Göteborgs Stad

Fördjupad kontroll 2024: Behandlingsregister enligt artikel 30 i GDPR

Granskningsrapport för stadsmiljönämnden

2024-12-17

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 förvaltningen 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	Förvaltningens svar på kontrollfrågor om behandlingsregistret
Bilaga 3	Stadsmiljöförvaltningens rutin för personuppgiftsbehandling

2 Fördjupad kontroll

2.1 Resultat av granskning av dokumenterade arbetssätt

2.1.1 Dataskyddsombudets bedömning

Dataskyddsombudets bedömning är att förvaltningen till stor del har dokumenterade arbetssätt på plats, men att det inte tydligt framgår av de rutindokument som förvaltningen bifogat att det finns ett utpekat ansvar för att säkerställa att behandlingsregistret uppfyller kraven i artikel 30 i GDPR. Mellan raderna kan det utläsas att det är förvaltningens dataskyddskontakt som bär huvudansvaret, men det anges inte uttryckligen. Av stadsmiljöförvaltningens rutin för personuppgiftsbehandling framgår vidare att det ska finnas särskilt utsedda personer som ansvarar för att registrera behandlingar i behandlingsregistret. Ansvaret som dessa personer har pekas tydligt ut i förvaltningens rutin, men dataskyddsombudet anser inte att det klart framgår vilka personerna är och hur de utses. Finns det en dokumenterad process för att utse dessa personer? Är de utsedda i praktiken? Förvaltningen uppger också att verksamheten aktivt arbetar med registret och verkar för att de anställda får information om det, vilket dataskyddsombudet ser som positivt. Slutligen så delar dataskyddsombudet bara i viss mån förvaltningens uppfattning om att beskrivningen i rutindokumentet uppfyller kraven på dokumenterade arbetssätt för att säkerställa ett aktuellt och uppdaterat register.

Dataskyddsombudet rekommenderar därför att förvaltningen förtydligar vem som internt ansvarar för att registret uppfyller kraven i artikel 30. Förvaltningen rekommenderas också att förtydliga de enskilda kontaktpersonernas ansvar och hur de utses, samt komplettera rutinen med dokumenterade arbetssätt för att säkerställa ett aktuellt och uppdaterat register.

2.2 Resultatet av granskning av behandlingsregister

2.2.1 Dataskyddsombudets bedömning

Av förvaltningens svar framgår att man anser att det register som tillhandahållits dataskyddsombudet innehåller komplett information i enlighet med kraven i artikel 30 i GDPR. Dataskyddsombudets samlade bedömning är att registret endast delvis innehåller den information som föreskrivs enligt artikel 30 och att de uppgifter som finns dokumenterade i registret har brister. Dataskyddsombudet rekommenderar att förvaltningen tar ett omtag kring: hur verksamheten dokumenterar sina behandlingar i behandlingsregistret, särskilt med fokus på att formulera tydliga, konkreta och specifika ändamål, beskrivning av de kategorier av personuppgifter och kategorier av registrerade

som förekommer i de olika behandlingarna, vilka som är mottagare av uppgifterna, tidsfrister för radering av personuppgifter och en allmän beskrivning av skyddsåtgärder. Dataskyddsombudet redogör i detalj för sin bedömning av behandlingsregistrets innehåll under avsnitt 2.2.2 nedan.

2.2.2 Granskning av behandlingsregister

2.2.2.1 Namn och kontaktuppgifter

Av artikel 30.1a i GDPR framgår att behandlingsregistret ska innehålla *namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombudet.* Det register som stadsmiljöförvaltningen tillhandahållit dataskyddsombudet innehåller inte dessa uppgifter, trots att de är obligatoriska. Syftet med informationen är att möjliggöra en tydlig identifiering av den eller de personuppgiftsansvariga och alla andra som är ansvariga enligt GDPR. Begreppet *kontaktuppgifter* är alltså inte begränsat till en enkel e-postadress. Informationen ska innehålla alla uppgifter (namn, fysisk adress, och kontaktväg, e-post och telefonnummer) som gör det möjligt att få kontakt med den personuppgiftsansvarige och dataskyddsombudet.[1]

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

2.2.2.2 Ändamålen med behandlingen

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

Ett väl definierat ändamål är centralt för en praktisk avgränsning av den personuppgiftsansvariges behandlingar. Ändamålet med en behandling ska vara tydligt, konkret och specifikt.[2] Det innebär att den som läser det enkelt ska kunna förstå vad som avses och varför personuppgifter behandlas, samt att personuppgifterna som behandlas ska ha en tydlig koppling till beslutade ändamål. Om ändamålet saknar tillräcklig precision, går det inte att bedöma om personuppgifterna är adekvata och relevanta, eller om för många

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

personuppgifter behandlas.[3] Det gäller särskilt för processorienterade ändamål som ofta är abstrakta och innehåller ett stort mått av subjektivitet, även om ändamålet kan vara tydligt språkligt formulerat. Att ändamålet ska vara specifikt innebär också att behandlingen inte ska innefattat något annat än det som direkt kan utläsas av beskrivningen, dvs. att det inte får finnas dolda eller underförstådda syften som inte direkt framgår.

Det betyder att ändamålsformuleringen 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 samlas in och till vad de ska användas.

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

Vad gäller stadsmiljöförvaltningens beskrivning av ändamål i sitt behandlingsregister, så gör dataskyddsombudet bedömningen att förvaltningens behandlingar till stor del saknar tillräckligt precisa och uttryckligt angivna ändamål. I en majoritet av fallen är det svårt att se sambandet mellan varför personuppgifter behandlas och ändamålet med behandlingen. Ändamålen är varken tydliga, konkreta eller specifika.

Dataskyddsombudet vill särskilt påtala att även om klassificeringsstruktur och dokumenthanteringsplaner kan vara en bra utgångspunkt i att ge vägledning för förvaltningens avgränsning av personuppgiftsbehandlingar, så är det efter avslutad granskning tydligt att det inte är funktionellt att bara kopiera poster i klassificeringsstrukturen rakt av och omvandla till behandlingar i behandlingsregistret. Detta eftersom utgångspunkten i klassificeringsstruktur och dokumenthanteringsplaner är processer och dokument, eller handlingar, och inte behandlingen av personuppgifter.

För de behandlingar som förvaltningen arbetat mer aktivt med genom konsekvensbedömningar och tröskelanalyser, så anser dataskyddsombudet att det genomgående finns en helt annan precision i ändamålsbeskrivningarna och att dessa ändamål är tillräckligt tydliga, konkreta och specifika. Förvaltningen behöver uppnå samma grad av precision i ändamålsformuleringen för samtliga behandlingar.

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

Dataskyddsombudet rekommenderar att förvaltningen tar ett helhetsgrepp i frågan och gör en genomgripande översyn av samtliga ändamålsformuleringar i registret och om hur avgränsningen av behandlingarna genomförs.

2.2.2.3 Beskrivning av kategorier av registrerade och kategorierna av personuppgifter

Enligt artikel 30.1c i GDPR ska behandlingsregistret innehålla *en beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter*. I sammanhanget är det viktigt att förtydliga att det som avses är en *beskrivning* av kategorier av registrerade och uppgifter. Det räcker alltså inte att bara ange vilka kategorierna är, utan läsaren ska av *beskrivningen* förstå vad kategorierna innefattar. Alltså vilka uppgifterna är, vilka de registrerade är, och hur de relaterar till varandra.[4] Beskrivningen i artikelns led c behöver således vara något utöver att bara ange, exempelvis, *sökande, anställda, kontaktuppgifter, uppgifter om sociala förhållanden,* med mera. Helt enkelt för att det ska gå att förstå behandlingen.

Dataskyddsombudet anser inte att stadsmiljöförvaltningens behandlingsregister lever upp till dessa krav. Även om det i strikt mening är så att kategorier av registrerade och personuppgifter finns med för samtliga behandlingar så bedömer dataskyddsombudet inte att de är beskrivna på ett sådant sätt att det av beskrivningen går att förstå vilka uppgifterna är, vilka de registrerade är, och hur de relaterar till varandra. För att leva upp till kraven skulle förvaltningen i stället för att skriva ”sökande” kunna skriva ”sökande som inkommer med ansökan om X”. Och i stället för att skriva ”hälsa” så skulle förvaltningen kunna skriva ” Uppgift om hälsa i läkarintyg bifogat från sökande vid ansökan”, och så vidare.

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

2.2.2.4 Kategorier av mottagare

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

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

[4] Se EDPB:s behandlingsregister EDPB records of processing activities - Access to documents request (hämtad 2024-11-27) för ett konkret exempel på hur detta kan dokumenteras i registret. Notera också skillnaden i hur led c och led d är formulerade i artikel 30.1. I led c anges specifikt att det handlar om en *beskrivning* av kategorierna. I led d framgår bara att *kategorier* av mottagare ska anges utan något krav på en beskrivning.

personuppgiftsbiträde är en mottagare, liksom underbiträden och under-underbiträden.

Som mottagare betraktas inte offentliga myndigheter som kan komma att motta personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller den nationella rätten. Däremot är det viktigt att påpeka att de funktioner som behandlar uppgifter *inom* en personuppgiftsansvarigs organisation också träffas av begreppet mottagare. Efter genomförd granskning kan dataskyddsombudet konstatera att uppgift om interna mottagare, alltså funktioner inom stadsmiljöförvaltningens egen organisation, genomgående saknas. Dataskyddsombudet har förståelse för att uppgiften om interna mottagare inte dokumenterats i förvaltningens register. Detta eftersom formuleringen i artikel 30.1d om att *personuppgifterna har lämnats eller ska lämnas ut*, tillsammans med formuleringen *utlämnas* i definitionen av mottagare i artikel 4.9, i den svenskspråkiga versionen av GDPR, gör att dataskyddsombudet tidigare gjort bedömningen, att den personuppgifts-ansvariges personal inte kan anses vara mottagare eftersom det kan ifrågasättas huruvida personuppgifter verkligen lämnas ut om de hanteras inom en förvaltning eller ett bolag.[5]

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

För att uppfylla kraven i artikel 30.1d rekommenderas därför stadsmiljöförvaltningen att dokumentera vilka interna avdelningar/funktioner som kan komma att ta del av personuppgifter inom ramen för den specifika behandlingen. Det finns däremot inte någon skyldighet att i registret dokumentera identiteten på de faktiska fysiska personer inom verksamheten som tar del av uppgifterna.[10]

Vad gäller förvaltningens övriga dokumentation av mottagare så har dataskyddsombudet noterat att på flera ställen i registret anges mottagaren som

[5] Se Öman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 4.9.
[6] EDPB, Data protection guide for small business, EDPB: Data protection guide for small business (hämtad 2024-11-26).
[7] Se till exempel i EDPB:s och EDPB:s behandlingsregister, EDPS record of processing activity - Personal Data Breach Notification, EDPB records of processing activities - Data subjects rights (hämtad 2024-11-27).
[8] Jämför till exempel med den engelska originalversionens *disclose*, det tyska *offengelegt,* franskans *recoit,* Italienskans *recive, och* spanskans *comuniquen*, så framstår det som klart att det som egentligen avses är vem som får ta del av uppgifterna, vilket också är så som EDPB uttrycker det i EDPB: Data protection guide for small business (hämtad 2024-11-27).
[9] Se Öman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 4.9, och SOU 1997:39 s. 335: ”*Begreppet mottagare omfattar i princip samtliga till vilka personuppgifter lämnas ut, även om den som tar emot uppgifterna inte skulle vara tredje man. Även den registrerade, personadatabiträdet och sådana personer som under den personadataansvariges eller personadatabiträdets direkta ansvar har befogenhet att behandla personuppgifter verkar således kunna betraktas som mottagare”.*
[10] Se EU-domstolens förhandsavgörande i mål C-579/21, C-579/21.

”leverantör”. Här är det oklart vad som avses, om det handlar om ett biträdesförhållande så ska det framgå. Vidare gäller att stadsmiljöförvaltningen genomgående i sitt register anger Intraservice som mottagare i egenskap av biträde, men av någon anledning har förvaltningen inte beskrivit till exempel Microsoft (MS) som en mottagare, trots att MS uppenbart är underbiträde för många av behandlingarna, och i registret anges som mottagare i tredjeland i enlighet med artikel 31.1e i GDPR. Dataskyddsombudet anser att när en personuppgift tillgängliggörs för en mottagare så ska det av behandlingsregistret, som bästa praxis, framgå varför mottagaren är just mottagare.[11] Det vill säga att om mottagaren till exempel är ett personuppgiftsbiträde eller underbiträde så ska det dokumenteras i registret. Dataskyddsombudet vill också lyfta att även om det är kategorier av mottagare som ska anges, så har den registrerade vid en begäran om tillgång enligt artikel 15 i GDPR rätt att få information om specifika mottagare[12], och det är även information som ska lämnas till den registrerade i enlighet med informations-skyldigheten i artikel 13.1d och 14.1d i GDPR. Eftersom förvaltningen ändå är tvungen att dokumentera den specifika mottagaren enligt artikel 13–15 i GDPR så anser dataskyddsombudet att uppgiften ska dokumenteras i behandlingsregistret.

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

2.2.2.5 Överföring av personuppgifter till tredjeland

Av artikel 30.1e framgår att behandlingsregistret ska innehålla information om: *i tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket, dokumentationen av lämpliga skyddsåtgärder.*

För att kunna redogöra för vilka faktiska överföringar som äger rum så måste den personuppgiftsansvarige veta vad som uttryckligen framgår av de avtal som träffats med personuppgiftsbiträden och eventuella underbiträden. Det är inte tillräckligt att veta ”på ett ungefär”, utan det är dom faktiska överföringarna som förvaltningen ska redogöra för. Förvaltningen har till exempel angett att en överföring av personuppgifter sker till USA som en följd av en biträdesrelation för samtliga behandlingar som utförs med stöd av någon del av MSO365.

Dataskyddsombudet utesluter inte på något sätt att personuppgifter faktiskt överförs till USA vid biträdesrelationer med detta biträde/underbiträde, det går dock inte att förutsätta att så sker bara för att biträdet råkar ha sin juridiska hemvist i just USA. Beroende på vilken typ av tjänst det avtalats om så kan det vara så att ingen överföring av personuppgifter utanför Europa sker överhuvudtaget, att överföring sker till just USA, eller att överföring inte sker

[11] Se EDPB:s behandlingsregister för ett konkret exempel, EDPB records of processing activities - Access to documents request (hämtad 2024-11-27). Se också mål C-154/21.
[12] Se mål C-154/21.

till USA, men väl till flera andra tredjeländer, som Indien, Kina, Malaysia med flera, till exempel för support och liknande ändamål.

Det faktum att det föreligger ett adekvansbeslut för ett tredjeland, som USA, 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 fråntar inte heller stadsmiljöförvaltningen skyldigheten att genomföra en kartläggning av vilka överföringar som sker till tredjeländer, med alldeles särskilt fokus på sådana tredjeländer som saknar adekvat skyddsnivå. Utan att genomföra en sådan kartläggning så är det inte möjligt för den personuppgiftsansvarige att bedöma om dessa överföringar är förenliga med GDPR.[13]

Det går inte heller att utgå ifrån att samma förutsättningar gäller för alla delar av, eller applikationer inom, MSO365-paketet. Geografisk hemvist för lagring och support kan skilja sig åt mellan olika applikationer. Återigen gäller att verksamheten måste ha koll på vilka avtal som finns, och ta höjd för att det kan finnas specifika applikationer som har sina egna förutsättningar, till exempel att ett verktyg som standard inte innebär en överföring av personuppgifter utanför EU, men att verksamheten valt att använda en särskild applikation utöver standardkonfigurationen som innebär att en sådan överföring sker.

Dataskyddsombudet vill också särskilt lyfta att den personuppgiftsansvarige har en skyldighet enligt artikel 28.3a i GDPR att tillse att ett personuppgiftsbiträde endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland. Det innebär att det i teorin aldrig ska finnas några situationer där 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.

Efter genomförd granskning anser dataskyddsombudet att det är starkt befogat att ifrågasätta hur väl stadsmiljöförvaltningen dokumenterat de faktiska överföringarna i sitt behandlingsregister.Dataskyddsombudet rekommenderar därför att förvaltningen kartlägger vilka överföringar som sker, i enlighet med vad som regleras i befintliga avtal, och därefter dokumenterar de faktiska överföringarna i sitt behandlingsregister.

2.2.2.6 Tidsfrister för radering

I artikel 30.1f i GDPR anges att den personuppgiftsansvarige ska, *om det är möjligt ange, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter*. Utifrån tillgänglig vägledning kan det konstateras att det finns högt ställda krav för att något ska kunna anses vara ”omöjligt”. Att något är omständligt, tar lång tid eller innebär mycket administration innebär fortfarande

[13] Se EDPS Investigation into use of Microsoft 365 by the European Commission (Case 2021-0518) Decision (8 March 2024) s. 105.

att det är ”möjligt”.[14] Viktigt att notera är även att tidsfristerna ska anges för de olika kategorierna av personuppgifter och inte för behandlingen som helhet eller per handlingstyp.

Efter genomförd granskning av stadsmiljöförvaltningens behandlingsregister anser dataskyddsombudet att registret genomgående uppvisar omfattande brister i dessa delar. Tidsfrister för gallring redovisas för mindre än tio procent av behandlingarna i registret. Dataskyddsombudet vill här särskilt förtydliga att artikel 30.1f föreskriver att det är tidsfristerna som ska anges. Det är inte tillräckligt att, som förvaltningen gör i flera fall, hänvisa till att gallringsbeslut saknas, eller att det finns rensningsrutiner. Detta helt enkelt eftersom ett sådant förfarande inte uppfyller kravet om att ange tidsfrister, utan endast informerar om att beslut om gallring finns (eller saknas). Det är inte heller meningen att berörda tillsynsmyndigheter, eller andra som vill ta del av registrets innehåll, ska behöva söka upp den obligatoriska informationen i andra källor. Dataskyddsombudets uppfattning är att om regleringen hade gett utrymme för en sådan hänvisning till andra dokument, så hade det uttryckts i artikel 30 i GDPR. Av de europeiska dataskydds-myndigheterna EDPB[15] och EDPS[16] register framgår de faktiska tidsfristerna direkt i registret, det samma gäller för den svenska tillsynsmyndighetens (IMY) eget register.[17]

Dataskyddsombudet rekommenderar därför att förvaltningen åtgärdar bristerna genom att ange de förutsedda tidsfristerna för radering (dvs när personuppgifterna kommer att gallras) för samtliga behandlingar i behandlingsregistret, i enlighet med vad som anges i artikel 30.1f.

2.2.2.7 Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder

En allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1 ska, om möjligt anges, enligt artikel 30.1g i GDPR. Precis som i fallet med tidsfrister för radering så innebär inte omständigheten att något är svårt, omständligt eller tidsödande att det är omöjligt. Det bör i princip inte förekomma något fall där det inte är möjligt för 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 skyddsåtgärder.[19] Efter genomförd granskning konstaterar dataskyddsombudet att uppgiften genomgående saknas i registret och endast förekommer i cirka fem procent av behandlingarna. I inget av dessa fall anser dataskyddsombudet att beskrivningen är tillräcklig utifrån de krav som finns på innehållet. Förvaltningen rekommenderas därför att ta ett omtag och tillse att

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

uppgifterna förs in i registret för samtliga behandlingar och i en omfattning som tillgodoser kraven i GDPR.

2.2.3 Övriga iakttagelser

2.2.3.1 Rättslig grund och motivering

Dokumentation av uppgift om en behandlings rättsliga grund och motivering av den rättsliga grunden i behandlingsregistret är inget krav enligt artikel 30 i GDPR. Den rättsliga grunden är dock en utgångspunkt för att lagligen få behandla personuppgifter och alla behandlingar måste stödjas på en av de rättsliga grunderna i GDPR. Utan en rättslig grund är behandlingen inte laglig. Den personuppgiftsansvarige behöver, innan en behandling påbörjas, ha klart för sig vilken rättslig grund som tillämpas. Flera rättsliga grunder kan vara tillämpliga för en behandling, men utgångspunkten är att en behandling för ett ändamål bara kan vila på en (enda) rättslig grund.[20]

Det följer också av informationsskyldigheten i artikel 13.1c och 14.1c i GDPR att den personuppgiftsansvarige ska informera den registrerade om den rättsliga grunden för en behandling. Eftersom uppgiften är något som den personuppgiftsansvarige ändå måste ha klart för sig rekommenderar dataskyddsombudet att den dokumenteras i behandlingsregistret, trots att det inte är obligatoriskt. Något som stadsmiljöförvaltningen också hörsammat.

Dataskyddsombudets bedömning är att stadsmiljöförvaltningen genomgående har kopplat en (enda) rättslig grund till varje enskilt ändamål, med undantag för några få behandlingar. Den absolut vanligaste hänvisningen är till den rättsliga grunden *uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning* i enlighet med artikel 6.1e i GDPR. Dataskyddsombudet har generellt inga synpunkter på valet av rättslig grund, det är endast i undantagsfallet som dataskyddsombudet haft anledning att ifrågasätta om förvaltningen verkligen hänvisar till korrekt rättslig grund. Av den kompletterande dataskyddslagen framgår däremot att uppgifter av allmänt intresse ska *följa av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning*.[21] Här anser dataskyddsombudet att förvaltningen i stora stycken slarvat när man hänvisat till lagstöd i den nationella rätten, många av hänvisningarna är direkt felaktiga.

Förvaltningen rekommenderas därför att genomgående se över vilket lagstöd i den nationella rätten man hänvisar till som stöd för att använda den rättsliga grunden uppgift av allmänt intresse och säkerställa att varje ändamål bara vilar på en rättslig grund.

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

[21] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning 2 kap 2 §.

3 Sammanfattande rekommendationer

Utifrån de förbättringsområden och brister som dataskyddsombudet har identifierat i kontrollen av stadsmiljöförvaltningens 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 att ta stöd i sitt arbete med behandlingsregistret utifrån den vägledning som dataskyddsombudet sammanställer i den övergripande granskningsrapport som är gemensam för hela staden.

- Förvaltningen rekommenderas att förtydliga vem som internt ansvarar för att behandlingsregistret uppfyller kraven i artikel 30. Förvaltningen rekommenderas också att förtydliga de enskilda kontaktpersonernas ansvar och hur de utses.
- Förvaltningen rekommenderas att komplettera sitt behandlingsregister med uppgift om personuppgiftsansvarig och dataskyddsombud samt kontaktuppgifter till dessa.
- Förvaltningen rekommenderas göra en genomgripande översyn av samtliga ändamålsformuleringar i registret för att säkerställa att de uppfyller kraven i GDPR. Förvaltningen rekommenderas också göra en översyn av hur avgränsningen av behandlingarna genomförs.
- Förvaltningen rekommenderas att utveckla beskrivningen av kategorier av registrerade och uppgifter, samt hur de relaterar till varandra.
- Förvaltningen rekommenderas göra en översyn av sitt register för att säkerställa att man anger alla specifika mottagare för samtliga behandlingar, inklusive interna mottagare, och att det i samtliga fall framgår varför mottagaren är mottagare.
- Förvaltningen rekommenderas kartlägga vilka faktiska överföringar som sker till tredjeland, i enlighet med vad som regleras i befintliga avtal, och därefter dokumentera överföringarna i sitt behandlingsregister.
- Förvaltningen rekommenderas att åtgärda den bristande informationen om tidsfrister för radering genom att ange de faktiska förutsedda tidsfristerna, för samtliga behandlingar i behandlingsregistret, i enlighet med vad som anges i artikel 30.1f i GDPR.
- Förvaltningen rekommenderas ta ett omtag i frågan om att tillhandahålla en allmän beskrivning av tekniska och organisatoriska skyddsåtgärder och tillse att uppgifterna förs in i registret för samtliga behandlingar och i en omfattning som tillgodoser kraven i GDPR.
- Förvaltningen rekommenderas att genomgående se över vilket lagstöd i den nationella rätten man hänvisar till som stöd för att använda den rättsliga grunden uppgift av allmänt intresse.