Stockholms stad

GDPR årsrapport

År 2025

SGA Fastigheter AB

GDPR årsrapport
Januari 2026

Dnr: 2026/2
Utgivningsdatum: 2026-01-14
Kontaktperson: Sara Billing Feinberg

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 SGA Fastigheter AB:s (”bolaget”) dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

Enligt instruktionerna ska dataskyddsombudet (”DSO”) i bilaga 1 genomföra en detaljerad redovisning av DSOs granskning. Med hänsyn till det låga antalet PU-behandlingar i bolaget och den hur pass få av dessa som är känsliga respektive integritetskänsliga, har DSO beslutat att enbart fylla i sammanfattningen och inte bilaga 1. Detsamma gäller bilaga 2. Detta förfarande har även godkänts av bolagets informationssäkerhetssamordnare tillika tillförordnad VD.

Sammantaget anser DSO att SGA Fastigheter har ett dataskyddsarbete som får anses väl avvägt relativt bolagets riskexponering, där inga höga eller medelhöga risker gällande de registrerades fri- och rättigheter har identifierats. Ansvarsskyldigheten (Art 5.2 GDPR) är uppfylld och upprättade rutiner tycks i huvudsak följas i den dagliga verksamheten, även om bolaget själv identifierat en önskan om att implementera ett arbetssätt som gör att uppdateringar i bolagets registerförteckning tydligare knyts samman med annat förändringsarbete, exempelvis gällande allmänna handlingar och informationsredovisning.

Avsaknaden av inrapporterade personuppgiftsincidenter under året väcker dock farhågan att där kan finnas ett mörkertal - och vi rekommenderar därför en fortbildning av personalen för att säkerställa att det finns en kunskap om vad som utgör en personuppgiftsincident och hur sådana ska hanteras när de inträffar. Fortbildningen kan också med fördel omfatta riskbedömning- och hantering för att förstärka medarbetarnas kunskaper om när tröskelanalyser (och i förlängningen konsekvensbedömningar) kan behöva göras inför nya eller förändrade personuppgiftsbehandlingar.

De tre största riskerna enligt dataskyddsombudets bedömning

Fråga/kontroll	**Risk**	**Rekommenderad åtgärd/åtgärder**
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		*Bolaget behöver arbeta för att finna rutin för uppdatering av registerförteckningen.*
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		*Det finns rutiner för att genomföra konsekvensbedömning vid behov, men dessa behöver uppdateras för att tydliggöra att det även behövs innefatta en inledande process för att avgöra om en personuppgiftsbehandling medför hög risk för*

		individers rättigheter, vilket i så fall kräver en konsekvensbedömning via DSO.
Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne ska agera vid en personuppgiftsincident?		*Det finns rutiner i bolaget för att agera vid incidenter. Det kräver dock kommunikation mellan berörd medarbetare - ansvarig chef - informationssäkerhetssamordnare - DSO för att kunna hantera en personuppgiftsincident. Hanteringen behöver bolaget fortsätta att informera om via månadsmöten för att säkerställa att kunskapen finns hos alla.*

Innehållsförteckning

Inledning

GDPR, eller dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. Dataskyddsreglerna (*kallas GDPR fortsättningsvis*) sätter tydliga ramar för hur personuppgifter får behandlas för att minimera risken för skada och säkerställa att hanteringen sker ansvarsfullt och rättvist. GDPR har sin grund i de mänskliga rättigheterna, där varje individ har rätt till respekt för sitt privat- och familjeliv samt skydd av sina personuppgifter.

I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten.

Dataskyddsombudets uppgift

Varje personuppgiftsansvarig (nämnd eller styrelse) ska utse ett dataskyddsombud. Dataskyddsombudets uppgifter framgår direkt av lagstiftningen. Ombudets roll är att kontrollera att GDPR följs inom organisationen. Det innebär bland annat att ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. Dataskyddsombudet har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs. DSO ska rapportera direkt till högsta förvaltnings-/bolagsnivå. I Stockholms stad innebär det att dataskyddsombudet rapporterar till nämnder och styrelser.

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

Granskning av dataskyddsarbetet

Kontroll av obligatoriska områden

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

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

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

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

Resultatsammanställning och centrala iakttagelser inom dataskyddsarbetet

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

Antal behandlingar som är registrerade:
Verksamheten har uppdaterat registerförteckningen utifrån JP Infonets tidigare förslag.

Föregående års antal inom parentes.

Verksamhetsområden, antal: 3 (3)

Verksamhetsprocesser (övergripande nivå), antal: 10 (18)

Verksamhetsprocesser (underliggande nivå), antal: 40 (35)

180 (165) behandlingar. Ett exempel på behandling är ”Tillstånd från myndigheter”.

Det finns delar i registerförteckningen som bolaget behöver fortsätta att arbeta med, till exempel ”Kategori registrerade ”och ”Behandlingsystem”.

Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?
Bolaget har informerat DSO om en tillsynsrapport från Stadsarkivet där det framgår att bolaget har mycket god hantering av allmänna handlingar. Bolaget behöver implementera ett arbetssätt som gör att uppdateringar i bolagets registerförteckning knyts samman med annat arbete inom bolaget, till exempel arbetet med allmänna handlingar och informationsredovisning. På så sätt kan dubbelarbete undvikas samt registerförteckningen bli en mer naturlig del av bolaget arbete med informationsredovisning.

Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?
Bolaget behandlar relativt få personuppgifter, främst hänförande till den egna personalen samt inloggningsuppgifter (som inte anses känsliga eller integritetskänsliga enligt regelverket). Detta beror bland annat på att bolaget endast har ett fåtal hyresgäster som samtliga är aktiebolag.

Främst gäller personuppgiftsbehandlingen egen personal och vissa uppgifter är känsliga enligt förordningen, t.ex. sjukdom, facklig tillhörighet och religiös övertygelse.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		*180 behandlingar.* *Uppdatera ”kategori registrerade” samt ”behandlingssystem”.*
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		*Att tillse att registerförteckningen får en naturlig koppling till bolaget övriga arbete med informationsredovisning.*
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		*Ja Men inte främst pga av rutiner som inarbetats, utan för att bolaget har relativt få personuppgiftsbehandlingar, då bolaget endast har ett fåtal hyresgäster som samtliga är aktiebolag.*
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		*Ja*

Säkerhet i samband med behandlingen

Sammanfattning

Bolaget har styrande dokument på plats. Det finns rutiner för personuppgiftsincidenter och konsekvensbedömningar.

De styrande dokumenten håller i huvudsak önskvärd kvalitet.

Vidareutveckling har skett genom att länken i de anställdas e-postsignatur lydande ”All e-post som skickas till SGA Fastigheter AB kommer att behandlas enligt upprättat dokument ”dataskyddsinformation för SGA Fastigheter” som återfinns på vår hemsida www.sgafastigheter.se” pekas direkt till den relevanta informationen på Bolagets hemsida.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Efter ett antal stickprov på genomförda informationsklassningar,		*Bolaget behandlar relativt få personuppgifter, främst hänförande till den egna personalen samt inloggningsuppgifter*

bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?		*(som inte anses känsliga eller integritetskänsliga enligt regelverket).*
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		*Tillräckligt.*
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		*Tillräckligt.*

Konsekvensbedömning avseende dataskydd

Sammanfattning

Bolaget har under året löpande genomfört översyn av behandlingar. En konsekvensbedömning har gjorts under 2025 i samband med införande av nytt inloggningsförfarande till fastighetssystem. Bolaget har inga högriskbehandlingar av personuppgifter.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?	🟡	*Det finns rutiner för att genomföra konsekvensbedömning vid behov, men dessa behöver uppdateras för att tydliggöra att det även behövs innefatta en inledande process för att avgöra om en personuppgiftsbehandling medför hög risk för individers rättigheter, dvs tröskelanalys, vilket i så fall kräver en konsekvensbedömning via DSO.*
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?	🟢	*Ja, vid behov.*
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?	🟢	*Ja*
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?	🟢	*Ja*
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?	🟢	*Ja, utifrån den övergripande årliga analysen av bolagets verksamhet och den kontakt som skett mellan bolaget och DSO så verkar samtliga personbehandlingar som kräver konsekvensanalys ha identifierats.*

Den registrerades rättigheter

Sammanfattning

Inga begäranden har inkommit under 2025.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		*Ja.*
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		*Inga begäranden har skett under 2025.*
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		*Inga begäranden har inkommit.*
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		*Inga begäranden har inkommit.*

Personuppgiftsincidenter

Sammanfattning

Inga personuppgiftsincidenter har skett 2025.

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?		*Det finns rutiner i bolaget för att agera vid incidenter. Det kräver dock kommunikation mellan berörd medarbetare - ansvarig chef - informationssäkerhetssamordnare - DSO för att kunna hantera en personuppgiftsincident.*

		*Dvs det behövs ytterligare kunskap hos medarbetarna för att förstå **vad** som utgör en personuppgiftsincident och **när** det är dags att hantera.*
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		*Det finns rutiner i bolaget för att agera vid incidenter och de är utformade enligt gängse principer.*
Hur många personuppgiftsincidenter har dokumenterats under året?		*Inga personuppgiftsincidenter har dokumenterats under året.*
Hur många personuppgiftsincidenter har anmälts till IMY under året?		*Inga personuppgiftsincidenter har anmälts till IMY under året.*

Överföring till tredje land

Sammanfattning

[Här beskriver DSO kortfattat de viktigaste iakttagelserna, inklusive områden där verksamheten utmärker sig positivt och bör fortsätta sitt arbete, samt identifierade brister som kan innebära dataskyddsrisker. Vidare ger DSO korta och konkreta rekommendationer för att hantera bristerna och stärka dataskyddsarbetet utifrån de identifierade iakttagelserna.]

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		*Inga tredjelandsöverföringar har utförts.*
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		*Inga tredjelandsöverföringar har utförts.*

Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		*Inga tredjelandsöverföringar har utförts.*

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Bilagor

Bilaga 1: Detaljerad redovisning av dataskyddsombudets granskning

Bilaga 2: Andra genomförda granskningar och omvärldsbevakning

Bilaga 1 - Detaljerad redovisning av dataskyddsombudets granskning

Med hänsyn till det låga antalet PU-behandlingar i bolaget och den hur pass få av dessa som är känsliga respektive integritetskänsliga, har denna del av rapporten inte fyllts i

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

[Se dokument ”Instruktion för dataskyddsombudets årsrapport” för vägledning. Instruktionen innehåller bland annat förslag på frågor som kan ställas till respektive rapporteringsområde.]

Antal behandlingar som är registrerade?

[Text]

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

[Text]

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

[Text]

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

[Text]

Dataskyddsombudets jämförelse med föregående års resultat

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

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

[Text]

Dataskyddsombudets bedömning samt rekommendationer

[DSO beskriver sin bedömning av verksamhetens efterlevnad inom aktuell obligatorisk område, både områden där verksamheten utmärker sig positivt och bör fortsätta sitt arbete, samt *identifierade risker. Vidare beskriver DSO rekommendationer om vad verksamheten ska fortsätta göra alternativt på åtgärder för att hantera identifierade dataskyddsrisker.]*

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

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

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

[Text]

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

[Text]

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

[Text]

Dataskyddsombudets jämförelse med föregående års resultat

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

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

[Text]

Dataskyddsombudets bedömning samt rekommendationer

[DSO beskriver sin bedömning av verksamhetens efterlevnad inom aktuell obligatorisk område, både områden där verksamheten utmärker sig positivt och bör fortsätta sitt arbete,

samt *identifierade risker. Vidare beskriver DSO rekommendationer om vad verksamheten ska fortsätta göra alternativt på åtgärder för att hantera identifierade dataskyddsrisker.]*

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

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

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

[Text]

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

[Text]

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

[Text]

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

[Text]

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

[Text]

Dataskyddsombudets jämförelse med föregående års resultat

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

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

[Text]

Dataskyddsombudets bedömning samt rekommendationer

[DSO beskriver sin bedömning av verksamhetens efterlevnad inom aktuell obligatorisk område, både områden där verksamheten utmärker sig positivt och bör fortsätta sitt arbete, samt *identifierade risker. Vidare beskriver DSO rekommendationer om vad verksamheten ska fortsätta göra alternativt på åtgärder för att hantera identifierade dataskyddsrisker.]*

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

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

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

[Text]

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

[Text]

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

[Text]

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

[Text]

Dataskyddsombudets jämförelse med föregående års resultat

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

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

[Text]

Dataskyddsombudets bedömning samt rekommendationer

[DSO beskriver sin bedömning av verksamhetens efterlevnad inom aktuell obligatorisk område, både områden där verksamheten utmärker sig positivt och bör fortsätta sitt arbete, samt *identifierade risker. Vidare beskriver DSO rekommendationer om vad verksamheten ska fortsätta göra alternativt på åtgärder för att hantera identifierade dataskyddsrisker.]*

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

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

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

[Text]

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

[Text]

Hur många personuppgiftsincidenter har dokumenterats under året?

[Text]

Hur många personuppgiftsincidenter har anmälts till IMY under året?

[Text]

Dataskyddsombudets jämförelse med föregående års resultat

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

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

[Text]

Dataskyddsombudets bedömning samt rekommendationer

[DSO beskriver sin bedömning av verksamhetens efterlevnad inom aktuell obligatorisk område, både områden där verksamheten utmärker sig positivt och bör fortsätta sitt arbete,

samt *identifierade risker. Vidare beskriver DSO rekommendationer om vad verksamheten ska fortsätta göra alternativt på åtgärder för att hantera identifierade dataskyddsrisker.]*

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

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

Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?

[Text]

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

[Text]

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

[Text]

Dataskyddsombudets jämförelse med föregående års resultat

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

---

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

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

[Text]

Dataskyddsombudets bedömning samt rekommendationer

[DSO beskriver sin bedömning av verksamhetens efterlevnad inom aktuell obligatorisk område, både områden där verksamheten utmärker sig positivt och bör fortsätta sitt arbete, samt *identifierade risker. Vidare beskriver DSO rekommendationer om vad verksamheten ska fortsätta göra alternativt på åtgärder för att hantera identifierade dataskyddsrisker.]*

Bilaga 2 – Andra genomförda granskningar och omvärldsbevakning

Med hänsyn till det låga antalet PU-behandlingar i bolaget och den hur pass få av dessa som är känsliga respektive integritetskänsliga, har denna del av rapporten inte fyllts i

Andra granskningar som dataskyddsombudet har genomfört under året

Genomförda granskningar och deras resultat

Granskning 1

Granskning 2

Dataskyddsombudets rekommendationer baserat på iakttagelserna ovan

Dataskyddsombudets rekommendationer
1. *Rekommendation,* 2. *Rekommendation,* 3. *Rekommendation, (m.fl.)*

Omvärldsbevakning

Resultatet av dataskyddsombudets omvärldsbevakning

[Kapitel där DSO kan informera personuppgiftsansvarig om viktiga händelser inom dataskydd, till exempel: ny praxis som särskilt berör personuppgiftsansvarig, nyheter kopplade till adekvansbeslut, nya regelverk som samspelar m.m..

Kan skrivas tillsammans med andra DSO:er.]

Övrigt att rapportera

[Kapitel där DSO har möjlighet att rapportera sådant som inte ryms inom övriga kapitel, men som DSO ändå bedömer är relevant att förmedla.

Om DSO inte har något övrigt att rapportera tas detta kapitel bort.]

Sammanfattning

Syfte

Övriga observationer