Stockholms stad

Bilaga 9

GDPR årsrapport

År 2025

Fastighetsnämnden

GDPR årsrapport 2025
Fastighetsnämnden

Dnr: FSK 2026/1
Utgivningsdatum: 2026-01-14
Kontaktperson: Patrik Pierd

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 Fastighetsnämndens dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

Fastighetsnämnden har under 2025 genomfört organisatoriska förändringar som innefattar att både ansvarsförhållanden för dataskyddsarbetet förändrats och att utökade resurser tillsats med tydligt uppdrag, ändamålsenlig erfarenhet och kompetens inom dataskyddsområdet.

Fastighetsnämnden har sedan tidigare identifierat ett flertal brister och risker kopplat till dataskyddsområdet. Under 2025 har flera risker hanterats eller riskreducerats, men det kvarstår fortfarande risker som behöver omhändertas och hanteras vilka analyserats och presenteras i denna årsrapport.

Fastighetsnämnden har därför påbörjat ett långsiktigt arbete med målsättningen att arbeta mer strategiskt, systematiskt och hållbart inom datasskyddsområdet. Det pågår även en utveckling av det systematiska arbetet med omvärldsbevakning i syfte att identifiera och förebygga risker med påverkan på nämndens verksamhet.

De tre största riskerna enligt dataskyddsombudets bedömning

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Fastställda och aktuella styrande och stödjande arbetssätt för ett systematiskt dataskyddsarbete		Fastighetsnämnden har identifierat en avsaknad av styrande och stödjande arbetssätt avseende dataskydd, och detta har sedan tidigare identifieras som en risk.
Konsekvensbedömningar		Fastighetsnämnden har sedan tidigare ett flertal fastställda arbetssätt som berör genomförande av riskanalys och konsekvensbedömningar. Det finns ett stort behov av att revidera och uppdatera dessa arbetssätt, likväl ett behov av att kommunicera och genomföra kompletterande utbildning till berörda målgrupper.
Registervård och uppdateringar av uppgifter i register över personuppgiftsbehandlingar		Det finns ett behov av att genomföra en grundlig revidering av innehållet i registerförteckningen för att säkerställa uppgifter, registreringar och behandlingar är aktuella och korrekta.

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 (DSO). 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

Det finns ett behov av att genomföra en grundlig revidering av innehållet i registerförteckningen för att säkerställa uppgifter, registreringar och behandlingar är aktuella och korrekta. En registerförteckning ska vara så fullständig så att den kan lämnas ut till tillsynsmyndigheten IMY vid begäran.

Översynen bör initialt omfatta de registreringar som är angivna med hög risk, samtliga registreringar som kan innehålla känsliga uppgifter och alla registerpunkter som rör HR-enheten.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		Fastighetsnämnden har 70 st. registrerade behandlingar i systemet Draftit. Uppdateringar av behandlingar och revidering av ansvariga har gjorts under året. Systematisk och periodiskt underhåll och utveckling kommer ske löpande.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		Fastighetsnämnden har identifierat vissa brister i arbetssätt gällande registrering av nya eller förändrade behandlingar. Ett arbete pågår med att revidera befintliga arbetssätt samt kartlägga behovet av nya arbetssätt, och arbetet fortsätter under 2026.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska		Fastighetsnämnden har påbörjat uppdatering av registret med behandlingar under 2025. Arbetet fortsätter under 2026, och därefter kommer

innehålla de behandlingar som personuppgiftsansvarig utför?		systematisk, periodisk uppdatering och registrering ske löpande.
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		Samtliga uppgifter som är obligatoriska enligt artikel 30 är besvarade i systemet Draftit. Systematisk och periodisk uppdatering och revidering sker löpande.

Säkerhet i samband med behandlingen

Sammanfattning

Fastighetsnämnden har en lokal anvisning för informationssäkerhet och fastställer årligen rapporten ledningens genomgång informationssäkerhet. Både dessa dokument innefattar dataskydd/GDPR och beskriver t ex. ansvarsförhållanden kopplat till informationsägarskap, informationssäkerhet och dataskydd.

Fastighetsnämnden har identifierat en avsaknad av styrande och stödjande arbetssätt avseende dataskydd, och detta har sedan tidigare identifieras som en risk. Därför har nämnden under 2025 påbörjat ett arbete med att utveckla nya arbetssätt som ska bidra till ett mer systematiskt dataskyddsarbete.

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?		Fastighetsnämnden har identifierat vissa brister i genomförda informationsklassningar med hänsyn till kategorier av personuppgifter. Ett arbete pågår med att revidera befintliga arbetssätt för att hantera risken samt kartlägga behovet av nya arbetssätt, och arbetet fortsätter under 2026.
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		Fastighetsnämnden har under 2025 påbörjat ett arbete med att utveckla nya arbetssätt inom flertalet olika säkerhetsområden som ska bidra till ett mer systematiskt dataskyddsarbete som ger nämndens verksamhet ska ges ett mer ändamålsenligt stöd i dataskyddsarbetet.

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		Fastighetsnämnden har under 2025 påbörjat ett arbete med att utveckla nya arbetssätt inom flertalet olika säkerhetsområden som ska bidra till ett mer systematiskt dataskyddsarbete som ger nämndens verksamhet ska ges ett mer ändamålsenligt stöd i dataskyddsarbetet.

Konsekvensbedömning avseende dataskydd

Sammanfattning

Fastighetsnämnden har sedan tidigare ett flertal fastställda arbetssätt som berör genomförande av riskanalys och konsekvensbedömningar. Det finns ett stort behov av att revidera och uppdatera dessa arbetssätt, likväl ett behov av att kommunicera och genomföra kompletterande utbildning till berörda målgrupper inom verksamheten.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		Fastighetsnämnden har fastställda rutiner för riskanalys och konsekvensbedömning. Det finns dock ett behov av revidering och uppdatering av dessa rutiner. Ett arbete pågår med att revidera befintliga arbetssätt för att hantera risken samt kartlägga behovet av nya arbetssätt, och arbetet fortsätter under 2026.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		Analyser genomförs, men inte i den omfattning och systematik som krävs enligt dataskyddsförordningen. Ett arbete pågår med att revidera befintliga arbetssätt för att hantera risken samt kartlägga behovet av nya arbetssätt, och arbetet fortsätter under 2026.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		Fastighetsnämnden har fastställda rutiner för riskanalys och konsekvensbedömning. Det finns dock ett behov av revidering och uppdatering av dessa rutiner.
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		Konsekvensbedömningar genomförs, men inte i den omfattning och systematik som krävs enligt dataskyddsförordningen.

		Ett arbete pågår med att revidera befintliga arbetssätt för att hantera risken samt kartlägga behovet av nya arbetssätt, och arbetet fortsätter under 2026.
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		Fastighetsnämnden har påbörjat kartläggning och identifiering av personuppgiftsbehandlingar som kräver att en konsekvensbedömning. Ett arbete som fortsätter och ska vara genomfört under 2026.

Den registrerades rättigheter

Sammanfattning

Det finns fastställda arbetssätt och utsedda personer för hantering av begäran från registrerad både vad det gäller registerutdrag och annan begäran. Rutinen har använts för enstaka registerutdrag och fungerar även om den är helt manuell i sammanställningsfasen.

Fastighetsnämnden har identifierat ett behov av revidering och uppdatering av dessa arbetssätt, och att det finns ett behov av systematisk och periodisk uppdatering och revidering som sker löpande.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	**Risk**	**Rekommendationer**
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		Fastighetsnämnden har mallar och rutiner för besvarande av begäran från registrerade. Systematisk och periodisk uppdatering och revidering sker löpande.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		Fastighetsnämnden har inte fått någon begäran om registerutdrag, begränsning eller radering från de registrerade under 2025.
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		Ej aktuell då någon begäran inte inkommit till fastighetsnämnden.

Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		Ej aktuell då någon begäran inte inkommit till fastighetsnämnden.

Personuppgiftsincidenter

Sammanfattning

Det finns fastställda arbetssätt hantering av personuppgiftsincidenter. Fastighetsnämnden har identifierat ett behov av revidering och uppdatering av dessa arbetssätt, och att det finns ett behov av systematisk och periodisk uppdatering och revidering som sker löpande.

Ansvarsförhållanden kopplat till anmälan om personuppgifteincidenter regleras i fastighetsnämndens delegationsordning.

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?		Fastighetsnämnden har infört krav på obligatorisk grundutbildning i dataskydd för samtliga anställda, med krav på repetitionsutbildning varje år. Systematisk uppföljning av genomförande ska ske kontinuerligt.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		Fastighetsnämnden har fastställda rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter Det finns dock ett behov av revidering och uppdatering av dessa rutiner.
Hur många personuppgiftsincidenter har dokumenterats under året?		Två (2) personuppgiftsincidenter har anmälts och dokumenterats under 2025.
Hur många personuppgiftsincidenter har anmälts till IMY under året?		En (1) personuppgiftsincidenter har anmälts till IMY under 2025 och avser Miljödataincidenten. Fastighetsnämnden har fått återkoppling i ärendet form av ett beslut där det framgår att IMY för närvarande inte vidtar några åtgärder med anledning av anmälan.

Överföring till tredje land

Sammanfattning

Fastighetsnämnden har identifierat brister vid registrering när det gäller tredjelandsöverföringar. Det är därför oklart om information och bedömningar stämmer gällande flera av behandlingarna. En ny bedömning och identifiering behöver göras för att säkerställa att tidigare bedömning är korrekt.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		Fastighetsnämnden har gjort en analys i samband med registreringen, med har inte identifierat några tredjelandöverföringar. En ny bedömning och identifiering behöver dock göras för att säkerställa att tidigare bedömning är korrekt.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		Då med har inte identifierat några tredjelandöverföringar har inget överföringsverktyg tillämpats. En ny bedömning och identifiering behöver dock göras för att säkerställa att tidigare bedömning är korrekt.
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		Då med har inte identifierat några tredjelandöverföringar har ingen bedömning av tredjelandsöverföring genomförts. En ny bedömning och identifiering behöver dock göras för att säkerställa att tidigare bedömning är korrekt.

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?

70 st.

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

Rutiner finns, men behöver uppdateras.

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

Arbete pågår.

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

Ja!

Dataskyddsombudets jämförelse med föregående års resultat

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

Ja, resultatet skiljer sig åt vilket är positivt och i rätt riktning. Organisatoriska förändringar har genomfört vilket innebär att ansvarsförhållanden tydliggjorts, och att resurser för arbete med dataskydd utökats och prioriteras. Styrande dokument inom dataskydd har fastställts, och det pågår en översyn av samtliga stödjande arbetssätt inom dataskyddsområdet.

Dataskyddsombudets bedömning samt rekommendationer

Fastighetsnämnden har påbörjat ett arbete och genomfört en del förändringar vilket påvisas i riskvärderingen i rapporten. De initiativ och pågående arbete som pågår bedöms reducera riskerna för fastighetsnämndens ansvar kopplat till integritets- och dataskyddsregelefterlevnad och vidare lämna information och råd till verksamheten och de anställda om deras skyldigheter enligt GDPR vid behandling av personuppgifter.

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?

Under 2025 har informationsklassningar i KLASSA 4.0 genomförts för merparten av system och applikationer. I klassningsarbetet har man tar hänsyn till olika kategorier av personuppgifter och värderat risker och konsekvenser. Det kvarstår dock ett arbete som planeras att genomföras under 2026.

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

Ett omfattande arbete med att ta fram stödjande arbetssätt pågår, där befintliga arbetssätt uppdateras och revideras, och nya arbetssätt tas fram där det saknas idag.

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

Det finns arbetssätt publicerade på en samarbetsyta som är tillgänglig för verksamheten, men som kommer ersättas av en ny plattform under 2026. I samband med detta kommer implementeringen ske genom kommunikation, workshops och riktade utbildningsinsatser.

Dataskyddsombudets jämförelse med föregående års resultat

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

Ja! Det har gjort förändringar under året och det pågår ett arbete som ska reducera riskerna som identifierats. En lokal anvisning informationssäkerhet har tagits fram och rapporten ledningens genomgång informationssäkerhets innefattar dataskydd, och kommer utvecklas ytterligare under 2026.

Dataskyddsombudets bedömning samt rekommendationer

Det arbetet som gjorts och som man planerar genomföra påvisar att dataskyddsarbetet prioriteras. Organisatoriska förändringar och tillsättning av nya tjänster som arbetar med dataskydd är till stor fördel för verksamheten. Att dataskyddsarbetet ska ske med systematik och med hållbarhet ses som positivt.

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 finns fastställda rutiner för riskanalys och konsekvensbedömning publicerade på en samarbetsyta. Det finns dock ett stort behov av revidering och uppdatering av dessa rutiner.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Man genomför konsekvensbedömningar i samband med informationsäkerhetsklassningar, men inte i den omfattning och systematik som krävs enligt dataskyddsförordningen.

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

Det finns både mall och rutiner för genomförande av konsekvensbedömning publicerade på en samarbetsyta. Det finns dock ett behov av översyn och uppdatering av dessa arbetssätt.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Det görs men inte i den omfattning och systematik som krävs enligt dataskyddsförordningen.

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

Man har påbörjat kartläggning och identifiering av personuppgiftsbehandlingar som kräver att en konsekvensbedömning där det saknas idag.

Dataskyddsombudets jämförelse med föregående års resultat

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

Det skiljer sig inte markant från föregående år då registerförteckningen behöver uppdateras, och i samband med det så bör även tröskelanalyser genomföras för att förnya behovet av konsekvensbedömningar.

Dataskyddsombudets bedömning samt rekommendationer

Det bör införas en rutin för att löpande revidera gjorda konsekvensbedömningar så att skyddsnivåer kan upprätthållas vilka har identifieras, och det pågår ett arbete med att revidera befintliga arbetssätt för att hantera risken samt kartlägga behovet av nya arbetssätt, och arbetet fortsätter under 2026.

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?

Det finns mallar och rutiner publicerade på en samarbetsyta. Det finns dock ett behov av översyn och uppdatering av dessa arbetssätt.

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

Ingen begäran har inkommit under 2025

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

Ej aktuell (se svar ovan)

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

Ej aktuell (se svar ovan)

Dataskyddsombudets jämförelse med föregående års resultat

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

Även om det har genomförts förändringar i verksamheten under året, så är resultatet mer eller mindre detsamma som föregående år.

Dataskyddsombudets bedömning samt rekommendationer

Det pågår ett arbete med att revidera befintliga arbetssätt vilket bedöms hantera risken samt säkerställa verksamhetens skyldigheter enligt GDPR vid behandling av personuppgifter.

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?

Man har infört krav på obligatorisk grundutbildning i dataskydd för samtliga anställda, med krav på repetitionsutbildning varje år. Systematisk uppföljning av genomförande ska ske kontinuerligt.

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

Det finns fastställda rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter. Det finns dock ett behov av revidering och uppdatering av dessa rutiner.

Hur många personuppgiftsincidenter har dokumenterats under året?

Två incidenter

Hur många personuppgiftsincidenter har anmälts till IMY under året?

En incident

Dataskyddsombudets jämförelse med föregående års resultat

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

Resultatet är mer eller mindre detsamma, även om det genomförts en del förändringar vilket är positivt. Det finns en fastställd rutin för hantering av personuppgiftsincidenter. Rutinen behöver uppdateras och publiceras.

Dataskyddsombudets bedömning samt rekommendationer

Ansvarsförhållandena i verksamheten har tydliggjort och nämndens delegationsordning har uppdaterat och innefattar numer tydliga ansvarsförhållanden inom dataskydd. Det pågående arbetet som planerar att genomföras under 2026, bedöms omhänderta risker som är identifierade.

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?

Enligt tidigare analys och i samband med registreringen har inga tredjelandöverföringar identifierats.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

Överföringsverktyg har inte tillämpats, då tredjelandsöverföringar inte identifierats.

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

Ingen bedömning av tredjelandsöverföring genomförts, då tredjelandsöverföringar inte identifierats.

Dataskyddsombudets jämförelse med föregående års resultat

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

Resultatet skiljer sig inte mot föregående år. I registerförteckningen framgår att det på flera frågor anges ”vet ej” exempelvis när det gäller tredjelandsöverföringar. Det är därför oklart om information lämnats på ett korrekt sätt gällande flera av behandlingarna.

Dataskyddsombudets bedömning samt rekommendationer

Registerförteckningen behöver uppdateras och en ny bedömning och identifiering behöver göras för att säkerställa att tidigare bedömning är korrekt. Fastighetsnämnden har påbörjat uppdatering av registret med behandlingar under 2025. Arbetet fortsätter under 2026, och därefter kommer systematisk, periodisk uppdatering och registrering ske löpande.

---

[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.

Bilaga 2 – Andra genomförda granskningar och omvärldsbevakning

Andra granskningar som dataskyddsombudet har genomfört under året

Genomförda granskningar och deras resultat

Fastighetsnämndens delegationsordning har uppdaterats 2025-03-31, och ansvar och rätten om att fatta beslut har tydliggjorts i enlighet med dataskyddsförordningen.

Dataskyddsombudets rekommendationer baserat på iakttagelserna ovan

Dataskyddsombudets rekommendationer
1. *En översyn och eventuell uppdatering i samband med nästkommande revidering av arbetsordningen rekommenderas, i syfte att säkerställa och tillgodose nya eller förändrade krav i dataskyddsförordningen.*

Omvärldsbevakning

Resultatet av dataskyddsombudets omvärldsbevakning

NIS2 – den nya cybersäkerhetslagen skulle varit implementerat oktober 2024, med senarelades för att nu träda ikraft 15 januari 2026. Den nya lagen har flertalet angränsande lagstiftningar, varav dataskyddsförordningen är en av dessa.

Fastighetsnämnden träffas av den nya lagen som offentlig förvaltning, och ställer ex. krav på informationssäkerhet och teknik, upphandling och avtal – krav, informationssäkerhetsdokumentation och incidentrutiner som behöver analyseras utifrån motsvarande krav i angränsande lagstiftningar som t ex. säkerhetsskyddslag, dataskyddsförordning, CER-direktiv m f.

Fastighetsnämnden har påbörjat kartläggning och analys för att anpassa organisation och arbetssätt för att tillmötesgå kraven i den nya cybersäkerhetslagen, och arbetet kommer att fortsätta under 2026.