Göteborgs Stad

Fördjupad kontroll 2024: Behandlingsregister enligt artikel 30 i GDPR

Granskningsrapport för Bostads AB Poseidon

2024-12-19

Innehåll

1 Inledning

1.1 Kontrollområdet

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

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

1.2 Syfte

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

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

1.3 Tillvägagångssätt

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

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

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

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

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

1.4 Bilagor

Bilaga 1	Informationsutskick fördjupad kontroll av behandlingsregistret
Bilaga 2	Bolagets svar på kontrollfrågor om behandlingsregistret
Bilaga 3	Bolagets dokument ”Årsplanering GDPR”

2 Fördjupad kontroll

2.1 Resultat av granskning av dokumenterade arbetssätt

2.1.1 Dataskyddsombudets bedömning

I samband med den fördjupade kontrollen ombads bolaget att översända de dokument och rutiner som beskriver hur bolaget har organiserat arbetet med behandlingsregistret. Ett word-dokument med namn ”Årsplanering GDPR” har skickats in till dataskyddsombudet.

Dataskyddsombudet anser att det är otydligt vilken ställning dokumentet med namn ”Årsplanering GDPR” har inom bolaget då det inte framgår att det är beslutat och fastställt. Då det varken framgår att dokumentet är beslutat och fastställt är dataskyddsombudets bedömning att det inte uppfyller kravet för att anses vara dokumenterade arbetssätt.

Vad gäller innehållet i ”Årsplanering GDPR” är dataskyddsombudets bedömning att det inte tydligt framgår ett utpekat ansvar för att säkerställa att behandlingsregistret uppfyller kraven i art. 30 i GDPR. Det framgår visserligen att registerförteckningen ska skickas ut på remiss till bolagets olika kompetenser samt att registerförteckningen ska gås igenom och revideras efter svar från/möten med verksamheten. Det framgår dock inte vilken roll som ska skicka ut registerförteckningen, vilken roll/vilka roller som går igenom och reviderar registerförteckningen, vilka som omfattas av skrivningen ”bolagets olika kompetenser” eller vilken roll som har det övergripande ansvaret för att behandlingsregistret uppfyller kraven i art. 30 i GDPR.

Dataskyddsombudet rekommenderar därför att bolaget upprättar dokumenterade arbetssätt för hantering av behandlingsregistret internt samt att dessa fastställs officiellt genom beslut. I detta ingår att fastställa tydligt utpekade roller och ansvar för att löpande hålla behandlingsregistret uppdaterat och i enlighet med lagkraven.

2.2 Resultatet av granskning av behandlingsregister

2.2.1 Dataskyddsombudets bedömning

Bolaget uppskattar att ca 75-100 % av bolagets behandlingar är upptagna i behandlingsregistret. Samtidigt uppger bolaget att det inte går att säkerställa att samtliga behandlingar finns upptagna i behandlingsregistret. Bolaget rekommenderas att särskilt se över hur behandlingarna är definierade och avgränsade i behandlingsregistret då det bedöms finnas ett behov av att bryta ner flera av behandlingarna i mindre delar.

Dataskyddsombudets samlade bedömning är att behandlingsregistret delvis innehåller den information som föreskrivs enligt art. 30 i GDPR och anser att det finns delar som behöver kompletteras. Dataskyddsombudet anser, i ett första steg, att ett särskilt fokus behöver läggas på att formulera tydliga, konkreta och specifika ändamål. Även beskrivning av de kategorier av personuppgifter och kategorier av registrerade som förekommer i de olika behandlingarna, tidsfrister för radering av personuppgifter och en allmän beskrivning av skyddsåtgärder behöver förtydligas. Dataskyddsombudet redogör i detalj för bedömningen 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 GDPR framgår att behandlingsregistret ska innehålla namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombudet.

I bolagets behandlingsregister framgår det att bolaget är personuppgiftsansvarig vid respektive behandling. Det framgår även kontaktuppgifter i form av e-postadress och telefonnummer till en ansvarig medarbetare. Det saknas dock adress till bolaget och även kontaktuppgifter till 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 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]

Exakt i vilken form som bolaget väljer att presentera informationen är upp till verksamheten att avgöra, antingen som kolumner vid varje behandling i registret, eller som en övergripande information i inledningen, där det tydligt framgår att uppgifterna gäller för samtliga behandlingar i registret.

Bolaget rekommenderas att komplettera sitt behandlingsregister med adress till bolaget samt kontaktuppgifter till dataskyddsombudet. Om bolaget väljer att ha en specifik medarbetare som kontaktpunkt är det viktigt att det tydligt framgår att medarbetaren företräder den personuppgiftsansvariga i frågan. Dataskyddsombudet rekommenderar även att bolaget säkerställer att det finns dokumenterade arbetssätt för att uppgifterna uppdateras vid förändringar.

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)

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

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 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 bolagets beskrivning av ändamål i sitt behandlingsregister, så gör dataskyddsombudet bedömningen att bolaget saknar tillräckligt precisa och uttryckligt angivna ändamål. För flera av behandlingarna anger bolaget vilka dokument som hanteras. För andra behandlingar anges endast ***att*** något görs. I en majoritet av fallen är det svårt att se sambandet mellan varför personuppgifter behandlas och ändamålet med behandlingen. Ändamålen är alltså varken tydliga, konkreta eller specifika.

Dataskyddsombudet vill särskilt påtala att även om klassificeringsstruktur och dokumenthanteringsplaner kan vara en bra utgångspunkt i att ge vägledning för bolagets avgränsning av personuppgiftsbehandlingar, så är det efter avslutad

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

granskning tydligt att det inte är funktionellt att kopiera poster ur 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.

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

2.2.2.3 Beskrivning av kategorier av registrerade och kategorierna av personuppgifter

Enligt artikel 30.1c i GDPR ska behandlingsregistret innehålla *en beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.* I sammanhanget är det viktigt att förtydliga att det som avses är en *beskrivning* av kategorier av registrerade och uppgifter. Det räcker alltså inte att bara ange vilka kategorierna är, utan läsaren ska av *beskrivningen* förstå vad kategorierna innefattar. Alltså vilka uppgifterna är, vilka de registrerade är, och hur de 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. I behandlingsregistret ska även samtliga kategorier av registrerade och samtliga kategorier av personuppgifter som behandlas beskrivas.

Bolaget uppger kategorier av registrerade och kategorier av personuppgifter för samtliga sina behandlingar. Dataskyddsombudet anser dock att det som anges inte uppfyller ovanstående krav. Dataskyddsombudets bedömning är att kategorier av registrerade och kategorier av personuppgift inte är beskrivna på ett sådant sätt att det av beskrivningen går att förstå vilka uppgifterna är, vilka de registrerade är, och hur de relaterar till varandra. I vissa fall anger bolaget kategorier som ”andra” eller ”invånare”, vilket gör det svårt att förstå vad kategorierna innefattar. Likaså när kategorierna ”leverantör” eller ”kunder” anges.

För vissa av behandlingarna finns även indikationer på att fler kategorier av personuppgifter behandlas än vad som anges i behandlingsregistret. Ett exempel är bland annat behandlingen ”Hantera bristande betalningar och handräckningar” där det under kolumnen kategorier av personuppgifter framgår att namn, adress, e-post, telefonnummer, födelsedata och kundnummer behandlas. Under behandlingens ändamål framgår dock att ansökan om betalningsförelägganden, begäran om avhysning samt konkurs- och skuldsaneringsansökningar hanteras. Utifrån vad som anges under behandlingens ändamål så behandlas sannolikt även andra kategorier av

[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.

personuppgifter än de angivna, som exempelvis uppgifter om skulder och eventuell annan finansiell information.

Bolaget rekommenderas att genomgående i sitt behandlingsregister utveckla beskrivningen av kategorier av registrerade och kategorier av personuppgifter på ett sådant sätt att det av beskrivningen framgår vilka uppgifter som behandlas om vilka registrerade. Därtill rekommenderas bolaget att se över behandlingsregistret så att samtliga kategorier av personuppgifter är angivna och beskrivna för respektive behandling.

2.2.2.4 Kategorier av mottagare

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

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

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

[5] Se Öhman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 4.9.
[6] EDPB, Data protection guide for small business, EDPB: Data protection guide for small business (hämtad 2024-11-26).
[7] Se till exempel i EDPB:s och EDPB:s behandlingsregister, EDPS record of processing activity - Personal Data Breach Notification, EDPB records of processing activities - Data subjects rights (hämtad 2024-11-27).

språkversioner av GDPR.[8] Dataskyddsombudets bedömning är att definitionen i artikel 4.9 inte ska läsas på annat sätt än att begreppet mottagare även omfattar den personuppgiftsansvariges egen organisation, en tolkning som också finner stöd i förarbetena till personuppgiftslagen.[9]

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

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

I bolagets behandlingsregistret anges specifika mottagare i vissa fall. I andra fall anges kategorier av mottagare. Dataskyddsombudet vill lyfta att även om det är kategorier av mottagare som ska anges, så har den registrerade vid en begäran om tillgång enligt artikel 15 i GDPR rätt att få information om specifika mottagare[12], och det är även information som ska lämnas till den registrerade i enlighet med informationsskyldigheten i artikel 13.1d och 14.1d i GDPR. Eftersom bolaget ändå är tvungen att dokumentera den specifika mottagaren enligt artikel 13-15 i GDPR så anser dataskyddsombudet att uppgiften ska dokumenteras i behandlingsregistret.

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

2.2.2.5 Överföring av personuppgifter till tredjeland

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

[8] Jämför till exempel med den engelska originalversionens *disclose*, det tyska *offengelegt,* franskans *recoit,* Italienskans *recive, och* spanskans *comuniquen*, så framstår det som klart att det som egentligen avses är vem som får ta del av uppgifterna, vilket också är så som EDPB uttrycker det i EDPB: Data protection guide for small business (hämtad 2024-11-27).
[9] Se Öman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 4.9, och SOU 1997:39 s. 335: ”*Begreppet mottagare omfattar i princip samtliga till vilka personuppgifter lämnas ut, även om den som tar emot uppgifterna inte skulle vara tredje man. Även den registrerade, personadatabiträdet och sådana personer som under den personadataansvariges eller personadatabiträdets direkta ansvar har befogenhet att behandla personuppgifter verkar således kunna betraktas som mottagare”.*
[10] Se EU-domstolens förhandsavgörande i mål C-579/21, C-579/21.
[11] Se EDPB:s behandlingsregister för ett konkret exempel, EDPB records of processing activities - Access to documents request (hämtad 2024-11-27). Se också mål C-154/21.
[12] Se mål C-154/21.

För att kunna redogöra för vilka faktiska överföringar som äger rum så måste den personuppgiftsansvarige veta vad som uttryckligen framgår av de avtal som träffats med personuppgiftsbiträden och eventuella underbiträden. Det är inte tillräckligt att veta ”på ett ungefär”, utan det är dom faktiska överföringarna som bolaget ska redogöra för. Bolaget anger att det inte sker några tredjelandsöverföringar för sina behandlingar, med något undantagsfall. Dataskyddsombudet utesluter inte att så är fallet. Samtidigt framgår att bolaget använder tredjelandsägda leverantörer för flera av behandlingarna, särskilt Microsoft. Detta behöver dock inte i sig innebära att det sker tredjelandsöverföringar.

Ett medskick är dock att det inte går att utgå ifrån att samma förutsättningar gäller för alla delar av, eller applikationer inom, M365-paketet. Geografisk hemvist för lagring och support kan skilja sig åt mellan olika applikationer. Bolaget måste därför 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 rekommenderar därför att bolaget ser över att det har skett en kartläggning av vilka överföringar som sker, i enlighet med vad som regleras i befintliga avtal, för att säkerställa att korrekt information anges om överföringar till tredjeländer.

2.2.2.6 Tidsfrister för radering

I artikel 30.1f i GDPR anges att den personuppgiftsansvarige ska*, om det är möjligt ange, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter*. Utifrån tillgänglig vägledning kan det konstateras att det finns högt ställda krav för att något ska kunna anses vara ”omöjligt”. Att något är omständligt, tar lång tid eller innebär mycket administration innebär fortfarande att det är ”möjligt”.[13] Viktigt att notera är även att tidsfristerna ska anges för de olika kategorierna av personuppgifter och inte för behandlingen som helhet eller per handlingstyp.

I majoriteten av fallen anges exempel på gallringsfristen per handlingstyp. I vissa fall kompletteras informationen med hänvisning till dokumenthanteringsplanen.

Det är inte 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 dataskyddsmyndigheterna EDPB[14] och

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

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

EDPS[15] register framgår de faktiska tidsfristerna direkt i registret, det samma gäller för den svenska tillsynsmyndighetens (IMY) eget register.[16]

Mot bakgrund av ovan rekommenderar dataskyddsombudet att bolaget anger de förutsedda tidsfristerna för radering (dvs när personuppgifterna kommer att gallras) för de olika kategorierna av personuppgifter för samtliga behandlingar i behandlingsregistret, i enlighet med vad som anges i artikel 30.1f.

2.2.2.7 Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder

En allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1 ska, om möjligt anges, enligt artikel 30.1g i GDPR. Precis som i fallet med tidsfrister för radering så innebär inte omständigheten att något är svårt, omständligt eller tidsödande att det är omöjligt. Det bör i princip inte förekomma något fall där det inte är möjligt för bolaget att ge en allmän beskrivning av skyddsåtgärder.[17] Att beskrivningen ska vara allmän betyder att det inte finns något krav om att återge en detaljerad beskrivning av alla skyddsåtgärder.[18] Det är dock inte tillräckligt att endast ange att säkerhetsåtgärder finns på plats. Efter genomförd granskning konstaterar dataskyddsombudet att det genomgående saknas en allmän beskrivning av organisatoriska säkerhetsåtgärder för behandlingarna.

Bolaget anger även ”dataskydd som standard” och ”inbyggt dataskydd” som säkerhetsåtgärder. Dataskyddsombudet vill framhålla att detta är dataskyddsrättsliga principer och inte allmänna beskrivningar av tekniska och organisatoriska säkerhetsåtgärder.

Bolaget rekommenderas att komplettera behandlingsregistret med allmänna beskrivningar av organisatoriska säkerhetsåtgärder för samtliga behandlingar.

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.

Det följer också av informationsskyldigheten i artikel 13.1c och 14.1c i GDPR att den personuppgiftsansvarige ska informera den registrerade om den rättsliga

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

grunden för en behandling. Eftersom uppgiften är något som den personuppgiftsansvarige ändå måste ha klart för sig rekommenderar dataskyddsombudet att den bör dokumenteras i behandlingsregistret, trots att det inte är obligatoriskt.

Flera rättsliga grunder kan vara tillämpliga för en behandling, men utgångspunkten är att en behandling för ett ändamål bara kan vila på en (enda) rättslig grund.[19]

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

En behandling kan avgränsas på olika sätt, dataskyddsombudet anser att ändamålet bör vara vägledande för avgränsningen av en behandling och att stadens verksamheter för funktionalitetens skull bör begränsa sig till ett ändamål för en behandling i behandlingsregistret. Det finns samtidigt inget förbud mot att konstruera behandlingar med flera närliggande ändamål. I sådana fall kan flera rättsliga grunder anges. En förutsättning för det är dock att varje enskilt ändamål är tydligt, konkret och specifikt och går att knyta till en rättslig grund, enligt devisen att personuppgifter bara kan behandlas för ett ändamål med stöd av en (enda) rättslig grund. Det ska också framgå vilka kategorierna av registrerade och personuppgifter är för dom enskilda ändamålen. Dvs. under kategori av registrerade och kategori av personuppgifter måste den personuppgiftsansvarige även beskriva vilka kategorier som hänför sig till vilket ändamål.[20] Att bygga mycket komplexa behandlingar med flera deländamål riskerar därför snabbt att bli väldigt rörigt.

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

Något som ytterligare talar emot att det är funktionellt att bygga väldigt komplexa behandlingsprocesser med flera rättsliga grunder är att det kommer vara svårt att informera de registrerade på ett korrekt sätt. Informationsskyldigheten i artikel 13.1c och 14.1c I GDPR kräver ju att den personuppgiftsansvarige tydligt informerar den registrerade om ändamålen med

[19] Article 29 Working Party, Guidelines 05/2020 on consent under Regulation 2016/679 s. 25, pt 121: "*Article 6 sets the conditions for a lawful personal data processing and describes six lawful bases on which a controller can rely. The application of one of these six bases must be established prior to the processing activity and in relation to a specific purpose".* Se också Öman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 6. *Vidare anser Artikel 29-gruppen att en behandling av personuppgifter för ett ändamål bara kan ha en (enda) rättslig grund.*

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

behandlingen och den rättsliga grunden. Om flera rättsliga grunder anges som stöd för behandlingen behöver verksamheten ändå definiera vilka uppgifter och delar av ändamålet som hänför sig till vilken av de rättsliga grunderna, vilket gör att det är svårt att se poängen med att bygga upp komplexa behandlingar med omfattande och svepande ändamålsbeskrivningar och flera rättsliga grunder.

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

3 Sammanfattande rekommendationer

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

- Ta fram dokumenterade arbetssätt för hantering av behandlingsregistret och säkerställ att dessa fastställs officiellt genom beslut. I detta ingår att fastställa tydligt utpekade roller och ansvar för att löpande hålla behandlingsregistret uppdaterat och i enlighet med lagkraven.
- Komplettera behandlingsregister med adress till bolaget samt kontaktuppgifter till dataskyddsombudet.
- Om bolaget väljer att ha en specifik medarbetare som kontaktpunkt är det viktigt att det tydligt framgår att medarbetare företräder den personuppgiftsansvariga i frågan. Säkerställ att det finns dokumenterade arbetssätt för att hålla uppgifterna aktuella.
- Gör en genomgripande översyn av samtliga ändamålsformuleringar i registret för att säkerställa att de uppfyller kraven i GDPR.
- Utveckla beskrivningen av kategorier av registrerade och kategorier av personuppgifter på ett sådant sätt att det av beskrivningen framgår vilka uppgifter som behandlas om vilka registrerade. Säkerställ även att samtliga kategorier av personuppgifter är angivna och beskrivna för respektive behandling.
- Gör en översyn av behandlingsregistret för att säkerställa att alla specifika mottagare för samtliga behandlingar anges, inklusive interna mottagare, och att det i samtliga fall framgår varför mottagaren är mottagare.
- Se över så att det har skett en kartläggning av vilka överföringar som sker, i enlighet med vad som regleras i befintliga avtal, för att säkerställa att korrekt information anges avseende överföringar till tredjeländer.
- Ange de förutsedda tidsfristerna för radering (dvs när personuppgifterna kommer att gallras) för de olika kategorierna av personuppgifter för samtliga behandlingar i behandlingsregistret.
- Komplettera behandlingsregistret med allmänna beskrivningar av organisatoriska säkerhetsåtgärder.
- Ser över hur personuppgiftsbehandlingarna är definierade och avgränsade. Förtydliga vilken rättslig grund som hänför sig till vilket specifikt ändamål och ange motiveringen till den rättsliga grunden.