Stockholms stad

Bilaga 9

GDPR årsrapport

År 2025

Valnämnden

GDPR årsrapport
Januari 2025

Dnr: YYYY
Utgivningsdatum: 202X-MM-DD
Kontaktperson: Namn Namn

Sammanfattning

GDPR, eller dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten. Ett dataskyddsombud har i uppdrag att oberoende granska verksamhetens efterlevnad av dataskyddsförordningen. I denna rapport redovisar dataskyddsombudet årets granskning av Valnämndens dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

Under tillsynsåret har Valnämndens verksamhet varit på en förhållandevis nedskalad nivå, med anledning av den karaktär på uppgifter som åligger nämnden mellan valår. DSO konstaterar att verksamhetens dataskyddsarbete håller en hög nivå och att majoriteten av förra tillsynsårets föreslagna åtgärder har åtgärdats på ett lämpligt sätt.

DSO har granskat de sex obligatoriska granskningsområdena, samt utfört en granskning utöver de obligatoriska. Inledningsvis konstaterar DSO att verksamheten i stor utsträckning uppfyller de krav som ställs enligt dataskyddsförordningen och Stockholms stads interna målsättningar. Nedan sammanfattas ändå de områden där vissa brister förekommer.

De tre största riskerna enligt dataskyddsombudets bedömning

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?	🟡	Det saknas dokumenterade rutiner för detta.
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?	🟡	Verksamhetens bedömning skiljer sig från vad som framgår av det underlag som DSO tagit del av. Kartläggningen behöver givet detta ses över.
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?	🟡	DSO har inte tagit del av mallar eller rutiner för detta.

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 fortsättningsvis GDPR*) 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 och kompletterande regelverk följs inom organisationen. Det innebär bland annat att ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. Dataskyddsombudet har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs. DSO ska rapportera direkt till högsta förvaltnings-/bolagsnivå. I Stockholms stad innebär det att dataskyddsombudet rapporterar till nämnder och styrelser.

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

Granskning av dataskyddsarbetet

Kontroll av obligatoriska områden

Dataskyddsombudet har granskat verksamhetens dataskyddsarbete utifrån sex obligatoriska områden. De sex områdena har identifierats genom en analys av kraven i GDPR om hur verksamheter bör arbeta systematiskt med dataskydd. Varje område innehåller ett antal kontrollfrågor som ger en bild av verksamhetens dataskyddsarbete. Dessa områden överensstämmer med de delar som enligt Integritetsskyddsmyndigheten (IMY) utgör grunden för en verksamhets systematiska och rättssäkra hantering av personuppgifter.

I rapporten används en riskmodell med fyra nivåer av risk. Modellen hjälper dataskyddsombudet att visa vilken bedömning hen gör av verksamhetens dataskyddsrisker utifrån de iakttagelser som gjorts i granskningen.

Risknivå	Beskrivning
Hög risk 	Iakttagelsen avser en brist som kan leda till betydande risker för de registrerades rättigheter och friheter. Bristen kräver omgående åtgärd och korrigering.
Medelhög risk 	Iakttagelsen avser en brist som kan leda till risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas skyndsamt, men kräver inte omedelbar korrigering.
Låg risk 	Iakttagelsen avser en brist som kan leda till mindre risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas, men kräver inte omedelbar korrigering.
Inget att anmärka 	Dataskyddsombudet har inga brister att rapportera avseende denna del.

Notera att risken för att tilldelas en sanktion vid tillsyn är större desto högre risken är.

Resultatsammanställning och centrala iakttagelser inom dataskyddsarbetet

I detta avsnitt presenteras en sammanställning av den bedömda risknivån för verksamhetens dataskyddsarbete, grundat på kontrollfrågorna inom de sex obligatoriska områdena. Vidare redovisas dataskyddsombudets centrala iakttagelser, inklusive områden där verksamheten uppvisar goda resultat och bör upprätthålla sitt arbete, samt identifierade brister som kan utgöra dataskyddsrisker. Avsnittet innehåller även dataskyddsombudets rekommenderade åtgärder för att hantera dessa risker och stärka dataskyddsarbetet.

En fullständig redovisning av dataskyddsombudets underlag och resultat från granskningen av de sex obligatoriska områdena finns att läsa i bilaga 1. Bilagan innehåller även en beskrivning av syftet och bakgrunden för varje område.

Register över personuppgiftsbehandlingar

Sammanfattning

DSO konstaterar att registerförteckningen är mer behandlingsorienterad än systemorienterad och att det talar för en god fullständighet. DSO konstaterar att verksamhetens samtliga personuppgiftsbehandlingar så vitt vi kunnat bedöma ingår i registerförteckningen. Det finns definitivt en sådan ambition i verksamheten.

Registerförteckningen har tagits fram i samråd med DSO. DSO konstaterade vid tillsynen 2021 att verksamheten saknade nedtecknade rutiner för arbetet med registerförteckningen. På grund av Valnämndens periodiska arbetssätt bedömer DSO att en utförlig nedtecknad rutin inte är nödvändig med beaktande av verksamhetens omfång, utan att det är tillräckligt att nämnden arbetar med registerförteckningen utifrån det systematiska kvalitetsarbetets årshjul samt att en översyn görs två gånger per år.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		36 stycken.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		Ja. Nämnden arbetar utifrån ett årshjul och kontrollerar behovet av registreringar och uppdateringar två gånger per år.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		Ja. Med hänsyn till verksamhetens storlek bedömer DSO det som sannolikt att samtliga behandlingar fångas upp med de nuvarande rutinerna för registrering och uppdatering.
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		Ja. Behandlingarna i registerförteckningen innehåller de uppgifter som är obligatoriska enligt artikel 30 GDPR.

Säkerhet i samband med behandlingen

Sammanfattning

DSO konstaterar att med beaktande av Valnämndens periodiska arbetssätt så är behovet av unik upprättad styrande dokumentation förhållandevis lågt, inte minst mellan valåren. Valnämnden tar dock del av och följer de av stadsledningskontorets skapade dokumenten och rutinerna inom dataskyddsområdet. I viss utsträckning anpassas dessa utifrån nämndens verksamhet. Valnämnden har under tillsynsåret antagit en rutin för användningen av tjänsten Säkra meddelanden.

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

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?		Ja. Valnämnden har endast genomfört en informationsklassning, vilken avser systemet Kaskelot. I Kaskelot behandlas inga känsliga personuppgifter, däremot behandlas integritetskänsliga uppgifter. Givet detta bedömer DSO att tillräcklig hänsyn tagits till de olika kategorierna av personuppgifter.
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		Ja. Valnämnden tar del och följer de av Stadsledningskontorets skapade dokument och rutiner inom dataskyddsområdet. I viss utsträckning anpassas dessa utifrån nämndens verksamhet.
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		Ja. DSO bedömer att de skriftliga styrande dokumenten och rutinerna är tillräckligt implementerade och väl kända inom organisationen. DSO har fått information om att de anställda har god kännedom om styrdokumenten samt att dessa efterlevs i praktiken. Samtliga nyanställda får information om styrdokumenten och var dessa finns.

Konsekvensbedömning avseende dataskydd

Sammanfattning

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

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

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

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		Det saknas dokumenterade rutiner för detta.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		Ja, dessa dokumenteras dock inte.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		Ja, det finns utpekade ansvariga för genomförandet av konsekvensbedömningar och verksamheten har tillgång till stadens mallar och metodstöd för genomförande av konsekvensbedömning.
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		Inte aktuellt i nuläget.
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en		Ja, hittills har Valnämnden inte identifierat några högriskbehandlingar i sin verksamhet.

konsekvensbedömning avseende dataskydd görs samt genomfört detta?		

Den registrerades rättigheter

Sammanfattning

Under 2025 har nämnden tagit emot fyra stycken begäranden om utövande av registrerades rättigheter. Samtliga begäranden avsåg registerutdrag och samtliga registrerade fick svar inom föreskriven tidsfrist. DSO bedömer därmed att verksamheten har goda förutsättningar för att hantera registrerades rättigheter inom föreskriven tid.

DSO har inte fått information om att det finns dokumenterade mallar eller rutiner för besvarande av begäran från den registrerade. DSO rekommenderar att verksamheten undersöker behovet av att utarbeta rutiner för detta, alternativt att verksamheten undersöker möjligheten att använda befintliga rutiner från staden.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		DSO har inte fått information om att det finns dokumenterade mallar eller rutiner för detta.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		Fyra stycken, samtliga avsåg begäranden om registerutdrag.
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		Samtliga.
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		Ja, DSO har dock bara granskat svar till de registrerade för fall där de registrerades uppgifter inte förekom hos nämnden. Notera att det finns formkrav för vad ett registerutdrag ska innehålla när det förekommer uppgifter om den registrerade hos nämnden.

Personuppgiftsincidenter

Sammanfattning

Under tillsynsåret har endast en personuppgiftsincident inträffat, vilken inom 72 h anmäldes till tillsynsmyndigheten. Verksamheten uppger att det finns kunskap om när en incident ska anmälas till IMY samt när de registrerade ska informeras om en incident. Detta säkerställs bland annat genom utbildningar, särskilt till nyanställda.

DSO har granskat rutinen för hantering av informationssäkerhetsincidenter, som även behandlar personuppgiftsincidenter. DSO rekommenderar att verksamheten kompletterar rutinen med information om när de registrerade ska informeras om en personuppgiftsincident.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?		Detta säkerställs genom utbildning, dokumenterade rutiner och kontinuerliga påminnelser.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		Ja, huvudsakligen, DSO rekommenderar att verksamheten kompletterar rutinen för hantering av informationssäkerhetsincidenter med information om när de registrerade ska informeras om en personuppgiftsincident.
Hur många personuppgiftsincidenter har dokumenterats under året?		En incident har dokumenterats under året.
Hur många personuppgiftsincidenter har anmälts till IMY under året?		En incident har anmälts till IMY under året.

Överföring till tredje land

Sammanfattning

Valnämnden har kunskap om vad en tredjelandsöverföring är och vad detta innebär. Verksamheten har gjort en kartläggning över aktuella personuppgiftsbehandlingar och har bedömt att inga tredjelandsöverföringar sker. DSO har dock noterat att i PUB-avtalet med Precio-Fishbone anges att tredjelandsöverföringar sker med stöd av DPF. DSO uppmanar givet detta Valnämnden att se över kartläggningen av tredjelandsöverföringar.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		Verksamhetens bedömning skiljer sig från vad som framgår av det underlag som DSO tagit del av. Kartläggningen behöver givet detta ses över.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		Inte aktuellt i nuläget.
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		Inte aktuellt i nuläget.

Bilagor

Bilaga 1: Detaljerad redovisning av dataskyddsombudets granskning

Bilaga 2: Andra genomförda granskningar och omvärldsbevakning

Bilaga 1 - Detaljerad redovisning av dataskyddsombudets granskning

Denna bilaga innehåller en beskrivning av syftet med respektive obligatoriskt område samt en mer detaljerad redovisning av dataskyddsombudets granskning och slutsatser. Här framgår vilka iakttagelser som gjorts och vilken information som samlats in under granskningsarbetet av de sex obligatoriska rapporteringsområdena. För varje område redovisas de underlag som har använts, de iakttagelser som har gjorts samt hur dessa har utgjort grunden för dataskyddsombudets riskbedömning och rekommenderade åtgärder.

1. Register över personuppgiftsbehandlingar

Syftet med området

I GDPR framkommer det att personuppgiftsansvariga (och personuppgiftsbiträden) ska föra ett register över sina personuppgiftsbehandlingar. Registret brukar benämnas ”behandlingsregister” eller ”registerförteckning”. Registret ska finnas tillgängligt i elektronisk form och ska omfatta samtliga personuppgiftsbehandlingar som personuppgiftsansvarig utför. Det ska hållas uppdaterat vilket innebär att det ska uppdateras vid nya eller förändrade personuppgiftsbehandlingar.

Syftet med detta rapporteringsområde är att rapportera om verksamheten har ändamålsenliga rutiner som möjliggör att nya/förändrade personuppgiftsbehandlingar registreras, huruvida personuppgiftsbehandlingar registreras/uppdateras såsom det krävs samt huruvida de uppgifter som är obligatoriska har besvarats kopplat till de registrerade personuppgiftsbehandlingarna.

Kontroller och iakttagelser gjord av dataskyddsombudet

Antal behandlingar som är registrerade?

36 stycken behandlingar är registrerade i den senaste versionen av registerförteckningen.

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

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

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

Ja. Nämnden arbetar utifrån ett årshjul och kontrollerar behovet av registreringar och uppdateringar två gånger per år. Vid behov uppdaterar nämnden registerförteckningen.

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

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

Dataskyddsombudets jämförelse med föregående års resultat

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

Föregående tillsyn rekommenderade DSO att verksamheten skulle komplettera registerförteckningen med namn och kontaktuppgifter för den personuppgiftsansvariga, den personuppgiftsansvarigas företrädare samt dataskyddsombudet. I Valnämndens senaste version av registerförteckningen har detta åtgärdats.

Dataskyddsombudets bedömning samt rekommendationer

DSO noterar att registerförteckningen är mer behandlingsorienterad än systemorienterad och att det talar för en god fullständighet. DSO konstaterar att verksamhetens samtliga personuppgiftsbehandlingar tycks ingå i registerförteckningen. Det finns definitivt en sådan ambition i verksamheten.

Registerförteckningen har tagits fram i samråd med DSO. DSO konstaterade vid tillsynen 2021 att verksamheten saknade nedtecknade rutiner för arbetet med registerförteckningen. På grund av Valnämndens periodiska arbetssätt bedömer DSO att en utförlig nedtecknad rutin inte är nödvändig med beaktande av verksamhetens omfång, utan att det är tillräckligt att nämnden arbetar med registerförteckningen utifrån det systematiska kvalitetsarbetets årshjul samt att en översyn görs två gånger per år.

DSO rekommenderar att verksamheten fortsätter arbeta löpande med registerförteckningen utifrån att nya behandlingar förs in eller att gällande behandlingar förändras. Vidare bör nämnden fortsätta granska registerförteckningen årsvis för att säkerställa att den återspeglar nämndens aktuella personuppgiftsbehandlingar.

2. Säkerhet i samband med behandlingen

Bakgrund och syfte

Personuppgiftsansvarig ska tillse att personuppgifter skyddas med lämpliga säkerhetsåtgärder, detta för att till exempel undvika att obehöriga får tillgång till uppgifterna eller att uppgifterna förloras.

Personuppgiftsansvarig behöver bedöma vilka tekniska- och organisatoriska säkerhetsåtgärder som ska vidtas för de behandlingar som utförs. Till tekniska säkerhetsåtgärder räknas till exempel kryptering, pseudonymisering och säkerhetskopiering. Organisatoriska säkerhetsåtgärder avser till exempel interna riktlinjer och rutiner.

För att skapa förutsättningar för att skydda information (inklusive personuppgifter) med rätt slags skydd ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. Genom riskanalyser identifierar informationsägaren risker och väljer åtgärder för att minska riskerna. Risker i samband med personuppgiftsbehandling är en typ av risk som informationsägaren behöver omhänderta i riskanalyser.

Att det finns skriftliga, beslutade och kommunicerade styrdokument samt kända rutiner medför att medarbetarna vet hur de ska agera avseende frågor som rör dataskydd. Den personuppgiftsansvariga måste kunna *visa* hur GDPR efterlevs och att det finns styrdokument och rutiner är en viktig del i detta.

Syftet med detta rapporteringsområde är därmed att rapportera huruvida DSO bedömer att det tas hänsyn till risker för den registrerade och om dessa beaktas i tillräcklig mån i genomförda informationsklassningar och riskanalyser. Vidare bedömer DSO huruvida det finns tillräckligt mycket reglerat om dataskydd i styrdokument och rutiner samt om dessa är tillräckligt implementerade och kända.

Kontroller och iakttagelser gjord av dataskyddsombudet

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

Ja. Valnämnden har endast genomfört en informationsklassning, vilken avser systemet Kaskelot. I Kaskelot behandlas inga känsliga personuppgifter, däremot behandlas integritetskänsliga uppgifter. Givet detta bedömer DSO att tillräcklig hänsyn tagits till de olika kategorierna av personuppgifter.

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

Ja. Valnämnden tar del och följer de av Stadsledningskontorets skapade dokument och rutiner inom dataskyddsområdet. I viss utsträckning anpassas dessa utifrån nämndens verksamhet.

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

Ja. DSO har fått information om att de anställda har god kännedom om styrdokumenten samt att dessa efterlevs i praktiken. Samtliga nyanställda får information om styrdokumenten och var dessa kan hittas. DSO bedömer att de skriftliga styrande dokumenten och rutinerna är tillräckligt implementerade och väl kända inom organisationen.

Dataskyddsombudets jämförelse med föregående års resultat

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

Föregående år rekommenderade DSO att nämnden skulle översända det förnyade PUB-avtalet med Precio Fishbone och den nya klassningen av Kaskelot för granskning. Valnämnden har översänt dokumentationen som har granskats av DSO. DSO:s bedömning är att dokumentationen håller lämplig kvalité.

Dataskyddsombudets bedömning samt rekommendationer

DSO konstaterar att med beaktande av Valnämndens periodiska arbetssätt så är behovet av unik upprättad styrande dokumentation förhållandevis lågt, inte minst mellan valåren. Valnämnden tar dock del av och följer de av stadsledningskontorets skapade dokumenten och rutinerna inom dataskyddsområdet. I viss utsträckning anpassas dessa utifrån nämndens verksamhet. Valnämnden har under tillsynsåret antagit en rutin för användningen av tjänsten Säkra meddelanden.

Framöver rekommenderar DSO att verksamheten successivt upprättar eller kompletterar existerande, centralt framtagna rutiner och riktlinjer med information som är av särskilt intresse för Valnämnden, i de fall ett sådant behov skulle uppstå. I övrigt bedömer DSO att med beaktande av Valnämndens periodiska arbetssätt så är verksamhetens arbete med styrande dokumentation på en lämplig nivå.

3. Konsekvensbedömning avseende dataskydd

Bakgrund och syfte

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

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

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

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

Kontroller och iakttagelser gjord av dataskyddsombudet

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

Det saknas dokumenterade rutiner för att vid nya eller förändrade personuppgiftsbehandlingar genomföra tröskelanalys.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Ja, däremot dokumenteras inte tröskelanalyserna.

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

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

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Hittills har Valnämnden inte identifierat några högriskbehandlingar i sin verksamhet och därmed har inga konsekvensbedömningar genomförts.

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

Ja, hittills har Valnämnden inte identifierat några högriskbehandlingar i sin verksamhet.

Dataskyddsombudets jämförelse med föregående års resultat

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

Föregående tillsyn gav DSO rådet att verksamheten skulle värdera och identifiera de personuppgiftsbehandlingar som kan tänkas utgöra hög risk och kräva konsekvensbedömning, särskilt vad gällde tjänsten Säkra meddelanden. Verksamheten har gjort en kartläggning över aktuella personuppgiftsbehandlingar och vid inventering har inga behandlingar hittills bedömts som högriskbehandlingar.

Dataskyddsombudets bedömning samt rekommendationer

Valnämnden har kunskap om vad en konsekvensbedömning är och när den ska göras. Verksamheten genomför tröskelanalyser men dokumenterar inte dessa. DSO rekommenderar att verksamheten dokumenterar tröskelanalyser för att säkerställa att principen om ansvarsskyldighet uppfylls. Enligt principen är det inte tillräckligt att följa GDPR, man behöver även kunna visa att man följer GDPR, ofta genom dokumentation.

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

DSO ger rådet att Valnämnden fortsättningsvis kontinuerligt värderar och identifierar vilka av nämndens personuppgiftsbehandlingar som kan antas utgöra hög risk och kräva konsekvensbedömning.

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?

DSO har inte fått information om att det finns dokumenterade mallar eller rutiner för detta.

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

Under 2025 har nämnden tagit emot fyra stycken begäranden om utövande av registrerades rättigheter, samtliga avsåg registerutdrag.

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?

Ja. Däremot har verksamheten endast tagit emot begäranden om registerutdrag från personer vars personuppgifter inte har behandlats av nämnden. DSO har därför endast granskat svar som innehåller information om att den registrerades personuppgifter inte förekommer hos nämnden. Notera att det finns formkrav för vad ett registerutdrag ska innehålla när det förekommer uppgifter om den registrerade hos nämnden.

Dataskyddsombudets jämförelse med föregående års resultat

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

Eftersom ingen begäran om att utöva de registrerades rättigheter inkom under föregående tillsynsår kunde inte DSO fullt ut uttala sig om Valnämndens förmåga att hantera dessa.

Verksamheten hade dock tidigare år visat god förmåga att kunna hantera dessa inom föreskriven tidsfrist.

Dataskyddsombudets bedömning samt rekommendationer

DSO har inte fått information om att det finns dokumenterade mallar eller rutiner för besvarande av begäran från den registrerade. DSO rekommenderar att verksamheten undersöker behovet av att utarbeta rutiner för detta, alternativt att verksamheten undersöker möjligheten att anta befintliga rutiner från staden.

I övrigt uppmuntrar DSO verksamheten att fortsättningsvis tillmötesgå begäran om att utöva registrerades rättigheter på en sådan god nivå som de hittills har gjort.

5. Personuppgiftsincidenter

Bakgrund och syfte

Med begreppet personuppgiftsincident avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Om en inträffad personuppgiftsincident medför en risk för fysiska personers rättigheter och friheter ska den anmälas till Integritetsskyddsmyndigheten (IMY) inom 72 timmar från upptäckt. Om personuppgiftsincidenten sannolikt leder till hög risk för de registrerade måste de informeras utan onödigt dröjsmål.

Om en personuppgiftsincident inte bedöms vara anmälningspliktig ska den dokumenteras.

Syftet med detta rapporteringsområde är att kontrollera huruvida det säkerställs att samtliga medarbetare har den kunskap som krävs om personuppgiftsincidenter, huruvida det finns ändamålsenliga rutiner för att hantera händelser som kan utgöra personuppgiftsincidenter och huruvida dessa rutiner följs.

Kontroller och iakttagelser gjord av dataskyddsombudet

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

Detta säkerställs genom dokumenterade rutiner och återkommande utbildningar. Samtliga nyanställda genomför utbildning inom området.

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

DSO har granskat rutinen för hantering av informationssäkerhetsincidenter, som även behandlar personuppgiftsincidenter. Rutinen är tydlig och efterlevs i praktiken. DSO rekommenderar att verksamheten kompletterar rutinen med information om när de registrerade ska informeras om en personuppgiftsincident.

Hur många personuppgiftsincidenter har dokumenterats under året?

En personuppgiftsincident har dokumenterats under året.

Hur många personuppgiftsincidenter har anmälts till IMY under året?

En personuppgiftsincident har anmälts till IMY under året. Anmälan gjordes inom 72 h från upptäckt.

Dataskyddsombudets jämförelse med föregående års resultat

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

Föregående tillsynsår rekommenderade DSO att Valnämnden skulle komplettera rutinen för hantering av informationssäkerhetsincidenter med information om när de registrerade ska informeras om en personuppgiftsincident. Sedan föregående tillsynsår har denna komplettering införts i den lokala anvisningen för informationssäkerhet. DSO rekommenderar att informationen även införs i rutinen för hantering av informationssäkerhetsincidenter, för att säkerställa att rutinen innehåller fullständig information om hur personuppgiftsincidenter ska hanteras.

Dataskyddsombudets bedömning samt rekommendationer

DSO rekommenderar att rutinen för hantering av informationssäkerhetsincidenter kompletteras enligt ovan. I övrigt uppmuntrar DSO Valnämnden att bibehålla den interna kunskapen om personuppgiftsincidenter genom kontinuerliga ut- och fortbildningar.

6. Överföring till tredje land

Bakgrund och syfte

För att säkerställa att den nivå av skydd för personuppgifter som ställs i GDPR inte undergrävs får överföringar av personuppgifter till länder utanför EU/EES (tredje land) endast ske under särskilda förutsättningar. Det innebär att sådan överföring måste stödjas på antingen ett beslut från EU-kommissionen om att landet ifråga upprätthåller en adekvat skyddsnivå, att överföringen omfattas av en lämplig skyddsåtgärd eller i särskilda undantagsfall. Vidare behöver även kompletterade skyddsåtgärder, utöver de lämpliga skyddsåtgärderna, vidtas i vissa fall.[1]

Syftet med detta rapporteringsområde är att rapportera huruvida personuppgiftsansvarig har identifierat de tredjelandsöverföringar som utförs, huruvida personuppgiftsansvarig tillämpar överföringsverktyg på de tredjelandsöverföringar som utförs och om nödvändiga bedömningar har gjorts avseende tredjelandsöverföringarna.

Kontroller och iakttagelser gjord av dataskyddsombudet

Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?

Valnämnden har kunskap om vad en tredjelandsöverföring är och vad detta innebär. Verksamheten har gjort en kartläggning över aktuella personuppgiftsbehandlingar och har bedömt att inga tredjelandsöverföringar sker. DSO har dock noterat att i PUB-avtalet med Precio-Fishbone anges att tredjelandsöverföringar sker med stöd av DPF. DSO uppmanar givet detta Valnämnden att se över kartläggningen av tredjelandsöverföringar.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

Sannolikt inte aktuellt i nuläget.

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

Sannolikt inte aktuellt i nuläget.

Dataskyddsombudets jämförelse med föregående års resultat

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

Det aktuella rapporteringsområdet granskades inte föregående år.

---

[1] Europeiska dataskyddsstyrelsens (EDPB) Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överenstämmelsen med EU-nivån för skydd av personuppgifter, Version 2.0, Antagna den 18 juni 2021.

Dataskyddsombudets bedömning samt rekommendationer

DSO rekommenderar att verksamheten ser över sin kartläggning i enlighet med rekommendationen ovan. Därefter bör nämnden fortsätta kartlägga aktuella och nya personuppgiftsbehandlingar för att identifiera eventuella tredjelandsöverföringar. Om tredjelandsöverföringar sker ska dessa ske med stöd av ett överföringsverktyg samt föregås av en TIA.

Se även under omvärldsanalys nedan.

Bilaga 2 – Andra genomförda granskningar och omvärldsbevakning

Andra granskningar som dataskyddsombudet har genomfört under året

Genomförda granskningar och deras resultat

Det granskande arbetet är en av dataskyddsombudets viktigaste uppgifter. Granskningsområdena har valts utifrån ett riskbaserat synsätt, det vill säga att fokus läggs på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister.

Med anledning av det kommande Riksdags- region- och kommunalvalet 2026, har DSO valt att granska verksamhetens dataskyddsarbete inför den kommande uppskalade verksamheten. DSO har lagt fokus på vilket stöd nyanställda får i dataskyddsfrågor, inbegripet utbildning, lättillgängliga rutiner och riktlinjer samt vilken nivå på generell dataskyddskultur som förekommer i det dagliga arbetet.

Resultat

Valnämnden tillhandahåller stöd i dataskyddsfrågor till nyanställda på flera olika sätt. Samtliga nyanställda får introduktion och utbildning inom både dataskydd och informationssäkerhet, detta sker genom obligatoriska webbkurser. Ett år efter genomförandet skickas en påminnelse ut om att genomföra kursen igen. Nyanställda informeras om rutiner och riktlinjer och dessa dokument är lättillgängliga för de anställda. Vidare får de nyanställda information om vad en personuppgiftsincident är och hur en sådan ska hanteras.

Sammanfattningsvis bedömer DSO att Valnämnden är väl rustade i sitt dataskyddsarbete.

Omvärldsbevakning

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

Den nuvarande amerikanska administrationen har emellertid vidtagit ett antal åtgärder, bl.a. genom att avskeda majoriteten av ledamöterna i den oberoende styrelse (PCLOB) som skulle övervaka att DPF följs, som föranlett de svenska och norska tillsynsmyndigheterna att komma med uttalanden. IMY påtalar att ifall det finns information som visar att ett adekvat skydd inte längre kan säkerställas kan EU-kommissionen återkalla, ändra eller upphäva ett beslut om adekvat skyddsnivå. Dessutom har EU-domstolen möjlighet att ogiltigförklara ett beslut om adekvat skyddsnivå. Den norska tillsynsmyndigheten Datatilsynet anger i information på sin hemsida att även om vi för närvarande har ett adekvansbeslut som gör att det är tillåtet att överföra personuppgifter till USA, förväntar man sig att adekvansbeslutet förr eller senare kommer att ifrågasättas i EU-domstolen. Man skriver vidare att verksamheter, när de köper amerikanska data-tjänster, behöver vara medvetna om att situationen i USA även har bidragit till osäkerhet. Det är därför viktigt att personuppgiftsansvariga som genomför tredjelandsöverföringar skaffar en exitstrategi för hur man ska agera om det inte längre är

tillåtet att överföra personuppgifter till USA på samma sätt som idag. Datatillsynet menar att även användningen av amerikanska molntjänster på europeisk mark skulle påverkas negativt om adekvansbeslutet upphävs.