Göteborgs Stad

Årsrapport för dataskyddsarbetet 2024

Renova AB

2024-12-20

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 värna om den enskildes rätt till integritet och kontroll över vad som sker med ens personuppgifter. Rätten till en fredad privat sfär och personlig integritet är grundläggande i ett demokratiskt samhälle och är ett av fundamenten på vilket många andra av våra demokratiska rättigheter vilar. Lagstiftningen finns till för att skydda individen från skada och sätter ramarna för hur personuppgifter får behandlas i en alltmer digital värld.

Att förvaltningar och bolag hanterar personuppgifter i enlighet med gällande lag bör vara en självklarhet i syfte att visa omsorg om det förtroende som getts den som har att hantera personuppgifter. För att säkerställa följsamhet gentemot GDPR behöver dataskyddsperspektivet 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.

2 Göteborgs Stads dataskyddsombud

Det är varje nämnd och bolag som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. För att stödja stadens nämnder och bolag i arbetet med dataskydd har ett dataskyddsombud utsetts. I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud åt stadens bolag och nämnder. 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.

Enligt lag ska dataskyddsombudet även rapportera om arbetet till högsta förvaltningsnivå[2], och utifrån detta lämnar dataskyddsombudet årligen en rapport om den egna verksamhetens dataskyddsarbete till nämnder och bolag i Göteborgs Stad. I rapporten redogör dataskyddsombudet för de iakttagelser som gjorts under året, både stadenövergripande och, i vissa fall, verksamhetsspecifika. Rapporten innehåller även information om årets fördjupade kontroll samt resultatet från den uppföljning som genomförts avseende hur verksamheten hanterat och arbetat med de rekommendationer som lämnades i årsrapporten 2023.

Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Det är upp till varje verksamhet att besluta om hur det interna dataskyddsarbetet ska utformas utifrån verksamhetens förutsättningar för att på bästa sätt hantera identifierade risker.

2.1 Stadenövergripande iakttagelser 2024

2.1.1 Ny central funktion för styrning och samordning i dataskyddsfrågor möjliggör ett stärkt dataskydd

Hur långt förvaltningar och bolag kommit i dess dataskyddsarbete skiljer sig stort åt inom Staden. Skillnaderna bedöms till stor del bero på bristande styrning och samordning i dataskyddsfrågor från centralt håll, något som lyfts av dataskydds-ombudet under flera år. Resultatet av detta är bland annat att skyddet för de registrerades personuppgifter varierar mellan verksamheterna, en ineffektiv

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

personuppgiftsincidenthantering och att hanteringen av rättigheter hanteras olika beroende på vilken verksamhet man vänder sig till.

Dataskyddsombudets förhoppning är att den nya dataskyddsfunktionen som införts på stadsledningskontoret ska bidra till att utveckla och stärka de grundläggande delarna av dataskyddsarbetet och därigenom generera ett mer enhetligt dataskydd inom Staden. Att stadsledningskontoret nu tar ansvar för att samordna dataskyddsarbetet bedöms ligga i linje med kommunstyrelsens uppdrag.

I sammanhanget vill dataskyddsombudet samtidigt poängtera att varje nämnd och bolag fortfarande är ytterst ansvariga för sina respektive personuppgifts-behandlingar. Det är därför även fortsatt upp till varje nämnd och bolag att säkerställa efterlevnad gentemot lagstiftningen. Att varje verksamhet tar det ansvaret är avgörande för att det arbete som görs inom dataskyddsfunktionen ska få genomslag och ha en positiv påverkan på dataskyddet som helhet i Staden.

2.1.2 Verksamhetens ledning avgörande för att GDPR inte ska fortsättas upplevas som ett hinder

I årsrapporten 2023 lyfte dataskyddsombudet att det inom Staden generellt bedömdes finnas en uppfattning om att det är omöjligt att följa GDPR och samtidigt driva den digitala utvecklingen framåt. Dataskyddsombudets upplevelse, utifrån de dialoger som varit under 2024, är att denna uppfattning fortfarande kvarstår och är något som i hög grad påverkar dataskyddsarbetet negativt. Dataskyddsombudet har i möten med funktioner från olika verksamheter inom Staden kontinuerligt fått höra att GDPR är något som är jobbigt och krångligt, och som blir ett hinder som försvårar deras arbete med att ta i bruk nya digitala lösningar. Som regel uttrycks detta efter eller precis inför att verksamheten ska teckna avtal, eller precis står inför att börja använda en ny digital lösning eftersom det ofta är först då som dataskyddsperspektivet beaktas. Dataskyddsombudet förstår att medarbetare i den situationen upplever GDPR som ett hinder, men ser samtidigt att GDPR inte kan klandras för de uppenbara brister i den interna styrningen som medfört att verksamheten inte arbetat med dataskyddsfrågorna i tid.

För att känslan av GDPR som något jobbigt och ett hinder inte ska fortsätta ha en negativ påverkan på dataskyddsarbetet behöver Staden som helhet arbeta för att öka medvetenheten om syftet med lagstiftningen. En del kan göras genom utbildningar, men centralt är också att det från ledningshåll inom stadens verksamheter börjar signaleras att dataskydd är något som ska beaktas och arbetas med. I den offentliga debatten hör man ofta representanter från näringslivet tala om att det offentliga måste vara modiga och testa nya saker. Dataskyddsombudets uppfattning att det modiga i dessa fall ofta handlar om att utmana den lagstiftning som styr offentlig sektor, till exempel då lagstiftningen begränsar möjligheterna att dela och/eller använda data. Lagstiftningen, inkluderat GDPR, utmålas då som ett administrativt hinder som hämmar utvecklingen. Denna bild av GDPR som ett hinder delas inte av dataskyddsombudet eftersom det inte finns någon motsättning mellan att följa lagkraven och samtidigt driva digitaliseringen framåt. Utifrån den

diskurs som råder bedömer dataskyddsombudet att det är viktigt att man på ledningsnivå har kunskap om syftet med GDPR och förståelse för att om GDPR sätter ”stopp” för en behandling eller en tjänst så finns det ett gott skäl till det. I praktiken innebär det att man på ledningsnivå behöver ta ansvar för att inte använda en digital tjänst eller inleda en behandling av personuppgifter som inte är förenlig med kraven i GDPR. En viktig del i detta är att ledningen börjar signalera en förväntan på att nya digitala lösningar ska vara långsiktigt hållbara, även utifrån ett integritetsperspektiv. På så sätt behöver verksamheter tänka på dataskydd tidigt i processen och kan förhoppningsvis undvika att hamna i situationer där GDPR enbart ses som något jobbigt eller ett administrativt hinder. Genom att integrera dataskyddsperspektivet från start i arbetet med nya tjänster och/eller vid utvecklandet av nya arbetssätt kan verksamheter hitta stabila och långsiktiga alternativ där människors grundläggande fri- och rättigheter inte äventyras. Något som blir, om möjligt, extra viktigt i takt med att användningen av ny teknik och AI ökar inom Stadens verksamheter.

2.1.3 Bristande ansvarstagande i Stadens arbete med AI medför risker för både enskilda och verksamheter

Fokus på ny teknik och AI har en enorm potential för att göra våra liv bättre, men den digitala utvecklingen blir inte hållbar utan begränsningar. Utan tydlig styrning i arbetet med digital innovation är risken att det går fort och att man i sin iver att röra sig framåt glömmer att hänsyn behöver tas till den personliga integriteten och att personuppgifter behandlas på ett korrekt sätt. Som en stor offentlig aktör har Göteborgs Stad att förvalta alla invånare och besökares förtroende. Oavsett om det handlar om elever, vårdnadshavare, anställda, brukare inom socialtjänst, eller någon annan kategori av kommuninvånare, så ska man kunna känna sig trygg med att användandet av innovativ teknik sker med respekt för den personliga integriteten och de regelverk som finns för att skydda enskildas personuppgifter.

Under året har dataskyddsombudet kunnat se att allt fler verksamheter inom Staden börjar utforska användningen av AI. Dataskyddsombudet har under året löpande kunnat identifiera stora risker med det arbete som bedrivs på stadenövergripande nivå. Riskerna kommer dels utifrån att det från centralt håll hittills saknas styrning och samordning i hur tekniken kan, och får, användas, dels utifrån att de tekniska lösningar som har lanserats ej först kontrollerats utifrån ett informationssäkerhets- och dataskyddsperspektiv. Dataskyddsombudets bedömning är att stadsledningskontoret och Intraservice behöver ta ett större ansvar i hanteringen av dessa risker, eftersom de båda verksamheterna är starkt drivande i användningen av AI inom Staden. Särskilda rekommendationer ställs därför till de båda verksamheterna i deras respektive årsrapporter.

Dataskyddsombudet vill utifrån identifierade risker med de stadenövergripande AI-lösningar som idag finns tillgängliga inom Staden (M365 Copilot i Edge, Svea GPT etc.) betona vikten av att förvaltningar och bolag innan en ny AI-lösning tas i bruk först kontrollerar så att denna är säkerställd utifrån ett informationssäkerhets- och dataskyddsperspektiv.

3 Dataskyddsombudets iakttagelser 2024

3.1 Verksamhetens dataskyddsarbete

Dataskyddsombudet har haft en aktivt rådgivande roll i arbetet med att genomföra delar av bolagets arbete under 2024. Dataskyddsombudet har involverats i avstämningsmöten och konsulterats av verksamheten i frågor rörande dataskydd hänförliga till granskning eller uppföljningsarbetet liksom förvaltning. Bolaget har utfört ett par konsekvensbedömningar varav en gällande bolagets behandlingar kring driftoptimering av resurser, registrering av kör- och vilotider, positioneringsteknik med mera. Dataskyddsombudet har involverats i konsekvensbedömningsarbetet och bolaget har utfört arbetet på ett föredömligt vis där lämnade råd har följts.

Dataskyddsombudet genomförde under hösten 2024 en fördjupad kontroll av bolagets behandlingsregister i enlighet med artikel 30 i GDPR.

Bolaget har varit transparanta med att registret inte är komplett. Den nuvarande dataskyddsorganisationen bestående av en person uppskattar att ca 50 % av behandlingar saknas liksom vetskap om vilka områden som berörs. Utifrån behandlingsregistrets stora brister och sårbarhet när arbetet centreras kring en person samt följdriktiga höga föreliggande risker för de registrerades fri- och rättigheter rekommenderas bolaget göra en genomgående översyn av samtliga behandlingar med fokus på en generell förbättring gällande behandlingsavgränsningen liksom ändamålsformuleringar. Bolaget rekommenderas säkerställa att dataskyddsorganisationen får de resurser som krävs för att komplettera behandlingsregistret för att i dess förlängning fortsatt kunna bedriva ett systematiskt dataskyddsarbete. Därutöver tillse att alla krav som anges i artikel 30 i GDPR uppfylls genom att omhänderta de rekommendationer som lämnas för varje del i rapporten för den fördjupade kontrollen, se bilaga 2.

Dataskyddsombudets sammantagna uppfattning är att bolaget är på god väg men att det finns fortfarande utmaningar för bolaget att omhänderta. Visat intresse och engagemang för dataskyddsfrågor upplevs positivt och är en viktig förutsättning för bolagets fortsatta utveckling. Det är också viktigt att bolagsledningen även framgent tydligt prioriterar frågor kopplat till integritet och dataskydd.

Avgörande för att bli framgångsrik i detta är att bedriva arbetet långsiktigt, uthålligt och kontinuerligt.

Eftersom arbetet berör hela verksamheten är det viktigt att alla medarbetare är medvetna om detta. God nivå i dataskyddsarbetet byggs genom kunskap underifrån och stöd av strukturer och arbetssätt för varje verksamhet.

4 Granskning av dataskyddsarbetet 2024

4.1 Fördjupad kontroll 2024

Renova AB har ingått i den fördjupade kontrollen av behandlingsregistret med hänvisning till fullständig rapport som framgår av bilaga 2.

Dataskyddsombudets samlade bedömning efter granskningen är att registret endast delvis innehåller den information som föreskrivs enligt artikel 30 i GDPR och att de uppgifter som finns dokumenterade för en stor del av behandlingarna har brister.

Dataskyddsombudet rekommenderar därför att bolaget i stort tar ett omtag kring dokumentationen av behandlingarna i behandlingsregistret. Bolaget rekommenderas utbilda och involvera andra medarbetare i kartläggningen men även framtida uppföljningen. Parallellt med uppdateringsarbetet rekommenderas bolaget anta och inkorporera ett arbetssätt för att hålla registret uppdaterat och korrekt.

I bolagets arbete med behandlingsregistret bör särskilt fokus ligga på behandlingsavgränsning och ändamålsformuleringar som ska vara tydliga, konkreta och specifika. Bolaget rekommenderas även att arbeta med sin beskrivning av de kategorier av personuppgifter och kategorier av registrerade som förekommer i de olika behandlingarna, vilka som är mottagare av uppgifterna, faktiska tredjelandöverföringar av personuppgifter och en allmän beskrivning av erforderliga organisatoriska och tekniska säkerhetsåtgärder.

Med hänsyn till att behandlingsregistret är ett viktigt verktyg för ett fungerande dataskyddsarbete är rekommendationen att bolaget vid uppdateringen av behandlingsregistret tar även del av den generella rapporten och beaktar rekommendationer som framgår däri. Bolaget rekommenderas säkerställa förbättringsåtgärderna och parallellt med uppdateringsarbetet tydliggöra all information.

4.2 Uppföljning av lämnade rekommendationer

4.2.1 Uppföljning av verksamhetens arbete med rekommenderade fokusområden 2024

Dataskyddsombudet har följt upp hur verksamheten arbetat med de fokusområden som rekommenderades för 2024. Utifrån uppföljningen lämnas rekommendationer.

Fokusområde 1: Personuppgiftsincidenter

Verksamheten gavs följande rekommendationer:

Verksamheten förordas följa lämnade rekommendationer inom ramen för den fördjupade kontrollen 2022.

Kommentarer och rekommendationer:

Bolaget uppger att en ny rutin har tagits fram som hela verksamheten har fått ta del av. Genomgång av personuppgiftsincidenter inkluderar hela processen och GDPR frågor på Ledarforum för alla chefer samt besök på arbetsplatsmötena APT:er. Bolaget har även tagit fram en enklare checklista hur medarbetare ska tänka kring GDPR och dataskydd. Checklistan är inskickad till dataskyddsombudet ihop med övrigt material kring den pågående fördjupade kontrollen om behandlingsregister. Bolaget uppger vidare att de har haft ett par inrapporterade personuppgiftsincidenter och upplever att antal inrapporteringar liksom övriga frågor kring GDPR har ökat jämfört med tidigare vilket är positivt i sammanhanget.

Uppföljningen visar att den interna dataskyddsorganisationen har en ambition och en vilja att bedriva ett systematiskt dataskyddsarbete och att verksamheten har vidtagit förbättringsåtgärder i enlighet med lämnade rekommendationer.

Fortsatt uppföljning kommer att ske löpande under ordinarie avstämningsmöten, inom ramen för den uppföljning som dataskyddsombudet genomför under hösten 2025 eller på förekommen anledning.

Fokusområde 2: Utbildning

Verksamheten gavs följande rekommendationer:

Öka den generella kunskapsnivån inom dataskydd hos medarbetare, inkluderat hantering av personuppgiftsincidenter.

Kommentarer och rekommendationer:

Bolaget uppger att det pågår mycket arbete för att öka den generella kunskapsnivån. Utöver ett par utbildningsgenomgångar kring personuppgiftsincidenter på Ledarforum samt några APT möten uppges även stadens utbildningar ge önskad effekt. Medvetenheten kring dataskyddsfrågorna och vikten av att hantera information korrekt ökar även mot bakgrund av pågående arbete med informationsklassning. Medarbetare pratar om olika GDPR frågor i lunchrum och är mer benägna att ställa frågor till dataskyddskontakterna.

I övrigt anges att den interna dataskyddsorganisationen försöker ta alla tillfällen i akt för att fortsatt sprida och öka medarbetarnas kunskaper. I utbildningsarbetet deltar och involveras även andra funktioner i verksamheten bland andra arkivansvarig. Utbildningsinsatserna mäts och dokumenteras.

Som ytterligare förbättringsåtgärd uppges att bolagets Säkerhetsenhet bygger ut en egen SharePoint sida, på bolagets intranät ’Insidan’, så att alla medarbetare kan få hjälp med samlad GDPR information och tillhörande rutiner, styrande dokument med mera.

Uppföljningen visar att verksamheten har vidtagit förbättringsåtgärder i enlighet med lämnade rekommendationer. Eftersom utbildningen är central del i ett systematiskt dataskyddsarbete kommer därför fortsatt uppföljning att ske löpande under 2025 samt med fokus på kunskaper kring behandlingsregister.

Fokusområde 3: Konsekvensbedömning/samråd

Verksamheten gavs följande rekommendationer:

Identifiera befintliga högriskbehandlingar och ta fram dokumenterade arbetssätt för att hantera riskerna liksom uppföljningen.

Kommentarer och rekommendationer:

Bolaget redogör för att arbetet med konsekvensbedömningar pågår och rullar på bra. Vidare uppges att bolaget jobbar med åtgärderna gällande positioneringsteknik och ytterligare en konsekvensbedömning är på gång gällande kamerabevakning. Samråd och dataskyddsombudets synpunkter kommer att inhämtas när ett nytt avtal med en ny leverantör är på plats.

Bolaget uppger också att arbetet med konsekvensbedömningar på andra områden inom verksamheten är nästa steg och inte riktigt i fas. För att få systematik och rätt resurser att delta måste kunskapsnivån höjas hos befintliga verksamhetsfunktioner eftersom det är de som äger och kan sina processer bäst. Enligt uppgift planerar bolaget att rikta in konsekvensbedömningsarbetet mot upphandlings-och avtalsområdet. Kopplat till komplexiteten och svårigheterna efterlyser bolaget mer stöd och hjälp i det fortsatta arbetet framåt.

Uppföljningen visar att verksamheten fortfarande har förbättringsområden inom denna kontroll. Fortsatt uppföljning kommer att ske löpande under 2025.

5 Rekommenderade fokusområden 2025

Dataskyddsombudet rekommenderar, utifrån gjorda iakttagelser samt resultaten av uppföljningen och den fördjupade kontrollen, verksamheten att under 2025 fortsätta prioritera arbetet med de kontrollpunkter som rekommenderas för 2024 med tilläggsfokus som listas i punktform enligt nedan.

Detta är områden som dataskyddsombudet särskilt kommer att följa upp under året. Uppföljningen kommer ske kontinuerligt under avstämningsmöten med verksamheten, och inom ramen för den uppföljning som dataskyddsombudet genomför under hösten 2025.

Bolaget rekommenderas under 2025 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Kartlägga och komplettera behandlingsregistret enligt artikel 30 i GDPR. Ta del av och beakta rekommendationerna som framgår i den fördjupade kontrollen men även i den generella granskningsrapporten som vägledning. Säkerställa förbättringsåtgärderna och inkorporera ett arbetssätt för att hålla registret uppdaterat och korrekt.

- Kontrollpunkt 6: Utbildning

Öka och dokumentera den generella kunskapsnivån inom dataskydd hos medarbetare som inkluderat involverad hantering av behandlingsregister.

- Kontrollpunkt 9: Konsekvensbedömning/samråd

Identifiera befintliga högriskbehandlingar och ta fram dokumenterade arbetssätt för att hantera riskerna liksom uppföljningen.

6 Bilagor

Bilaga 1: Kontrollplan för dataskyddsarbetet 2024–2025

Bilaga 2: Rapport fördjupad kontroll 2024

Göteborgs Stad

Kontrollplan för dataskyddsarbetet 2024–2025

Förvaltningar och bolag i Göteborgs Stad

2024-05-06

Innehåll

1 Bakgrund

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 värna om den enskildes rätt till integritet och kontroll över vad som sker med ens personuppgifter. 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 personuppgifter.

Det är varje nämnd och bolaget som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. För att stödja stadens nämnder och bolag i arbetet med dataskydd har ett dataskyddsombud utsetts. I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud. Dataskyddsombudet har särskild sakkunskap i dataskyddslagstiftning och arbetar bland annat för att hålla nämnden/bolaget informerade om hur verksamheten lever upp till dataskyddslagstiftningen. Vad som är dataskydds-ombudets uppgifter framgår direkt av GDPR. En av dessa uppgifter är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. När dataskyddsombudet kontrollerar efterlevnaden av dataskyddslagstiftningen sker det bland annat genom att samla in information om hur personuppgifter behandlas inom en verksamhet och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

1.1 Ändrad utformning av den fördjupade kontrollen 2024

Med anledning av den omorganisation som dataskyddsenheten genomgår under 2024 har den fördjupade kontrollen i år behövt anpassas till rådande förutsättningar. Detta innebär att dataskyddsombudet inte kommer att kunna genomföra kontroller inom alla Stadens verksamheter under 2024. I stället kommer kontrollen att hanteras genom stickprov och enbart genomföras inom ett urval av Stadens verksamheter. Även om alla verksamheter inte kommer kontrolleras under 2024 är dataskyddsombudets förhoppning att resultaten från kontrollen som helhet ska kunna användas av flera verksamheter och därigenom bidra till att stärka Stadens sammantagna dataskyddsarbete.

1.1.1 Uppföljning av informationsinsatsen 2023

Under våren 2023 genomförde dataskyddsenheten en informationsinsats med fokus behandlingsregistret enligt artikel 30 i GDPR. Syftet med informations-insatsen var att höja kunskapen inom området och skapa enhetlighet inom Göteborgs Stad. Som uppföljning på denna informationsinsats kommer under 2024 en fördjupad kontroll av verksamheters efterlevnad av artikel 30 i GDPR, och därigenom skyldigheten att systematiskt dokumentera alla personuppgifts-behandlingar i form av ett register, att genomföras.

2 Kontrollarbetet 2024–2025

Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att organisationen följer dataskyddsförordningen. I Göteborgs Stad innebär detta bland annat att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom förvaltningar och bolag. 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 denna kartläggning kan sedan användas som ett stöd av verksamheten i dess fortsatta arbete med dataskydd. Dessa kontroller specificeras genom denna kontrollplan, som syftar till att informera personuppgiftsansvariga om upplägg och tidplan för kontrollarbetet åren 2024 och 2025. Dataskyddsombudets kontrollarbete löper över tvåårsperioder. En ny kontrollplan skickas ut årligen, vilken omfattar både innevarande och nästkommande kalenderår.

Syftet med att arbeta utefter en på förhand fastställd kontrollplan är att det ska bidra till att sätta fokus på verksamhetens dataskyddsarbete och därmed:

1. Säkerställa ett kontinuerligt dataskyddsarbete som skapar förutsättningar för efterlevnad av förordningen.
2. Uppmuntra ett riskbaserat arbetssätt och därigenom minimera risken för lagbrott.
3. Göra dataskyddsarbetet till en integrerad del i verksamhetens informationssäkerhetsarbete.

2.1 Kontrollarbetets delar

Kontrollarbetet består av tre delar som tillsammans syftar till att ge, såväl dataskyddsombud som personuppgiftsansvariga, en överblick över verksamhetens dataskyddsarbete och dess följsamhet gentemot GDPR.

Del	Beskrivning	Frekvens
Övergripande kontroll (tidigare kallad ”fasta kontrollpunkter”)	En övergripande kontroll av verksamhetens dataskyddsarbete. Verksamheten skattar det interna arbetet i en enkät uppdelad i tolv fasta kontrollpunkter.	Vartannat år
Fördjupad kontroll	En fördjupad kontroll av en eller flera utvalda kontrollpunkter.	Vartannat år
Uppföljning	Uppföljning och bedömning av hur verksamheten omhändertagit lämnande rekommendationer.	Årligen

2.1.1 Övergripande kontroll

Den övergripande kontrollen utgår från principerna om inbyggt dataskydd och dataskydd som standard (enligt artikel 25 i GDPR). Verksamhetens följsamhet mot förordningen beror till stor del på hur väl dessa principer har integrerats i ordinarie arbetsprocesser. Att principerna har en central roll i arbetet med dataskydd blir särskilt tydligt i beaktandesats (skäl) 78 i GDPR, som anger att ”skyddet av fysiska personers rättigheter och friheter i samband med behandling av personuppgifter förutsätter att lämpliga tekniska och organisatoriska åtgärder vidtas”, och därtill att den personuppgiftsansvarige, för att kunna visa att förordningen efterlevs, bör anta interna strategier och vidta åtgärder särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard. Med principerna som utgångspunkt har tolv kontrollpunkter identifierats. Dessa är av både teknisk och organisatorisk karaktär och är gemensamma för alla verksamheter inom Göteborgs Stad.

Den övergripande kontrollen genomförs genom en enkät. Enkäten utgår från de tolv kontrollpunkterna där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Resultaten från enkäten ger en generell ögonblicksbild för respektive kontrollpunkt och kan användas som vägledning för verksamheten i sitt dataskyddsarbete. Syftet är att få till ett långsiktigt och systematiskt arbetssätt, samt åskådliggöra de förändringar som vidtas över tid.

För beskrivning av de olika kontrollpunkterna, se bilaga 1.

Fasta kontrollpunkter
1. Dataskyddsorganisation
2. Personuppgiftsincidenter
3. Biträdesavtal och andra överenskommelser
4. Register över personuppgiftsbehandlingar
5. Övergripande styrning av dataskyddsarbetet
6. Utbildning
7. Informationsplikt
8. E-post och dokumenthantering
9. Konsekvensbedömning/samråd
10. IT-projekt och upphandling
11. IT-system och digitala verktyg
12. Hantering av registrerades rättigheter

2.1.2 Fördjupad kontroll

Den fördjupade kontrollen kan utgå från både staden övergripande och verksamhetsspecifika risker. I utformningen av kontrollen utgår dataskyddsombudet från de risker som identifierats, både inom enskilda verksamheter och på en övergripande nivå. Hänsyn tas även till

dataskyddsombudets resurser samt vad som bedöms kunna få störst effekt för flest verksamheter inom Staden.

2.1.3 Uppföljning av genomförda kontroller

Uppföljning av genomförda kontroller görs årligen för att se hur verksamheten har hanterat tidigare lämnade rekommendationer. Denna uppföljning kan göras både muntligen och skriftligen. Resultatet av genomförd uppföljning kommer redovisas i årsrapporten.

2.2 Tidplan för kontrollarbetet 2024–2025

I tabellerna nedan anges huvuddragen i kontrollarbetet för åren 2024–2025 för stadens förvaltningar och bolag.

2024	Aktivitet
Maj	Kontrollplan för 2024–2025 lämnas till nämnder och bolag.
Augusti – november	Fördjupad kontroll genomförs. **För 2024 har följande fokusområde för den fördjupade kontrollen fastställts:** • Kontrollpunkt 4: Register över personuppgiftsbehandlingar Kontrollen genomförs inom ett urval av Stadens verksamheter. Under augusti månad kommer information om vilka verksamheter som ingår i urvalet att tillhandahållas samtliga förvaltningar och bolag. Resultaten från kontrollen kommer redogöras för i årsrapporten samt genom särskilt informationsmöte.
November – december	Genomgång av innehåll i årsrapport med respektive förvaltning och bolag.
December	Fastställd årsrapport översänds till respektive förvaltning och bolag.

2025	Aktivitet
Februari	Kontrollplan för 2025–2026 lämnas till nämnder och bolag.
September	Övergripande kontroll genomförs.
November – december	Genomgång av innehåll i årsrapport med respektive förvaltning och bolag.
December	Fastställd årsrapport översänds till respektive förvaltning och bolag.

3 Rapportering

3.1 Årsrapport

Det är nämnd/bolag som har det yttersta ansvaret för att verksamheten följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå. Därför sammanställer dataskyddsombudet årligen en rapport om verksamhetens dataskyddsarbete. I rapporten redogörs för eventuella risker och brister som dataskyddsombudet har identifierat. I rapporten redogörs också för de råd och rekommendationer som dataskyddsombudet har lämnat. För att möjliggöra en direkt kommunikation mellan dataskyddsombud och högsta ansvarsnivå inom verksamheten ska årsrapporten tillhandahållas nämnd respektive bolagsstyrelse.

3.2 Särskilt yttrande

Dataskyddsombudet kan i vissa situationer komma att rikta ett särskilt yttrande till högsta ansvarsnivå. En sådan situation kan vara om dataskyddsombudet har identifierat höga risker för de registrerade som kräver omgående åtgärder från ansvarig nämnd/bolag. Det kan också vara om dataskyddsombudet uppmärksammar att det inom verksamheten fattats beslut som är oförenliga med dataskyddslagstiftningen och dataskyddsombudets råd.

4 Kontakt

Eventuella frågor och synpunkter på kontrollplanen hänvisas i första hand till dataskyddsenhetens enhetschef Elin Olsson Norrblom.

Frågor kan också alltid ställas till dataskyddsenheten via mejladressen; dso@intraservice.goteborg.se.

Bilaga 1 - Beskrivning av fasta kontrollpunkter

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.

Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar för att identifiera och hantera personuppgiftincidenter. För att uppfylla ansvarsskyldigheten bör verksamhetens rutin för hanteringen vara dokumenterad. I de fall verksamheten är både personuppgiftsansvarig och personuppgiftsbiträde bör rutinen omfatta båda scenarier. I kontrollpunkten ingår även översyn av verksamhetens rutin för att bedöma incidenter, hantering av eventuell anmälan till tillsynsmyndigheten, samt hur rutinerna tillgängliggörs och kommuniceras inom verksamheten. Även efterlevnad av verksamhetens dokumentationsskyldighet, att alla inträffade personuppgiftsincidenter registreras, innefattas.

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.

Kontrollpunkt 4: Register över personuppgiftsbehandlingar

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 register innefattas.

Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Kontrollpunkten avser verksamhetens övergripande styrning för att arbeta med dataskydd. Tydlig styrning sätter ramarna för arbetet med dataskydd och främjar ett riskbaserat arbetssätt. Kontrollpunkten innefattar även verksamhetens arbete för att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet, samt hur verksamheten arbetar med egna interna kontroller för att säkerställa att dataskyddslagstiftningen efterlevs.

Kontrollpunkt 6: Utbildning

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

Kontrollpunkt 7: Informationsplikt

Kontrollpunkten avser hur väl verksamheten uppfyller principen om öppenhet och kravet på att lämna information till de registrerade om hur deras personuppgifter behandlas. Punkten omfattar även hur verksamheten säkerställer att informationen är uppdaterad.

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 dataskyddslagstiftningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt genomföra denna. Även verksamhetens rutiner för arbetet med konsekvensbedömningar samt hur dataskyddsombudet involveras i arbetet ingår. Därtill tillkommer verksamhetens rutin för att hantera de risker som identifieras i konsekvensbedömningen, samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

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.

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 dataskyddslagstiftningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar för att hantera de registrerades rättigheter. En förutsättning för att verksamheten ska kunna hantera de registrerades rättigheter är att man har en process och rutiner för arbetet, så att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan. Även verksamhetens rutin för att hantera ett tillbakadragande av samtycke ingår i kontrollpunkten.

Göteborgs Stad

Fördjupad kontroll 2024: Behandlingsregister enligt artikel 30 i GDPR

Granskningsrapport för Renova AB

2024-12-20

Innehåll

1 Inledning

1.1 Kontrollområdet

I enlighet med vad som aviserats i kontrollplan för år 2024/2025 har dataskyddsombudet genomfört en fördjupad kontroll under hösten 2024. Det fördjupade kontrollområdet som valts ut för årets kontroll är verksamheternas register över personuppgiftsbehandlingar.

GDPR ställer höga krav på organisationers behandling av enskildas personuppgifter. Varje enskild nämnd eller bolag i Göteborgs stad är personuppgiftsansvarig för de behandlingar som utförs under dess ansvar. Enligt artikel 5.2 i GDPR är det den personuppgiftsansvarige som ansvarar för och ska kunna visa att organisationen följer GDPR och efterlever de grundläggande principerna i artikel 5.1 i GDPR. Som ett led i ansvarsskyldigheten följer det av artikel 30.1 och skäl 82 i GDPR och att den personuppgiftsansvarige ska föra ett register över sina behandlingar. Det framgår vidare av artikel 30.3 att registret ska vara skriftligt, och av artikel 30.4 att registret på begäran ska göras tillgängligt för tillsynsmyndigheten.

1.2 Syfte

Under våren 2023 genomförde dataskyddsenheten en informationsinsats med fokus på behandlingsregistret enligt artikel 30 i GDPR. Syftet med informationsinsatsen var att höja kunskapen inom området och skapa enhetlighet inom Göteborgs Stad, och i förlängningen tillse att stadens verksamheter har behandlingsregister som uppfyller kraven i GDPR. Som uppföljning på denna informationsinsats har dataskyddsenheten under hösten 2024 genomfört en fördjupad kontroll av några förvaltningars och bolags efterlevnad av artikel 30 i GDPR, och därigenom skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register.

Syftet med den fördjupade kontrollen av behandlingsregistret är att undersöka om förvaltningar och bolag uppfyller kraven om att systematiskt dokumentera alla behandlingar i form av ett register, om det finns en organisation för att säkerställa detta i form av dokumenterade och tydligt fastställda roller och ansvar, samt om det finns dokumenterade arbetssätt för att säkerställa att behandlingsregistret hålls aktuellt. Den fördjupade kontrollen har även inkluderat hur behandlingsregistret används i det systematiska dataskyddsarbetet inom verksamheten.

1.3 Tillvägagångssätt

Den fördjupade kontrollen har genomförts i två steg. Den första delen av kontrollen genomfördes i form av en skrivbordskontroll. I denna del fick verksamheten svara på ett antal kontrollfrågor och tillhandahålla sitt

behandlingsregister, dokumentation i form av roll och ansvarsbeskrivningar, samt dokumenterade arbetssätt gällande hur verksamheten arbetar med att säkerställa att man har ett fullständigt och uppdaterat behandlingsregister i enlighet med kraven i artikel 30 i GDPR.

Utifrån inkomna underlag har dataskyddsombudet därefter granskat hela behandlingsregistret för att kontrollera om de registrerade behandlingarna uppfyller kraven enligt artikel 30 i GDPR. Dataskyddsombudet har också granskat verksamhetens organisation avseende arbetet med behandlingsregistret i form av de roll/ansvarsbeskrivningar samt dokumenterade arbetssätt som verksamheten tillhandahållit dataskyddsombudet.

Som del två av kontrollen har dataskyddsombudet lämnat rekommendationer till verksamheten avseende eventuella åtgärder som dataskyddsombudet bedömer behöver genomföras i arbetet med behandlingsregistret utifrån organisation, fastställande av roller och ansvar, samt dokumenterade arbetssätt för att säkerställa att registret uppfyller kraven i artikel 30 och hålls kontinuerligt uppdaterat. Detta har gjorts genom att dataskyddsombudet haft möte med verksamheten och vid detta gått igenom verksamhetens behandlingsregister, för att i dialog med verksamheten kunnat påvisa och förklara eventuella förbättringsområden och identifierade brister. Syftet med denna metod är att få till en lärandeprocess utöver dataskyddsombudets rent kontrollerande funktion. Dataskyddsenhetens målsättning är att efter genomförd kontroll ska verksamheten ha förutsättningar för att uppnå en godtagbar nivå på behandlingsregistret, samt att med stöd av dataskyddsombudens rekommendationer ha fått vägledning i hur arbetet med att hålla registret aktuellt kan utformas.

Dataskyddsombudets sammantagna bedömning och rekommendationer har därefter sammanställts i denna granskningsrapport.

1.4 Bilagor

Bilaga 1	Informationsutskick fördjupad kontroll av behandlingsregistret
Bilaga 2	Bolagets svar på kontrollfrågor om behandlingsregistret
Bilaga 3	Bolagets rutin *Checklista GDPR* och *Rutin inkommande förfrågningar för personuppgifter*

2 Fördjupad kontroll

2.1 Resultat av granskning av dokumenterade arbetssätt

2.1.1 Dataskyddsombudets bedömning

I samband med kontrollfrågor ombads bolaget att översända de dokument och rutiner som beskriver hur bolaget har organiserat arbetet med behandlingsregistret. Två dokument, *Checklista GDPR* och *Rutin inkommande förfrågningar för personuppgifter*, har skickats in till dataskyddsombudet, se bilaga 3.

Som svar på dataskyddsombudets kontrollfrågor har bolaget uppgett att man har utpekade roller och ansvar för att säkerställa att behandlingsregistret uppfyller kraven i artikel 30 i GDPR. Bolaget anser också att det finns utpekade roller och ansvar som tydligt fastställer ansvaret för att säkerställa att nya personuppgiftsbehandlingar upptas i registret, och att det finns dokumenterade arbetssätt som säkerställer att registret uppdateras med nya och förändrade personuppgiftsbehandlingar.

Av bolagets svar i kontrollfrågeformuläret under avsnitt 4 *Användning och översyn av behandlingsregistret* framgår att informationssäkerhetshandläggaren ska kontaktas vid antingen upprättandet eller uppdatering av behandlingsregister. Vidare kan viss intern ansvarsfördelning ändå utläsas då olika kontaktpersoner finns namngivna gällande befintliga behandlingar i själva behandlingsregistret.

Dataskyddsombudets bedömning är att bolaget har en ambition och målsättning att på sikt arbeta systematiskt mer med registret och sitt dataskyddsarbete. Bifogade dokument är dock inte relevanta då ansvar för behandlingsregistrets hantering inte alls berörs varmed korrekt dokumenterade arbetssätt saknas.

Ansvarsfördelningsfrågan är otydlig eftersom hanteringen av registret i nuläget är knuten till informationssäkerhetshandläggarens roll. Bolaget påvisar en sårbarhet när hanteringen centreras kring en person.

Dataskyddsombudet rekommenderar därför att bolaget tar fram och antar dokumenterade arbetssätt för hur verksamheten systematiskt ska arbeta med behandlingsregistret. Bolaget behöver också ta fram och dokumentera en tydlig intern ansvarsfördelning för att säkerställa att behandlingsregistret kontinuerligt uppdateras med nya och förändrade personuppgiftsbehandlingar. Ett förtydligande av ansvar samt dokumenterade arbetssätt som flera anställda känner till och involveras i kan vara ett verksamt sätt att åtgärda de risker som uppstår då arbetet med registret centreras kring en nyckelperson.

Obligatorisk information i behandlingsregistret

Bolaget uppger att behandlingsregistret innehåller all information som ska finnas med i behandlingsregistret enligt artikel 30 i GDPR och bolaget använder också dataskyddsombudets mallstruktur med alla obligatoriska fält. Bolaget uppskattar att ca 25-50 % av bolagets behandlingar är upptagna i behandlingsregistret och uppger samtidigt att det i nuläget inte finns vetskap om vilka områden som saknar personuppgiftsbehandlingar.

Dataskyddsombudet rekommenderar därför att bolaget skyndsamt åtgärdar bristerna genom att involvera andra medarbetare i behandlingskartläggningen, ta fram dokumenterade arbetssätt med tydlig intern ansvarsfördelning och därefter tillser att behandlingsregistret är komplett.

Användning och översyn av behandlingsregistret

Bolaget uppger att behandlingsregistret inte används som en naturlig del i det systematiska arbetet med dataskydd. Medarbetare uppges ha kännedom om behandlingsregistret dock inte tillgång till det eftersom kunskapen och förståelsen för hur man fyller i och besvarar frågorna inte är tillräcklig.

Bolaget har under det gångna året genomfört olika riktade utbildnings- och informationsinsatser. Dataskyddsombudet ser det som mycket positivt och uppmuntrar bolaget att fortsätta på den inslagna linjen. För att uppfylla dataskyddsförordningens efterlevnad fullt ut krävs kontinuerliga interna utbildningsinsatser i kombination med andra åtgärder som anses nödvändiga och på så vis hitta sätt att utöka användningen av behandlingsregistret.

2.2 Resultatet av granskning av behandlingsregister

2.2.1 Dataskyddsombudets bedömning

Dataskyddsombudets bedömning är att registret endast delvis innehåller den information som föreskrivs enligt artikel 30. Även de uppgifter som finns dokumenterade i registret har stora brister, och bolaget rekommenderas att ta ett omtag kring hur man dokumenterar sina behandlingar i behandlingsregistret, särskilt med fokus på att formulera tydliga, konkreta och specifika ändamål. Dataskyddsombudet redogör i detalj för sin bedömning av behandlingsregistrets innehåll under avsnitt 2.2.2 nedan.

2.2.2 Granskning av behandlingsregister

2.2.2.1 Namn och kontaktuppgifter

Av artikel 30.1a i GDPR framgår att behandlingsregistret ska innehålla *namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombudet.* Det register som bolaget tillhandahållit dataskyddsombudet innehåller inte namn och kontaktuppgifter för den

personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare, trots att de är obligatoriska. Syftet med informationen är att möjliggöra en tydlig identifiering av den eller de personuppgiftsansvariga och alla andra som är ansvariga enligt GDPR. Begreppet *kontaktuppgifter* är alltså inte begränsat till en enkel e-postadress. Informationen ska innehålla alla uppgifter (namn, fysisk adress, och kontaktväg, e-post och telefonnummer) som gör det möjligt att få kontakt med den personuppgiftsansvarige och dataskyddsombudet.

Bolaget rekommenderas komplettera behandlingsregistret med uppgift om personuppgiftsansvarig samt kontaktuppgifter till dessa. Exakt i vilken form som bolaget väljer att presentera informationen är upp till verksamheten att avgöra, antingen som kolumner vid varje behandling i registret, eller som en övergripande information i inledningen, där det i så fall tydligt framgår att uppgifterna gäller för samtliga behandlingar i registret.

2.2.2.2 Beskrivning av ändamål

Enligt artikel 30.1b i GDPR ska behandlingsregistret innehålla en *beskrivning av ändamålen med behandlingen*. Av GDPR:s grundläggande principer (artikel 5.1b i GDPR) framgår att personuppgifter endast får behandlas för *särskilda, uttryckligt angivna och berättigade ändamål.* Det betyder att uppgifterna måste vara adekvata och relevanta för ändamålen, och att de inte får vara mer omfattande än nödvändigt.

Ett väl definierat ändamål är centralt för en praktisk avgränsning av den personuppgiftsansvariges behandlingar. Ändamålet med en behandling ska vara tydligt, konkret och specifikt.[1] Det innebär att den som läser det enkelt ska kunna förstå vad som avses och varför personuppgifter behandlas, samt att personuppgifterna som behandlas ska ha en tydlig koppling till beslutade ändamål. Om ändamålet saknar tillräcklig precision, går det inte att bedöma om personuppgifterna är adekvata och relevanta, eller om för många personuppgifter behandlas.[2] Det gäller särskilt för processorienterade ändamål som ofta är abstrakta och innehåller ett stort mått av subjektivitet, även om ändamålet kan vara tydligt språkligt formulerat. Att ändamålet ska vara specifikt innebär också att behandlingen inte ska innefattat något annat än det som direkt kan utläsas av beskrivningen, dvs. att det inte får finnas dolda eller underförstådda syften som inte direkt framgår.

Det betyder att ändamålsformuleringen aldrig ska innehålla formuleringar som *bland annat, med mera*, *et cetera* eller *till exempel*. Ett ändamål som formulerats med en sådan beskrivning är inte specifikt då det inte är begränsat till vad som direkt kan utläsas av ändamålsbeskrivningen och saknar därför tillräcklig precision.

Sammanfattningsvis så ska den registrerade, dataskyddsombudet, eller tillsynsmyndigheten kunna läsa ändamålsbeskrivningen, och utan ytterligare

[1] IMY - innovationsportalen
[2] Se Öhman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 5.1b

kännedom om verksamheten, kunna förstå varför uppgifterna behöver samlas in och till vad de ska användas.

Dataskyddsombudet vill särskilt poängtera att ändamålet även är något som den personuppgiftsansvarige är skyldig att informera de registrerade om enligt rätten till information i artikel 13.1c och 14.1c i GDPR, likväl som i enlighet med rätten till tillgång i artikel 15.1a i GDPR. När en personuppgiftsansvarig avgränsar sina behandlingar måste denne ha i åtanke att kunna uppfylla GDPR i alla dess delar.

Vad gäller bolagets beskrivning av ändamål i sitt behandlingsregister, så gör dataskyddsombudet bedömningen att bolagets har en alltför bred behandlingsindelning. Bolaget behöver generellt arbeta med att formulera ändamålen så att de blir tydliga, konkreta och specifika. Flertal behandlingar behöver brytas upp och få egna ändamål formulerade för att bli begripliga.

För de behandlingar och konsekvensbedömningar som bolaget arbetat mer aktivt med under året genom att involvera dataskyddsombudet, så anser dataskyddsombudet att bolaget tycks ha förstått bättre vad som krävs när det gäller precision i ändamålsbeskrivningarna. Ändamålen ska vara tillräckligt tydliga, konkreta och specifika. Samma precision respektive behandlingsavgränsning som görs i en konsekvensbedömning bör återspeglas i behandlingsregistret. Bolaget uppmuntras därför att fortsatt arbeta med behandlingsavgränsningar liksom precisa ändamålsformuleringar för samtliga behandlingar.

Dataskyddsombudet rekommenderar att bolaget tar ett helhetsgrepp i frågan och gör en genomgripande översyn av samtliga ändamålsformuleringar inklusive behandlingar som saknas i registret samt ser över hur avgränsningen av behandlingarna genomförs.

2.2.2.3 Beskrivning av kategorier av registrerade och kategorierna av personuppgifter

Enligt artikel 30.1c i GDPR ska behandlingsregistret innehålla *en beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter*. I sammanhanget är det viktigt att förtydliga att det som avses är en *beskrivning* av kategorier av registrerade och uppgifter, dvs det räcker inte att bara ange vilka kategorierna är. Läsaren ska av *beskrivningen* förstå vad kategorierna innefattar. Alltså vilka uppgifterna är, vilka de registrerade är, och hur de relaterar till varandra.[3] Beskrivningen i artikelns led c behöver alltså vara något utöver att bara ange, exempelvis, *sökande, anställda, kontaktuppgifter, uppgifter om sociala förhållanden,* med mera. Helt enkelt för att det ska gå att förstå behandlingen.

[3] Se EDPB Processing of personal data in the context of an access to documents request för ett konkret exempel på hur detta kan dokumenteras i registret. Notera också skillnaden i hur led c och led d är formulerade i artikel 30.1. I led c anges specifikt att det handlar om en *beskrivning* av kategorierna. I led d framgår bara att *kategorier* av mottagare ska anges utan något krav på en beskrivning.

Dataskyddsombudet anser inte att bolagets behandlingsregister lever upp till dessa krav. Även om det i strikt mening är så att kategorier av registrerade och personuppgifter finns med för samtliga behandlingar så bedömer dataskyddsombudet inte att de är beskrivna på ett sådant sätt att det av beskrivningen går att förstå vilka uppgifterna är, vilka de registrerade är, och hur de relaterar till varandra.

Bolaget rekommenderas därför genomgående att i sitt behandlingsregister utveckla beskrivningen av kategorier av registrerade och uppgifter, samt hur de relaterar till varandra.

2.2.2.4 Kategorier av mottagare

I artikel 30.1d i GDPR anges att behandlingsregistret ska innehålla uppgift om d*e kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer*.

I artikel 4.9 i GDPR definieras begreppet mottagare. Mottagare kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte. Ett personuppgiftsbiträde är en mottagare, liksom underbiträden och under-underbiträden.

Som mottagare betraktas inte offentliga myndigheter som kan komma att motta personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller den nationella rätten. Däremot är det viktigt att påpeka att de funktioner som behandlar uppgifter *inom* en personuppgiftsansvarigs organisation också träffas av begreppet mottagare.

Bolaget uppger att för vissa behandlingar delas uppgifterna internt dock att de specifika behandlingar saknar uppgift om vilka avdelningar eller funktioner inom bolagets egen organisation kan komma att ta del av personuppgifterna. Dataskyddsombudet har förståelse för att uppgiften om interna mottagare inte dokumenterats i bolagets register utifrån att dataskyddsombudets bedömning tidigare har varit att den personuppgiftsansvariges personal inte kan anses vara mottagare. Den tidigare bedömningen har gjorts utifrån formuleringen i artikel 30.1d om att *personuppgifterna har lämnats eller ska lämnas ut*, tillsammans med användandet av begreppet *utlämnas* i definitionen av mottagare i artikel 4.9 i den svenskspråkiga versionen av GDPR, eftersom det kan ifrågasättas huruvida personuppgifter verkligen lämnas ut om de hanteras inom en förvaltning eller ett bolag.[4] Under arbetet med den fördjupade kontrollen har dataskyddsombudet beaktat nya omständigheter som medfört en förändrad bedömning. Den förändrade bedömningen baseras på nya riktlinjer från den europeiska dataskyddsstyrelsen (EDPB)[5], vägledning utifrån de europeiska tillsynsmyndigheternas egna register[6], och det faktum att formuleringen

[4] Se Öhman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 4.9.
[5] EDPB: Data protection guide for small business
[6] EDPB Processing of personal data in the context of an access to documents request
EDPS record of processing activity - Whistleblowing procedure

utlämnas inte förekommer i den engelska, eller i flertalet andra språkversioner av GDPR.[7] Tolkningen finner också stöd i förarbetena till personuppgiftslagen.[8]

För att uppfylla kraven i artikel 30.1d förordas därför att dokumentera vilka interna avdelningar eller funktioner som kan komma att ta del av personuppgifter inom ramen för den specifika behandlingen. Det finns däremot inte någon skyldighet att i registret dokumentera identiteten på de faktiska fysiska personer inom verksamheten som tar del av uppgifterna.[9]

Vad gäller bolagets övriga dokumentation av mottagare så har dataskyddsombudet noterat att "innehållet på Renova.se är offentliggjort till en obestämd krets" vilket enligt definitionen inte är en mottagare. På några ställen i bolagets register anges mottagaren som "leverantör". Här är det oklart vad som avses och om det handlar om ett biträdesförhållande så ska det framgå. Bolagets befintliga behandlingar i registret saknar genomgående uppgift om biträden och underbiträden som mottagare.

Dataskyddsombudet anser att när en personuppgift tillgängliggörs för en mottagare så ska det av behandlingsregistret, som bästa praxis, framgå varför mottagaren är just mottagare.[10] Det vill säga att om mottagaren till exempel är ett personuppgiftsbiträde eller underbiträde så ska det dokumenteras i registret. Dataskyddsombudet vill också lyfta att även om det är kategorier av mottagare som ska anges, så har den registrerade vid en begäran om tillgång enligt artikel 15 i GDPR rätt att få information om specifika mottagare[11], och det är även information som ska lämnas till den registrerade i enlighet med informations-skyldigheten i artikel 13.1d och 14.1d i GDPR. Eftersom bolaget ändå är tvungen att dokumentera den specifika mottagaren enligt artikel 13-15 i GDPR så anser dataskyddsombudet att uppgiften ska dokumenteras i behandlingsregistret.

Utifrån detta rekommenderar dataskyddsombudet att bolaget gör en översyn av sitt register för att säkerställa att man anger alla specifika mottagare för samtliga behandlingar, inklusive interna mottagare, och att det i samtliga fall framgår varför mottagaren är mottagare.

2.2.2.5 Överföring av personuppgifter till tredjeland

Av artikel 30.1e framgår att behandlingsregistret ska innehålla information om: *i tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den*

[7] Jämför till exempel med den engelska originalversionens *disclose*, det tyska *offengelegt,* franskans *recoit,* Italienskans *recive, och* spanskans *comuniquen*, så framstår det som klart att det som egentligen avses är vem som får ta del av uppgifterna, vilket också är det sätt som EDPB uttrycker det i vägledningen för små företag. EDPB: Data protection guide for small business
[8] Se Öhman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 4.9, och SOU 1997:39 s. 335 *Begreppet mottagare omfattar i princip samtliga till vilka personuppgifter lämnas ut, även om den som tar emot uppgifterna inte skulle vara tredje man. Även den registrerade, personadatabiträdet och sådana personer som under den personadataansvariges eller personadatabiträdets direkta ansvar har befogenhet att behandla personuppgifter verkar således kunna betraktas som mottagare.*
[9] Se mål C-579/21
[10] Se EDPB Processing of personal data in the context of an access to documents request för ett konkret exempel, Se också mål C-154/21
[11] Se mål C-154/21

internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket, dokumentationen av lämpliga skyddsåtgärder.

För att kunna redogöra för vilka faktiska överföringar som äger rum så måste den personuppgiftsansvarige veta vad som uttryckligen framgår av de avtal som träffats med personuppgiftsbiträden och eventuella underbiträden.

Bolaget har angett genomgående att en överföring av personuppgifter inte sker.

Dataskyddsombudet vill också särskilt lyfta att den personuppgiftsansvarige har en skyldighet enligt artikel 28.3a i GDPR att tillse att ett personuppgiftsbiträde endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland. Det innebär att det i teorin aldrig ska finnas några situationer där bolaget inte redan på förhand vet till vilka tredjeländer som personuppgifter kommer att överföras. Det ska därför i princip inte kunna förekomma något fall där det inte är möjligt att dokumentera förekomsten av en tredjelandsöverföring i behandlingsregistret på grund av bristande kännedom eller okunskap.

Dataskyddsombudet rekommenderar därför att bolaget kartlägger vilka överföringar som sker, i enlighet med vad som regleras i befintliga avtal, och därefter dokumenterar de faktiska överföringarna i sitt behandlingsregister.

2.2.2.6 Tidsfrister för radering

I artikel 30.1f i GDPR anges att den personuppgiftsansvarige ska, *om det är möjligt ange, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter*. Utifrån tillgänglig vägledning kan det konstateras att det finns högt ställda krav för att något ska kunna anses vara "omöjligt". Att något är omständligt, tar lång tid eller innebär mycket administration innebär fortfarande att det är "möjligt".[12] Viktigt att notera är även att tidsfristerna ska anges för de olika kategorierna av personuppgifter och inte för behandlingen som helhet eller per handlingstyp.

Efter genomförd granskning av bolagets behandlingsregister anser dataskyddsombudet att tidsfrister för gallring redovisas och framgår dock i majoriteten av fallen per handlingstyp eller på dokumentnivå. GDPR medger vidarebehandling av uppgifterna för arkivändamål av allmänt intresse eller forskningsändamål. För att registret ska vara mera komplett bör tidsfristerna för radering i en specifik kategori som kommer att vidarebehandlas för dessa ändamål anges. För flera av behandlingarna uppger bolaget att uppgifter "gallras när informationen ej är relevant för ändamålet".

Dataskyddsombudet rekommenderar därför att bolaget kompletterar samtliga behandlingar i behandlingsregistret och anger vilka kriterier som används för att fastställa när uppgifterna inte är relevanta för ändamålet samt de förutsedda

[12] Se Article 29 Working Party Guidelines on transparency under Regulation 2016/679 s 29, pt 59. *The situation where it "proves impossible" under Article 14.5(b) to provide the information is an all or nothing situation because something is either impossible or it is not; there are no degrees of impossibility.*

tidsfristerna för radering (dvs när personuppgifterna kommer att gallras) för de olika kategorierna av personuppgifter för samtliga behandlingar i behandlingsregistret, i enlighet med vad som anges i artikel 30.1f.

2.2.2.7 Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder

En allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1 ska, om möjligt anges, enligt artikel 30.1g i GDPR. Precis som i fallet med tidsfrister för radering så innebär inte omständigheten att något är svårt, omständligt eller tidsödande att det är omöjligt. Det bör i princip inte förekomma något fall där det inte är möjligt för bolaget att ge en allmän beskrivning av skyddsåtgärder.[13] Att beskrivningen ska vara allmän betyder att det inte finns något krav om att återge en detaljerad beskrivning av alla skyddsåtgärder.

Efter genomförd granskning konstaterar dataskyddsombudet att bolaget anger att rutiner och instruktioner finns. Uppgiften är dock inte tillräcklig enligt kriterierna i artikel 32.1. Av en allmän beskrivning av relevanta organisatoriska säkerhetsåtgärder för de rutiner och instruktioner som bolaget hänvisar till ska det alltid framgå vad rutinerna syftar till för att uppfylla de krav som finns på innehållet.

Bolaget rekommenderas därför att komplettera tekniska och främst relevanta organisatoriska säkerhetsåtgärder, tillse att uppgifterna förs in i registret för samtliga behandlingar och i en omfattning som tillgodoser kraven i GDPR.

2.2.3 Övriga iakttagelser

2.2.3.1 Rättslig grund och motivering

Dokumentation av uppgift om en behandlings rättsliga grund och motivering av den rättsliga grunden i behandlingsregistret är inget krav enligt artikel 30 i GDPR. Den rättsliga grunden är dock en utgångspunkt för att lagligen få behandla personuppgifter och alla behandlingar måste stödjas på en av de rättsliga grunderna i GDPR. Utan en rättslig grund är behandlingen inte laglig. Den personuppgiftsansvarige behöver, innan en behandling påbörjas, ha klart för sig vilken rättslig grund som tillämpas. Flera rättsliga grunder kan vara tillämpliga för en behandling, men utgångspunkten är att en behandling för ett ändamål bara kan vila på en (enda) rättslig grund[14]. Det följer också av informationsskyldigheten i artikel 13.1c och 14.1c i GDPR att den personuppgiftsansvarige ska informera den registrerade om den rättsliga grunden för en behandling. Eftersom uppgiften är något som den personuppgiftsansvarige ändå måste ha klart för sig rekommenderar

[13] Se Article 29 Working Party Guidelines on transparency under Regulation 2016/679 s 29, pt 59.
[14] Article 29 Working Party, Guidelines 05/2020 on consent under Regulation 2016/679 s. 25, pt 121: "*Article 6 sets the conditions for a lawful personal data processing and describes six lawful bases on which a controller can rely. The application of one of these six bases must be established prior to the processing activity and in relation to a specific purpose".*

dataskyddsombudet att den bör dokumenteras i behandlingsregistret, trots att det inte är obligatoriskt. Något som bolaget också hörsammat.

Dataskyddsombudets bedömning är att bolaget genomgående har begränsat sig till att hänvisa till en rättslig grund per behandling. Den absolut vanligaste hänvisningen är till den rättsliga grunden *avtal*, åtföljt av *rättslig förpliktelse och i något fall uppgift av allmänt intresse eller intresseavvägning* i enlighet med artikel 6 i GDPR. Dataskyddsombudet har dock anledning att ifrågasätta om avtal verkligen är korrekt som bolaget hänvisar till.

Bolaget rekommenderas därför att genomgående se över den rättsliga grunden för alla behandlingar och motivera sina val. I samband med kompletteringar och uppdatering av behandlingsregistret är rekommendationen också att tydliggöra och uppdatera all information till de registrerade.

3 Sammanfattande rekommendationer

Utifrån de förbättringsområden och brister som dataskyddsombudet har identifierat i kontrollen av bolagets behandlingsregister lämnas ett antal rekommendationer. Rekommendationerna framgår av punktlistan nedan. Dataskyddsombudet kommer särskilt följa upp vilka åtgärder som bolaget har vidtagit med anledning av rekommendationerna under kommande år. Bolaget rekommenderas också att ta stöd i sitt arbete med behandlingsregistret utifrån den vägledning som dataskyddsombudet sammanställer i den övergripande granskningsrapport som är gemensam för hela staden.

- Bolaget rekommenderas komplettera behandlingsregistret med behandlingar som saknas samt med uppgift om personuppgiftsansvarig, gemensamt personuppgiftsansvarig samt kontaktuppgifter till dessa.
- Bolaget rekommenderas åtgärda bristerna genom att involvera andra medarbetare i behandlingskartläggningen, ta fram och anta dokumenterade arbetssätt med tydlig intern ansvarsfördelning och därefter tillse att behandlingsregistret är komplett och uppdateras.
- Bolaget rekommenderas göra en genomgripande översyn av samtliga behandlingar med fokus på generell förbättring gällande behandlingsavgränsningen liksom ändamålsformuleringar.
- Bolaget rekommenderas genomgående utveckla beskrivningen av kategorier av registrerade och uppgifter, samt hur de relaterar till varandra.
- Bolaget rekommenderas göra en översyn av sitt register för att säkerställa att man anger alla specifika mottagare för samtliga behandlingar, inklusive interna mottagare, och att det i samtliga fall framgår varför mottagaren är mottagare.
- Bolaget rekommenderas kartlägga vilka faktiska överföringar som sker till tredjeland, i enlighet med vad som regleras i befintliga avtal, och därefter dokumentera överföringarna i sitt behandlingsregister.
- Bolaget rekommenderas åtgärda bristerna som saknas och ange vilka kriterier som används för att fastställa när uppgifterna inte är relevanta för ändamålet och när arkivering sker samt gällande uppgifter som bevaras förtydliga och ange att uppgifterna bevaras för arkivändamål.
- Bolaget rekommenderas komplettera tekniska och främst organisatoriska säkerhetsåtgärder för samtliga behandlingar.
- Bolaget rekommenderas se över den rättsliga grunden för behandlingarna och motivera sina val.
- Bolaget rekommenderas tydliggöra all information parallellt med komplettering och uppdatering av sitt behandlingsregister.

Information om fördjupad kontroll 2024

Behandlingsregister

Varje personuppgiftsansvarig ska föra ett register över behandlingar som utförts under dess ansvar. Behandlingsregistret är enligt artikel 30 i GDPR ett krav och ska kunna visas för tillsynsmyndigheten vid efterfrågan. I artikel 30 framgår också vilken information som ska finnas i registret över personuppgiftsbehandlingar. Där framgår bland annat att registret ska innehålla information om ändamål med behandlingen, kategorier av registrerade och personuppgifter, samt huruvida överföring av personuppgifter till tredjeland sker.

Varför behandlingsregistret kontrolleras

Dataskyddsenheten genomförde under våren 2023 en informationsinsats angående behandlingsregister över behandlingar enligt artikel 30 i GDPR. Syftet med informationsinsatsen var att höja kunskapen inom området och skapa enhetlighet inom Göteborgs Stad, och i förlängningen tillse att stadens verksamheter har behandlingsregister som uppfyller kraven i GDPR. Som uppföljning på denna informationsinsats görs 2024 en fördjupad kontroll av förvaltningars och bolags efterlevnad av artikel 30 i GDPR, och därigenom skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett behandlingsregister.

I skäl 82 framgår att personuppgiftsansvariga ska föra register över behandlingar som sker under deras ansvar för att kunna påvisa att GDPR följs, arbetet med behandlingsregistret är alltså kopplat till ansvarsskyldigheten. Utöver ansvarsskyldigheten utgör behandlingsregistret grunden i ett systematiskt dataskyddsarbete. Om en verksamhet inte har kännedom och kunskap om de behandlingar som sker under dess ansvar är det till exempel svårt att kunna tillgodose de registrerades rättigheter, fullgöra den personuppgiftsansvariges informationsplikt, samt att anta ett riskbaserat arbetssätt. Det är därför av yttersta vikt att verksamheten dokumenterar sina behandlingar korrekt i behandlingsregistret och kontinuerligt håller registret uppdaterat.

Kontrollen avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett behandlingsregister.

Urval

Den fördjupade kontrollen kommer att genomföras för ett antal förvaltningar och bolag som dataskyddsombudet anser utgör ett representativt urval för stadens verksamheter med en bred spridning.

För 2024 kommer följande verksamheter att ingå i den fördjupade kontrollen:

- Utbildningsförvaltningen
- Socialförvaltningen centrum
- Äldre samt vård- och omsorgsförvaltningen
- Stadsmiljöförvaltningen

- Miljöförvaltningen
- Renova AB
- Bostads AB Poseidon
- Störningsjouren i Göteborg AB
- Liseberg AB

Tillvägagångssätt

Den fördjupade kontrollen kommer genomföras i två steg. Steg ett genomförs i form av en skrivbordskontroll, genom att de deltagande förvaltningarna och bolagen får svara på ett antal kontrollfrågor och tillhandahålla sitt behandlingsregister, dokumentation i form av roll och ansvarsbeskrivningar, samt dokumenterade arbetssätt gällande hur verksamheten arbetar med att säkerställa att man har ett fullständigt och uppdaterat behandlingsregister i enlighet med kraven i artikel 30 i GDPR.

Dataskyddsombudet kommer därefter granska hela behandlingsregistret för att kontrollera om de registrerade behandlingarna uppfyller kraven enligt artikel 30 i GDPR. Dataskyddsombudet kommer också granska verksamheternas organisation avseende arbetet med behandlingsregistret i form av de roll/ansvarsbeskrivningar samt dokumenterade arbetssätt som verksamheten tillhandahåller dataskyddsombudet. Dataskyddsombudet kommer sedan i steg två att lämna sina rekommendationer direkt till verksamheten avseende eventuella åtgärder som dataskyddsombudet bedömer behöver genomföras i arbetet med behandlingsregistret utifrån organisation, fastställande av roller och ansvar, samt dokumenterade arbetssätt för att säkerställa att registret uppfyller kraven i artikel 30 och hålls kontinuerligt uppdaterat.

Dataskyddsombudet kommer också direkt tillsammans med respektive deltagande bolag och förvaltning gå igenom verksamhetens behandlingsregister och i dialog med verksamheten påvisa och förklara eventuella förbättringsområden/brister genom ett eller flera uppföljningsmöten. Syftet med denna metod är att få till en lärandeprocess utöver dataskyddsombudets rent kontrollerande funktion. Dataskyddsenhetens målsättning är att efter genomförd kontroll ska samtliga deltagande verksamheter ha förutsättningar för att uppnå en godtagbar nivå på behandlingsregistret, samt att med stöd av dataskyddsombudens rekommendationer ha fått vägledning i hur arbetet med att hålla registret aktuellt kan utformas.

Tid för utskick

Under v. 35 kommer steg ett av kontrollen att skickas ut till de verksamheter som ingår i den fördjupade kontrollen.

Rapportering

Dataskyddsombudets iakttagelser, synpunkter och rekommendationer kommer sammanfattas i en rapport till respektive deltagande verksamhet. Dataskyddsombudet kommer även sammanfatta sina iakttagelser på övergripande nivå med syfte att identifiera sådant som generellt sett kan vara till hjälp för stadens verksamheter i arbetet med sina behandlingsregister.

Frågor?

Eventuella frågor hänvisas till dataskyddsenhetens funktionsbrevlåda, dso@intraservice.goteborg.se.

Kontrollfrågor om behandlingsregistret

Vänligen besvara frågorna så utförligt och detaljerat som möjligt. Bifoga hela behandlingsregistret i Excel-format samt även de dokument och rutiner som beskriver hur ni organiserat ert arbete med behandlingsregistret och visar hur roller och ansvar har fastställts för att säkerställa att registret uppfyller kraven i artikel 30 i GDPR, att det hålls uppdaterat, att samtliga behandlingar finns med och hur ni säkerställer att nya eller förändrade behandlingar förs in i registret.

Svaren ska ha inkommit till dataskyddsombudet (dso@intraservice.goteborg.se) **senast den 11 september 2024**.

Frågor om kontrollen hänvisas till dso@intraservice.goteborg.se

1. Roller och ansvar

1.1 Har ni dokumenterat utpekade roller och ansvar för att säkerställa att behandlingsregistret uppfyller kraven i art. 30?

☒Ja ☐Nej ☐Vet ej

1.2 Har ni dokumenterat utpekade roller och ansvar som tydligt fastställer ansvaret för att säkerställa att nya personuppgiftsbehandlingar upptas i registret samt att det hålls uppdaterat vid förändringar i befintliga behandlingar?

☒Ja ☐Nej ☐Vet ej

2. Obligatorisk information i behandlingsregistret

2.1 Är all information enligt artikel 30 i dataskyddsförordningen komplett för personuppgiftsbehandlingarna i registret (de obligatoriska fälten)?

☒Ja ☐Nej ☐Vet ej

2.2 Hur stor del av de personuppgiftsbehandlingar som utförs i verksamheten uppskattar ni finns upptagna i ert behandlingsregister?

☐0-25 % ☒25-50 % ☐50-75 % ☐75-100 %

Om ni inte dokumenterat alla personuppgiftsbehandlingar, vet ni inom vilka verksamhetsområden ni saknar dokumenterade behandlingar? Beskriv nedan.

Vi har i dagsläget inte koll på inom vilka områden som vi saknar personuppgiftsbehandlingar.

3. Dokumenterade arbetssätt

3.1 Finns det dokumenterade arbetssätt för att säkerställa att ni kontinuerligt uppdaterar behandlingsregistret med nya och förändrade personuppgiftsbehandlingar?

☒Ja ☐Nej ☐Vet ej

4. Användning och översyn av behandlingsregistret

4.1 Använder ni behandlingsregistret som en naturlig del i det systematiska arbetet med dataskydd? Beskriv nedan hur och när det används eller varför inte.

☐Ja ☒Nej ☐Vet ej

Verksamheten är inte på den nivån att vi kan använda oss av behandlingsregister som en naturlig del av ett systematiskt arbete.

4.2 Har anställda i er förvaltning/bolag kännedom om behandlingsregistret och tillgång till det vid behov? Beskriv nedan varför/varför inte samt hur behandlingsregistret tillgängliggörs inom verksamheten.

☒Ja ☒Nej ☐Vet ej

Svaret på frågan är både jag och nej, eftersom anställda har kännedom om att behandlingsregister finns, men tillgängligheten ser olika ut.
I dagsläget är det informationssäkerhetshandläggare som ska kontaktas vid antingen upprättandet eller uppdatering av behandlingsregister. Ambitionen är för tillfället inte heller att verksamheten ska ha tillgång, eftersom kunskapen och förståelsen för hur man fyller i och besvarar frågorna inte är tillräcklig.

4.3 När gjorde ni senast en översyn av behandlingsregistrets innehåll?
Beskriv nedan.

Våren 2024

Renova	Inkommande förfrågningar för personuppgifter	ID-nr: R0350
	Fastställare: Elin Ekfeldt	Dokumenttyp: Rutin
	Handläggare: Frida Eilertsson	Senast fastställt: 2024-05-27

Inkommande förfrågningar för personuppgifter

Syfte

Säkerställa att vi på Renova hanterar inkomna förfrågningar om personuppgifter på ett säkert sätt som även uppfyller gällande lagstiftning.

Omfattning

Hela Renovas verksamhet omfattas av rutinen.

Beskrivning

När en förfrågan om personuppgifter inkommer

En begäran om registerutdrag kan komma in via e-post, vanlig post, muntligen, telefon eller på annat sätt. Oavsett hur förfrågan inkommer ska du kontakta säkerhetsenheten på dataskyddsarenden@renova.se.

Håll leveransdatum

Utdraget ska normalt sett lämnas ut inom 30 dagar från att begäran kommit in. Lämna registerutdraget i tid, annars riskerar Renova ett tillsynsärende och kritik från tillsynsmyndighet.

Ansvarig chef eller vid behov Säkerhetsenheten ska:

Ställa en kontrollfråga för att undvika merarbete

Är eller har den som begär information varit anställd hos Renova? Kontakta HR och Lön, så vet du om det är relevant att leta i register som rör personal eller om sökningarna skall ske i kundregister.

Begär kompletterande information

Kan du identifiera den person som begär registerutdrag i era IT-system? Om inte, begär in kompletterande information. Var noga med att inte avslöja om den omfrågade personen finns i era register om du inte är helt säker på vem du kommunicerar med.

Fråga hur den registrerade vill ta emot personuppgifterna

Det finns tre sätt för Renova att lämna ut handlingar på:

a) Via den mejladress som den registrerade uppgett vid identitetskontrollen – gäller ej när det rör sig om känsliga personuppgifter.
b) Via post till folkbokföringsadressen
c) Personligt överlämnande

Kontrollerar den registrerades identitet

Ansvarig chef eller vid behov Säkerhetsenheten ska svara den registrerade direkt och bekräfta att Renova har tagit emot ansökan. Är det en anställd är identiteten enkel att kontrollera och är det en extern person behöver personen komma till Renova för att identifiera sig med en godkänd ID-handling. Tänk på att det är mycket viktigt att säkerställa mottagarens identitet. En enskild individs personuppgifter ska absolut inte skickas till fel person.

Ta fram innehållet

Att ta fram ett registerutdrag handlar om att plocka ut de faktiska uppgifterna, inte bara informationen om den. Utdraget kan levereras i form av utskrifter, textfiler, skärmdumpar eller annat, beroende på vad som passar i det aktuella fallet.

Hämta in information från organisationen

Det är dataskyddsarenden@renova.se som ansvarar för att sända e-post till kontaktpersonerna i registerförteckningen. Det kan vara svårt att avgöra hur mycket tid vi egentligen måste lägga ner för att leta efter personuppgifter till ett registerutdrag, men arbetsinsatsen ska vara rimligt ställt i relation till begäran.

Tänk också på att rätten till tillgång även omfattar sådan information som finns i fritextfält och i löpande text. Vanligt förekommande sökfunktioner för att hitta uppgifterna ska kunna användas, men i de fall Renova inte kan identifiera den registrerades uppgifter kan vi inte heller lämna ut dem.

Se över informationen

Titta på den information som kommit in från kontaktpersonerna. Tänk på att all information som finns registrerad måste lämnas ut. Det är inte ett alternativ att låta bli att lämna ut information som man har lagrad om en person när han eller hon begärt ett utdrag.

Rensa bort information om andra personer

Kontrollera att informationen inte innehåller uppgifter om någon identifierbar tredje person. Registerutdraget ska bara tala om vad som finns registrerat om den som begär registerutdrag, inte om andra enskilda personer.

Använd följebrev

Vid sidan om själva registerutdraget ska det bifogas ett följebrev som ska innehålla information om:

- Varför personuppgifterna behandlas (ändamålet)
- Vilka kategorier av personuppgifter vi har behandlat.
- Om vi lämnat ut personuppgifterna och i sådana fall till vilka kategorier av mottagare.
- Hur länge vi avser att behandla uppgifterna.
- Om uppgifterna förs över till tredje land eller en internationell organisation, i sådana fall vart och vilka skyddsåtgärder som vidtagits med anledning av det.
- Individens rättigheter, vilket kan vara att rätta, begränsa eller invända mot behandlingen av dennes personuppgifter samt rätt till att radera sina personuppgifter och inge klagomål till tillsynsmyndighet.
- Källan som uppgifterna hämtas från (om man inte samlar in informationen själv).

Detta tar den/de som ansvarar för dataskyddsarenden@renova.se fram.

Posta brevet eller sänd till mejladressen

Skicka aldrig utdraget till en adress eller e-postadress där ni inte har säkerställt att mottagaren faktiskt är rätt person.

Är du det minsta osäker, använd folkbokföringsadressen. Försändelser som skickas med post ska dessutom skickas med rekommenderat brev om det innehåller känsliga personuppgifter.

Diarieför informationen

Efter det att informationen överlämnats till den registrerade skall både all kommunikation och mejlkonversationer mellan Renova och den registrerade samt den information som överlämnats skickas till diariet.

CHECKLISTA FÖR GDPR OCH DATASKYDD

☐ **Spara information på rätt plats.** Använd avsedda system (LIS Diarium, Agda, Visma Recruit, IFS, Sharepoint, T-katalogen osv) Ha inte kopior sparade lokalt eller på andra platser.

☐ **Arbetsmaterial (yngre än 3 månader) kan tillfälligt sparas på H-katalog.** Gäller dokument som innehåller personuppgifter eller annan skyddsvärd/känslig information. Därefter ska det flyttas till rätt system eller till T-katalogen.

☐ **Kontrollera behörigheter.** Kontrollera behörigheterna i mappar på T-katalog och i dina system. Enbart personer som *behöver informationen för att kunna utföra sitt arbete* ska ha informationen.

☐ **Rensa!** Rensa bland dina dokument, vi får bara spara sådant som vi *behöver* för att kunna utföra vårt jobb. Undantag är allmän handling där vi måste följa de gallringsbeslut som framgår av dokumenthanteringsplanen.

☐ **Rensa mejlen regelbundet**. Tänk på att innehållet i din Outlook kan begäras ut.

☐ **Anmäl alla behandlingar med personuppgifter.** Om du har listor/register som innehåller personuppgifter måste dessa anmälas in. Exempel på sådana listor kan vara kundregister, lönelistor, bemanningslistor, listor över personer med särskilda behörigheter osv. Ta kontakt med Säkerhetsenheten så hjälper vi dig.
Dataskyddsarenden@renova.se

☐ **Lås alltid din dator när du lämnar den.**

☐ **Tänk på att** inte ha papper innehållandes personuppgifter framme på ditt skrivbord.

☐ **Om du upptäcker eller misstänker personuppgiftsincident,** följ rutinen för personuppgiftsincident.