Stockholms stad

GDPR årsrapport

År 2025

Bostadsförmedlingen i Stockholm AB

GDPR årsrapport
Januari 2025

Dnr: BOST 2026/13
Kontaktperson: Dani Cohen

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 **Bostadsförmedlingen i Stockholm AB**'s dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet. Årets rapport följer ny mall och nya områden som granskar – även beskrivning av risknivåer har förändrats. Jämförelse av risker mot föregående år blir därmed delvis missvisande.

Bolaget har i huvudsak mycket god förståelse för och arbetar aktivt med frågor som rör dataskydd. Organisationen har haft en löpande kontakt med dataskyddsombudet och arbetat förebyggande och åtgärdande inom flera områden. Vissa riskområden har definierats som medelhöga risker.

De tre största riskerna enligt dataskyddsombudets bedömning

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Klassningar av system		Organisationen föreslås tydligare beskriva information och hur handlingsplaner följs upp för att säkra informationen.
Cookies på hemsidan		Organisationen bör säkra att information är korrekt och säkra undvikandet av tredjepartsskript eller tydligt arbeta med avtal för dessa.
Kompletterande information vid registerutdrag		Registerutdrag utlämnas i tid, men vid begäran om tillgång från registrerade behöver korrekt information lämnas. Dessa är i nuläget inte helt korrekt.

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 från granskningen av de sex obligatoriska områdena

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

Bolaget har ett register som i lagom omfattning och omfång väl beskriver den verksamhet som bedrivs. Bolaget har även tagit fram en särskild rutin för ansvarsroller och hur uppdatering av registret ska göras. Vissa justeringar behöver dock göras.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		Behandlingarna i registret motsvarar vad dataskyddsombudet kan bedöma de faktiska behandlingarna inom bolaget.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		Bolaget har 2025 uppdaterat rutiner för hantering och registrering av behandlingar.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		Registret kontrolleras årligen enligt rutin och är i huvudsak aktuell, men vid genomgång har viss avsaknad av information noterats, eller uppgifter varit gamla.
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		Det saknas viss obligatorisk information eller beskrivs ska tillkomma senare. Registret behöver uppdateras på några punkter, och laglig grund för behandling av personalens personuppgifter behöver kompletteras. Det saknas även kategorier av registrerade

		för närstående till personal när det kan förekomma. Det saknas viss obligatorisk information eller beskrivs ska tillkomma senare. Laglig grund för behandling av personalens personuppgifter behöver kompletteras/ är felaktig.

Säkerhet i samband med behandlingen

Sammanfattning

Årets uppföljning har inneburit att stickprovskontroller har gjorts för hur man arbetar med dataskydd (security by design och default). Vissa brister i dokumentation vad gäller uppföljning och faktiska säkerhetsåtgärder har noterats vilket gjort det svårt att följa verklig säkerhet. För de stora mängder, och delvis känsliga uppgifter som bolaget hanterar, krävs proportionerliga åtgärder för att skydda personuppgifterna. Dataskyddsombudet har gett särskilda råd inom det området.

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?		Informationsklassningar har gjorts, men är otillräckligt dokumenterade för specifikt de behandlingarna som görs inom system. Vissa brister i säkerhetsåtgärder och dokumentation om det (”security by design and default”) saknas.
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		Bolaget har goda förutsättningar för att bedriva god informationssäkerhet genom egna styrande dokument, och kompletterande dokumentation från staden.
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		Det saknas tydlig dokumentation om åtgärder och hur säkerhet implementerats, vilket kan tyda på bristande implementation. Vid uppföljning muntligt har dock flera åtgärder kunnat visas, medan andra åtgärder är pågående.

Konsekvensbedömning avseende dataskydd

Sammanfattning

Bolaget har genomfört en tröskelanalys av samtliga behandlingar 2022. I samband med dessa gjordes även ett antal konsekvensbedömningar. Dessa har sedan genomförandet, inte återbesökts. Vid granskning saknar dessa konsekvensbedömningar tydliga riskanalyser, och bör förnyas med hänsyn till de anpassningar som staden gjort av sina mallar, eller de nya IMY-mallar som numera finns. Riskanalyser för behandlingar bör göras särskilt med hänsyn till risker för registrerades fri och rättigheter, där hög risk inte kan bedömas enligt samma nivåer som de metoder bolaget använder för informationssäkerhetsbedömningar.

Dataskyddsombudet vill rikta särskilt beröm för det arbetet som tidigare har genomförts med fullständig genomlysning av samtliga behandlingar.

Bedömning av risknivå och rekommendationer från dataskyddsombudet:

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?	🟡	Rutiner för tröskelanalyser och förnyad personuppgiftsbehandling finns i stadens metodstöd för informationssäkerhet, men lokala rutiner saknas ännu. Bolaget arbetar med att ta fram rutiner.
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?	🟢	Tröskelanalyser har gjorts för samtliga behandlingar. Dataskyddsombudet rekommenderar förnyad tröskelanalys för uppgifter för bolagets personal särskilt inom rehabilitering. Inga nya behandlingar har tillkommit 2025
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?	🟡	Konsekvensbedömningar har inte återbesökts sedan genomförandets. Konsekvensbedömningar ska följas upp kontinuerligt. Mallar som använts har varit Stockholms stad, men har vid dåvarnade utförande saknat utrymme för dataskyddsombudets rekommendationer och med otillräckliga riskanalyser. Rekommenderat användning av IMY's mallar eller stadens nya mallar baserade på dessa.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		Rekommenderas förnyad tröskelanalys för rehabiliteringsärenden m.m. för personal.
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning avseende dataskydd görs samt genomfört detta?		Där tröskelanalys visat att konsekvensbedömning behövs har sådan också gjorts. Dataskyddsombudet rekommenderar bolaget ändå att återbesöka konsekvensbedömning för vissa HR-processer.

Den registrerades rättigheter

Sammanfattning:

Bolaget har förmåga och kapacitet att hantera begäran från registrerade, och har skötts inom tidsramarna. Brister rör främst den kompletterande information som ska följa med till den registrerade, som gäller specificerad information om varför uppgifterna hanteras, mottagare, gallringstider, var uppgifter hämtats och information om möjlighet att lämna klagomål till IMY.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	**Risk**	**Rekommendationer**
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		Bolaget har rutiner för att besvara och hantera begäran från registrerade, men dessa behöver kompletteras med mer tydlig uppgift för hur begäran om radering och begränsning ska hanteras. Därutöver kan rutinen behöver kompletteras för att tydliggöra så all information registrerade har rätt till verkligen tillgodoses.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?	8	
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?	8	Personuppgiftsansvarig har hanterat begäran på ett snabbt sätt inom utsatt tid.
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		Svar till registrerade saknar tydlig information om laglig grund, ändamål och hur länge uppgifterna bevaras.

Personuppgiftsincidenter

Sammanfattning

Bedömningen är att personalen har fått information om hantering av personuppgiftsincidenter. Antalet personuppgiftsincidenter har varit relativt få under året, men vid analys av kunskapsnivå har det varit svårt att se att det beror på minskad rapporteringsvilja eller förståelse för vikten av rapportering. Bolaget har arbetat aktivt med att nå ut med information om vikten av att rapportera personuppgiftsincidenter, t.ex. genom information på enhetsmöten m.m.
Viss brist finns i diskrepans mellan information i digitala utbildningar och hur bolaget väljer att hantera personuppgiftsincidenter vad gäller vägar för rapportering. Rekommendation att ha systemstöd för rapporter kvarstår.

Bolaget har mycket goda rutiner för hantering av incidenter, och visat mycket bra förmåga att omsätta dessa i praktiken.

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?		Medvetenheten kan anses vara god, men rapporteringsvägar blir otydlig med olika information i digitala utbildningar mot hur bolaget valt att arbeta med rapporteringsvägar.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		Bolaget har mycket goda rutiner för hantering av incidenter, och visat mycket bra förmåga att omsätta dessa i praktiken.
Hur många personuppgiftsincidenter har dokumenterats under året?	*7*	
Hur många personuppgiftsincidenter har anmälts till IMY under året?	*0*	

Överföring till tredje land

Sammanfattning

Bolaget har få tredjelandsöverföringar, och har i nuläget identifierat dessa i huvudsak. Överföringar när så skett sker med kända överföringsverktyg. När överföring ska göras till tredjeland och där standardavtalsklausuler ska användas är det viktigt att göra en bedömning om dessa avtal kan bedömas också kunna följas enligt tredjelands lagstiftning. Detta måste göras innan överföring sker. Risk har noterats för att verktyg integrerat i besöksplattformen på hemsidan idag kan innebära viss tredjelandsöverföring av IP-adresser som inte identifierats av bolaget själv.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		Viss risk finns för tredjelandsöverföring i specifikt verktyg. I övrigt har bolaget god kontroll över sina överföringar.
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		Det kan antas att spårningstekniker, eller funktionsscript och cookies innebär överföring till tredjeland, som inte bedömts. Men för de som faktiskt bedömts tillämpas överföringsteknik.
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?		Vissa av personals användaruppgifter i ett mindre system förs över till tredje land. Pågående TIA sker, men systemet är taget i bruk.

Resultatsammanställning från övriga granskningar

Behörighetsstyrning i verksamhetssystem

Under året har en uppföljning av behörighetsstyrning av verksamhetssystem gjorts. Bolaget har en generell rutin för behörighetstilldelning samt avslut av behörigheter i system. Bolaget följer även årligen upp behörigheter i olika system, vissa högrisksystem följs upp med större frekvens. Vid kontroll hade samtliga system en dokumenterad senast uppföljning av behörigheter. Generellt arbetar bolaget mycket väl med behörighetsstyrning. Vissa verksamhetssystem skulle dock behöva definiera hur ofta

Cookies på hemsidan

En särskild granskning av faktisk information och cookie-hantering har gjorts under året. Bolaget har en handlingsplan för brister som visats under pågående granskning. Bolagets information om cookies är korrekt, och bannern har tydliga möjligheter att tacka nej till ej nödvändiga cookies, samt möjlighet att återta samtycket. Kvarstår gör dock vissa brister.

Det är viktigt att ansvariga för hemsida och spårningstekniker har de resurser som krävs för att säkra GDPR-frågor. Viss överföring till annan personuppgiftsansvarig har kunnat ses genom inbäddade funktioner. Främst bör även funktionen för kartvisning och hur relationen till den som skapat kartfunktionaliteten gällande personuppgiftsansvar fastställas. Frågan om den lagstiftning som styr information gällande cookies (Lagen om elektronisk kommunikation) är också bredare än enbart för textfils-cookies, och kan även innefatta information i URL och genom script och pixlar. Det innebär att cookie-information ska ges vid varje överföring, och att frågan om pixlar och URL-taggar är strikt nödvändiga ska övervägas för samtycke enligt LEK. Användande av tredjeparts cookiebanner och uppsättning genom Google Tag manager och sättande av kakor innan samtycke är i tveksamt område där det rekommenderas utredning eller åtgärder.

Gallring i verksamhetssystem

Uppföljning har gjorts av gallring i verksamhetssystem utifrån tidigare årsrapporter som visat på brister. Flera av dessa brister kvarstår än, även om bolaget arbetar med att åtgärda dessa. Bolaget rekommenderas fortsätta med och avsluta det arbetet.

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig rutiner för tilldelning av behörigheter i verksamhetssystem?		Verksamheten har generella rutiner för avslutande av behörigheter samt återkommande uppföljningar av behörigheter till verksamhetssystem Behörighetsnivåer och

		regler för behörighetsnivåer behöver kompletteras för vissa verksamhetssystem
Följer hemsidans information och användning av spårningstekniker		Verksamheten skapar en policy för hemsidehantering för att undvika oplanerade spårningstekniker, samt säkrar att alla former av tekniker som omfattar spårning informeras och samtycks på ett korrekt sätt.
Gallring i verksamhetssystem		Verksamheten har påbörjat möjliggörande gallring i verksamhetssystem. Arbetet behöver fortgå och avslutas för att kunna garantera att informationen för registrerades och verksamheten bara hanteras i system så länge det är nödvändigt för ändamål

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

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

Ja

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

Delvis

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

Ja , men delvis otillfredställande

Dataskyddsombudets jämförelse med föregående års resultat

Personuppgiftsbehandlingarna har uppdaterats under året, och en tydlig rutin har gjorts för uppdatering.
En genomgång av samtliga behandlingar har dock gjorts och arbetet med uppföljning har arbetats om med ny mall för kontroll vilket gör jämförelsen svår gentemot föregående *år.*

Dataskyddsombudets bedömning samt rekommendationer

Registerförteckningen beskriver behandlingarna som bostadsförmedlingen har. Den har i huvudsak besvarat de obligatoriska frågorna, men vissa oklarheter kvarstår efter granskning. Bolagets förvaltning har fått separata rekommendationer om oklarheter att arbete med samt förbättringsförslag. Främst behöver bolaget fokusera på laglig grund när avtal används. Detta då avtal är begränsat till strikt nödvändigt för att administrera ett avtal. Bolaget rekommenderas att även tydligare beskriva sina intresseavvägningar samt uppdatera de icke obligatoriska fälten som visar användning av systemstöd samt personuppgiftsbiträde.

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?

Stickprov har tagits på ett antal verksamhetssystem som främst rör bolagets kärnverksamhet. Klassningar har genomförts, och tillräckligt hög klassning har satts på de flesta hanteringarna. Däremot är bedömningarna inte tydligt dokumenterade. Övriga brister kan omfattas av sekretess och noteras i en separat rapport till verksamheten.

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

Stadens riktlinjer för att informationsklassa och säkerställa informationen är av god kvalité och ger tillräckligt stöd. Uppföljande dokumentation hos bolaget gör det dock svårt att följa upp att handlingsplaner har gjorts. Riskanalyser har gjorts under året men inte i konsekvensbedömning för att säkerställa att inga höga risker kvarstår.

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

Styrande dokument är kända, men inte alltid fullt ut implementerade. Bolaget rekommenderas att aktivt arbeta med dokumentation kring dataskydd för personuppgifter. Bolaget har informerats om noterade brister löpande under året från dataskyddsombud och har påbörjat aktiva åtgärder för att hantera bristerna.

Dataskyddsombudets jämförelse med föregående års resultat

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

Tidigare års rapportering har inte aktivt följt upp säkerheten i systemen, utan noterat att klassningar gjorts och rätt nivå har satts. Det innebär att årets granskning är mer omfattande och därför ger annat resultat. Gällande grundläggande säkerhet för informationen har klassningar genomförts varpå det resultatet i sig inte förändrats utan är fotsatt god. Men vissa brister i implementeringen har noterats.

Dataskyddsombudets bedömning samt rekommendationer

Bolaget har arbetat med att klassa sina verksamhetssystem och därmed den information som ingår där. Bolaget följer även delvis upp klassningar årligen. Rekommendationer har gjorts i en separat rapport till bolaget.
Riskanalyser bör göras för personuppgifter för behandlingar för att notera specifika risker,

vilket för system sker i samband med konsekvensbedömningen (se avsnitt e)

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?

Rutiner har tagits fram för registerhantering. Vid registerhantering i behandlingsregistret ställs frågor om behandlingen har bedömts behöva en konsekvensbedömning. Däremot saknas ännu rutiner för konsekvensbedömningar och ny behandling, som är utöver stadens egna. Stadens mallar och rutiner är tillfredställande. Under 2022-2023 genomförde bolaget en genomlysning av samtliga processer i verksamheten och genomförde därefter konsekvensbedömningar. Arbetet med konsekvensbedömningar är dock ett ständigt återkommande arbete. Behovet av återkommande uppföljningar har påtalats tidigare.

Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?

Vid kontroll av registerförteckning kan dock inte ses att några nya personuppgiftsbehandlingar gjorts vilket krävt förnyade konsekvensbedömningar.

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

Se tidigare svar.

Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?

Bolaget har i sin genomlysning av behov av konsekvensbedömning argumenterat för behovet. Högriskområden som rör sjukskrivningshantering och rehabilitering bör dock åter följas upp.

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

Samtliga behandlingar har gjorts en tröskelanalys.

Dataskyddsombudets jämförelse med föregående års resultat

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

Resultatet motsvarar föregående år, men då konsekvensbedömningar inte har återbesökts av organisationen ökar riskerna för att de inte längre är aktuella.

Dataskyddsombudets bedömning samt rekommendationer

Bolaget har en gång genomfört en tröskelanalys för samtliga behandlingar samt genomfört konsekvensbedömningar. Dataskyddsombudet rekommenderar att personalfrågor som är av känsligare karaktär återbesöks för förnyad tröskelanalys. Konsekvensbedömningarna bör återbesökas med jämna mellanrum. Det rekommenderas att dessa görs snart och att mer andra mallar används.

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 sedan tidigare en rutin för besvarande, rutinen har i dagsläget vissa brister och är under bearbetning för 2025.

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

8 st

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?

Det finns risk att samtliga relevanta system inte söks igenom enligt tidigare rutiner för registerutdrag. Mallen för beskrivningen av utdraget innehåller för lite uppgifter, även om tillgången till de faktiska uppgifterna är kompletta.

Följande uppgifter ska i rätt till tillgång följa med:

- Uppgifter om till vilka som personuppgifter har överförts
- Laglig grund för hantering av uppgifterna
- Vad syftet varit med insamlandet av de specifika uppgifterna
- Hur länge informationen ska bevaras
- Var uppgifterna hämtats.

En hänvisning generellt till personuppgiftspolicyn på hemsidan kan inte anses tillräckligt. Därutöver är logginformation om personer som läst ett ärende, också att räkna som en personuppgift även om exakt person med tillgång (anställdas namn och identifikation) inte behöver följa med. Uppgift om möjlighet att lämna klagomål till IMY har inte heller lämnats.

Dataskyddsombudets jämförelse med föregående års resultat

Ny rutin har tagits fram men saknar mall-del och är ännu inte i bruk. Tidigare brister kvarstår.

Dataskyddsombudets bedömning samt rekommendationer

Nya rutiner och mallar för att tillgodose tillgångens alla delar behöver göras. I övrigt har bolaget visat god förmåga att i huvudsak uppfylla kravet om att ge registrerade tillgång till sina faktiska uppgifter och göra det inom utsatt tid enligt dataskyddsförordningen. En

förenklad möjlighet att ta del av generella uppgifter som bolaget har tillgång till i en automatiserad process till enskild (t.ex. till bankid-inloggad tjänst) skulle kunna

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?

Information har gått ut till alla medarbetare om nödvändigheten att rapportera incidenter och särskilda insatser för att informera har gjorts under året. Hur man rapporterar incidenter skiljer sig åt mot utbildningen i stadens gemensamma utbildningsplattform, och den information som ges på intranätssidan. Ett fullgott systemstöd för hantering av personuppgiftsincidenter används dock inte i nuläget.

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

Nya rutiner har tagits fram för 2025. Rutinerna har följts.

Hur många personuppgiftsincidenter har dokumenterats under året?

7

Hur många personuppgiftsincidenter har anmälts till IMY under året?

0

Dataskyddsombudets jämförelse med föregående års resultat

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

Ny förbättrad rutin för hantering av incidenter har tagits fram. Skillnaden mellan utbildningens information om hur man rapporterar incidenter och faktisk rutin kvarstår.

Dataskyddsombudets bedömning samt rekommendationer

Bolaget har god förmåga att hantera och följa upp incidenter, och har rutiner på plats för hanteringen om dem. Information om vikten av att rapportera personuppgiftsincidenter görs kontinuerligt. Rådet att skaffa bra

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?

Personuppgiftsansvarig har angett tredjelandsöverföringar i registerförteckningen. De har kontrollerats med stickprov av dataskyddsombudet under året genom kontroll av personuppgiftsbiträdesavtal. Noteras viss osäkerhet gällande personuppgifter kopplade till

[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.

tilläggstjänster på hemsidan kopplat till överföring av IP-adresser eller funktionalitet av hemsida.

Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?

I de fall det är aktuella förlitar man sig på adekvansbeslut i huvudsak. Bolaget har få tredjelandsöverföringar, men genom relationen med Hitta.se finns en sådan risk.

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

En TIA görs under året för hantering av viss information, men är ännu inte färdigställd. Adekvansbeslut i sig kräver inte en TIA (aktuellt för användande av spårtekniker på hemsida). Viss osäkerhet finns gällande deltjänster och vilken överföringsteknik

Dataskyddsombudets jämförelse med föregående års resultat

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

Frågan är ny och ingen jämförelse finns med tidigare års resultat. Dock innefattade uppföljningen av personuppgiftsbiträdesavtal även en kontroll av tredjelandsöverföringen det året. Då åtgärdades frågetecken som framkommit.

Dataskyddsombudets bedömning samt rekommendationer

Bolaget har god kontroll över sina överföringar, undantaget relationen till hitta.se (se mer information under den särskilda uppföljningen för cookies) och vissa andra cookies-tjänster.

Bilaga 2 – Andra genomförda granskningar och omvärldsbevakning

Andra granskningar som dataskyddsombudet har genomfört under året

Genomförda granskningar och deras resultat

Granskning av behörighetsstyrning

Under året har en granskning genomförts av behörighetsstyrning. Bakgrunden är tidigare årsrapporters uppmärksamhet av bristande behörighetsstyrning.

Granskningen har delats in genom kontroll av behörighetsrutiner för verksamhetssystem, samt att uppföljningar har gjorts för behörighetskontrollen. I de kontrollerade verksamhetssystemen var uppföljningar gjorda under året för samtliga system för behörigheter. Det fanns även en central rutin för behörighetstilldelningar som använts för samtliga system. Vissa system har bättre utvecklad dokumentation för behörighetstilldelning.

Granskning av spårningstekniker (cookies)

Granskning har gjorts av cookie-hantering på hemsidan. Cookie-hantering görs även med kompletterande direktiv från EU, genom lagen om elektronisk kommunikation (LEK). Granskning har gjorts av faktisk trafik och faktiska cookies på hemsidan, information som ges på hemsidan och överföring av cookies. Bolaget har arbetat aktivt under året för att lösa mindre frågor som behöver korrigeras i informationen.
Bannern för cookies innehåller korrekt information och det är lika lätt för den registrerade att klicka ja som nej. Bland de cookies och de script som kontrollerats noteras att ett tredjeparts-script används genom kartfunktionen till hitta.se. Det innebär att IP-adresser och besökt sida från besökare på bostadsbolaget överförs till hitta.se. Det saknas tydlig relation till hitta.se om det i den funktionen agerar personuppgiftsbiträde eller personuppgiftsansvarig. Även om hitta.se har förflyttats under året till funktionella kakor, sker överföring av information till hitta.se av vilken sida som besöks och kart-val för t.ex. lägenhet som kollas. Den funktionen görs även om inte en text-kaka sätts, och bör ses som användning av information i URL översänds till tredjepart utan klar information och där relationen inte är klarlagd med hitta.se.

Det noteras också att viss trafik görs även innan användaren accepterats, dels sker det genom den tredjepartslösning som en extern cookie-banner innebär och användandet av google tag-manager. Domstol i de-noz i Hannover har nyligen kommit fram till just användandet av google- tag-manager inte bör göras innan samtycke. Samma problem uppstår med vissa sidor på bostad.stockholm.se som använder sig av google-fonts.

Granskning har även gjorts av det nyhetsbrevs utskick som används genom plattformsstöd. Även detta innehåller pixlar och individualiserade utm-koder m.m. som möjliggör spårning av mottagare. Statistiken används inte av Bostadsförmedlingen. Men teknikens användning innebär ändå att informationen trots detta samlas in och spårningstekniker i nyhetsbrev är inte tillåtet utan samtycke. Samtycket ska vara tydligt och informerat, själva acceptansen att man mottar ett nyhetsbrev är inte tillräckligt.

Gallringar i verksamhetssystem

Tidigare dataskyddsombud har påtalat bristen av gallring i verksamhetssystem. Dataskyddsombudet har efterfrågat vilka åtgärder som gjorts för att säkra att uppgifterna bara sparas så länge det behövs, och skiljs från verksamheten om anledning för bevarandet beror på arkivlagen och långsiktigt bevarande. Verksamheten har fortsatt utveckling av systemet för att kunna hantera en gallring som bättre är anpassad efter lagringsminimering. Detta är dock ett pågående projekt som inte avslutats under 2025 varpå risken fortsatt kvarstår.

Dataskyddsombudets rekommendationer baserat på iakttagelserna ovan

Dataskyddsombudets rekommendationer
1. *Bolaget fortsätter enligt nuvarande metoder samt utvecklar rutiner för specifika verksamhetssystem. Det för att säkerställa minsta möjliga behörighet tilldelas användare.* 2. *Det rekommenderas att hemsidan har en policy för att undvika onödiga spårningstekniker eller överföring av information till annan personuppgiftsansvarig. Kontrollera att nödvändigt avtal finns på plats, att val av lagrings och spårningstekniker är strikt nödvändiga endast när det verkligen behövs för en tjänst som besökaren uttryckligen kan antas efterfråga.* 3. *Det rekommenderas att förändringar i verksamhetssystem och lagringsminimering fortsätter och avslutas.*

Omvärldsbevakning

Under året bör det särskilt nämnas att EU-kommissionen lanserat ett förslag för omfattande förändringar i GDPR, det s.k. omnibusdirektivet. Det kan dels påverka hemsida och digitala tjänsten för hur bolaget ska spara och hantera samtycke för spårningstekniker och funktionalitet. Läget i omvärlden bör fortsatt anses osäker, varpå överföringar med adekvansbeslut till t.ex. USA är förenade med risker då den oberoende kommitté tillsatt för att övervaka överföringen av personuppgifter och garantera registrerades rättigheter inte på samma sätt kan hävda samma oberoende. Det är därmed även viktigt att vid tillfällen man baserar överföring till USA också har en exitstrategi om rättsläget förändras, det då detta skett tidigare i samband med de s.k. ”Safe Harbor” och ”Privacy Shield” underkändes.

Ytterligare ny praxis som bör uppmärksammas gäller inhämtning av uppgifter från skatteverket gällande bostadsadresser. Beslut från IMY i ett tillsynsärende, menar på att adresser från skatteverket i deras fall inte kan hämtas in med avtal som laglig grund, och att säkerheten för att dela adress och personnummer kräver högre skydd vid visning (avtal inte kan användas som accept för t.ex. lägre säkerhet.) . Det är oklart om och hur detta påverkar bolaget.

Övrigt att rapportera

Zoom är ett verktyg som används inom bolaget för att hantera möteskommunikation m.m. Verktyget sköts av staden centralt, men uppgifterna i verktyget och hur personuppgifter ska hanteras tillhör fortfarande bolaget. Det noteras att funktioner sätts på och möjliggörs utan vetskap för bolaget. Ett sådant exempel är transkribering samt inspelning, som innebär en stor risk för att bolaget i interna möten och samtal inte uppgifts-minimerar på korrekt sätt. Det saknas även korrekt information till registrerade för detta.