Göteborgs Stad

Årsrapport för dataskyddsarbetet 2024

Liseberg 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

Under året har kontakten mellan dataskyddsombudet och bolaget varit relativ begränsad. Kontakten har främst utgjorts av deltagande vid bolagets gruppmöten inom dataskydd, där representanter från olika verksamhetsområden deltar. Det är positivt att dataskyddsombudet blir inbjuden och något som bolaget uppmuntras att fortsätta med. Samtidigt är dataskyddsombudets uppfattning att formerna för dataskyddsombudets involvering fortsatt behöver utvecklas. I årsrapporten 2023, under kontrollpunkt 1: Dataskyddsorganisationen, identifierade dataskyddsombudet en risk i att dataskyddsombudet ej involveras i tillräcklig utsträckning i det interna dataskyddsarbetet. Rekommendation om att framåt se över hur verksamheten kan involvera dataskyddsombudet mer i arbetet med dataskydd kvarstår med anledning av detta. Detta med syftet att säkerställa att bolaget uppfyller sin skyldighet enligt artikel 38.1 i GDPR gällande att involvera dataskyddsombudet i alla frågor som gäller dataskydd.

4 Granskning av dataskyddsarbetet 2024

4.1 Fördjupad kontroll 2024

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

Dataskyddsombudets samlade bedömning är att behandlingsregistret delvis innehåller den information som föreskrivs enligt art. 30 i GDPR och anser att det finns delar som behöver kompletteras eller förtydligas. Dataskyddsombudet anser, i ett första steg, att ett särskilt fokus behöver läggas på att formulera tydliga, konkreta och specifika ändamål. Genom att göra detta bör det bli tydligare vilken laglig grund som bolaget kan stödja sin behandling på. Även beskrivning av de kategorier av personuppgifter och kategorier av registrerade som förekommer i de olika behandlingarna, tidsfrister för radering av personuppgifter och en allmän beskrivning av säkerhetsåtgärder behöver förtydligas.

För samtliga rekommendationer, se granskningsrapporten bilaga 2.

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: Register över personuppgiftsbehandlingar

Verksamheten gavs följande rekommendationer:

- Arbeta med att revidera behandlingsregistret och säkerställ att behandlingarna är definierade och avgränsade på ett ändamålsenligt sätt. Kontrollera för respektive behandling att informationen uppfyller kraven enligt art. 30 i GDPR.

Kommentarer och rekommendationer:

Under året har verksamheten meddelat att det pågår ett arbete med behandlingsregistret, vilket är ett arbete som påbörjades redan 2023. I samband med uppföljningen uppger verksamheten att arbetet påbörjades i systemstödet Draftit. Verksamheten upplevde dock att upplägget i systemstödet var otydligt med många och omfattande frågor som behövdes besvaras. Arbetet pausades mot bakgrund av Oceana-branden. Vid tidpunkten för uppföljningen hade verksamhet återupptagit arbetet med behandlingsregistret. Verksamheten har dock frångått att arbeta i systemstödet då det inte har bedömts som ändamålsenligt. I arbetet ser verksamheten dels över hur behandlingarna är avgränsade och definierade, dels så har ett nytt formulär för behandlingsregistret anpassat till bolaget tagits fram.

Bolaget har ingått i dataskyddsombudets fördjupade kontroll 2024. För dataskyddsombudets rekommendationer, se granskningsrapporten, bilaga 2. Bolaget rekommenderas att arbeta utifrån dataskyddsombudets lämnade rekommendationerna i bolagets granskningsrapport.

Fokusområde 2: IT-system och digitala verktyg

Verksamheten gavs följande rekommendationer:

- Då de rekommendationer som lämnades i årsrapporten 2022 gällande bolagets cookiehantering inte har omhändertagits rekommenderas bolaget under 2024 att prioritera arbetet med att se över och vidta åtgärder för att säkerställa att användningen av cookies på bolagets hemsida uppfyller kraven enligt såväl dataskyddsförordningen som LEK (lagen (2022:482) om elektronisk kommunikation).

Kommentarer och rekommendationer:

Under året har verksamheten gjort justeringar avseende cookies. Bland annat har den visuella utformningen av samtyckesknapparna ändrats. Alternativen för att acceptera alla cookies och tack nej till icke-nödvändiga cookies är numera likvärdiga.

Vid en översiktlig översyn av bolagets hemsida bedömer dataskyddsombudet fortsatt att cookiehantering behöver ses över. Bland annat behöver bolaget säkerställa att samtycken som inhämtas är informativa, att det är lika lätt att återkalla som att ge samtycke och att alla cookies som har kategoriserats som nödvändiga faktiskt omfattas av undantaget i 9 kap. 28 §, lag (2022:482) om elektronisk kommunikation. Vid arbetet med cookiehanteringen rekommenderas bolaget att ta del av Post- och telestyrelsens (PTS) tillsynsbeslut avseende cookiehantering från 2023. Bolaget kan även kontakta dataskyddsombudet för verksamhetsspecifika rekommendationer.

Dataskyddsombudet kommer fortsättningsvis följa bolagets arbete med rekommendationen, men rekommendationen kommer inte att följas upp särskilt i samband med årsrapporten 2025, om inget föranleder att det behöver följas upp separat.

4.2.2 Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller

Dataskyddsombudet har under året följt upp vilka åtgärder som vidtagits avseende tidigare års lämnade rekommendationer av gjorda kontroller.

Kontroll (2022): Kamerabevakning

Verksamheten gavs följande rekommendationer:

- Omhänderta de rekommendationer som dataskyddsombudet tidigare lämnat gällande bolagets kamerabevakning (se punkt 3.3.1 i årsrapporten 2023).

- Säkerställ att kamerabevakningen på den nya anläggningen uppfyller gällande lagkrav och att nödvändig dokumentation finns på plats inför öppningen.

Kommentarer och rekommendationer:

Uppföljningen visar att det pågår ett arbete med att se över kamerabevakningen inom verksamheten. Bland annat uppger bolaget att det sker interna dialoger. Verksamheten arbetar även med att sammanställa dokumentationen kring kamerorna på ett enhetligt sätt. När underlaget är sammanställt kommer det att översändas till dataskyddsombudet. Dataskyddsombudet ser det som positivt att arbete pågår och bolaget rekommenderas att särskilt arbeta med rekommendationerna 2025. Då uppföljningen visar att arbetet är pågående kvarstår rekommendationer som tidigare har lämnats och uppföljning kommer att ske 2025.

Då det pågår arbete kring lagändringar avseende tillståndsplikt på nationell nivå rekommenderas bolaget att följa rättsutvecklingen på området. Fram till att eventuella lagändringar har trätt i kraft kvarstår dock dataskyddsombudets rekommendation kring att motivera och dokumentera gjorda bedömningar avseende tillståndsplikt.

5 Rekommenderade fokusområden 2025

Dataskyddsombudet har under arbetet med årsrapporten identifierat ett antal områden som verksamheten rekommenderas att särskilt arbeta med under det kommande året. Dessa 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 1: Dataskyddsorganisation

Se över hur verksamheten kan involvera dataskyddsombudet mer i arbetet med dataskydd, med syftet att säkerställa att bolaget uppfyller kravet enligt artikel 38.1 i GDPR gällande att involvera dataskyddsombudet i alla frågor som gäller dataskydd.

- Kontrollpunkt 4: Registret över personuppgiftsbehandlingar

Ta del av granskningsrapporten från dataskyddsombudets fördjupade kontroll och arbeta med behandlingsregistret utifrån rekommendationerna som framgår av granskningsrapporten.

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 Liseberg 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	Direktiv för hantering av personuppgifter och dataskydd
Bilaga 4	Anvisningar Lisebergs hantering av personuppgifter och dataskydd

2 Fördjupad kontroll

2.1 Resultat av granskning av dokumenterade arbetssätt

2.1.1 Dataskyddsombudets bedömning

På dataskyddsombudets kontrollfrågor har bolaget angett att det finns utpekade roller och ansvar dokumenterade för att säkerställa att kraven i artikel 30 i GDPR uppfylls. Det framgår dock av samma kontrollfrågor att det saknas 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.

Bolaget uppger även att det saknas dokumenterade arbetssätt för att säkerställa att bolaget kontinuerligt uppdaterar behandlingsregistret med nya och förändrade personuppgiftsbehandlingar.

Bolaget har skickat in ett dokument som heter ”DIREKTIV FÖR HANTERING AV PERSONUPPGIFTER OCH DATASKYDD Dnr 23-0216 antagen 2023-05-15”. I det framgår de antagna direktiven för hur bolaget ska arbeta med personuppgifter och dataskydd.

I det inskickade dokumentet ”Anvisningar Lisebergs hantering av personuppgifter och dataskydd Dnr 23-0262 antagen 2023-05-23.” beskriver bolaget hur personuppgifter ska hanteras för att säkerställa att personuppgifter hanteras i enlighet med dataskyddslagstiftningen. Dataskyddsombudet anser att dessa arbetssätt, om de efterföljs, är tillräckliga för att säkerställa att kraven i artikel 30 i GDPR uppfylls.

Bedömningen som gjorts utifrån det inskickade materialet är dock att de dokumenterade arbetssätten inte efterföljs av bolaget. Bolaget rekommenderas därmed att vidta åtgärder för att säkerställa att arbetssätten får genomslag i praktiken.

2.2 Resultatet av granskning av behandlingsregister

2.2.1 Dataskyddsombudets bedömning

Av Lisebergs svar framgår att de har påbörjat ett arbete med framtagning av nytt behandlingsregister. Dataskyddsombudet har utgått från bolagets nuvarande behandlingsregister i kontrollen.

Bolaget uppskattar att ca 75–100 % av bolagets behandlingar är upptagna i behandlingsregistret.

Bolaget uppger att behandlingsregistret inte uppfyller kraven för all information som ett behandlingsregistret ska innehålla enligt artikel 30 i GDPR. Dataskyddsombudet delar bolagets bedömning. För närmare iakttagelser från dataskyddsombudet av informationen som behöver finnas med i behandlingsregistret enligt artikel 30 i GDPR hänvisar dataskyddsombudet till avsnitt 2.2.1 i den här rapporten. Dataskyddsombudet vill uppmärksamma att flera iakttagelser och råd som lämnats kopplat till det befintliga behandlingsregistret är aktuella i arbetet med det nya behandlingsregistret.

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 Liseberg tillhandahållit dataskyddsombudet innehåller inte dessa uppgifter, 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.[1]

Liseberg rekommenderas att komplettera sitt behandlingsregister med uppgift om personuppgiftsansvarig och dataskyddsombud samt kontaktuppgifter till dessa. Exakt hur Liseberg väljer att utforma detta är upp till verksamheten att avgöra, antingen i kolumner vid varje behandling eller som en övergripande information i inledningen.

2.2.2.2 Ändamålen med behandlingen

Enligt artikel 30.1b i GDPR ska behandlingsregistret innehålla *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. [2] 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

[1] Jämför med, Article 29 Working Party Guidelines on transparency under Regulation 2016/679 s.35
[2] Integritetsskyddsmyndigheten, Innovationsportalen, IMY - innovationsportalen (hämtad 2024-11-20). Begreppen ”tydligt, konkret och specifikt” kan relateras till de tidigare nämnda begreppen ”särskilda, uttryckligt angivna och berättigade ändamål”.

ändamål. Om ändamålet saknar tillräcklig precision, går det inte att bedöma om personuppgifterna är adekvata och relevanta, eller om för många personuppgifter behandlas.[3] 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 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 bolaget saknar tillräckligt precisa och uttryckligt angivna ändamål. För flera av behandlingarna anger bolaget vilka dokument som hanteras. För andra behandlingar anges endast att något hanteras. I en majoritet av fallen är det svårt att se sambandet mellan varför personuppgifter behandlas och ändamålet med behandlingen. Ändamålen är alltså varken tydliga, konkreta eller specifika.

Dataskyddsombudet rekommenderar att bolaget tar ett helhetsgrepp i frågan och gör en genomgripande översyn av samtliga ändamålsformuleringar i registret och av 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. Det räcker alltså inte att bara ange vilka kategorierna är, utan läsaren ska av *beskrivningen* förstå vad kategorierna innefattar. Alltså vilka uppgifterna är, vilka de registrerade är, och hur de

[3] Öman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 5.1b.

relaterar till varandra.[4] Beskrivningen i artikelns led c behöver således 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.

Bolaget uppger kategorier av registrerade och kategorier av personuppgifter för samtliga sina behandlingar. Dataskyddsombudet anser dock att det som anges inte uppfyller ovanstående krav. Dataskyddsombudets bedömning är att kategorier av registrerade och kategorier av personuppgift inte 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. I vissa fall anger bolaget kategorier som ”andra” eller ”invånare”, vilket gör det svårt att förstå vad kategorierna innefattar. Likaså när kategorierna ”leverantör” eller ”kunder” anges.

Bolaget rekommenderas att genomgående i sitt behandlingsregister utveckla beskrivningen av kategorier av registrerade och personuppgifter på ett sådant sätt att det av beskrivningen framgår vilka uppgifter som behandlas om vilka registrerade.

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. Efter genomförd granskning kan dataskyddsombudet konstatera att uppgift om interna mottagare, alltså funktioner inom bolagets egen organisation, genomgående saknas. Dataskyddsombudet har förståelse för att uppgiften om interna mottagare inte dokumenterats i bolagets register. Detta eftersom formuleringen i artikel 30.1d om att *personuppgifterna har lämnats eller ska lämnas ut,* tillsammans med formuleringen *utlämnas* i definitionen av mottagare i artikel 4.9, i den svenskspråkiga versionen av GDPR, gör att dataskyddsombudet tidigare gjort bedömningen, att den personuppgiftsansvariges personal inte kan anses vara

[4] Se EDPB:s behandlingsregister EDPB records of processing activities - Access to documents request (hämtad 2024-11-27) 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.

mottagare eftersom det kan ifrågasättas huruvida personuppgifter verkligen lämnas ut om de hanteras inom en förvaltning eller ett bolag.[5]

Under arbetet med den fördjupade kontrollen har dataskyddsombudet gjort en förnyad bedömning utifrån ny vägledning från EDPB[6], vägledning utifrån de europeiska tillsynsmyndigheternas egna register[7], och det faktum att formuleringen utlämnas inte förekommer i den engelska, eller flera andra språkversioner av GDPR.[8]. Dataskyddsombudets bedömning är att definitionen i artikel 4.9 inte ska läsas på annat sätt än att begreppet mottagare även omfattar den personuppgiftsansvariges egen organisation, en tolkning som också finner stöd i förarbetena till personuppgiftslagen.[9]

För att uppfylla kraven i artikel 30.1d i GDPR rekommenderas därför bolaget att dokumentera vilka interna avdelningar/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.[10].

Dataskyddsombudet anser att när en personuppgift tillgängliggörs för en mottagare så ska det av behandlingsregistret, som bästa praxis, framgå varför mottagaren är just mottagare.[11] Det vill säga att om mottagaren till exempel är ett personuppgiftsbiträde eller underbiträde så ska det dokumenteras i registret.

I bolagets behandlingsregistret anges specifika mottagare i vissa fall. I andra fall anges kategorier av mottagare. Dataskyddsombudet vill 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[12], 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 alla specifika mottagare för samtliga

[5] Se Öhman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 4.9.
[6] EDPB, Data protection guide for small business, EDPB: Data protection guide for small business (hämtad 2024-11-26).
[7] Se till exempel i EDPB:s och EDPB:s behandlingsregister, EDPS record of processing activity - Personal Data Breach Notification, EDPB records of processing activities - Data subjects rights (hämtad 2024-11-27).
[8] 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 så som EDPB uttrycker det i EDPB: Data protection guide for small business (hämtad 2024-11-27).
[9] Se Öman, 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”.*
[10] Se EU-domstolens förhandsavgörande i mål C-579/21, C-579/21.
[11] Se EDPB:s behandlingsregister för ett konkret exempel, EDPB records of processing activities - Access to documents request (hämtad 2024-11-27). Se också mål C-154/21.
[12] Se mål C-154/21

behandlingar anges, 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 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. Det är inte tillräckligt att veta ”på ett ungefär”, utan det är dom faktiska överföringarna som bolaget ska redogöra för. Bolaget har till exempel angett att en överföring av personuppgifter sker till USA som en följd av en biträdesrelation för samtliga behandlingar som utförs med stöd av någon del av M365.

Dataskyddsombudet utesluter inte på något sätt att personuppgifter faktiskt överförs till USA vid biträdesrelationer med detta biträde/underbiträde, det går dock inte att förutsätta att så sker bara för att biträdet råkar ha sin juridiska hemvist i just USA. Beroende på vilken typ av tjänst det avtalats om så kan det vara så att ingen överföring av personuppgifter utanför Europa sker överhuvudtaget, att överföring sker till just USA, eller att överföring inte sker till USA, men väl till flera andra tredjeländer, som Indien, Kina, Malaysia med flera, till exempel för support och liknande ändamål.

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.

Rekommendationen från dataskyddsombudet blir därför att se över de behandlingar där frågan om överföring till tredje land besvarats med ”vet ej” ses över.

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”.[13] Viktigt att notera är även att tidsfristerna ska anges för de olika kategorierna av personuppgifter och inte för behandlingen som helhet eller per handlingstyp.

Dataskyddsombudet vill här särskilt förtydliga att artikel 30.1f föreskriver att det är tidsfristerna som ska anges. Det är inte tillräckligt att, som bolaget gör i flera fall, hänvisa till att gallringsbeslut saknas, eller att det finns rensningsrutiner. Detta helt enkelt eftersom ett sådant förfarande inte uppfyller kravet om att ange tidsfrister, utan endast informerar om att beslut om gallring finns (eller saknas).

Det är inte heller meningen att berörda tillsynsmyndigheter, eller andra som vill ta del av registrets innehåll, ska behöva söka upp den obligatoriska informationen i andra källor. Dataskyddsombudets uppfattning är att om regleringen hade gett utrymme för en sådan hänvisning till andra dokument, så hade det uttryckts i artikel 30 i GDPR. Av de europeiska dataskydds-myndigheterna EDPB[14] och EDPS[15] register framgår de faktiska tidsfristerna direkt i registret, det samma gäller för den svenska tillsynsmyndighetens (IMY) eget register.[16]

Mot bakgrund av ovan rekommenderar dataskyddsombudet att bolaget anger de förutsedda 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.[17] Att beskrivningen ska vara allmän betyder att det inte finns något krav om att återge en detaljerad beskrivning av alla skyddsåtgärder.[18]

Att beskrivningen ska vara allmän betyder att det inte finns något krav om att återge en detaljerad beskrivning av alla skyddsåtgärder. Det är dock inte tillräckligt att endast ange att säkerhetsåtgärder finns på plats. Efter genomförd

[13] 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”.*
[14] Se exempel i EDPB:s behandlingsregister EDPB records of processing activities - Access to documents request (hämtad 2024-11-27).
[15] Se exempel i EDPS:s behandlingsregister EDPS record of processing activity - Whistleblowing procedure (hämtad 2024-11-27).
[16] Se IMY:s förteckning över personuppgiftsbehandlingar (aktuell version från 2024-10-23
[17] Se Article 29 Working Party Guidelines on transparency under Regulation 2016/679 s. 29, pt 59.
[18] Se till exempel i EDPS:s och EDPB:s behandlingsregister: EDPS record of processing activity - Staff recruitment, EDPS record of processing activity - Personal Data Breach Notification, EDPB records of processing activities - Data subjects rights (hämtad 2024-11-27).

granskning konstaterar dataskyddsombudet att det genomgående saknas en allmän beskrivning av organisatoriska säkerhetsåtgärder för behandlingarna.

Bolaget hänvisar till ” IT-Säkerhetsdirektiv. Uppdaterades senast 2016-06-30.” men specificerar inte ytterligare vad det innebär för säkerhetsåtgärder.

Bolaget rekommenderas att komplettera behandlingsregistret med allmänna beskrivningar av samtliga vidtagna tekniska och organisatoriska säkerhetsåtgärder 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.[19]

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 dataskyddsombudet att den bör dokumenteras i behandlingsregistret, trots att det inte är obligatoriskt.

Bolaget anger rättslig grund för samtliga behandlingar i behandlingsregistret. För flera av behandlingarna saknas dock en motivering till den rättsliga grunden. Vidare anges flera rättsliga grunden för flera av behandlingarna.

En behandling kan avgränsas på olika sätt, dataskyddsombudet anser att ändamålet bör vara vägledande för avgränsningen av en behandling och att stadens verksamheter för funktionalitetens skull bör begränsa sig till ett ändamål för en behandling i behandlingsregistret. Det finns samtidigt inget förbud mot att konstruera behandlingar med flera närliggande ändamål. I sådana fall kan flera rättsliga grunder anges. En förutsättning för det är dock att varje enskilt ändamål är tydligt, konkret och specifikt och går att knyta till en rättslig grund, enligt devisen att personuppgifter bara kan behandlas för ett ändamål med stöd av en (enda) rättslig grund. Det ska också framgå vilka kategorierna

[19] 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”.* Se också Öman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 6. *Vidare anser Artikel 29-gruppen att en behandling av personuppgifter för ett ändamål bara kan ha en (enda) rättslig grund.*

av registrerade och personuppgifter är för dom enskilda ändamålen. Dvs. under kategori av registrerade och kategori av personuppgifter måste den personuppgiftsansvarige även beskriva vilka kategorier som hänför sig till vilka ändamål.[20] Att bygga mycket komplexa behandlingar med flera deländamål riskerar därför snabbt att bli väldigt rörigt.

Ett sådant upplägg kräver enligt dataskyddsombudets mening att de enskilda delarna av behandlingen preciseras på en sådan nivå att de ändå hade kunnat utgöra en egen post i behandlingsregistret, det hade dessutom blivit betydligt enklare att hålla reda på vad de olika behandlingarna faktiskt innefattar. Dataskyddsombudet avråder därför i normalfallet starkt från en sådan uppdelning då det helt enkelt kommer vara mycket svårt för verksamheten att hålla reda på vilka personuppgifter i behandlingen som behandlas med stöd av-vilken rättslig grund och för vilket ändamål.

Något som ytterligare talar emot att det är funktionellt att bygga väldigt komplexa behandlingsprocesser med flera rättsliga grunder är att det kommer vara svårt att informera de registrerade på ett korrekt sätt. Informationsskyldigheten i artikel 13.1c och 14.1c I GDPR kräver ju att den personuppgiftsansvarige tydligt informerar den registrerade om ändamålen med behandlingen och den rättsliga grunden. Om flera rättsliga grunder anges som stöd för behandlingen behöver verksamheten ändå definiera vilka uppgifter och delar av ändamålet som hänför sig till vilken av de rättsliga grunderna, vilket gör att det är svårt att se poängen med att bygga upp komplexa behandlingar med omfattande och svepande ändamålsbeskrivningar och flera rättsliga grunder.

Även möjligheten att på ett korrekt sätt hantera de registrerades rätt till radering i artikel 17 i GDPR och rätten att göra invändningar i artikel 21 i GDPR kräver att den personuppgiftsansvarige har klart för sig på uppgiftsnivå vilken den rättsliga grunden är för en behandling. Dataskyddsombudet vill särskilt poängtera att den rättsliga grunden likväl som ändamålet, ska vara knuten till den faktiska behandlingen, dvs. det kan inte finnas en behandlingsindelning för hur den personuppgiftsansvarige informerar de registrerade, en för behandlingsregistret, en tredje för de konsekvensbedömningar som genomförs och en fjärde för att ta ställning till en begäran från de registrerade om att utöva sina rättigheter.

Mot bakgrund av ovan är dataskyddsombudets rekommendation att bolaget ser över hur personuppgiftsbehandlingarna är avgränsade. Dataskyddsombudet rekommenderar även att bolaget gör det tydligt i behandlingsregistret vilken rättslig grund som hänför sig till vilket specifikt ändamål samt att den rättsliga grunden motiveras. Anges exempelvis rättslig förpliktelse som rättslig grund rekommenderar dataskyddsombudet att bolaget anger vilken/vilka bestämmelser som den rättslig förpliktelsen grundar sig på.

[20] Guidelines 05/2020 on consent under Regulation 2016/679 s 24 pt 118 *Controllers should therefore be clear from the outset about which purpose applies to each element of data and which lawful basis is being relied upon.*

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 att uppdatera behandlingsregistret med uppgifter om dataskyddsombudet samt komplettera registret med kontaktuppgifter till personuppgiftsansvarig.
- Bolaget rekommenderas att säkerställa att ändamålet i behandling är tydligt, korrekt och specifik så att det uppfyller kraven i enlighet med GDPR. Detta kan uppnås genom att se över de kommentarer som ni fått av dataskyddsombudet dels i detta dokument, dels i ert befintliga behandlingsregister.
- Bolaget rekommenderas specificera beskrivningen av kategorier av registrerade och personuppgifter samt förtydliga hur de relaterar till varandra.
- Bolaget rekommenderas göra en översyn av sitt behandlingsregister för att säkerställa att man anger alla specifika mottagare för samtliga behandlingar, inklusive interna mottagare.
- Bolaget rekommenderas att göra en granskning av de överföringar som sker till tredje land i enlighet med de avtal som bolaget har samt att dokumentera överföringarna i behandlingsregistret.
- Bolaget rekommenderas att åtgärda informationen om tidsfrister för radering genom att ange de faktiska tidsfristerna för samtliga behandlingar i behandlingsregistret, i enlighet med vad som anges i artikel 30.1f i GDPR.
- Bolaget rekommenderas ta ett omtag i frågan om att tillhandahålla en allmän beskrivning av tekniska och organisatoriska skyddsåtgärder och tillse att uppgifterna förs in i registret för samtliga behandlingar och i en omfattning som tillgodoser kraven i GDPR.
- Bolaget rekommenderas se över hur personuppgiftsbehandlingarna är avgränsade. Förtydliga vilken rättslig grund som hänför sig till vilket specifikt ändamål och ange motiveringen till den rättsliga grunden.