Göteborgs Stad

Årsrapport för dataskyddsarbetet 2024

Miljö- och klimatnämnden

2024-12-18

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

Dataskyddsombudets bedömning är att miljöförvaltningen ligger i framkant med sin interna dataskyddsorganisation. Kompetensnivån är hög och arbetet bedrivs strukturerat och metodiskt. Problemen, i den mån man kan tala om problem, är de samma för miljöförvaltningen som för de flesta andra verksamheter i Staden, så till vida att det finns en betydande skuld i åtgärder som borde ha genomförts då GDPR trädde i kraft i maj 2018, och förvaltningen kämpar kontinuerligt för att komma i kapp och få på plats samtliga delar som krävs. Dataskyddsombudet anser inte att något särskilt sticker ut, precis som för många andra verksamheter handlar mycket om arbetet om att få ut dataskyddsfrågorna i hela verksamheten. I mångt och mycket handlar det om en resursfråga, där förvaltningen har behövt prioritera vissa delar av dataskyddsarbetet framför andra. I arbetet med konsekvensbedömningar har förvaltningen kommit en bra bit på vägen, och rent generellt anser dataskyddsombudet att de delar av dataskyddsarbetet som förvaltningen riktar sina resurser mot också genomförs på ett bra och strukturerat sätt.

4 Granskning av dataskyddsarbetet 2024

4.1 Fördjupad kontroll 2024

Dataskyddsombudet genomförde under hösten 2024 en fördjupad kontroll av miljöförvaltningens 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 sammanfattande bedömning av dom organisatoriska förutsättningarna för att förvaltningen ska kunna uppfylla kraven i artikel 30 i GDPR, är att verksamheten i och för sig har tydligt utpekade roller och ansvar, men att förvaltningen också behöver dokumentera hur man i praktiken säkerställer att behandlingsregistret hålls uppdaterat med nya och förändrade personuppgiftsbehandlingar. Dataskyddsombudet rekommenderar också att

förvaltningen antar ett dokumenterat arbetssätt för att säkerställa att behandlingsregistret kontinuerligt uppdateras Verksamheten behöver också i ett nästa steg göra behandlingsregistret till en naturlig del av förvaltningens systematiska dataskyddsarbete.

Vad gäller granskningen av själva behandlingsregistret framgår att förvaltningen anser att informationen i behandlingsregistret är komplett enligt artikel 30. Dataskyddsombudet instämmer inte i detta svar, utan ser att förvaltningen behöver komplettera behandlingsregistret med viss information. Kompletteringar behöver bland annat göras kopplat till information om kontaktuppgifter, mottagare, gallringsfrister och tekniska och organisatoriska säkerhetsåtgärder. Vad gäller kategorier av registrerade och kategorier av personuppgifter behöver dessa uppgifter kopplas samman så att man förstår vem personuppgifterna hänför sig till. Även om det inte är ett obligatoriskt krav rekommenderas förvaltningen ange risk för tredjelandsöverföringar och motivering av rättslig grund. Dataskyddsombudet ser också att förvaltningen behöver omarbeta sina ändamålsbeskrivningar, men anser att det som utgångspunkt finns en god grundstruktur för förvaltningen att bygga vidare på. Dataskyddsombudet redogör i detalj för sin bedömning i rapporten för den fördjupade kontrollen, se 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: Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Verksamheten gavs följande rekommendationer:

Anta ett dokumenterat arbetssätt för att säkerställa efterlevnad av kraven enligt GDPR vid anordnade av fysiska och digitala sammankomster (till exempel möten/utbildningar/föreläsningar eller större evenemang).

Vidta åtgärder för att implementera dataskyddsarbetet på bredden så att frågorna och perspektivet blir integrerat i det dagliga arbetet.

Anta ett internt styrande dokument för behandling av personuppgifter som på en övergripande nivå anger principer för hur man inom organisationen ska hantera personuppgifter vad gäller skydd av bland annat IT-system, datorer och mobila enheter.

Kommentarer och rekommendationer:

Förvaltningen har, i samförstånd med dataskyddsombudet och till förmån för åtgärder med högre risk, inte prioriterat åtgärden gällande att anta ett dokumenterat arbetssätt för att säkerställa efterlevnad av kraven enligt GDPR vid anordnade av fysiska och digitala sammankomster (till exempel möten/utbildningar/föreläsningar eller större evenemang).

Vad gäller frågan om att implementera dataskyddsarbetet på bredden uppger förvaltningen att detta ingår i det kontinuerliga arbetet med uppdateringar och information om styrande dokument och arbetssätt. Exempelvis har man tagit fram ett särskilt APT-material om att skydda information, översyn av arbetssätt för hantering av personuppgiftsincidenter, framtagande av nya digitala utbildningar, informationsmaterial till chefer om konsekvensbedömningar, och en rutin för att följa upp biträdesavtal.

Förvaltningen uppger att det finns flera styrande dokument som tillsammans täcker in rekommendationen avseende dokumenterade principer för den interna hanteringen av personuppgifter, till exempel ”Policy för informationshantering”, ”Anvisning för roller och ansvar inom informationshantering”, Dokumenthanteringsplan, ”Regler för behörighet och åtkomst”, ”Anvisning för klass 2-information”, ”Rutin för e-postanvändning”, ”Regler och Anvisning för Microsoft 36”5, ”Anvisning, regler och rutin för geodata”, ”Rutin för arbetsdator och telefoni”, och ”Rutin för att skydda information” (ej fastställd).

Dataskyddsombudets bedömning är att förvaltningen omhändertagit rekommendationerna och att ingen särskild uppföljning krävs.

Fokusområde 2: Kontrollpunkt 8: E-post och dokumenthantering

Verksamheten gavs följande rekommendationer:

Förvaltningen rekommenderas vidta åtgärder för att säkerställa att det finns teknisk möjlighet att gallra och att gallring görs enligt gallringsbeslut.

Kommentarer och rekommendationer:

Förvaltningen uppger att ett arbete pågår med att kartlägga funktionalitet och att ta fram rutiner och arbetssätt för att verkställa gallring ,vilket förväntas påbörjas under 2025 avseende verksamhetssystemet EDP Vision. Arbete pågår även med avveckling av Notes, enligt Stadens projekt där planering av gallringsåtgärder ingår.

Dataskyddsombudets bedömning är att förvaltningen verkar vara på god väg att omhänderta rekommendationerna, men att fokusområdet kvarstår och uppföljning kommer ske under 2025 för att säkerställa att gallring kan genomföras.

Fokusområde 3: Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamheten gavs följande rekommendationer

Utred vad som behöver göras för att förvaltningen bättre ska säkerställa att konsekvensbedömningar genomförs innan riskfyllda behandlingar påbörjas och vidta åtgärder för att åstadkomma en sådan förbättring.

Anta ett dokumenterat arbetssätt för att säkerställa att konsekvensbedömningar uppdateras vid förändringar.

Anta ett dokumenterat arbetssätt vad gäller hantering av risk. Få på pränt hur verksamheten ska hantera beslutsfattande om att vidta åtgärder för att möta kvarstående risker och hur detta ska dokumenteras. Dokumentera hur verksamheten ska arbeta med uppföljning av beslutade riskhanteringsåtgärder.

Kommentarer och rekommendationer:

Förvaltningen uppger att man har tagit fram ett stödmaterial och informerat samtliga chefer. Rutin för konsekvensbedömningar är under framtagande.

Hantering av beslutsfattande och dokumentation sker genom riskbedömningsmall och delegationsordning med vidaredelegation. Arbetet med dokumentation av uppföljning ingår i rutinen för konsekvensbedömningar som är under framtagande.

Samtliga konsekvensbedömningar görs med stöd av förvaltningens dataskyddskontakter.

Dataskyddsombudets bedömning är att förvaltningen verkar vara på god väg att omhänderta rekommendationerna, men att fokusområdet kvarstår och uppföljning kommer ske under 2025.

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.

Förvaltningen rekommenderas 2025 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Dataskyddsombudet genomförde under hösten 2024 en fördjupad kontroll av förvaltningens arbete med behandlingsregister enligt artikel 30 i GDPR (se även fördjupad kontroll). Kontrollen visade på brister i förvaltningens dokumentation av behandlingar i sitt behandlingsregister. Förvaltningen rekommenderas därför att fokusera på att omhänderta de rekommendationer som dataskyddsombudet lämnat i rapporten för den fördjupade kontrollen.

- Kontrollpunkt 8: E-post och dokumenthantering

Förvaltningen rekommenderas fortsätta arbetet med vidta åtgärder för att säkerställa att det finns teknisk möjlighet att gallra och att gallring görs enligt gallringsbeslut.

- Kontrollpunkt 9: Konsekvensbedömning/samråd

Förvaltningen rekommenderas färdigställa arbetet med att anta ett dokumenterat arbetssätt för att säkerställa att konsekvensbedömningar uppdateras vid förändringar.

6 Bilagor

Bilaga 1: Kontrollplan för dataskyddsarbetet 2024–2025

Bilaga 2: 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 miljö- och klimatnämnden

2024-12-18

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	Kontrollfrågor om behandlingsregistret
Bilaga 3	Miljöförvaltningens anvisning för roller och ansvar i informationshanteringen

2 Fördjupad kontroll

2.1 Resultat av granskning av dokumenterade arbetssätt

Dataskyddsombudets bedömning är att förvaltningen i och för sig har tydligt utpekade roller och ansvar, men att förvaltningen också behöver dokumentera hur förvaltningen i praktiken säkerställer att behandlingsregistret hålls uppdaterat med nya och förändrade personuppgiftsbehandlingar. Förvaltningen behöver också i ett nästa steg göra behandlingsregistret till en naturlig del av förvaltningens systematiska dataskyddsarbete. Mer detaljer redogörs för nedan.

2.1.1 Dataskyddsombudets bedömning

Dataskyddsombudet har fått ta del av förvaltningens behandlingsregister rörande verksamhetsområde 3-6 som hanteras i två olika dokument.

Utifrån det material som förvaltningen har bifogat gör dataskyddsombudet bedömningen att förvaltningen har pekat ut roller och ansvar för att säkerställa att förvaltningen uppfyller kraven i artikel 30 i GDPR och tydligt pekat ut roller och ansvar för att säkerställa att nya behandlingar tas upp i registret och att befintliga behandlingar hålls uppdaterade.

Förvaltningen har uppgett att man saknar dokumenterade arbetssätt för att säkerställa att behandlingsregistret kontinuerligt uppdateras med nya och förändrade personuppgiftsbehandlingar. Dataskyddsombudet rekommenderar därför att förvaltningen antar ett dokumenterat arbetssätt för att säkerställa att behandlingsregistret kontinuerligt uppdateras.

Dataskyddsombudet vill understryka att behandlingsregistret är en grundbult för att kunna arbeta systematiskt och riskbaserat med dataskydd och rekommenderar därför att förvaltningen använder registret som ett verktyg för att kunna göra detta.

2.2 Resultatet av granskning av behandlingsregister

2.2.1 Dataskyddsombudets bedömning

Förvaltningen har uppgett att informationen i behandlingsregistret är komplett enligt artikel 30. Dataskyddsombudet instämmer inte i detta svar, utan ser att förvaltningen behöver komplettera behandlingsregistret med viss information. Kompletteringar behöver bland annat göras kopplat till information om kontaktuppgifter, mottagare, gallringsfrister och tekniska och organisatoriska säkerhetsåtgärder. Vad gäller kategorier av registrerade och kategorier personuppgifter behöver dessa uppgifter kopplas samman så att man förstår

vem personuppgifterna hänför sig till. Även om det inte är ett obligatoriskt krav rekommenderas förvaltningen ange risk för tredjelandsöverföringar och motivering av rättslig grund. Dataskyddsombudet ser också att förvaltningen behöver omarbeta sina ändamålsbeskrivningar, men anser att det som utgångspunkt finns en god grundstruktur för förvaltningen att bygga vidare på. Mer detaljer kring dataskyddsombudets bedömning och konkreta rekommendationer redogörs för 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*. Syftet med informationen är att möjliggöra en entydig identifiering av den eller de personuppgiftsansvariga och alla andra som är ansvariga enligt GDPR. Begreppet *kontaktuppgifter* är 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]

Det är upp till förvaltningen att bestämma hur informationen ska presenteras, antingen som kolumner vid varje behandling i registret, eller som en övergripande information i inledningen där det tydligt framgår att uppgifterna gäller för samtliga behandlingar i registret. För vissa behandlingar kan två eller flera vara personuppgiftsansvariga tillsammans (gemensamt personuppgiftsansvariga). Om så är fallet ska identitet och kontaktuppgifter till samtliga som är personuppgiftsansvariga framgå av behandlingsregistret per varje behandling för vilket detta är aktuellt.

I förvaltningens behandlingsregister framgår det att ”Miljöförvaltningen” är personuppgiftsansvarig. Vidare framgår kontaktuppgifter i form av e-postadress till ansvarig representant inom förvaltningen. Några ytterligare kontaktuppgifter framgår inte. I dokumentet för verksamhetsområde 3-5 saknas kontaktuppgifter till dataskyddsombudet. I dokumentet för verksamhetsområde 6-9 finns dock en e-postadress till dataskyddsenheten.

Förvaltningen rekommenderas komplettera behandlingsregistret med den information kopplat till namn och kontaktuppgifter som saknas och att ange att det är miljö- och klimatnämnden som är personuppgiftsansvarig (det är ju nämnden som formellt sett är personuppgiftsansvarig).

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*

[1] Jämför Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, s.35.

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 ändamål. Om ändamålet saknar tillräcklig precision, går det inte att bedöma om personuppgifterna är adekvata och relevanta, eller om för många personuppgifter behandlas.[3] Detta gäller särskilt för processorienterade ändamål som ofta är väldigt abstrakta. Att ändamålet ska vara specifikt innebär också att behandlingen inte ska innefatta något annat än det som direkt kan utläsas av beskrivningen, d.v.s. det får finnas dolda eller underförstådda syften som inte direkt framgår. Det betyder att ändamålsformuleringen inte 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 behandlas 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.

Nedan följer några konkreta kommentarer och rekommendationer kopplat till förvaltningens behandlingsregister gällande frågan om ändamål och behandlingars avgränsningar.

Systematiken kring hur namn och ändamålsbeskrivning konstrueras

Dataskyddsombudet konstaterar att förvaltningen i sitt behandlingsregister har en systematisk, enhetlig struktur och jämn abstraktionsnivå på hur namn på behandlingar samt ändamål konstrueras. Detta skapar igenkänning och överblick och ger en bra grundstruktur som förvaltningen kan bygga vidare på för en funktionell avgränsning av sina behandlingar.

Dataskyddsombudet anser dock att förvaltningen behöver arbeta om sina ändamålsformuleringar då de inte är formulerade som ändamåls- eller

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

syftesbeskrivningar. Ur ändamålsbeskrivningarna behöver det också framgå tydligare vad personuppgiftsbehandlingarna består i.

Nuvarande ändamålsbeskrivningar inleds med ”processen omfattar...” och följs av en övergripande beskrivning. I beskrivningen framgår i och för sig processen konkret, men det saknas tydlig koppling till vad personuppgiftsbehandlingen består i och vad som är syftet med de olika personuppgiftsbehandlande momenten.

Dataskyddsombudet rekommenderar därför att förvaltningen omarbetar formuleringarna så att det framgår tydligare vad som är syftet med att behandla personuppgifterna och vilka personuppgiftsbehandlingsmoment som ingår.

Nedan kommer ett exempel på hur man skulle kunna omarbeta en ändamålsbeskrivning. Observera att det kan finnas många olika sätt att bygga upp en ändamålsbeskrivning på, så exemplet nedan är inte ett exakt facit. Vilka personuppgiftsbehandlingsmoment som ingår och vad som är syftet med dessa behöver förvaltningen själva kontrollera, så det som beskrivs nedan är bara ett försök till att illustrera på vilken nivå dataskyddsombudet anser att ändamålet behöver beskrivas. Förvaltningen rekommenderas också ta inspiration av exempelvis EDPB:s och EDPS:s behandlingsregister för att se hur ett ändamål lämpligen kan beskrivas.[4]

Miljöförvaltningens ändamålsbeskrivning	**Förslag på omformulering**
3.1.1 Hantera registrering av livsmedelsverksamhet Processen omfattar all hantering av registrering av livsmedelsverksamhet. Processen startar när anmälan inkommer, följt av bedömning och avslutas med registrering eller återkoppling till anmälaren om undantag från krav på registrering. Processen omfattar även anmälan om ändrad adress.	*3.1.1 Hantera registrering av livsmedelsverksamhet* Ändamålet med personuppgiftsbehandlingen är att hantera registrering av livsmedelsverksamhet enligt reglerna i lagen X. Personuppgiftsbehandling behövs för att kunna identifiera vem som ansöker om registrering av livsmedelsverksamhet, för att kunna återkoppla registrering till sökande och för att kunna hantera anmälan om ändrad adress.

För att behålla en enhetlig systematik kan det vara bra att förvaltningen dokumenterar sina principer för hur behandlingar avgränsas. Detta underlättar

[4] EDPB:s behandlingsregister, Tillgänglig: EDPB centralised register of records | European Data Protection Board (hämtad 2024-11-25).
EDPS:s behandlingsregister, Tillgänglig: Records Register | European Data Protection Supervisor (hämtad 2024-11-25).

för det fall nya behandlingar uppstår och behöver föras in i behandlingsregistret längre fram i tiden.

Att skilja på planerad respektive händelsestyrd kontroll

I behandlingsregistret finns olika exempel på kontroll och förvaltningen har valt att separera planerad kontroll från händelsestyrd kontroll. Dataskyddsombudet undrar om ändamålen verkligen är så pass olika eller om ett gemensamt ändamål skulle kunna formuleras som täcker in båda förfaranden? Dataskyddsombudet ser i dagsläget dock inget direkt fel eller någon direkt uppenbar risk med det upplägg som förvaltningen har valt och lämnar därför över till förvaltningen att göra en bedömning av vad som är en lämplig avgränsning.

Att hantera ”besvara frågor av generell karaktär” inom olika ämnesområden som olika separata behandlingar

Förvaltningen har valt att avgränsa hantering av generella frågor utifrån vilka olika ämnes- och/eller regleringsområden som frågorna gäller. Dataskyddsombudet utesluter inte att det skulle kunna vara möjligt att hantera hela den generella frågehanteringen som en och samma behandling oberoende av vad frågorna handlar om. Dataskyddsombudet ser i dagsläget dock inget direkt fel eller någon direkt uppenbar risk med det upplägg som förvaltningen har valt och lämnar därför över till förvaltningen att göra en bedömning av vad som är en lämplig avgränsning.

Dataskyddsombudet rekommenderar dock att förvaltningen tydliggör vad som avses med ”generella frågor”. Är till exempel frågor som ställs av sakägare kopplat till konkreta handläggningsärenden inte en del av behandlingen? Förvaltningen behöver säkerställa att det inte finns någon oklarhet gällande detta.

Att hantera remisser i olika ämnesområden som olika separata behandlingar

Förvaltningen har genomgående valt att avgränsa olika remisshanteringar från varandra beroende på föremålet eller ämnet för remissen. Förutsatt att remissförfarandena har viss likhet tänker dataskyddsombudet att de skulle kunna hanteras som en och samma behandling oberoende av vad remisserna handlar om. Dataskyddsombudet ser i dagsläget dock inget direkt fel eller någon direkt uppenbar risk med det upplägg som förvaltningen har valt och lämnar därför över till förvaltningen att göra en bedömning av vad som är en lämplig avgränsning.

Behandlingar som kallas ”hantering av information”

Förvaltningen har ett antal behandlingar som kallas ”hantering av information…” följt av en angivelse som knyter informationen till exempelvis en viss reglering, en viss typ av ärende, någon åtgärd eller någon annan viss typ av fråga. Dataskyddsombudet ställer sig frågande till den här typen av avgränsning eftersom det ur ändamålsbeskrivningarna inte framgår tydligt vad som är slutmålet med informationshanteringen eller vad informationshanteringen mynnar ut i. Förvaltningen rekommenderas att se över

de olika behandlingarna som handlar om informationshantering och tydliggöra ändamålet med dessa.

2.2.2.3 Beskrivning av kategorier av registrerade och kategorierna av personuppgifter

Enligt artikel 30.1c ska behandlingsregistret innehålla *en beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.* Efter genomförd granskning vill dataskyddsombudet särskilt förtydliga att det som avses är just en *beskrivning* av kategorier av registrerade och uppgifter, d.v.s. det räcker inte att bara ange vilka kategorierna är. Läsaren ska av *beskrivningen* förstå vad kategorierna innefattar. Alltså vilka personuppgifterna är och vilka de registrerade är, och hur de relaterar till varandra.[5] Beskrivningen i artikelns led c behöver alltså vara något utöver att bara ange, exempelvis, *sökande, anställda, kontaktuppgifter, uppgifter om sociala förhållanden*. Helt enkelt för att det ska gå att förstå behandlingen. I stället för att skriva ”sökande” så skulle förvaltningen kunna skriva ”sökande som inkommer med ansökan om X”. I stället för att skriva ”anställda” så skulle förvaltningen kunna skriva ”anställda handläggare som har till arbetsuppgift att handlägga ärenden gällande Y”, och så vidare.

Förvaltningen har separata kolumner för kategorier av registrerade respektive kategorier personuppgifter. Förvaltningen rekommenderas klargöra kopplingen mellan kategorier registrerade och vilka kategorier av personuppgifter som behandlas om respektive kategori registrerad.

Förvaltningen har angett följande kategorier av registrerade på samtliga behandlingar: anställda, företagare, invånare, tjänstepersoner på andra förvaltningar, myndigheter och domstolar. Dataskyddsombudet anser att kategorin ”invånare” är väldigt abstrakt. I de fall det går att konkretisera kategorin utifrån sammanhanget, rekommenderas förvaltningen göra detta. Det måste vara möjligt att förstå i vilken egenskap invånare blir registrerade per varje behandling. Även kategorin ”tjänstepersoner på andra förvaltningar, myndigheter och domstolar” är väldigt abstrakt och dataskyddsombudet rekommenderar därför att förvaltningen, i de fall det går, konkretiserar detta utifrån sammanhanget som gäller för varje behandling.

Dataskyddsombudet har inte granskat i detalj om samtliga angivna kategorier av registrerade verkligen är aktuella på varje enskild behandling (det anges ju exakt samma kategorier per varje behandling). Dataskyddsombudet har inte heller undersökt om ytterligare kategorier av registrerade skulle kunna vara aktuella. Dataskyddsombudet har samtidigt inte fått någon indikation på att informationen skulle vara inkorrekt eller ofullständig.

[5] Se EDPB behandlingsregister för ett konkret exempel på hur detta kan dokumenteras i registret, EDPB Processing of personal data in the context of an access to documents request (hämtad 2024-11-25).
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 rekommenderar att förvaltningen säkerställer att samtliga tillämpliga kategorier av registrerade redogörs för vid varje behandling i behandlingsregistret och att de redogörs för på en tillräckligt konkret nivå.

Förvaltningen har ett antal olika kolumner som relaterar till frågan om kategorier av personuppgifter. Det finns separata kolumner för ”generella” kategorier av personuppgifter (alltså inte känsliga och extra skyddsvärda), känsliga personuppgifter (en kolumn där man anger JA/NEJ och en kolumn där man preciserar) och en för extra skyddsvärda personuppgifter. Det finns även en kolumn i vilken det kan anges om sekretessbelagda personuppgifter behandlas.

Förvaltningen har angett information om kategorier av personuppgifter på samtliga behandlingar och har specificerat om huruvida känsliga eller extra skyddsvärda personuppgifter behandlas. Dataskyddsombudet har inte granskat i detalj om samtliga angivna kategorier av personuppgifter är korrekta och kompletta, men har samtidigt inte fått någon indikation på att informationen skulle vara inkorrekt eller ofullständig.

Dataskyddsombudet rekommenderar att förvaltningen säkerställer att samtliga tillämpliga kategorier av personuppgifter redogörs för vid varje behandling i behandlingsregistret och att de redogörs för på en tillräckligt konkret nivå. Ett exempel på en angivelse som kan konkretiseras och beskrivas ytterligare är kategorin hälsa. På vilken detaljnivå behandlar förvaltningen personuppgifter om hälsa? Är det t.ex. fråga om läkarintyg som innehåller diagnos eller är det mer allmänt hållen information? Motsvarande frågor kan behöva ställas kopplat till andra kategorier personuppgifter som också angetts på en abstrakt nivå.

2.2.2.4 Kategorier av mottagare

I artikel 30.1d i GDPR anges att behandlingsregistret ska innehålla uppgift om de 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.

Tidigare har dataskyddsombudet gjort bedömningen att interna mottagare, alltså funktioner inom miljöförvaltningens egen organisation, inte omfattas av begreppet ”mottagare”. I den svenska översättningen används begreppet ”utlämnas” vilket kan få det att låta som att det verkligen ska vara fråga om ett utlämnande till någon extern (se artikel 30.1d och artikel 4.9).[6]

[6] Se även Öman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 4.9.

Dataskyddsombudet har dock gjort en förnyad bedömning att funktioner som behandlar personuppgifter inom en personuppgiftsansvarigs organisation också träffas av begreppet mottagare. Det innebär att även ”interna” mottagare ska tas upp som mottagare i behandlingsregistret. Dataskyddsombudet har gjort denna bedömning mot bakgrund av ny vägledning från EDPB,[7] samt utifrån vad som framgår ur de europeiska tillsynsmyndigheternas egna behandlingsregister,[8] men också utifrån ordvalet i andra språkversioner.[9] Det finns även stöd för den här tolkningen i förarbetena till personuppgiftslagen.[10] Det finns däremot inte någon skyldighet att i registret dokumentera identiteten på de faktiska fysiska personer inom verksamheten som tar del av uppgifterna.[11]

Dataskyddsombudet anser att när en personuppgift tillgängliggörs för en mottagare så ska det som bästa praxis, av behandlingsregistret framgå varför mottagaren är just mottagare.[12] 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 identiteten på specifika mottagare[13], och samma gäller även information som ska lämnas till den registrerade i enlighet med informationsskyldigheten i artikel 13.1d och 14.1d i GDPR. Eftersom förvaltningen ändå är tvungen att dokumentera den specifika mottagaren enligt artikel 13-15 i GDPR så anser dataskyddsombudet att uppgiften lämpligen också ska dokumenteras i behandlingsregistret.

Förvaltningen har i sitt register ett antal olika kolumner som dataskyddsombudet förmodar kan knytas till begreppet mottagare. Förutom en kolumn som kallas ”ange mottagare” finns bland annat en kolumn som heter ”lämnas några personuppgifter ut till tredje part?” och en som heter ”vilka avdelningar har tillgång till uppgifterna”. Dataskyddsombudet noterar att kolumnen som nu har rubriken ”ange mottagare” inte innehåller någon information.

Dataskyddsombudet rekommenderar att förvaltningen har *en* kolumn i vilken samtliga mottagare anges. Förvaltningen rekommenderas fylla på med information om mottagare så att informationen är komplett. Även mottagare

[7] EDPB, Data protection guide for small business, EDPB: Data protection guide for small business (hämtad 2024-11-25).
[8] Se exempel i EDPS:s behandlingsregister, 32-Record_of_processing_activity-EDPS_Data_Protection-Breach_Register_EN.pdf (hämtad 2024-11-25).
Se även exempel från EDPB:s behandlingsregister, EDPB records of processing activities - Data subjects rights (hämtad 2024-11-25).
[9] 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).
[10] 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”.*
[11] Se EU-domstolens förhandsavgörande i mål C-579/12, C-579/21.
[12] Se exempel från EDPB:s behandlingsregister, EDPB records of processing activities - Access to documents request (hämtad 2024-11-25).
[13] EU-domstolens förhandsavgörande i mål C-154/21, C-154/21.

inom den egna organisationen ska anges, exempelvis avdelningar och funktioner. Förvaltningen rekommenderas ange varför mottagaren är mottagare och när det är möjligt också ange identiteten på specifika mottagare och inte bara kategorin 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.*

I frågan om tredjelandsöverföringar behöver den personuppgiftsansvarige ha kännedom om och kartlägga vad som gäller i aktuella avtalsrelationer med personuppgiftsbiträden och underbiträden. Den personuppgiftsansvarige har en skyldighet enligt artikel 28.3a i GDPR att tillse att personuppgiftsbiträden endast behandlar personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, vilket också inbegriper frågan om överföringar av personuppgifter till ett tredjeland. Det innebär att det i teorin aldrig ska finnas några situationer där förvaltningen 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.

Bara för att biträdet råkar ha sin juridiska hemvist i ett specifikt land så behöver det inte vara så att det faktiskt sker avtalad eller planerad överföring till just det landet. Det faktum att det föreligger ett adekvansbeslut i ett tredjeland som ett biträde omfattas av medför inte per automatik att det är just dit som personuppgifter överförs, eller att de uteslutande överförs till det tredjelandet och inte till andra tredjeländer.

Det finns inte någon skyldighet att ange i behandlingsregistret när det endast finns en risk för tredjelandsöverföring. Dataskyddsombudet rekommenderar dock att förvaltningen även tar upp risk för tredjelandsöverföringar i sitt behandlingsregister. Ett företag eller en organisation kan finnas i EU, men samtidigt ha sin juridiska hemvist i ett tredjeland. Det tredjelandet kan ha en lagstiftning som innebär en rättslig skyldighet för företaget eller organisationen att oavsett faktisk lagringsplats för personuppgifterna, överföra uppgifter till myndigheter i det tredjelandet (detta gäller t.ex. USA, Kina, Ryssland). Detta påverkar naturligtvis skyddet för personuppgifterna, varför informationen är viktigt att dokumentera. Det behöver dock framgå tydligt när det är fråga om faktisk planerad eller avtalad överföring och när det endast föreligger en risk.

Förvaltningen har angett att inga behandlingar medför överföring av personuppgifter till tredjeland. Dataskyddsombudet har inte granskat i detalj om uppgifterna stämmer, men rekommenderar att förvaltningen säkerställer att informationen är korrekt. Förvaltningen behöver enligt principen om ansvarsskyldighet ha koll på hela kedjan av biträden och underbiträden och veta

vad som gäller för respektive tjänst och personuppgiftsbehandling. Förvaltningen saknar en kolumn som anger *risk* för tredjelandsöverföring. Även om det inte är ett obligatoriskt krav, så rekommenderar dataskyddsombudet att förvaltningen har med en sådan kolumn.

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 anses vara ”omöjligt”.[14] Att något är omständligt, tar lång tid eller innebär mycket administration innebär inte att det är ”omöjligt”. Viktigt att notera är att tidsfristerna ska anges för de olika kategorierna av personuppgifter och inte bara för behandlingen som helhet eller per handlingstyp. Dataskyddsombudet är av uppfattningen att det inte är tillräckligt att hänvisa till dokumenthanteringsplan. Av de europeiska dataskyddsmyndigheterna EDPB[15] och EDPS[16] register framgår de faktiska tidsfristerna direkt i registret, det samma gäller för IMY:s eget register[17].

Dataskyddsombudet konstaterar att uppgiften om lagringstid inte är tillräckligt preciserad i förvaltningens behandlingsregister. Förvaltningen rekommenderas att ange faktisk lagringstid per personuppgiftskategori.

Antingen anger förvaltningen att t.ex. hälsouppgifter förekommer i handling a som har en gallringsfrist på 2 år och att hälsouppgifter även förekommer i handling b för vilken gallringsfristen är 3 månader. Alternativt anges endast att gallringsfristen för hälsouppgifter är (som längst) 2 år.

2.2.2.7 Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder

Det är obligatoriskt enligt artikel 30.1g i GDPR, att i sitt behandlingsregister, om möjligt, ange *en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna enligt artikel 32.1*.

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 förvaltningen att ge en allmän beskrivning av skyddsåtgärder.[18] Att beskrivningen ska vara allmän betyder att det inte finns något krav om att återge en detaljerad beskrivning av alla säkerhetsåtgärder.[19]

---

[14] 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”.*
[15] Se exempel från EDPB:s behandlingsregister, EDPB records of processing activities - Access to documents request (hämtad 2024-11-25).
[16] Se exempel från EDPS:s behandlingsregister, 07-Record_of_processing_activity_whistleblowing_procedure_EN.pdf (hämtad 2024-11-25).
[17] Se IMY:s förteckning över personuppgiftsbehandingar (aktuell version från 2024-10-23).
[18] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 s. 29, pt 59.
[19] Se exempel från EDPS:s och EDPB:s behandlingsregister här: 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 2024-11-25).

I förvaltningens behandlingsregister har förvaltningen angett NEJ vid varje behandling som svar på om det finns en allmän beskrivning. Förvaltningen rekommenderas att komplettera behandlingsregistret med information om vilka säkerhetsåtgärder som gäller för samtliga behandlingar.

2.2.3 Övriga iakttagelser

2.2.3.1 Rättslig grund och motivering

Det finns inte något formellt krav enligt artikel 30 i GDPR att uppgift om en behandlings rättsliga grund och motivering av den rättsliga grunden, ska återges i ett behandlingsregister. 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.[20]

Det finns inget förbud mot att ha flera rättsliga grunder i en och samma behandling, en förutsättning är dock att varje rättslig grund kan knytas till ett specifikt ändamål, att ett specifikt ändamål bara kan ha en (enda) rättslig grund, och att varje enskilt ändamål och rättslig grund går att knyta till de kategorier av registrerade och personuppgifter som behandlas för det ändamålet[21].

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. Även av den anledningen kan det vara lämpligt att dokumentera rättslig grund i behandlingsregistret.

Förvaltningen har dokumenterat rättslig grund på samtliga behandlingar, men har inte angett en motivering till rättslig grund d.v.s. konkret hänvisning till lagstiftning, reglemente, avtal eller liknande som skriver fram stödet för den konkreta behandlingen. Om förvaltningen väljer att dokumentera rättslig grund inom ramen för behandlingsregistret, så rekommenderar dataskyddsombudet att även motiveringen till rättslig grund anges. Förvaltningen rekommenderas därför komplettera behandlingsregistret med denna information.

Förvaltningen har angett ”myndighetsutövning eller uppgifter av allmänt intresse” på samtliga behandlingar. Förvaltningen rekommenderas klargöra om det antingen är fråga om myndighetsutövning eller om det är fråga om uppgift av allmänt intresse som är tillämplig för varje enskild behandling alternativt

[20] 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”.
[21] 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*

klargöra vilka delmoment/deländamål i personuppgiftsbehandlingen som hänför sig till myndighetsutövning respektive uppgift av allmänt intresse.[22]

3 Sammanfattande rekommendationer

Utifrån de förbättringsområden och brister som dataskyddsombudet har identifierat i kontrollen av miljöförvaltningens behandlingsregister lämnas ett antal rekommendationer. Rekommendationerna framgår av punktlistan nedan. Dataskyddsombudet kommer särskilt följa upp vilka åtgärder som förvaltningen har vidtagit med anledning av rekommendationerna under kommande år. Förvaltningen rekommenderas också ta stöd i den vägledning som dataskyddsombudet sammanställer i den övergripande granskningsrapporten som är gemensam för hela staden.

Förvaltningen rekommenderas följande:

- Anta ett dokumenterat arbetssätt för att säkerställa att behandlingsregistret kontinuerligt uppdateras.
- Använd registret som ett verktyg för att arbeta systematiskt och riskbaserat med dataskydd.
- Komplettera behandlingsregistret med information kopplat till namn och kontaktuppgifter som saknas och att ange att det är miljö- och klimatnämnden som är personuppgiftsansvarig.
- Omarbeta ändamålsformuleringarna så att det framgår tydligare vad som är syftet med att behandla personuppgifterna och vilka personuppgiftsbehandlingsmoment som ingår.
- Tydliggör kopplat till de behandlingar som har med att besvara generella frågor, vad som utgör ”generella” frågor.
- Se över de olika behandlingarna som handlar om ”informationshantering” och tydliggör ändamålet.
- Klargör kopplingen mellan kategorier registrerade och kategorier personuppgifter så att man förstår vilka personuppgifter som behandlas om respektive kategori registrerad.
- Säkerställ att samtliga tillämpliga kategorier av registrerade redogörs för vid varje behandling i behandlingsregistret och att det redogörs för på en tillräckligt konkret nivå.
- Säkerställ att samtliga tillämpliga kategorier personuppgifter redogörs för vid varje behandling i behandlingsregistret och att det på en tillräckligt konkret nivå.
- Tydliggör och komplettera informationen kopplat till mottagare. Ange mottagare även inom den egna organisationen. Ange varför mottagaren

[22] 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”.*

är mottagare och när det är möjligt, ange också identiteten på specifika mottagare.

- Säkerställ att informationen gällande tredjelandsöverföringar är korrekt och ange även risk för tredjelandsöverföringar.
- Ange konkret lagringstid per personuppgiftskategori.
- Komplettera behandlingsregistret med information om vilka säkerhetsåtgärder som gäller för samtliga behandlingar.
- Klargör om det är myndighetsutövning specifikt eller om det är en uppgift av allmänt intresse alternativt klargör vilka delmoment/deländamål i personuppgiftsbehandlingen som hänför sig till myndighetsutövning respektive uppgift av allmänt intresse. Ange motivering till rättslig grund per varje behandling.

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.

VO1 - Styra, planera och följa upp: Saknas.
VO2 - Ge verksamhetsstöd: Saknas.
VO3 - Bedriva myndighetsutövning inom livsmedelsområdet: Finns.
VO4 - Bedriva myndighetsutövning inom miljö- och hälsoskyddsområdet: Finns.
VO5 - Bedriva myndighetsutövning inom alkohol- och tobaksområdet: Finns.
VO6 - Bedriva miljöövervakning: Finns.
VO7 - Driva och samordna stadens arbete inom den ekologiska dimensionen av hållbar utveckling: Finns.
VO8 - Medverka i samhälls- och stadsplanering: Finns.
VO9 - Förvalta och utveckla stadens energi- och klimatrådgivning: Finns.

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

Steg 1 för förvaltningen är att ta fram register för samtliga verksamhetsområden.
Det steget är inte klart.

Vi har inte tagit fram register för VO1-VO2 eftersom vi väntar på resultatet för det pågående arbetet med dokumenthanteringsplanen.

För VO6-VO9 finns väsentliga delar av behandlingsregistret i excelformat. Vi har däremot pausat inläggandet i Draftit eftersom det kräver mycket tid samtidigt som andra uppgifter behöver prioriteras.

Steg 2 att ta fram arbetssätt för att hålla registret komplett och aktuellt.

Delar av registret finns dock i den gällande dokumenthanteringsplanen. Verksamheten arbetar utifrån denna.

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

Information om registret ges vid utbildningar i informationshantering.

För tillfället har endast medarbetare som arbetar med att ta fram och uppdatera registret behörighet till Draftit. Övriga medarbetare får för tillfället ta del av registret för VO3-VO5 i verksamhetshandboken. Där finns ett utdrag ur draftit.

Registret för VO6-VO9 är inte färdigställt varför det inte finns i draftit. Det finns inte heller i verksamhetshandboken. Önskar anställd att ta del av registret får anställd ta del av det i form av excelfilen.

Väsentliga delar av registret finns i dokumenthanteringsplanen. Där tar både anställda och chefer del av det i praktiken.

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

Vi är fortfarande i fasen att vi tar fram register för samtliga verksamhetsområden.

Innehållet avseende VO3-VO9 har tagits fram successivt från sommar 2022-2023. Därefter har ingen aktualiseringsprövning gjorts.

Vi har också säkerställt att registret är i enlighet med DSE:s mall för register.

Göteborgs Stad

Dokumentnamn: Miljöförvaltningens anvisning för roller och ansvar i informationshanteringen

Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
Direktör	Miljöförvaltningen		
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Anvisning	Tills vidare	2024-06-28	Avdelningschef ärende- och informationshantering
Bilagor:			

Miljöförvaltningens anvisning för roller och ansvar i informations-hanteringen

Syftet med denna anvisning

Denna anvisning är en konkretisering av miljö- och klimatnämndens policy för informationshantering. Syftet med anvisningen är att tydliggöra chefers, medarbetares och stödfunktioners roller och ansvar för hanteringen av förvaltningens information.

Vem omfattas av anvisningen

Denna anvisning gäller tills vidare för samtliga anställda på miljöförvaltningen.

Koppling till andra styrande dokument

Styrande dokument	Beskrivning
Miljö- och klimatnämndens policy för informationshantering	Nämndens övergripande styrande dokument för informationshantering.
Göteborgs Stads riktlinje för informations-säkerhet	Stadens gemensamma styrdokument för informationssäkerhet.
Göteborgs Stads regel för IT-användare	Stadens regler för användare av stadens IT-resurser, behörighetshantering med mera.
Göteborgs Stads anvisning för tillämpningen av Föreskrifter och riktlinjer om arkiv- och informationshantering	Stadens styrande dokument med detaljerad information om vad som krävs för att uppfylla kraven i arkiv- och offentlighetslagstiftningen.

Nämndens och chefers ansvar

Nämndens och direktörens informationsägaransvar

Miljö- och klimatnämnden har det yttersta och övergripande ansvaret för verksamhetens informationshantering. Nämnden har beslutat om en policy för informationshantering.

Direktören ska se till att förvaltningen kan fullgöra nämndens ansvar genom att arbeta aktivt, samordnat och systematiskt med informationsstyrningen och den dagliga informationshanteringen. Direktören ska säkerställa att förvaltningen har tydliga roller och delegerade ansvar för informationshanteringen samt att det finns förutsättningar för chefer att ta det ansvar som följer deras informationsägarskap.

Avdelnings- och enhetschefers informationsägaransvar

Informationsägaransvaret följer ansvaret i förvaltningens linjeorganisation. Det innebär att det är avdelnings- och enhetschefer som är informationsägare för sina respektive verksamhetsområden. Ansvaret för informationen följer ansvaret för verksamheten, på samma sätt som ansvaret för personal, ekonomi och resultat.

Informationsägares ansvar:

- Se till att all information inom det egna verksamhetsområdet hanteras i enlighet med de lagar, regelverk och lokala styrande dokument som reglerar förvaltningens informationshantering.
- Se till att medarbetare får den kompetensutveckling och de förutsättningar de behöver för att kunna hantera information korrekt inom ramen för sitt uppdrag.
- Se till att medarbetare har rätt åtkomst och behörighet till olika informationstillgångar inklusive att se över behörigheter när medarbetare byter befattning och se till att behörigheter tas bort när medarbetare slutar.
- Se till att verksamhetens information är korrekt klassad enligt stadens klassningsmodell.[1]
- Se till att registret över verksamhetens personuppgiftsbehandlingar är komplett och aktuellt.
- Se till att verksamhetens allmänna handlingar registreras skyndsamt och korrekt.
- Se till att allmänna handlingar som är av tillfällig och ringa betydelse för verksamheten gallras löpande enligt gallringsbeslut.
- Se till att det för varje samarbetsgrupp inom Microsoft 365 finns en utsedd informationsansvarig[2] som tar det ansvar som följer av rollen.
- Ta stöd från berörda stödfunktioner vid oklarheter kring informationshanteringen i den egna verksamheten och så tidigt som möjligt informera berörda stödfunktioner när risker, incidenter eller andra brister i den egna verksamheten upptäcks.

[1] Informationstillgångarna beskrivs utifrån verksamhetens processer och ges rätt skyddsnivå utifrån konfidentialitet, tillgänglighet och riktighet enligt den klassningsmodell som beskrivs i *Göteborgs Stads riktlinje för informationssäkerhet*.

[2] Vad rollen som informationsansvarig innebär beskrivs i Kunskapsportalen för Microsoft 365.

Medarbetares ansvar

Alla anställda på förvaltningen hanterar information till vardags i sitt arbete, ofta i stor omfattning. Nästan allt vi jobbar med omfattar någon form av informationshantering. Det handlar om allmänna handlingar och personuppgifter i olika register, men också om inloggningsinformation, e-post, kalenderbokningar, chattar, egna anteckningar, foton i mobiltelefonen etcetera. För att informationshanteringen ska vara säker och effektiv i praktiken krävs att varje medarbetare tar ansvar för den information de själva hanterar.

Medarbetares ansvar:

- Ha kännedom om de lagar, regelverk och lokala styrande dokument som reglerar förvaltningens informationshantering.
- Skaffa sig rätt kunskaper för att kunna hantera information korrekt inom ramen för sitt uppdrag.
- Vid osäkerhet i frågor om informationshantering rådfråga sin närmaste chef eller berörd stödfunktion.
- Snarast rapportera uppmärksammade risker eller brister i verksamhetens informationshantering, såsom misstänkta säkerhets- eller personuppgiftsincidenter, till närmaste chef och berörd stödfunktion.
- Följa förvaltningens dokumenthanteringsplan inom det egna verksamhetsområdet.
- Löpande och utan dröjsmål registrera allmänna handlingar enligt förvaltningens rutiner.
- Löpande gallra allmänna handlingar som är av tillfällig och ringa betydelse för verksamheten (gäller exempelvis e-post i den egna mejlbrevlådan och dokument på olika fillagringsytor).

Särskilda roller, uppdrag och stödfunktioner

För att chefer och medarbetare ska kunna fullgöra sina uppgifter inom informationshantering finns ett antal stödjande roller och funktioner på förvaltningen. Rollerna och funktionerna nedan beskrivs mer utförligt i sina respektive uppdragsbeskrivningar.

Roll/funktion	Uppdrag/ansvar
Avdelningschef för ärende- och informationshantering	Driver, samordnar och utvecklar förvaltningens samordnade systematiska informationshanteringsarbete inom områdena informationsförvaltning och arkiv, dataskydd och integritet samt informationssäkerhet.
Övriga avdelningschefer inom förvaltningens verksamhetsstöd	Driver, samordnar och utvecklar förvaltningens arbete inom sina respektive ansvarsområden, exempelvis digitalisering, styrning och uppföljning samt HR-området med särskild hänsyn till informationshanteringens regelverk och krav.

Arkivfunktionen (med särskilt utsedd arkivansvarig och arkiv-redogörare)	Utvecklar och uppdaterar den processorienterade informationsredovisningen. Sköter de analoga och digitala arkiven. Ger stöd och råd i frågor om arkiv och allmänna handlingar.
Dataskyddsombud, DSO (på dataskyddsenheten intraservice)	Informerar och ger råd om behandling av person-uppgifter, deltar i konsekvensbedömningar samt övervakar efterlevnaden av dataskyddsförordningen.
Dataskyddskontakt, DSK (på förvaltningen)	Samordnar, driver och utvecklar förvaltningens interna dataskyddsarbete. Ger stöd och råd internt i dataskyddsfrågor. Är förvaltningens kontaktpersoner gentemot DSO.
IT-funktionen	Sköter förvaltning, drift och utveckling av IT-stöd, tjänster och infrastruktur som förvaltningen använder inom IT- och geodataområdet.
Registraturen	Sköter den löpande hantering av förvaltningens allmänna handlingar och diarium. Ger stöd och råd i frågor om diarieföring och utlämnande av allmänna handlingar.
Säkerhetschef och säkerhets-samordnare	Driver, samordnar och utvecklar förvaltningens säkerhetsarbete. Ger stöd och råd i informations-säkerhetsfrågor.
Säkerhetsskyddsansvarig	Driver, samordnar och utvecklar förvaltningens säkerhetsskyddarbete.