Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Boplats Göteborg AB

2022-12-22

Innehåll

1 Dataskydd i kommunal verksamhet

Att få ta del av och hantera andra människors personliga uppgifter på ett sådant sätt som kommunala förvaltningar och bolag gör innebär att förvalta ett stort förtroende. Dataskyddsförordningen (GDPR) har tillkommit för att särskilt skydda människors rätt till integritet, och för att värna var och ens rätt att få ha kontroll över vad som sker med uppgifter om ens person. Att förvaltningar och bolag hanterar personuppgifter i enlighet med gällande lag bör vara en självklarhet i syfte att visa omsorg om det förtroende som givits den som har att hantera uppgifterna.

Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i GDPR behöver genomsyra arbetet inom de kommunala verksamheterna på alla olika plan. Det gäller allt från rutiner och processer för det dagliga arbetet, till arbetet med innovations- och digitaliseringslösningar för framtidens arbetssätt på förvaltningar och bolag inom Göteborgs Stad. I det framåtsyftande arbetet är GDPR ett viktigt redskap för att kunna säkerställa en digitalisering som håller över tid.

1.1 Göteborgs Stads dataskyddsombud

Dataskyddsenheten på Intraservice är Göteborgs Stads dataskyddsombud. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen i GDPR.[1] Dataskyddsombudets viktigaste uppgift är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Detta sker bland annat genom att samla in information om hur personuppgifter behandlas och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

Dataskyddsombudet har också till uppgift att ge råd och information till förvaltningar och bolag i dataskyddsfrågor. Detta sker genom att dataskyddsombudet är behjälplig när frågor rörande behandlingen av personuppgifter uppkommer hos verksamheterna. Dataskyddsombudet erbjuder också regelbundet utbildningar för stadens medarbetare. Rådgivning ges även till förvaltningar och bolag när dessa genomför konsekvensbedömningar, vilket är en skyldighet som följer av GDPR. Efter att ha identifierat ett särskilt behov av stöd i arbetet med konsekvensbedömningar, har dataskyddsenheten under 2022 tagit fram mallar och mallstöd för det arbetet.

Det är nämnd/styrelse som har det yttersta ansvaret för att verksamheterna följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå.[2] Dataskyddsombudet har inte mandat att fatta beslut åt verksamheterna. Det är i stället genom råd och rekommendationer som

[1] Artikel 39 i GDPR
[2] Artikel 38.3 i GDPR

dataskyddsombudet bistår verksamheterna med underlag för att dessa själva ska kunna fatta väl underbyggda beslut.

2 Granskning av dataskyddsarbetet 2022

2.1 Dataskyddsombudets kontrollfunktion

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 i GDPR. I Göteborgs Stad innebär en del av denna övervakning att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom den personuppgiftsansvariges organisation.

Enligt dataskyddsregelverket ska dataskyddsombudet arbeta utifrån en riskbaserad metod som utgår från risker för de registrerades fri- och rättigheter. Genom att utgå från en sådan metod minskas risken för negativa konsekvenser även för verksamheten själv. Sådana konsekvenser kan omfatta bland annat skadestånd, sanktionsavgifter, försämrat varumärke eller minskad tillit för verksamheten.

För dataskyddsombudet är kontrollarbetet ett sätt att få en bild av vilka risker och/eller brister som eventuellt föreligger inom en verksamhet. Genom kontroller kan dataskyddsombudet kartlägga verksamhetens dataskyddsarbete, och därigenom hjälpa verksamheten att få en nulägesbild av hur de faktiskt ligger till i sitt dataskyddsarbete. Denna kartläggning kan sedan användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Kontrollarbetets syfte är inte främst att peka ut brister utan ska ses som en vägledning för verksamheten och ett verktyg för att identifiera relevanta prioriteringar. Det är sedan upp till varje verksamhet att besluta om hur det interna dataskyddsarbetet ska utformas utifrån verksamhetens förutsättningar för att på bästa sätt kunna hantera identifierade risker. I det arbetet är dataskyddsombudet behjälplig med rådgivning utifrån verksamhetens behov och de risker som identifierats.

2.2 Fördjupad kontroll

2.2.1 Kontroll av behörighetsstyrning 2022

Den fördjupade kontrollen har bestått av kontroll av behörighetsstyrning i Förmedlingssystemet Boplats Office. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen haft vissa anmärkningar och lämnat ett antal rekommendationer till verksamheten / att vidta justeringar. Verksamheten gavs följande rekommendationer:

- Se över behovet av konsekvensbedömning för en eller flera behandlingar i systemet, eftersom det i en sådan kan identifieras risker med för vida behörigheter.
- Se över behovet av loggkontroller i form av stickprov för att kontrollera medarbetarnas behörigheter i systemet.
- Se över behörigheter även vid ändring av anställning.

2.3 Årlig kontroll av dataskyddsarbetet

Verksamhetens interna dataskyddsarbete följs årligen upp genom en enkät. Enkäten består av tolv punkter (”fasta kontrollpunkter”) där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Metoden syftar till att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

2.3.1 Metod och risknivåer

I arbetet används en modell som består av fyra kategorier, vilka representerar fyra olika risknivåer. Verksamheten får utifrån sina svar ett värde som visar vilken risknivå verksamheten befinner sig på inom respektive kontrollpunkt. Genom att arbeta med risknivåer möjliggörs ett riskbaserat arbetssätt för både verksamhet och dataskyddsombud, då resultaten ger en bild av vad verksamheten behöver prioritera i dataskyddsarbetet framåt.[3]

Beskrivning av risknivåer

Risknivåer	Färgkod
Nivå 1. Höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.	
Nivå 2. Risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.	
Nivå 3. Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.	
Nivå 4. Inga direkta risker av betydelse identifierade. Indikerar att verksamheten har ett systematiskt dataskyddsarbete.	

2.4 Boplats dataskyddsarbete 2022

I detta avsnitt anges vilken risknivå verksamheten befinner sig inom för respektive kontrollpunkt, baserat på verksamhetens svar på de fasta kontrollpunkterna. Under varje kontrollpunkt presenteras även dataskyddsombudets bedömning gällande

[3] I arbetet med enkäten har dataskyddsenheten utgått från Myndigheten för samhällsskydd och beredskaps (MSB) uppföljningsstruktur för den offentliga förvaltningens systematiska informationssäkerhetsarbete.

verksamhetens risker utifrån de iakttagelser som dataskyddsombudet gjort under året.

2.4.1 Kontrollpunkt 1: Dataskyddsorganisation

Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete, och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

Dataskyddsombudets kommentarer:

Dataskyddsombudet har inget att invända mot bolagets skattning gällande den interna dataskyddsorganisationen då den hållit sig intakt och inte ändrat personer under de senaste åren, vilket gjort att rutiner och hanteringssätt kunnat löpa på. Dataskyddsombudet anser att det är bra att det finns utpekade roller och ansvar för de fall då dataskyddsfrågorna blir aktuella inom bolaget, så att frågorna kan lyftas till rätt ansvarsområde.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att identifiera och hantera personuppgiftincidenter.

Dataskyddsombudets kommentarer:

Bolaget har angett högsta värdet på alla punkter inom kontrollpunkten vilket indikerar att inga risker föreligger. Dataskyddsombudet har tidigare granskat bolagets hantering av incidenter och verksamheten har därefter vidtagit åtgärder utifrån rekommendationerna. Bolaget rekommenderas att ändå regelbundet se över rutinerna för att säkerställa så att de är effektiva och ändamålsenliga.

2.4.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd, och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer i förvaltningens bedömning och anser att det finns kvarstående åtgärder att vidta när det kommer till hanteringen av biträden och biträdesavtal. Dataskyddsombudet ser framför allt en stor risk när det kommer till bolagets kompetens att bedöma hela kedjan av underbiträden vid anlitande av personuppgiftsbiträden, eftersom det ofta förekommer tredjelandsöverföringar som är av högsta vikt att man har koll på. Bolaget uppger också att det saknas rutiner för efterlevnadskontroller av anlitade biträden. Det är särskilt viktigt eftersom bolaget har ett antal biträden där avtal ingicks när dataskyddsförordningen trädde i kraft och att det därefter inte skett någon uppföljning av avtalen. Ett sätt att göra detta är att utgå ifrån de instruktioner som lämnats till biträdet och följa upp om dessa följs. Om det saknas instruktioner till några biträden bör det åtgärdas snarast.

2.4.4 Kontrollpunkt 4: Personuppgiftsregister

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande personuppgiftsregister innefattas.

Dataskyddsombudets kommentarer:

Bolagets resultat på kontrollpunkten kopplat till personuppgiftsregistret är något lägre än förra året och indikerar att vissa förbättringspunkter finns. Det är framför allt viktigt att bolaget dokumenterar alla sina behandlingar i registret och att samtliga innehåller all information som krävs. Dataskyddsombudet kontrollerade bolagets användning av registret i förra årets fördjupade kontroll och verksamheten har uppgett att de åtgärder som rekommenderades har vidtagits. Dock uppger bolaget i skattningen att det inte finns en ansvarsfördelning för registret eller fungerande rutin för att uppdatera registret, vilket var två saker bolaget förra året uppgav som vidtagna åtgärder. Bolaget uppger i dialog att ett arbete har påbörjats och rutin finns framtagen, men den behöver implementeras och följas i verksamheten. Dataskyddsombudets uppfattning är därmed att det delvis kvarstår rekommendationer från förra årets fördjupade kontroll som behöver följas upp kommande år.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Bolagets skattning på kontrollpunkten ger ett relativt högt resultat vilket tyder på att inga större risker föreligger. Bolaget uppger att det finns en övergripande strategi för arbetet med dataskydd och bolaget arbetar systematiskt, har en övergripande informationssäkerhetspolicy samt antagit ett riskbaserat arbetssätt i dataskyddsfrågor. Däremot saknas det delvis dokumenterade rutiner för att säkerställa att styrande dokument kopplat till personuppgifter hålls uppdaterade, vilket bolaget bör se över. Det är också viktigt att bolaget genomför egna interna kontroller för att säkerställa följsamhet mot GDPR.

Slutligen vill dataskyddsombudet rekommendera bolaget att ta fram rutiner för hantering av personuppgifter vid anordnande av fysiska och digitala sammankomster, för att säkerställa att kraven i GDPR följs.

2.4.6 Kontrollpunkt 6: Utbildning

Kontrollpunkten avser verksamhetens arbete med att utbilda och upprätthålla kunskapsnivån i dataskyddsfrågor hos anställda.

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer i bolagets bedömning kopplat till utbildning. Den generella kunskapen om dataskydd hos bolagets medarbetare kan förbättras och utbildningsinsatser krävs för att säkerställa att behandling av personuppgifter sker på ett korrekt sätt. Bolaget har själva också identifierat detta och efterfrågat ytterligare utbildning ifrån dataskyddsenheten. Det är viktigt att bolaget fortsätter att utvärdera nivån och behoven som finns inom verksamheten. Dataskyddsombudet rekommenderar att bolaget som miniminivå erbjuder de anställda de digitala och/eller lärarledda grundutbildningarna som dataskyddsenheten erbjuder.

2.4.7 Kontrollpunkt 7: Integritetspolicy

Kontrollpunkten avser verksamhetens utformning samt tillhandahållande av dess integritetspolicy till registrerade (både internt och externt). Även verksamhetens rutin för att upprätthålla en aktuell integritetspolicy omfattas.

Dataskyddsombudets kommentarer:

Dataskyddsombudet har inte under det senaste året granskat bolagets integritetspolicy men har tidigare varit involverad, och kan inte se några direkta risker kopplat till hanteringen. Det är viktigt att bolaget ser över policyn i den mån det utförs nya eller förändrade behandlingar.

Dataskyddsombudet rekommenderar att bolaget tar fram fungerande rutiner för att informera medarbetarna om hur deras personuppgifter behandlas.

2.4.8 Kontrollpunkt 8: E-post och dokumenthantering

Kontrollpunkten avser verksamhetens rutiner för e-post och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddsförordningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Dataskyddsombudets kommentarer:

Bolaget svar på kontrollpunkten kopplat till mejl och dokumenthantering är samma som förra året och visar på att arbetet fungerar bra. En uppdaterad dokumenthanteringsplan med gallringsrutiner är en förutsättning för att bolaget ska kunna säkerställa principen om lagringsminimering enligt GPDR. Bolaget rekommenderas också se över hur medarbetarna får information om dokumenthantering och gallring, då det också säkerställer medarbetarnas möjlighet att själva följa GDPR.

Det är också en risk att bolaget inte har någon bra uppfattning om hur aktuell informationen är för de behandlingar som har informationsklassificerats. Detta bör således ses över.

2.4.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras, samt rutiner kopplat till detta.

Dataskyddsombudets kommentarer:

Bolaget skattning på kontrollpunkten visar att det fortfarande föreligger höga risker kopplat till konsekvensbedömning/samråd. Dataskyddsombudets uppfattning är att det idag inte jobbas aktivt med konsekvensbedömningar alls, eftersom det varken finns några framtagna eller planerade konsekvensbedömningar.
Dataskyddsombudet har inte sett att bolaget har rutin för att bedöma risker, acceptera risker, besluta, följa upp åtgärder eller inhämta dataskyddsombudet synpunkter.

Dataskyddsombudet rekommenderar att bolaget ser över hur arbetet kopplat till att bedöma risker för behandlingar ser ut och tar fram ett arbetssätt där konsekvensbedömningar är en del av den övergripande strategin för dataskydd. Eftersom det är ett krav enligt GDPR i vissa fall är det ytterst viktigt att bolaget har

kunskap om hur en konsekvensbedömning ska genomföras och framför allt *när* en sådan ska göras. Bolaget rekommenderas att utreda vilka resurser som kan behövas för att genomföra konsekvensbedömningar och säkerställa att dessa involveras vid behov. De mallar och mallstöd som dataskyddsenheten tagit fram kan vara ett bra stöd vid uppstart av det interna arbetet med konsekvensbedömningar.

2.4.10 Kontrollpunkt 10: IT-projekt och upphandling

Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.

Dataskyddsombudets kommentarer:

Bolagets skattning på kontrollfrågan visar att inga större risker föreligger. Eftersom dataskyddsombudet inte blivit involverad i några IT-projekt eller upphandlingar under året saknas insyn i hur verksamheten arbetar i dessa frågor. Dataskyddsombudet vill dock lyfta, i och med att kunskapen om dataskydd generellt kan behöva höjas inom verksamheten, att det finns risker att dataskyddsperspektivet missas vid uppstart av IT-projekt eller vid upphandlingar.

2.4.11 Kontrollpunkt 11: IT-system och digitala verktyg

Kontrollpunkten avser verksamhetens rutiner för att säkerställa att verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg är förenlig med dataskyddsförordningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Dataskyddsombudets kommentarer:

Bolagets skattning kopplat till behörigheter kommer att bemötas i den fördjupade kontrollen och berörs ej ytterligare här.

Bolaget uppger att det saknas fullständiga rutiner för att systematiskt kunna följa upp och kontrollera att användning av system/digitala verktyg följer antagna rutiner/riktlinjer/policys. För det fall som verksamheten har eller kommer att införa appar och/eller sociala medier, behöver bolaget också säkerställa att dataskyddsperspektivet omhändertas.

Bolaget uppger att det finns en rutin för att införa nya tjänster där GDPR är med som punkt, vilket dataskyddsombudet ser som positivt.

2.4.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering.

Dataskyddsombudets kommentarer:

Dataskyddsombudet ser ingen anledning att ifrågasätta bolagets bedömning av kontrollpunkten. Dataskyddsombudet har inte blivit involverad i några frågor gällande registrerades rättigheter under året och saknar därför inblick i hur arbetet med att säkerställa dessa fungerar på bolaget. Medvetenheten gällande registrerades rättigheter är kopplat till den generella kunskapen om dataskydd och kan alltid höjas.

2.5 Sammanfattande rekommendationer

För att på ett praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en noggrann genomgång av enkätresultaten. I detta rekommenderas verksamheten att samråda med dataskyddsombudet för att se hur arbetet framåt bör utformas och vilka delar som bör prioriteras utifrån verksamhetens risker. Även för verksamheter med låga risker krävs kontinuerliga insatser för att denna risknivå ska bibehållas.

Utifrån identifierade risker rekommenderar dataskyddsombudet att förvaltningen/bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

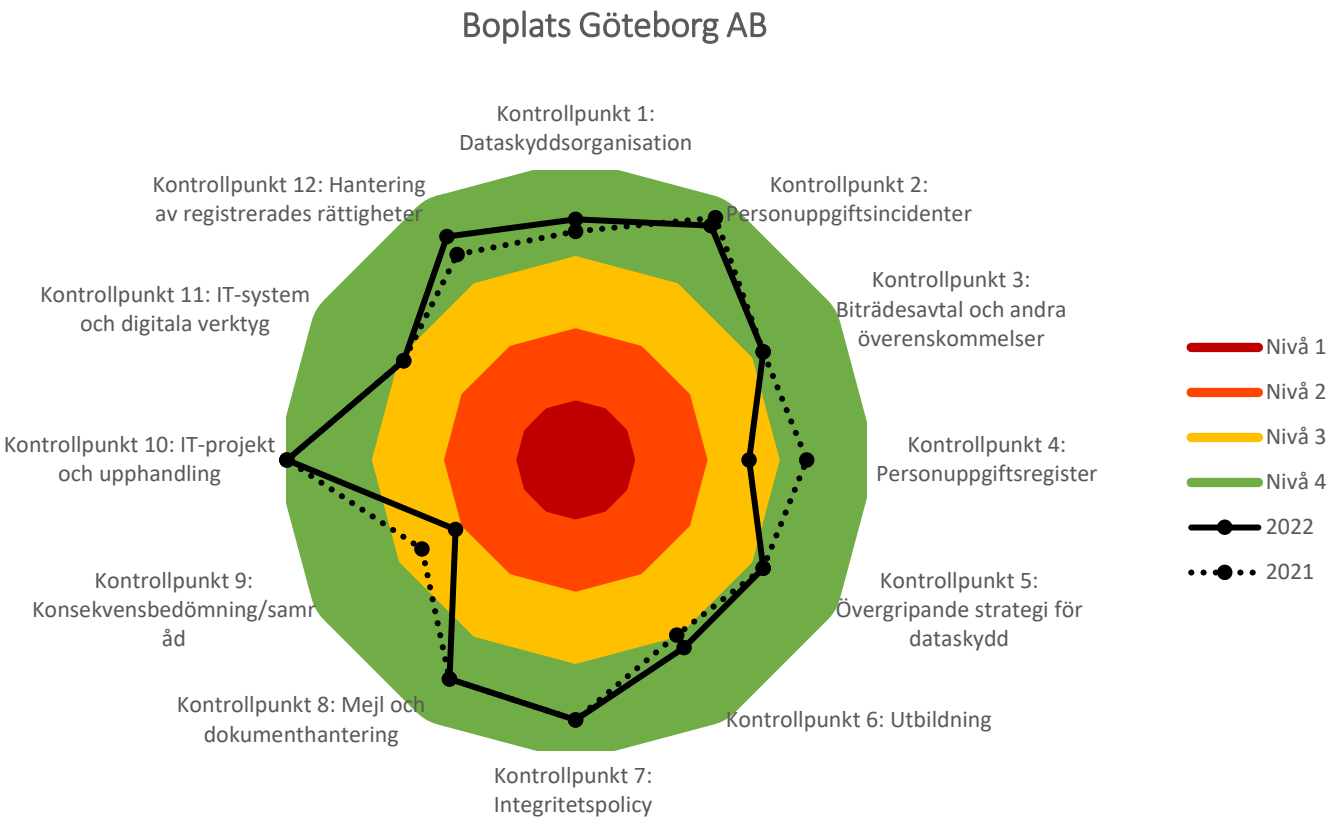
- Kontrollpunkt 4: Personuppgiftsregister
    - Utifrån att vissa rekommendationer delvis kvarstår ifrån förra årets granskning rekommenderas bolaget att säkerställa att den nya rutinen och arbetssättet implementeras i verksamheten.
- Kontrollpunkt 6: Utbildning
    - Utifrån att bolaget själva har identifierat ett utbildningsbehov rekommenderar dataskyddsombudet att bolaget prioriterar denna fråga under kommande år.
- Kontrollpunkt 8: Konsekvensbedömning och samråd
    - Bolaget rekommenderas:
        - Lyfta in arbetet med tröskelanalyser/konsekvensbedömningar i den riskbaserade strategin för dataskydd.

3 Bilagor

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.

Bilaga 2: Fördjupad kontroll 2022 – behörighetsstyrning

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.



Fördjupad kontroll

Kontrollpunkt 11: Behörighetsstyrning - Boplats Office

Bakgrund

Den fördjupade kontrollen av behörighetsstyrning syftar till att se om verksamhetens hantering av personuppgifter är säker och korrekt utifrån både tekniska och organisatoriska åtgärder. Med utgångspunkt i artikel 32.2 har kontrollen granskat verksamhetens bedömning av lämplig säkerhetsnivå med hänsyn till risker i synnerhet från bland annat obehörig åtkomst till personuppgifter. Därför har fokus legat på behörighetsstyrning och hur det används för att begränsa vilka personuppgifter som medarbetarna får ta del av.

Kontrollen har genomförts i två delar, den första som ett generellt frågeutskick och den andra som ett kompletterande frågeutskick. I kontrollen ingick verksamhetens rutiner för tilldelning av behörigheter och åtkomster i ett särskilt utvalt IT-system, uppföljning av behörigheter samt användning av logg-/åtkomstkontroller.

Iakttagelser från kontrollen

En medarbetare i en verksamhet ska enbart ha tillgång till personuppgifter som är anpassade och begränsade till det som är nödvändigt för att medarbetaren ska kunna utföra sina arbetsuppgifter. För att säkerställa detta bör verksamheten ha rutiner för tilldelning av behörighet, uppföljning av behörigheter samt hur användningen av logg-/åtkomstkontroller sker.

Kontrollen har genomförts på Boplats Förmedlingssystem Boplats Office om används av både Boplats egen personal och bostadsbolagens uthyrare. I systemet finns personuppgifter tillhörande bostadssökande, anställda på Boplats, uthyrare hos bostadsbolagen samt personer som ska visa lägenheter (nuvarande hyresgäst eller hyresvärdens kvartersvärd). Totalt finns 356 216 inloggningsbara konton hos Boplats. Personuppgifter som behandlas i systemet är namn, personnummer, kontaktinformation, folkbokföring, sysselsättning, inkomst, medsökande och hushållsuppgifter. Vid behov tas även dokument in som styrker inkomst, sysselsättning, fastighetsinnehav samt vid behov kreditupplysning. För de anställda (47 hos Boplats och stadens Kontaktcenter) behandlas personuppgifter om namn, arbetsgivare, telefonnummer och epost. Motsvarande behandlas också för de 142 externa uthyrarna. Totalt har 189 personer behörighet till systemet.

Behörighetsstruktur och roller i system

Boplats hantering av behörigheter är dokumenterade i rutinen “behörighetstilldelning Boplats personal Boplats Office”. I dokumentet finns det beskrivet hur behörigheter tilldelas, vem som ansvarar för radering och tilldelning av behörigheter, periodisk genomgång av behörigheter samt användarens, avdelningschef och IT-supports ansvar. Det finns också anvisningar för själva systemet. Behörighet beställs via blankett hos IT-supporten. Motsvarande rutin finns även för uthyrare (bostadsbolagen) för att säkerställa korrekt hantering av behörigheter. Ansvaret ligger dock hos uthyraren.

I systemet tilldelas behörigheter till medarbetare genom fördefinierade roller i systemet. Varje roll har behörighet till en begränsad del av funktionerna i systemet som motsvarar det arbete som respektive roll ska utföra i processen för förmedling av lägenheter.

För Boplats egen personal finns 10 olika roller (behörighetstyper). Exempelvis har rollen uthyrar-admin tillgång till organisation och användare. För personal inom systemdrift och systemutveckling krävs förutom kraftfulla roller i systemet också behörighet till servrar och källkod. Fem olika behörighetstyper finns.

För bostadsbolagens personal finns fyra organisationsbegränsade roller definierade i systemet. Exempelvis har *säljare köp nytt* full tillgång till *köp nytt* processen för egen organisation.

Specifika funktioner är byggda som begränsar behörighet till användarens egen organisations uppgifter. I behörighetssystemet har samtliga externa roller endast tilldelats funktioner med organisationsbehörighet. Boplats personal har tilldelats roller som har behörighet till funktioner som inte är begränsade till data för den egna organisationen och kan därför se data från alla organisationer.

Tilldelning av behörighet utifrån bedömning

Bedömningen om vem som får vilken behörighet görs av avdelningschefen och baseras på det arbete som varje anställd ska utföra. Exempelvis är det endast personal inom systemdrift och systemutveckling som kan få roller som innebär att dessa kan tilldela behörigheter i förmedlingssystemet till andra. Utgångspunkten för behörighetstilldelning är att användare ska ha behörighet till det som är nödvändigt för att ge en god service till de sökande. Dataskyddsombudetanser att detta överensstämmer med principen om uppgiftsminimering och uppgiftsminimering - att anställda enbart ska ha tillgång till och får behandla de personuppgifter som krävs för specifika ändamål.

Beslut om behörighet

Boplats IT-support administrerar tilldelningen av behörigheter efter beslut ifrån avdelningschef.

Uppföljning av behörighet

Behov ska styra behörighet, vilket bland annat innebär att om någon byter roll eller arbetsuppgifter, begär tjänstledigt eller är föräldraledig ska behovet av behörighet ses över och justeras. Om någon avslutar sin anställning är det särskilt viktigt att omedelbart inaktivera behörighet och stoppa tillgång till system och information. Därför behövs rutiner både för ändrat behov under anställning och vid anställnings slut.

Borttag av behörighet görs av ansvarig chef, för att säkerställa att behörighet till Boplats Office avaktiveras vid avslut av anställning eller då medarbetaren byter arbetsuppgifter.

Boplats uppger att avdelningschef även en gång per år ska initiera en genomgång av avdelningens alla användare i Boplats Office och av aktuella behörighetsnivåer. Detta för att säkerställa att behörigheterna är korrekta. Eventuella ändringar görs via avsedd blankett och avdelningschefen ska dokumentera den periodiska genomgången för möjlig uppföljning. Dataskyddsombudet anser att det är positivt att borttag av behörigheter görs

vid avslut, ändring av tjänst samt periodiskt en gång per år. Detta minskar risken för att felaktiga behörigheter finns i systemet.

Motsvarande rutin finns för bostadsföretagen och ansvariga chefer hos uthyraren. Förutom det görs enligt Boplats en kontroll var fjärde vecka då Boplats skickar ett utskick till alla aktiva uthyrare i systemet. Om meddelandet inte går fram till en uthyrare kontaktar Boplats det aktuella bolagets uthyrningsansvarige för att stämma av anledningen och korrigerar vid behov behörigheter. Kontinuerlig dialog förs med externa uthyrningsansvariga där de stämmer av vilka som arbetar i systemen.

Åtkomstkontroll/kontroll av loggar

Boplats uppger att systemet loggar en del händelser som bolaget själva har definierat som säkerhetsrelevanta.

Beställning till systemtekniker för kontroll av loggar görs enbart vid behov i dagsläget. Beställning görs ofta av kundtjänst eller vid behov av systemägaren. Boplats uppger att ett exempel på behov är när de genom att granska systemloggen kan se mönster som visar på ett onormalt användande av systemet vilket gör att de kan upptäcka försök till intrång.

Dataskyddsombudet tolkar bolagets svar som att kontrollerna som genomförs i dagsläget är mer inriktade på intrångsförsök ifrån utomstående. Dataskyddsombudet vill lyfta att det även är viktigt att ha kontroller internt, eftersom logg och åtkomstkontroller är viktiga redskap för att upptäcka och förebygga obehörig åtkomst till personuppgifter. Kontrollerna behöver dock såklart utföras på ett så icke-integritetskränkande sätt som möjligt. Dataskyddsombudet anser att det bör finnas rutiner för regelbundna kontroller som inte enbart riktar in sig på en enskild medarbetare (även om kontroll vid misstanke om brott såklart också ska utredas), förslagsvis stickprovskontroller. Dessa ska dock vara utformade utan att kränka den enskildes integritet.

Bolaget uppger att det finns förslag på rutin för logghantering inför kommande år, med en rapportfunktion där man identifierat säkerhetsrelevanta händelser.

Annan lagstiftning/bestämmelser som påverkar behörighetstilldelningen

Boplats uppger att man i sin informationsklassning identifierat lagar och bestämmelser som hela verksamheten måste följa vid hantering av information och man har vid designen av systemet tagit hänsyn till dessa. Vilka lagrum som identifierats framgår ej av bolagets svar varpå dataskyddsombudet inte kan bedöma dessa.

Andra risker och åtgärder

Boplats har inte identifierat några inbyggda svårigheter i systemet för att begränsa behörigheterna, eftersom systemets behörigheter är byggt genom att roller tilldelas funktioner.

Boplats har inte gjort någon konsekvensbedömning för behandlingarna i systemet. Bolaget uppger att de för aktuella personuppgifter analyserat behovet för verksamheten, gjort en informationsklassning samt fastställt laglig grund och därmed ansett att en konsekvensbedömning inte är nödvändig.

Dataskyddsombudet vill uppmärksamma bolaget på att en konsekvensbedömning kan behöva göras trots ovan nämnda åtgärder. En behandling kan innebära höga risker för den

registrerade även om bolaget "får" behandla personuppgifterna för det angivna ändamålet. Det kan också vara så att behandlingen uppfyller ett eller flera krav på IMY:s lista över när en konsekvensbedömning bör göras. Dataskyddsombudet rekommenderar bolaget att se över behovet av en konsekvensbedömning. Det är troligtvis så att det förekommer flera behandlingar i samma system och en viss behandling av till exempel känsliga personuppgifter kan innebära högre risker än en annan behandling i samma system.

För Förmedlingssystemet finns två personuppgiftsbiträden, ett för vidareutveckling/förvaltning/teknisk support av systemet med tillgång till produktionsmiljö och behörighet i systemet, samt ett för driften av servrarna med teknisk tillgång till systemet. Det finns personuppgiftsbiträdesavtal för båda leverantörerna.

Dock har bolaget själva identifierat risker som har med behörighet att göra.

1. Vid skapande/förändring av rollerna ges behörighet till fel funktion vilket leder till tillgång till obehörig information
2. Vid behörighetstilldelning ges fel roll till en användare vilket leder till tillgång till obehörig information

Som åtgärder anger Boplats att endast ett fåtal anställda får utbildning och behörighet att hantera behörigheter i förmedlingssystemet, vilket minskar risken att misstag enligt punkterna 1 och 2 sker. Dataskyddsombudet instämmer i bolagets bedömning om åtgärder och uppmuntrar bolaget att vidta åtgärder för att minska riskerna.

Sammanfattade rekommendationer

- Se över behovet av konsekvensbedömning för en eller flera behandlingar i systemet, eftersom det i en sådan kan identifieras risker med för vida behörigheter.
- Se över behovet av loggkontroller i form av stickprov för att kontrollera medarbetarnas behörigheter i systemet.

Bilagor

1. Informationsutskick fördjupad kontroll behörighetsstyrning
2. Frågeutskick del 1
3. Frågeutskick del 2

Information om fördjupad kontroll 2022

Kontrollpunkt 11: Behörighetsstyrning

För att säkerställa säkerheten och en korrekt personuppgiftshantering inom en verksamhet behöver både tekniska och organisatoriska åtgärder vidtas. Exempel på tekniska säkerhetsåtgärder är att system utformas så att endast behöriga personer kan göra sökningar och att det finns behörighetskontrollsystem. En viktig och effektiv organisatorisk åtgärd i en verksamhet är behörighetsstyrning.

I artikel 32.2 i dataskyddsförordningen ställs krav på att den personuppgiftsansvarige i samband med bedömning av lämplig säkerhetsnivå ska ta särskild hänsyn till risker i synnerhet från bland annat obehörig åtkomst till personuppgifter. Obehörig är den som inte har legitim anledning att ta del av en handling eller uppgift i sin tjänsteutövning. Bestämmelser om sekretess utgör ofta men inte alltid en utgångspunkt för vilka uppgifter som någon får ta del av. Genom en ändamålsenlig behörighetsstyrning kan det säkerställas att ingen obehörig åtkomst sker inom verksamheten. Behörighetsstyrning sker genom att bland annat bedriva ett arbete med att avgöra hur stor tillgång till uppgifter i ett verksamhetssystem som en medarbetare med en viss funktion eller roll ska ha. Det är viktigt att behörigheterna är anpassade och begränsade till det som är nödvändigt och i enlighet med gällande rättslig reglering. Dessutom behöver behörigheterna löpande kontrolleras och följas upp samt att åtkomstkontroller genomförs. En felaktig eller bristfällig behörighetsstyrning kan leda till exempelvis inskränkningar av den enskildes integritet eller personuppgiftsincidenter.

Den fördjupade kontrollen avser undersöka hur behörighetsstyrning används för att begränsa vilka uppgifter som medarbetarna får ta del av. Verksamhetens rutiner för tilldelning av behörigheter och åtkomster i IT-system kommer att granskas. Kontrollen kommer även omfatta verksamhetens uppföljning av medarbetares behörigheter och åtkomst till personuppgifter i IT-system samt om logg-/åtkomstkontroller används för att upptäcka och motverka obehörig åtkomst.

Syftet med den fördjupade kontrollen är att undersöka om medarbetares tillgång till personuppgifter är anpassade och begränsade till det som är nödvändigt för att medarbetaren ska kunna utföra sina arbetsuppgifter, att åtkomstkontroller genomförs och att därmed risken för obehörig åtkomst inom verksamheten minimeras.

Tillvägagångssätt

Den fördjupade kontrollen kommer att genomföras i två delar. I del ett ombeds ni att besvara ett antal frågor samt att skicka in dokumenterade rutiner, styrande dokument eller liknande underlag avseende tilldelning av behörigheter och åtkomst till IT-systemet Förmedlingssystemet. I del två kommer uppföljande frågor att ställas.

Dataskyddsombudet kommer sedan att sammanställa underlaget i en delårsrapport som lämnas till er i maj/juni.

Obs! Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar inom förvaltningen/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet.

Fördjupad kontroll 2022

Kontrollpunkt 11: Behörighetsstyrning (del 1)

Del 1: Ni ombeds besvara frågorna nedan samt skicka in dokumenterade rutiner, styrande dokument eller liknande underlag avseende tilldelning av behörigheter och åtkomst till IT-systemet Förmedlingssystemet.

- Beskriv systemets behörighetsstruktur och olika roller i systemet.
- Vilka roller får vilka behörigheter och vad baseras den bedömningen på?
- Vem beslutar om vilka som ska ha vilken behörighet?
- Hur ofta följs behörigheterna upp för att kontrollera att dessa är korrekta och anpassade efter medarbetarens arbetsuppgifter? Vem/vilka ansvarar för det?
- Beskriv hur åtkomstkontroller/kontroll av loggar kan genomföras i systemet.
- När och hur ofta genomförs åtkomstkontroller/kontroll av loggar?
- Vem/vilka ansvarar för åtkomstkontrollerna/kontroll av loggar?
- Finns det annan lagstiftning eller andra bestämmelser, utöver dataskyddsförordningen, som er verksamhet behöver beakta i arbetet med behörighetstilldelning? I så fall, vilken/vilka?
- Vilka andra åtgärder vidtas för att förhindra obehörig åtkomst till personuppgifter i systemet?
- Har verksamheten identifierat några personuppgiftsincidenter kopplat till felaktiga behörigheter?

Obs! Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar inom förvaltningen/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet.

Underlaget ska ha inkommit till dataskyddsombudet **senast den 10 mars 2022.**

Har du frågor, kontakta ditt huvudansvarige dataskyddsombud.

Fördjupad kontroll 2022

Kontrollpunkt 11: Behörighetsstyrning (del 2)

Del 2: Utifrån vad som framkommit i del 1 av den fördjupade kontrollen ombeds ni besvara frågorna nedan.

- Vad är det för personuppgifter som behandlas i systemet?
- Hur många registrerades personuppgifter hanteras i systemet?
- Hur många personer har behörigheter (både inom Boplats och hos bostadsbolagen)
- Hur kontrollerar Boplats att bostadsbolagen kontrollerar behörigheterna enligt rutinen (en gång per år)?
- Föreligger det inbyggda svårigheter i aktuellt systemstöd att begränsa behörigheterna på så vis att personer enbart kan se sådana uppgifter som härrör till den egna förvaltningen? Varför/varför inte?
- Har ni något personuppgiftsbiträde för personuppgifterna i systemet?
    - Hur kontrolleras personuppgiftsbiträdets behörigheter i systemet?
    - Finns det instruktioner till personuppgiftsbiträdet? Om ja, översänd dessa. Om nej, varför inte?
- Har ni konsekvensbedömt behandlingarna i systemet? Varför/varför inte?
- Har ni identifierat specifika risker kopplat till nuvarande hantering av behörigheter? Varför/varför inte? Beakta såväl risker inifrån organisation som utanför (ex, intrång) för de registrerades rättigheter.
- Kan ni ge ett exempel på vad som utgör ett ”behov” att kontrollera loggar?

Obs! Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar inom förvaltningen/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet.

Underlaget ska ha inkommit till dataskyddsombudet **senast den 8 juni 2022.** Dataskyddsombudet kan komma att ställa kompletterande frågor i samband med sammanställande av rapporten och/eller begära visning av systemet. Frågor kan komma att ställas såväl muntligen som skriftligen.

Har du frågor, kontakta ditt huvudansvarige dataskyddsombud.