växande intresse av att nyttja AI i ordinarie verksamhet som leder till behov av ökad kompetens

Intresset av att undersöka möjligheter till att nyttja AI i verksamheternas utvecklingsarbete ökar. Detta gör att behovet av att ha ett utpekat ansvar inom förvaltningen att bevaka bestämmelser som AI-förordningen, hur ett införande kan genomföras utan att registrerades rättigheter äventyras och att arbetet sker i linje med stadens övergripande inriktning i införande ökar.

Som en del i ansvaret bör även ingå att omvärldsbevaka det som framkommer inom området för att se hur detta påverkar eller kan dras nytta av i förvaltningens eget utvecklingsarbete såsom exempelvis:

- Regeringen har presenterat förslag på budget för att stärka IMY:s regulatoriska sandlådor för att offentlig förvaltning i högre grad ska kunna testa AI under säkra former. Bland annat finns regulatorisk sandlåda för att testa transkribering inom socialtjänst i syfte att spela in och sammanfatta samtal som förs med klienter
- Förslag på förändringar i AI-förordningen har presenterats av EU-kommissionen som kan komma att införas

DSO:s rekommendation:

- Förvaltningen bör fastställa ett övergripande ansvar för att hantera och bevaka frågor om AI och som fungerar som kontaktyta mot AI-samordnare i staden
- En lokal riktlinje av utvecklingsarbete som inkluderar AI-lösningar som går i linje med stadens övergripande riktning bör formuleras, implementeras och göras känd för förvaltningens medarbetare och chefer

Ny organisation IMY och IMY:s ambitioner för 2026:

Från den 1 januari 2026 införs en ny organisation på Integritetsskyddsmyndigheten (IMY). Två nya avdelningar inrättas: avdelning för tillsyn och klagomål samt avdelning för vägledning, innovation och teknik.

De nya avdelningarna ska bidra till att:

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

I samband med IMY:s DSO-konferens i december 2025 framfördes även att de har som ambition att genomföra mer tillsyn på eget initiativ vilket möjliggörs genom organisationsförändringen.

Detta tyder på att det finns en syn att verksamheter efter snart åtta år efter att GDPR trädde i kraft anses ha haft tillräckligt med tid för att säkerställa att regelverket efterföljs och att detta nu kommer att kontrolleras i högre grad även utan att klagomål från enskilda inkommit.

IMY – dataskydd för unga

Den 10 december 2025 lanserade IMY en informationssida med fokus på dataskydd för unga. Informationen riktar sig både till unga (ca 8-13 år) och deras vårdnadshavare i syfte att på ett enkelt sätt förklara hur man kan skydda sina uppgifter på nätet och för att göra unga uppmärksamma på hur personuppgifter sprids på nätet och vilka rättigheter man har att tillse att ens personuppgifter inte delas på ett sätt man inte fått information om.

DSO:s rekommendation:

- Sprida kunskap om informationssidan till de verksamheter som möter unga samt deras vårdnadshavare

Resultat av några av de tillsyner IMY genomfört under 2025:

Spotify

Spotify dömdes till att betala sanktionsavgifter på 58 miljoner kronor. Som grund för domen fastslogs att de brutit mot GDPR genom att de:

- Inte gett tillräcklig tydlig information om hur registrerade kan tillvarata sina rättigheter
- Brustit i information om lagringstider och kriterier för dessa
- Inte gett tillräcklig information om skyddsåtgärder vid tredjelandsöverföringar.

Moderaterna och Sverigedemokraterna

Båda partierna genomförde direkta utskick via sms och e-post 2022 och 2024 till personer som inte var medlemmar i partierna. Bland annat nämndes personernas namn i en film som bifogades i utskicket via länk.

Som rättslig grund för utskicket uppgavs *intresseavvägning* vilket IMY inte ansåg var berättigat.

IMY ansåg efter tillsyn att:

- Behandlingen skett utan rättslig grund
- SMS och e-post utan samtycke (från mottagaren) är särskilt påträngande reklam
- Partierna har begränsat utrymme att skicka politisk reklam till annan än medlem

Sanktionsavgifter utfärdades inte men partierna fick reprimander för överträdelserna.

Tele2

Tele2 anses ha överfört personuppgifter till USA i strid mot GDPR:

- Tele2 har använt sig av Google Analytics
- Uppgifterna har bedömts som personuppgifter då de kunnat sammankopplas med andra uppgifter som Google haft tillgång till
- Tele2 har inte vidtagit tillräckliga skyddsåtgärder som krävs vid tredjelandsöverföring

Tele2 dömdes till sanktionsavgifter på 12 miljoner kronor.