Framtiden®
Byggutveckling

Styrelsehandling nr: 11
Styrelsedatum: 2026-03-26
Diarienummer: FBU-2026-00052

Handläggare: Jenny-Maria Ericsson Deogan
Telefon: 031-719 31 56
E-post: jenny-maria.ericsson.deogan@framtidenbyggutveckling.se

Årsrapport för dataskyddsarbete 2025

Informationsärende

Styrelsen för Framtiden Byggutveckling AB:

Årsrapport för dataskyddsarbetet 2025, antecknas

Ärendet

Bolaget har erhållit en årsrapport över verksamhetens dataskyddsarbete för 2025.

Det är varje nämnd och bolag som är ytterst ansvarig för att dess verksamhet följer dataskyddslag-stiftningen. För att stödja stadens nämnder och bolag i arbetet med dataskydd har ett dataskydds-ombud utsetts.
I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud åt stadens bolag och nämnder.
Ombudets uppgifter framgår direkt av lagstiftningen i GDPR (artikel 39).

Dataskyddsombudets viktigaste uppgift är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen.
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 till högsta förvaltningsnivå, och utifrån detta lämnar dataskyddsombudet årligen en rapport om den egna verksamhetens dataskyddsarbete till nämnder och bolag.

I årsrapporten 2025 redogör dataskyddsombudet resultatet av årets granskning av fasta kontrollpunkter och uppföljning av verksamhetens hantering av rekommendationer från årsrapporten 2024 samt resultatet av fördjupad kontroll 2024: Behandlingsregister enligt artikel 30 i GDPR.

Utifrån identifierade risker rekommenderar dataskyddsombudet att bolaget under 2026 prioriterar följande delar av dataskyddsarbetet:

- Kontrollpunkt 1: Dataskyddsorganisationen
- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Inom koncernen sker ett samordnat arbete utifrån alla bolagens rapporter avseende dataskydd. Vi har utifrån vår rapport och koncernens gemensamma arbete identifierat åtgärder som prioriteras på kort sikt men även på längre sikt.

Bedömning ur ekonomisk-, ekologisk- och social dimension

Ärendet är av administrativ karaktär och bolaget har inte funnit några särskilda aspekter på frågan utifrån dessa dimensioner.

Samverkan

Ärendet har inte varit föremål för samverkan

Bilagor

1. Årsrapport dataskyddarbete 2025
2. Kontrollplan för dataskyddsarbete 2026-2027
3. Fördjupad kontroll 2024 – Register över personuppgiftsbehandling

Styrelsehandling nr: 11
Bilaga nr: 1
FBU-2026-00052
2026-03-26

Årsrapport för dataskyddsarbetet 2025

Framtiden byggutveckling AB

2025-12-19

Innehåll

1 Inledning

Dataskyddsförordningen (GDPR) tillkom för att särskilt skydda människors rätt till integritet, samt var och ens rätt till insyn i 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. Dataskyddsreglerna styr hur personuppgifter får samlas in, användas och hanteras för att säkerställa att uppgifterna används korrekt och rättvist. Lagstiftningen finns till för att skydda individen från skada och sätter ramarna för hur personuppgifter får behandlas i en alltmer digital värld.

1.1 Göteborgs Stads dataskyddsombud

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 oberoende övervaka och granska att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Dataskyddsombudet har också till uppgift att ge råd och stöd till förvaltningar och bolag i dataskyddsfrågor.

Det är varje nämnd och bolag som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. Utifrån detta, och då dataskyddsombudet enligt lag ska rapportera om arbetet till högsta förvaltningsnivå, 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 och årets kontrollarbete, samt för resultatet av den uppföljning som genomförts av hur verksamheten hanterat och arbetat med de rekommendationer som lämnats tidigare. Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd.

1.2 Ändringar i kontrollarbetet 2025

I kontrollplanen för 2025–2026 aviserades att utformningen av den övergripande kontrollen skulle revideras under 2025. Revideringen innebär att kontrollpunkterna är tio i stället för tolv, samt att antalet frågor att besvara för varje kontrollpunkt är färre.[2] Kontrollpunkterna utgår även fortsättningsvis ifrån principerna i GDPR.

Syftet med ändringarna är att skapa bättre förutsättningar för dataskyddsenhetens uppföljningsarbete och rapportering till nämnder/styrelser, samt att förtydliga och förenkla verksamheternas arbete med kontrollen. Genom tydligare kontrollpunkter och enkätfrågor är dataskyddsenhetens förhoppning att resultatet av kontrollen ska kunna utgöra ett bättre stöd för verksamheterna i deras eget dataskyddsarbete.

[1] Artikel 39 i GDPR.
[2] Se bilaga 1 för information om reviderade kontrollpunkter.

2 Stadenövergripande iakttagelser 2025

2.1 Arbete med digitalisering och AI kräver dataskyddsresurser

Dataskyddsenheten har under året fortsatt kunnat konstatera att många verksamheter inte avsätter de resurser som krävs utifrån dataskydd i projekt som rör digitalisering och AI. Detta medför att dataskyddsperspektivet kommer in alldeles för sent vid införandet av nya tekniska lösningar. Då många initiativ inom digitalisering och AI drivs i projektform finns ofta en utarbetad tidsplan som verksamheterna förhåller sig till. Om verksamheten inte har med dataskyddsperspektivet från start i dessa projekt, innebär det även att dataskyddsenheten involveras i ett skede där det ofta redan är bestämt hur en personuppgiftsbehandling ska genomföras. Om dataskyddsenheten då har synpunkter på personuppgiftsbehandlingen, innebär det att verksamheten inte har möjlighet utifrån sin tidsplan att omhänderta dessa synpunkter. Eftersom dataskyddsenheten inte utgår från verksamhetens tidsplan, utan fokuserar på att säkerställa att dataskyddsperspektivet omhändertas, blir följden av detta många gånger irritation och att dataskydd ses som ett hinder för verksamhetsutveckling. Utifrån dataskyddsenhetens perspektiv är det dock inte dataskyddslagstiftningen som är problemet, utan problemet ligger i stället i att verksamheterna inte har tillräckliga resurser eller kunskap nog för att omhänderta dataskyddsperspektivet inom ramen för sitt digitaliseringsarbete.

Dataskyddsenheten vill i sammanhanget påminna stadens verksamheter att det är den personuppgiftsansvariges skyldighet att involvera dataskyddsombudet i god tid i frågor som rör skyddet av personuppgifter.[3] Detta innebär att det är viktigt att stadens verksamheter tar ansvar för att på ett korrekt sätt och i god tid involvera dataskyddsombudet i alla frågor som rör skyddet av personuppgifter. Om dataskyddsperspektivet fortsätter förbises i digitaliseringsarbetet, kommer det på sikt att ge upphov till uppenbara risker för de registrerades fri- och rättigheter.

2.2 Årets incidenter visar på betydelsen av grundläggande dataskyddsarbete

Under året har det inträffat flera större personuppgiftsincidenter inom verksamheter i Göteborgs Stad. En del incidenter har omfattat större delen av Stadens verksamheter, medan andra varit verksamhetsspecifika. Oavsett omfattning har alla incidenter tydligt visat på hur viktigt det är att verksamheten har koll på sina personuppgiftsbehandlingar. Här har dataskyddsenheten under året tyvärr kunnat

[3] Detta ansvar framgår av artikel 38.1 i GDPR.

konstatera att det finns stora brister inom många av stadens förvaltningar och bolag.

En grundläggande förutsättning för att en verksamhet ska kunna hantera en personuppgiftsincident är att verksamheten har koll på vilken eller vilka personuppgiftsbehandlingar incidenten gäller, samt hur ansvarsfördelningen för behandlingen ser ut. Detta är nödvändigt för att verksamheten ska kunna veta vilka registrerade samt vilka personuppgifter som incidenten omfattar, och utifrån det kunna genomföra en riskbedömning som i sig styr hur incidenten ska hanteras. En felaktig riskbedömning skulle kunna resultera i en bristande incidenthantering och medföra ytterligare risker för de registrerade.

En följd av de inträffade personuppgiftsincidenterna, och den uppmärksamhet som dessa har fått, är att antalet registrerade som vill utöva sina rättigheter och begär registerutdrag eller att deras uppgifter raderas har ökat. Även i verksamheters hantering av dessa har dataskyddsenheten kunnat konstatera brister kopplat till att det inom vissa verksamheter saknas kunskap om vilka personuppgiftsbehandlingar som utförs eller att verksamheter saknar möjligheter att tekniskt söka fram de personuppgifter som finns. Särskilt tydligt har detta visats efter incidenten hos stadens leverantör Miljödata, som utöver detta även aktualiserade frågor om interna biträdesrelationer och enskilda verksamheters möjligheter för att bestämma över hanteringen av sin information. Dataskyddsenheten kan konstatera att flera av de identifierade bristerna som aktualiserats i ljuset av dessa incidenter har påpekats av dataskyddsenheten tidigare. Dataskyddsenheten hoppas att årets inträffade incidenter blir en väckarklocka för förvaltningar och bolag i Göteborgs Stad, och att verksamheterna framåt prioriterar arbetet med grundläggande delar, som behandlingsregister och information till registrerade, i deras interna dataskyddsarbete.

I skrivande stund har Integritetsskyddsmyndigheten (IMY) inlett en tillsyn av Göteborgs Stad med anledning av incidenten hos Miljödata. Dataskyddsombudet förutsätter att Stadens verksamheter följer ärendet och framåt vidtar eventuella åtgärder utifrån resultatet av tillsynen.

3 Verksamhetsspecifika iakttagelser 2025

3.1 Verksamhetens dataskyddsarbete

Under året har kontakten mellan dataskyddsombudet och bolaget varit väldigt begränsad. Precis som under 2023 och 2024 har kontakten huvudsakligen utgjorts av deltagande vid Framtidenskoncernens gruppmöten inom dataskydd, där representanter för de olika bolagen deltar. Utöver det har bolaget informerat dataskyddsombudet om en inträffad personuppgiftsincident. Dataskyddsombudet har utifrån detta begränsad insyn i bolagets dataskyddsarbete.

I tidigare årsrapporter har dataskyddsombudet identifierat en risk i att dataskyddsombudet inte involveras i tillräcklig utsträckning i bolagets interna dataskyddsarbete. Denna risk gäller för flera av bolagen inom Framtidenkoncernen. Utifrån detta rekommenderas bolaget att i samverkan med övriga bolag inom koncernen se över hur koncernen som helhet kan arbeta med att involvera dataskyddsombudet i arbetet med dataskydd. I detta ingår att säkerställa att det finns dokumenterade arbetssätt för hur och när dataskyddsombudet ska involveras. Detta med syftet att säkerställa att koncernen som helhet uppfyller kravet enligt artikel 38.1 i GDPR gällande att dataskyddsombudet ska involveras i alla frågor som gäller dataskydd.

4 Granskning av dataskyddsarbetet 2025

4.1 Övergripande kontroll 2025

Under 2025 har dataskyddsombudet kontrollerat verksamhetens dataskyddsarbete utifrån tio kontrollpunkter. Kontrollen har genomförts genom en enkät. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Metoden syftar till att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

Enkäten består av tio kontrollpunkter där varje punkt innehåller ett antal delfrågor utformade som påståenden. Verksamheten ska i svaret uppskatta hur väl påståendet stämmer in på verksamheten utifrån en fyrgradig skala. Nytt för i år är att verksamheten även ska motivera sina svar i vissa fall. Syftet med detta är att öka dataskyddsombudets möjlighet till insyn. Om något saknas i verksamheternas dokumenterade arbetssätt behöver det framgå så att det blir tydligt för dataskyddsombudet och för verksamheten var bristerna finns i det systematiska arbetet, så att det kan åtgärdas.

4.1.1 Ett riskbaserat arbetssätt

I kontrollarbetet används en modell som består av fyra kategorier, vilka representerar fyra olika risknivåer. Verksamheten får utifrån sina svar ett värde som visar vilken risknivå verksamheten befinner sig på inom respektive kontrollpunkt. Genom att arbeta med risknivåer möjliggörs ett riskbaserat arbetssätt för både verksamhet och dataskyddsombud, då resultaten ger en bild av vad verksamheten behöver prioritera i dataskyddsarbetet framåt.

Risknivå	Beskrivning	Färgkod
Nivå 1	Höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.	
Nivå 2	Risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.	
Nivå 3	Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.	
Nivå 4	Inga direkta risker av betydelse identifierade. Indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete.	

4.1.2 Verksamhetens resultat

Verksamhetens resultat illustreras genom diagram, se bilaga 2. Diagrammet visar vilken risknivå verksamheten befinner sig inom för respektive kontrollpunkt, och utgår enbart från verksamhetens egna svar på frågorna i enkäten.

Dataskyddsombudet gör i årsrapporten ingen bedömning eller analys av resultatet som helhet, utan kommenterar företrädesvis resultatet för de kontrollpunkter som varit rekommenderade fokusområden för 2025 i samband med uppföljningen samt de delar som uppenbart avviker från dataskyddsombudets bedömning.

Resultatet av kontrollen kommer, tillsammans med de rekommenderade fokusområdena för 2026, utgöra grunden för dataskyddsombudets arbete med verksamheten under kommande år.

4.2 Uppföljning av lämnade rekommendationer

4.2.1 Uppföljning av verksamhetens arbete med rekommenderade fokusområden 2025

Dataskyddsombudet har följt upp hur verksamheten arbetat med de fokusområden som rekommenderades för 2025.

Fokusområde 1: Dataskyddsorganisation

Verksamheten gavs följande rekommendationer:

- Se över hur verksamheten kan involvera dataskyddsombudet mer i arbetet med dataskydd, med syftet att säkerställa att bolaget uppfyller kravet enligt artikel 38.1 i GDPR gällande att dataskyddsombudet ska involveras i alla frågor som gäller dataskydd. I rekommendationen ingår det att säkerställa att det finns dokumenterade arbetssätt för hur dataskyddsombudets involveras.

Kommentarer och rekommendationer: Bolaget anger i uppföljningen att dataskyddsombudet har involverats i specifika dataskyddsfrågor, samt att bolaget har en dokumenterad rutin att alltid kontakta dataskyddsombudet vid personuppgiftsincidenter och konsekvensanalyser. Dataskyddsombudet uppges även vara inbjuden till Framtiden koncernens gemensamma dataskyddsmöten några gånger per termin, för gemensamma avstämningar och uppdateringar av hur bolaget arbetar, i nuläget.

Dataskyddsombudets kontakt med bolaget under 2025 har varit ytterst begränsad. Utifrån detta kvarstår ett behov av att se över hur bolaget säkerställer efterlevnad av artikel 38.1 i GDPR gällande att dataskyddsombudet ska involveras i alla frågor som gäller dataskydd. Kontrollpunkten kommer därför att kvarstå för 2026.

Fokusområde 2: Register över personuppgiftsbehandlingar

Verksamheten gavs följande rekommendationer:

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

Kommentarer och rekommendationer: Bolaget uppger att de har tagit del av den stadengemensamma granskningsrapporten och arbetar med behandlingsregistret utifrån rekommendationerna som framgår där i.

Utifrån att bolaget anger att det pågår ett arbete kommer kontrollpunkten kvarstå som ett fokusområde för 2026.

5 Rekommenderade fokusområden 2026

Dataskyddsombudet rekommenderar, utifrån gjorda iakttagelser och resultaten av uppföljningen, verksamheten att under 2026 fortsätta prioritera arbetet med de kontrollpunkter som rekommenderas för 2025. 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 2026.

Bolaget rekommenderas under 2026 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 1: Dataskyddsorganisation och övergripande styrning i dataskyddsarbetet

Bolaget rekommenderas att i samverkan med övriga bolag inom koncernen se över hur koncernen som helhet kan arbeta med att involvera dataskyddsombudet i arbetet med dataskydd. I detta ingår att säkerställa att det finns dokumenterade arbetssätt för hur och när dataskyddsombudet ska involveras.

- Kontrollpunkt 2: Register över personuppgiftsbehandlingar

Bolaget rekommenderas fortsätta arbetet med kartlägga och dokumentera bolagets personuppgiftsbehandlingar enligt artikel 30 i GDPR.

6 Bilagor

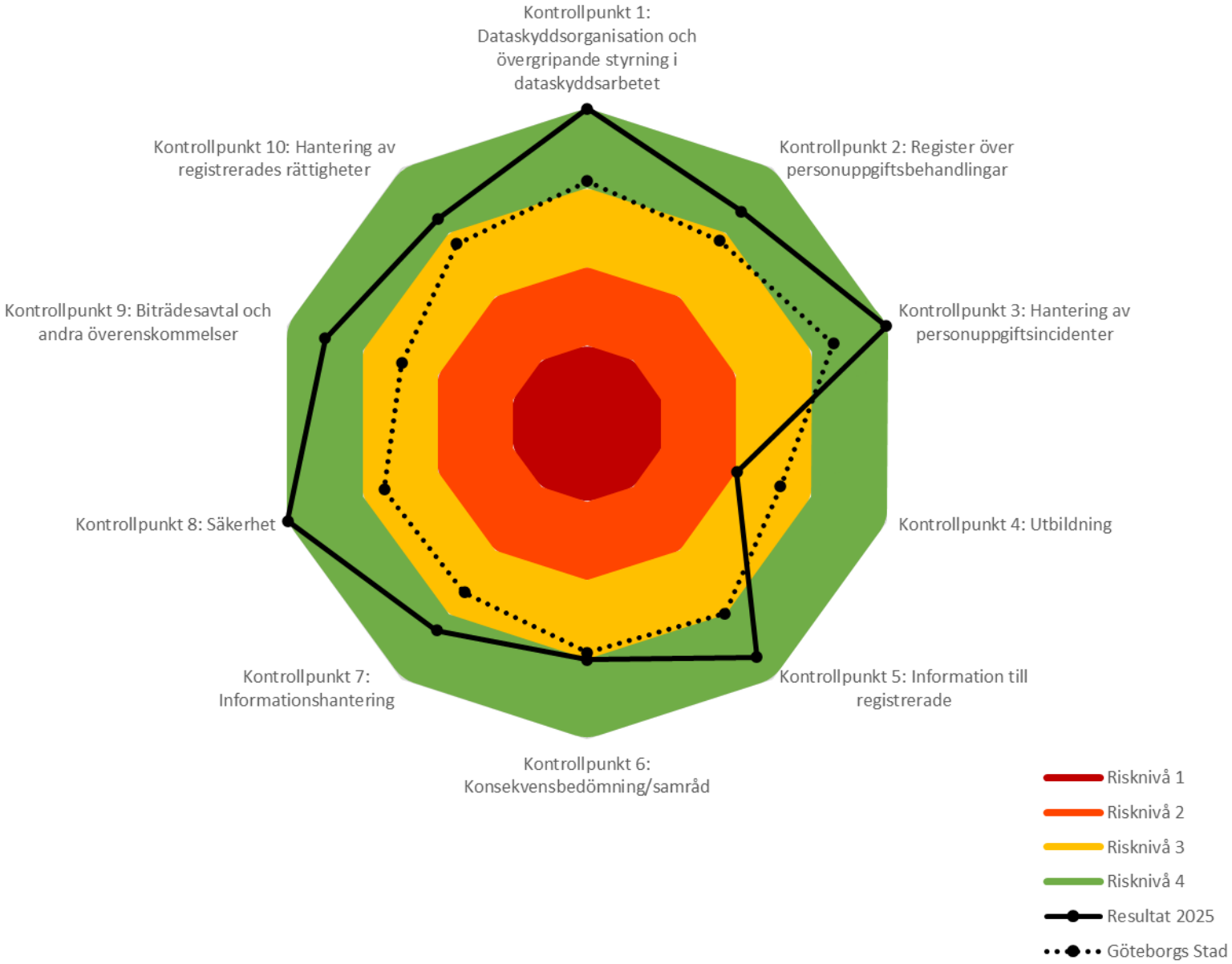
Bilaga 1: Reviderade kontrollpunkter

Bilaga 2: Verksamhetens resultat från den övergripande kontrollen 2025

Bilaga 1: Reviderade kontrollpunkter

Kontrollpunkter 2025	**Kommentar**
Kontrollpunkt 1: Dataskyddsorganisation och övergripande styrning i dataskyddsarbetet	Ersätter de tidigare kontrollpunkterna *Dataskyddsorganisation* och *Övergripande styrning i dataskyddsarbetet*.
Kontrollpunkt 2: Register över personuppgiftsbehandlingar	Namn på kontrollpunkt oförändrat.
Kontrollpunkt 3: Hantering av personuppgiftsincidenter	Ersätter den tidigare kontrollpunkten *Personuppgiftsincidenter*.
Kontrollpunkt 4: Utbildning	Namn på kontrollpunkt oförändrat.
Kontrollpunkt 5: Information till registrerade	Ersätter den tidigare kontrollpunkten *Informationsplikt*.
Kontrollpunkt 6: Konsekvensbedömning/samråd	Namn på kontrollpunkt oförändrat.
Kontrollpunkt 7: Informationshantering	Ersätter den tidigare kontrollpunkten *E-post och dokumenthantering*, samt delar av kontrollpunkterna *IT-projekt och upphandling* och *IT-system och digitala verktyg.*
Kontrollpunkt 8: Säkerhet	Ersätter delar av de tidigare kontrollpunkterna *IT-projekt och upphandling* och *IT-system och digitala verktyg.*
Kontrollpunkt 9: Biträdesavtal och andra överenskommelser	Namn på kontrollpunkt oförändrat. Kompletteras med delar från den tidigare kontrollpunkten *IT-projekt och upphandling*.
Kontrollpunkt 10: Hantering av registrerades rättigheter	Namn på kontrollpunkt oförändrat.

Bilaga 2: Verksamhetens resultat 2025



Styrelsehandling nr: 11
Bilaga nr: 2
FBU-2026-00052
2026-03-26

Kontrollplan för dataskyddsarbetet 2026–2027

Nämnder och bolag i Göteborgs Stad

2026-02-27

Innehåll

1 Inledning

Dataskyddsförordningen (GDPR) tillkom för att särskilt skydda människors rätt till integritet, samt var och ens rätt till insyn i 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. Dataskyddsreglerna styr hur personuppgifter får samlas in, användas och hanteras för att säkerställa att uppgifterna används korrekt och rättvist. Lagstiftningen finns till för att skydda individen från skada och sätter ramarna för hur personuppgifter får behandlas i en alltmer digital värld.

Det är varje nämnd och bolag som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. Att nämnder 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.

1.1 Göteborgs Stads dataskyddsombud

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] Dataskyddsombudet har särskild sakkunskap i dataskyddslagstiftning och arbetar oberoende med att övervaka och granska att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Dataskyddsombudet har också till uppgift att ge råd och stöd till förvaltningar och bolag i dataskyddsfrågor.

Varje verksamhet ansvarar för att stödja dataskyddsombudet i utförandet av uppdraget genom att tillhandahålla de resurser som krävs för arbetet samt tillgång till personuppgifter och behandlingsförfaranden.[2] Det är också verksamhetens ansvar att säkerställa att dataskyddsombudet inte tar emot instruktioner eller utsätts för repressalier för att ha utfört sina uppgifter.[3]

[1] Artikel 39 i GDPR.
[2] Artikel 38.2 i GDPR.
[3] Artikel 38.3 i GDPR.

2 Kontrollarbetet 2026–2027

Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att verksamheten 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. 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. Genom kontroller kan dataskyddsombudet kartlägga verksamhetens dataskyddsarbete, och denna kartläggning kan sedan användas som ett stöd av verksamheten i dess fortsatta arbete med dataskydd.

Dataskyddsombudets kontrollarbete specificeras genom denna kontrollplan, som syftar till att informera personuppgiftsansvariga om upplägg och tidplan för kontrollarbetet åren 2026 och 2027. Dataskyddsombudets kontrollarbete löper över tvåårsperioder, och en ny kontrollplan kommer att skickas ut vartannat år.

Syftet med att arbeta utefter en på förhand fastställd kontrollplan är att det ska bidra till att sätta fokus på verksamhetens dataskyddsarbete och därmed säkerställa ett kontinuerligt dataskyddsarbete som skapar förutsättningar för efterlevnad av förordningen samt göra dataskyddsarbetet till en integrerad del i verksamhetens informationssäkerhetsarbete.

2.1 Kontrollarbetets delar

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

2.1.1 Övergripande kontroll

Den övergripande kontrollen utgår från tio kontrollpunkter[4] och genomförs genom en enkät som fylls i av verksamheten. Varje kontrollpunkt innehåller ett antal delfrågor utformade som påståenden och verksamheten ska uppskatta hur väl påståendet stämmer in på verksamheten. I vissa fall efterfrågar dataskyddsombudet även att verksamheten motiverar sina svar.

Resultaten från enkäten är tänkt att ge en bild av verksamhetens dataskyddsarbete och ska kunna användas som underlag i verksamhetens löpande dataskyddsarbete. Syftet är att få till ett långsiktigt och systematiskt arbetssätt, samt åskådliggöra de förändringar som vidtas över tid.

[4] Kontrollpunkterna har utformats utifrån 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 verksamhetens processer. Se bilaga 1 för beskrivning av kontrollpunkterna.

2.1.2 Fördjupad kontroll

I utformningen av den fördjupade kontrollen utgår dataskyddsombudet från de risker som identifierats, både inom enskilda verksamheter och på en övergripande nivå. Hänsyn tas även till vad som bedöms kunna få störst effekt för flest verksamheter inom Staden. Den fördjupade kontrollen är utformad som en stickprovskontroll, vilket innebär att alla verksamheter inte kontrolleras. I stället genomförs kontrollen inom ett antal förvaltningar och bolag som dataskyddsombudet anser utgör ett representativt urval för stadens verksamheter.

Resultaten från kontrollen redovisas dels på verksamhetsnivå genom separata rapporter till berörda nämnder och bolag, dels på övergripande nivå genom en stadengemensam rapport. Den stadengemensamma rapporten är tänkt att kunna användas av flera verksamheter och genom denna kan även de verksamheter som ej varit med i kontrollen ta del av och dra lärdom från resultaten av kontrollen.

2.1.3 Uppföljning

Uppföljning av de rekommendationer som tidigare lämnats till verksamheten i samband med årsrapportering eller fördjupade kontroller genomförs årligen. Resultatet redovisas till styrelse eller nämnd i verksamhetens årsrapport.

2.2 Tidplan för kontrollarbetet 2026–2027

2026	Aktivitet
Februari	Kontrollplan för 2026–2027 lämnas till nämnder och styrelser.
April-Oktober	Fördjupad kontroll genomförs. Under 2026 är fokus för den fördjupade kontrollen verksamheternas hantering av personuppgiftsincidenter, med syftet att kontrollera verksamheternas efterlevnad av artikel 33 och 34 i GDPR.
Oktober	Uppföljning av lämnade rekommendationer.
November – december	Genomgång av innehåll i årsrapport med respektive verksamhet.
December	Årsrapport översänds till nämnd eller styrelse.

2027	Aktivitet
September	Övergripande kontroll genomförs.
Oktober	Uppföljning av lämnade rekommendationer.
November – december	Genomgång av innehåll i årsrapport med respektive verksamhet.
December	Årsrapport översänds till nämnd eller styrelse.

3 Rapportering

3.1 Årsrapport

Det är varje nämnd och bolag som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. Utifrån detta, och då dataskyddsombudet enligt lag ska rapportera om arbetet till högsta förvaltningsnivå, lämnar dataskyddsombudet årligen en rapport om respektive verksamhets dataskyddsarbete till nämnder och bolag i Göteborgs Stad. I rapporten redogör dataskyddsombudet för de iakttagelser som gjorts under året och årets kontrollarbete, samt för resultatet av den uppföljning som genomförts av hur verksamheten hanterat och arbetat med de rekommendationer som lämnats tidigare. Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd.

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 eller bolag. Det kan också vara om dataskyddsombudet uppmärksammar att det inom verksamheten fattats beslut som är oförenliga med dataskyddslagstiftningen och dataskyddsombudets råd.

Kontakt

Frågor avseende kontrollplanen hänvisas till dataskyddsenhetens funktionsbrevlåda; dso@intraservice.goteborg.se.

Bilaga 1 – Beskrivning av kontrollpunkter

Kontrollpunkter	Beskrivning
Kontrollpunkt 1: Dataskyddsorganisation och övergripande styrning i dataskyddsarbetet	Kontrollpunkten avser verksamhetens övergripande styrning samt organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete. Dataskyddsarbetet behöver vara systematiskt med tydliga roller, ansvar och intern uppföljning. Tydlig styrning sätter ramarna för arbetet med dataskydd och främjar ett riskbaserat arbetssätt. Punkten följer upp verksamhetens dataskyddsorganisation, definierade ansvarsområden och tillhandahållna resurser för arbetet. Även verksamhetens systematiska arbete utifrån en plan för dataskyddsarbetet och hur verksamheten säkerställer involvering av dataskyddsombudet ingår i punkten.
Kontrollpunkt 2: Register över personuppgiftsbehandlingar	Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med att säkerställa ett uppdaterat och heltäckande behandlingsregister och dokumenterade arbetssätt för detta omfattas av kontrollpunkten.
Kontrollpunkt 3: Hantering av personuppgiftsincidenter	Kontrollpunkten avser verksamhetens förutsättningar för att identifiera och hantera personuppgiftincidenter, samt hur verksamheten arbetar med uppföljning av såväl arbetssätt som inträffade incidenter.
Kontrollpunkt 4: Utbildning	Kontrollpunkten avser verksamhetens arbete med att utbilda och upprätthålla kunskaper och medvetenhet i dataskyddsfrågor hos anställda.
Kontrollpunkt 5: Information till registrerade	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. Informationen som lämnas till registrerade ska överensstämma med behandlingsregistret.
Kontrollpunkt 6: Konsekvensbedömning/samråd	Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras och genomföra denna. I detta ingår att verksamheten har dokumenterade arbetssätt för arbetet med konsekvensbedömningar och hur dataskyddsombudet involveras i arbetet. Därtill tillkommer att verksamheten har dokumenterade arbetssätt för att hantera de risker som identifieras i konsekvensbedömningen samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

Kontrollpunkt 7: Informationshantering	Kontrollpunkten avser verksamhetens informationshantering. En aktuell och fastställd dokumenthanteringsplan med gallringsbeslut är en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddsförordningen. Vidare behöver verksamheten ha tydliga instruktioner för hur olika kategorier av personuppgifter ska hanteras i olika medel. Kontrollpunkten omfattar dessa delar samt verksamhetens arbete med att säkerställa att gallring samt användning av medel följs.
Kontrollpunkt 8: Säkerhet	Dataskydd och informationssäkerhet hänger ihop. Kontrollpunkten avser verksamhetens dokumenterade arbetssätt för arbetet med säkerhet i samband med behandlingarna, enligt kraven i artikel 32 i GDPR.
Kontrollpunkt 9: Biträdesavtal och andra överenskommelser	Kontrollpunkten avser verksamhetens bedömning kopplat till, samt hantering av, biträdesavtal och andra överenskommelser gällande dataskydd. Verksamhetens dokumenterade arbetssätt för uppdatering och uppföljning av tecknade biträdesavtal omfattas av kontrollpunkten.
Kontrollpunkt 10: 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 dokumenterade arbetssätt för arbetet, och att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan. I kontrollpunkten ingår även verksamheternas dokumenterade arbetssätt för att hantera skadeståndsanspråk enligt artikel 82 i GDPR.

Göteborgs Stad

Styrelsehandling nr: 11
Bilaga nr: 3
FBU-2026-00052
2026-03-26

Fördjupad kontroll 2024: Register över personuppgiftsbehandlingar

Dataskyddsombudets övergripande rapport från arbetet med granskning av behandlingsregister enligt artikel 30 GDPR

2025-02-10

Innehåll

1 Inledning

1.1 Kontrollområdet

I enlighet med vad som aviserades i kontrollplan för år 2024/2025 genomförde dataskyddsombudet en fördjupad kontroll under hösten 2024. Det fördjupade kontrollområdet som valdes ut för 2024 års kontroll var 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 utvalda förvaltningars och bolags efterlevnad av artikel 30 i GDPR, och därigenom skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register.

I kontrollen av behandlingsregistret har ingått 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 inkluderade även att se undersöka hur behandlingsregistret används i det systematiska dataskyddsarbetet inom verksamheten.

1.3 Tillvägagångssätt

Den fördjupade kontrollen genomfördes i två steg. Den första delen av kontrollen genomfördes i form av en skrivbordskontroll. I denna del fick de deltagande verksamheterna 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 behandlingsregistret för att kontrollera om de registrerade behandlingarna uppfyller kraven 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 verksamheterna 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 verksamheterna och vid detta gått igenom verksamhetens behandlingsregister, för att i dialog med verksamheten kunna påvisa och förklara eventuella förbättringsområden och identifierade brister. Syftet med denna metod var att få till en lärandeprocess utöver dataskyddsombudets rent kontrollerande funktion. Dataskyddsenhetens målsättning var att de kontrollerade verksamheterna efter genomförd kontroll skulle ha förutsättningar att uppnå en godtagbar nivå på behandlingsregistret samt att med stöd av dataskyddsombudets rekommendationer ha fått vägledning i hur arbetet med att hålla registret aktuellt kan utformas. Resultatet av kontrollen har därefter sammanställts och redovisats i enskilda rapporter för respektive verksamhet.

1.4 Rapportering och uppföljning

Resultatet av kontrollen visade sammantaget på stora brister i omhändertagandet av artikel 30 i GDPR. För att även de verksamheter som ej ingått i kontrollen under 2024 ska få ta del av, och kunna lära utifrån, resultaten av kontrollen har dataskyddsombudet tagit fram denna övergripande rapport.

Rapporten innehåller både generella iakttagelser från kontrollen, dataskyddsombudets bedömningar i olika sakfrågor och konkreta exempel på hur behandlingsregistret kan utformas med hänvisningar till olika rättskällor som dataskyddsombudet anser har ett generellt värde för hela Staden. Rapporten blir en form av ytterligare vägledning avseende hur arbetet med behandlingsregistret kan utformas för att skapa förutsättningar för ett funktionellt dataskyddsarbete där kraven i artikel 30 i GDPR kan uppfyllas.

Dataskyddsombudet kommer under 2025 följa upp dels att samtliga av Stadens verksamheter har tagit del av rapporten, dels hur verksamheterna avser omhänderta de generella rekommendationerna i arbetet med det egna behandlingsregistret.

2 Dataskyddsombudets generella iakttagelser

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 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]

Dataskyddsombudets granskning av utvalda förvaltningar och bolag visar att Stadens verksamheter valt att omhänderta denna fråga på olika sätt. En del register innehåller inte dessa uppgifter överhuvudtaget, trots att de är obligatoriska, andra innehåller bara uppgifterna delvis. Ingen av de granskade verksamheterna har angett fullständig information i sina register. För det fall att ett bolag eller en förvaltning inte dokumenterat information om namn och kontaktuppgifter till den personuppgiftsansvarige, samt dataskyddsombudets kontaktuppgifter, så bör detta åtgärdas snarast eftersom uppgifterna är obligatoriska.

Exakt i vilken form som Stadens verksamheter väljer att presentera informationen är upp till respektive bolag och förvaltning att avgöra. Informationen kan antingen anges som kolumner vid varje enskild behandling i registret, eller som en övergripande information i inledningen, där det tydligt framgår att informationen gäller för samtliga behandlingar. 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 för den aktuella behandlingen framgå av behandlingsregistret.

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.

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

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 innefatta något annat än det som direkt kan utläsas av beskrivningen, det får alltså inte finnas dolda eller underförstådda syften som inte direkt framgår.

Det betyder att ändamålsbeskrivningen inte ska innehålla formuleringar som *bland annat, med mera, et cetera* eller *till exempel*. Ett ändamål som formulerats med en sådan beskrivning uppfyller inte kravet på att vara uttryckligt och är inte specifikt, då det inte är begränsat till vad som direkt kan utläsas av ändamålsbeskrivningen, och saknar därför, enligt dataskyddsombudets uppfattning, 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 (se också avsnittet om rättslig grund i denna rapport).

Efter genomförd granskning bedömer dataskyddsombudet att det finns omfattande brister inom Staden avseende arbetet med att avgränsa behandlingar och att formulera funktionella ändamål som är tydliga, konkreta och specifika. Ändamålen i de register som granskats är genomgående otydliga, abstrakta och ospecifika. I flera fall är beskrivningarna så otydliga att det helt enkelt inte går att utläsa vad som avses, i andra är ändamålet så omfattande och abstrakt att den direkta kopplingen till varför personuppgifter behandlas inte går att förstå, och, slutligen, så är flera behandlingar så omfattande och ospecifika att det är omöjligt att bedöma vad som egentligen innefattas i ändamålet.

Ett problem som dataskyddsombudet identifierat är att många av Stadens verksamheter utan urskiljning verkar ha utgått ifrån klassificeringsstrukturen när de upprättat sina behandlingsregister. Dataskyddsombudet anser visserligen att klassificeringsstrukturen kan ge förutsättningar för att på ett systematiskt och tydligt sätt identifiera ändamål och de behandlingar som sker i en

[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.

personuppgiftsansvarigs verksamhet. Det är dock tydligt efter avslutad granskning att det inte är funktionellt att bara infoga poster ur klassificeringsstrukturen som de är, och rakt av omvandla dessa till behandlingar i behandlingsregistret. Detta eftersom utgångspunkten i klassificeringsstrukturen och dokumenthanteringsplaner är verksamhetsprocesser och dokument eller handlingar, och inte behandlingen av personuppgifter. Att kopiera direkt från klassificeringsstrukturen och använda den för att avgränsa behandlingarna i behandlingsregistret leder till otydliga ändamålsformuleringar och till behandlingsavgränsningar som inte är funktionella, till behandlingar som egentligen kanske hänger ihop i en större behandling, eller till behandlingar som kanske inte alls borde vara egna behandlingar, utan i stället utgör en naturlig del i andra behandlingar. Ett ytterligare problem med att bara utgå ifrån klassificeringsstrukturen är att processgrupperna och verksamhetsprocesserna som beskrivs ofta är för breda och generella för att kunna utgöra en enskild personuppgiftsbehandling. Det medför att ändamål som formuleras direkt utifrån strukturen tenderar att bli abstrakta och ospecifika, i motsats till det som eftersträvas, alltså att ändamålen ska vara konkreta och specifika.

I praktiken innebär det att verksamhetsprocesser många gånger inte rakt av kan formuleras som ett ändamål, utan i stället behöver brytas ner i flera olika ändamål för att uppfylla kraven i artikel 5.1b i GDPR. Dataskyddsombudet rekommenderar i första hand att varje enskilt ändamål dokumenteras som en behandling/rad i behandlingsregistret. Det finns dock inget som hindrar att flera närliggande ändamål tillsammans ingår i en behandling om det kan anses motiverat.[4] En förutsättning för ett sådant upplägg är att varje enskilt ändamål uppfyller kraven på att vara *särskilda, uttryckligt angivna och berättigade,* att det tydligt framgår att det handlar om olika ändamål, och att varje ändamål har en rättslig grund enligt artikel 6.1 i GDPR.

I en behandling med flera olika ändamål behöver också varje enskilt ändamål kopplas till all information i led c-g i artikel 30.1 i GDPR. Det innebär att även kategorierna av registrerade och personuppgifter[5] enligt led c, mottagare enligt led d, förekomsten av tredjelandsöverföringar enligt led e, och tidsfristerna för radering och en allmän beskrivning av säkerhetsåtgärder enligt led f och g behöver beskrivas för varje ändamål. Ytterligare en förutsättning för att det ska fungera är också att ändamålen är relaterade på ett sådant sätt att det är logiskt att gruppera dom tillsammans inom ramen för en behandling. Det här kan vara ett lockande sätt att lägga upp arbetet med behandlingsregistret på, men tänk på att ett sådant arbetssätt ställer stora krav på den som utformar registret. För en behandling med flera närliggande ändamål blir det snabbt väldigt mycket information.

[4] Se också Öman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 30. Öman anser att: *Varje ändamål för behandling av personuppgifter (led a)* [Öman menar naturligtvis led b här, dataskyddsombudets anmärkning] *utgör således en rad i registret, med efterföljande kolumner med upplysningarna enligt led b–g.* Det vill säga varje ändamål utgör en egen behandling i registret. Dataskyddsombudet anser visserligen att detta oftast är att föredra, men att det inte finns något som hindrar att en behandling innehåller flera ändamål under förutsättning att det är motiverat och tydligt framgår att det är olika ändamål, att varje ändamål har en egen rättslig grund, och att varje ändamål är kopplat till informationen i led c-g.

[5] EDPB, 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."*

Att formulera tydliga ändamål som uppfyller kraven i GDPR är inte enkelt. Många verksamheter har formulerat sina ändamål med utgångspunkt i vad man *gör* med uppgifterna och/eller *hur* man behandlar uppgifterna, utgångspunkten är ofta, som tidigare nämnts, verksamhetens arbetsprocess. Detta missar dock målet eftersom ändamålet utgår ifrån *varför* personuppgifter behöver behandlas. I offentlig verksamhet har detta *varför* i många personuppgiftsbehandlingar sin grund i den lagstiftning som reglerar verksamheten. Ett tips till Stadens verksamheter är därför att utgå ifrån de lagkrav som organisationen har att förhålla sig till och formulera sina ändamål utefter dessa. Det går så klart inte att säga att det alltid fungerar, men det är en god utgångspunkt, om inte annat för att få in rätt tänk i hur välformulerade ändamål kan beskrivas. Sammantaget så är dataskyddsombudets övergripande rekommendation till samtliga förvaltningar och bolag i Staden att aktivt arbeta med just ändamålen som vägledande för avgränsningen av behandlingar och att lägga extra vikt vid att formulera genomtänkta och tydliga ändamål som utgår ifrån varför personuppgifter behandlas. För ytterligare vägledning i hur behandlingar kan avgränsas och hur ändamål kan formuleras på ett funktionellt sätt hänvisas till dataskyddsenhetens informationsmaterial om behandlingsregistret[6], samt European Data Protection Board (EDPB) och European Data Protection Supervisor (EDPS) register över personuppgiftsbehandlingar.[7]

2.3 Beskrivning av kategorierna av registrerade och av 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 vill säga det räcker inte att bara ange vilka kategorierna är. Läsaren ska av *beskrivningen* förstå vad kategorierna innefattar. För att uppfylla kraven i artikeln ska det därför framgå vilka uppgifterna är, vilka de registrerade är, och hur de relaterar till varandra, det vill säga kopplingen mellan de registrerade och de uppgifter som behandlas.[8] Beskrivningen i artikelns led c behöver alltså vara något utöver att bara ange, exempelvis, *sökande*, *anställda*, *kontaktuppgifter*, *uppgifter om sociala förhållanden*, med mera. Helt enkelt för att det ska gå att förstå behandlingen. I sammanhanget är det viktigt att påpeka att kategoriseringen ska vara objektiv och värdeneutral. Vid beskrivningen av registrerade ska inte kategorier som kan tolkas som nedsättande eller värderande förekomma.

[6] Behandlingsregister – en del av dataskyddsenhetens informationsinsats våren 2023, Tillgänglig: DSE Information om behandlingsregister (2023) (hämtad 2025-01-24).
[7] EDPB:s behandlingsregister, Tillgänglig: EDPB records of processing activities pursuant to article 31 of Regulation 2018/1725 (hämtad 2025-01-23).
EDPS:s behandlingsregister, Tillgänglig: Records Register | European Data Protection Supervisor (hämtad 2025-01-23).
[8] Se EDPB:s behandlingsregister, Tillgänglig: EDPB Processing of personal data in the context of an access to documents request (hämtad 2025-01-24) 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.

En förutsättning för att kunna uppfylla GDPR:s grundläggande princip om ändamålsbegränsning, den så kallade finalitetsprincipen, är att den personuppgiftsansvarige på något sätt behöver hålla reda på för vilka ändamål varje personuppgift har samlats in. I praktiken innebär det att det inte är tillräckligt att veta vilka kategorier av uppgifter som behandlas, den personuppgiftsansvarige behöver veta vilka de faktiska uppgifterna är och koppla dessa till ett specifikt ändamål[9].

Efter avslutad granskning kan dataskyddsombudet konstatera att de granskade verksamheterna generellt har fyllt i kategorier av registrerade och kategorierna av personuppgifter i behandlingsregistret. Dataskyddsombudets bedömning är dock generellt sett att de inte att 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. Detta eftersom det i princip aldrig beskrivs vilka personuppgifter som behandlas för vilken kategori av registrerade (när flera kategorier av registrerade anges). Vidare beskrivs kategori av registrerade ofta bristfälligt. Även om begrepp som kan uppfattas vara tydliga används för att beskriva en kategori registrerade kan kategorin i många fall utvecklas och beskrivas med större precision. Som framgår ovan behöver exempelvis kategori av registrerade beskrivas tydligare än att bara ange, till exempel, *sökande eller anställda.* I stället för att skriva ”sökande” så skulle verksamheten kunna skriva ”s*ökande som inkommer med ansökan om X*”. I stället för att skriva ”anställda” så skulle verksamheten kunna skriva *”anställda handläggare som har till arbetsuppgift att handlägga ärenden gällande Y”,* och så vidare. Detsamma gäller för beskrivning av kategorierna av personuppgifter. Att enbart ange kategorier av personuppgifter som exempelvis *kontaktuppgifter eller uppgifter om sociala förhållanden,* ger inte svar på vilka personuppgifter som behandlas.

Därmed behöver även kategorierna av personuppgifter beskrivas så att det går att förstå vilka personuppgifterna som behandlas faktiskt är. I stället för att enbart ange ”kontaktuppgifter” så behöver verksamheten också ange vad kategorin innefattar, till exempel enligt följande: ”*kontaktuppgifter: namn, adress, e-post, telefonnummer”*, och så vidare. I stället för att enbart ange *uppgifter om sociala förhållanden* så behöver verksamheten ange vad kategorin innefattar, till exempel enligt följande: ”*Uppgifter om sociala förhållanden: Uppgifter om den sökandes ekonomiska situation såsom inkomst och skulder, boendemiljö, familjerelationer”,* och så vidare.

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

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

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. Till exempel anses inte Skatteverket vara en mottagare när en verksamhet skickar över kontrolluppgifter, eller Försäkringskassan när myndigheten mottar löneuppgifter.[10] Ett offentliggörande av personuppgifter innebär inte heller att uppgifterna har lämnats ut till mottagare. Att personuppgifter har offentliggjorts till en obestämd krets behöver därför inte föras in i behandlingsregistret.[11]

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 saknas i en övervägande majoritet av de register som granskats inom ramen för den fördjupade kontrollen.

Utifrån de rekommendationer som tidigare lämnats av dataskyddsombudet är det inte konstigt att uppgift om interna mottagare överlag saknas i registren. Detta eftersom formuleringen i artikel 30.1d i GDPR 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.[12] Under arbetet med den fördjupade kontrollen har dataskyddsombudet gjort en förnyad bedömning utifrån ny vägledning från EDPB[13], vägledning utifrån de europeiska tillsynsmyndigheternas egna register[14], och det faktum att formuleringen *utlämnas* inte förekommer i den engelska, eller flera andra språkversioner av GDPR.[15]

I sin vägledning för småföretag beskriver EDPB mottagare som: *vem som har tillgång till uppgifterna (mottagarna – t.ex. den avdelning som ansvarar för rekryteringen, IT-tjänsten, ledningen, tjänsteleverantörerna, partner...).*[16] Vidare framgår det även ur EDPB:s riktlinje avseende begreppen personuppgiftsansvarig och personuppgiftsbiträde att *definitionen omfattar alla*

[10] Se skäl 31 i GDPR, se också Öman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 4.9.
[11] Se Öman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 4.9.
[12] Se Öman, Dataskyddsförordningen (GDPR) m.m. (JUNO 2024-10-16) kommentar till artikel 4.9.
[13] EDPB, Data protection guide for small business, EDPB: Data protection guide for small business (hämtad 2024-11-26).
[14] Se till exempel i EDPS: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).
[15] 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 vägledningen för småföretag EDPB: Data protection guide for small business (hämtad 2024-11-27).
[16] EDPB, Data protection guide for small business, EDPB: Data protection guide for small business (hämtad 2024-11-26).

som tar emot personuppgifter.[17] Det framgår också tydligt av EDPB:s eget register såväl som av den europeiska datatillsynsmannen EDPS[18], den franska tillsynsmyndigheten Commission Nationale de l'Informatique et des Libertés (CNIL)[19], och av Integritetsskyddsmyndighetens (IMY) eget register[20], att personal och avdelningar eller funktioner inom den personuppgiftsansvariges egen organisation ska betraktas som mottagare.

Dataskyddsombudet anser därför att definitionen i artikel 4.9 inte ska läsas på annat sätt än att begreppet mottagare omfattar den personuppgiftsansvariges egen organisation, en tolkning som också finner stöd i förarbetena till personuppgiftslagen.[21] För att uppfylla kraven i artikel 30.1d behöver därför samtliga verksamheter i Staden dokumentera vilka 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.[22]

I 30.1d i GDPR anges vidare att det är *kategorier av mottagare* som ska anges. Dataskyddsombudet vill dock i sammanhanget lyfta att vid en begäran om tillgång enligt artikel 15 i GDPR har den registrerade rätt att få information om specifika mottagare[23], såvida det inte är omöjligt. Information om specifika mottagare ska också lämnas till den registrerade i enlighet med informationsskyldigheten i artikel 13.1e och 14.1e i GDPR. Utifrån det rekommenderar dataskyddsombudet att Stadens verksamheter anger specifika mottagare i registret, även om det i artikel 30.1d i GDPR anges att *kategorier av mottagare* ska anges. Detta eftersom de registrerade har rätt att få veta detta vid en begäran om tillgång i enlighet med artikel 15.1c, och att det därför är en uppgift som Stadens verksamheter måste ha dokumenterat. Om det inte framgår i behandlingsregistret behöver verksamheten vid en begäran ändå leta fram uppgiften, varför det blir mer effektivt att ha det angivet i registret.

Vidare gäller att när en personuppgift tillgängliggörs för en mottagare så anser dataskyddsombudet att det av behandlingsregistret, som bästa praxis, ska framgå varför mottagaren är just mottagare.[24] Det vill säga att om mottagaren till exempel är ett personuppgiftsbiträde eller underbiträde så ska det dokumenteras i registret.

---

[17] Se *EDPB:s Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgifts-biträde i GDPR* pt 92.
[18] Se till exempel i EDPS: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).
[19] CNIL, Record of processing activities, Tillgänglig: CNIL GDPR toolkit - Record of processing activities (hämtad 2025-01-24).
[20] IMY:s förteckning över personuppgiftsbehandlingar (aktuell version från 2024-10-23).
[21] 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".*
[22] Se EU-domstolens förhandsavgörande i mål C-579/21, C-579/21. Se *även EDPB:S Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR pt 85-92.*
[23] Se mål C-154/21.
[24] 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.

Efter genomförd granskning kan dataskyddsombudet konstatera att det finns genomgående brister i dokumentationen av mottagare. I många fall saknas uppgift om till exempel personuppgiftsbiträden även i sådana fall där det är uppenbart att den behandling som beskrivs utförs med hjälp av personuppgiftsbiträden. Dataskyddsombudet vill därför uppmärksamma Stadens verksamheter om att samtliga mottagare behöver anges i registret.

2.5 Överföring av personuppgifter till tredjeland

Av artikel 30.1e i GDPR 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 verksamheten 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.

Det är inte tillräckligt att veta ”på ett ungefär”, utan det är dom faktiska överföringarna som Stadens verksamheter ska redogöra för. Flera av de granskade verksamheterna har till exempel på flera ställen i sina register uppgett att det sker en överföring av personuppgifter till USA, till följd av en biträdessituation med någon amerikansk molntjänstleverantör som Microsoft, Google, eller Amazon. Dataskyddsombudet utesluter inte på något sätt att personuppgifter faktiskt överförs till USA vid biträdessituationer som innefattar dessa eller andra biträden, det går dock inte att förutsätta att så sker bara för att biträdet råkar ha sin juridiska hemvist i just USA. Beroende på vilken typ av tjänst det avtalats om, så kan det vara så att ingen överföring av personuppgifter utanför Europa sker överhuvudtaget, att överföring sker till just USA, eller att överföring inte sker till USA, men väl till flera andra tredjeländer, som Indien, Kina, Malaysia med flera, till exempel för support och liknande ändamål.

Det faktum att det föreligger ett adekvansbeslut för 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. Att det finns ett adekvansbeslut för det land som ett biträde har sin juridiska hemvist i fråntar inte heller den

personuppgiftsansvarige från skyldigheten att genomföra en kartläggning av vilka överföringar som sker till andra tredjeländer som biträdet har verksamhet i, eller där underbiträden anlitas. Utan att genomföra en sådan kartläggning så är det inte möjligt för den personuppgiftsansvarige att bedöma om dessa överföringar är förenliga med GDPR.[25]

Det går inte heller att utgå ifrån att samma förutsättningar gäller för alla delar av tjänster eller digitala lösningar som innebär ett biträdesförhållande. Geografisk hemvist för lagring och support kan skilja sig åt mellan olika applikationer som en leverantör tillhandhåller inom ramen för en biträdesrelation. Återigen gäller att Stadens verksamheter måste ha kännedom om 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 medför att det sker en överföring till tredjeland.

Det finns inte någon skyldighet att ange i behandlingsregistret när det endast finns en risk för tredjelandsöverföring. Dataskyddsombudet rekommenderar dock att Stadens verksamheter även tar upp risk för tredjelandsöverföringar i sina register. 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 till exempel USA, Kina, Ryssland, med flera länder). Detta påverkar naturligtvis skyddet för personuppgifterna, varför informationen är viktig att dokumentera. Det behöver dock framgå tydligt när det är fråga om faktisk planerad eller avtalad överföring och när det endast föreligger en risk.

Avslutningsvis vill dataskyddsombudet också nämna att det av artikel 30.1e framgår att behandlingsregistret ska innehålla dokumentation av lämpliga skyddsåtgärder för sådana överföringar som avses i artikel 49.1 andra stycket. Av artikel 49.1 andra stycket framgår när en tredjelandsöverföring får göras i de fall den inte kan grundas på en bestämmelse i artikel 45 (adekvat skyddsnivå) eller artikel 46 (lämpliga skyddsåtgärder till exempel standardavtalsklausuler, bindande företagsbestämmelser med mera.) och inget undantag i artikel 49.1 första stycket led a-g är tillämpligt.

Enligt EDPB ska detta undantag ses som en sista utväg[26] eftersom det endast kan tillämpas under väldigt specifika omständigheter och är omgärdat av en lång rad tvingade krav. Det ska också sägas att artikel 49.1 andra stycket inte gäller ”*åtgärder som vidtas av offentliga myndigheter som ett led i utövandet av deras offentliga befogenheter*”.[27] Utifrån detta är dataskyddsombudets uppfattning att bestämmelsen väldigt sällan, om ens någon gång, kommer kunna tillämpas av Stadens verksamheter. I de fall någon verksamhet avser att

[25] EDPS Investigation into use of Microsoft 365 by the European Commission (Case 2021-0518) Decision (8 March 2024) s 105
[26] EDPB:s riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679, s. 14
[27] Artikel 49.3 GDPR

använda detta undantag bör det därför först stämmas av med dataskydds-ombudet. Dataskyddsombudet bedömer inte att undantaget varit tillämpligt på någon av de behandlingar som granskats under den fördjupade kontrollen.

Efter genomförd granskning anser dataskyddsombudet att det inom Staden finns oklarheter avseende vilken information som ska anges i behandlingsregistret avseende tredjelandsöverföringar. Dataskyddsombudet bedömer att det i vissa fall är uppenbart att de granskade behandlingsregistren inte uppfyller de krav som framgår av artikel 30.1e, och att det i andra fall måste anses vara starkt befogat att ifrågasätta hur väl verksamheterna dokumenterat de faktiska överföringarna som sker. Den information som de granskade verksamheterna har angett i sina respektive behandlingsregister skiljer sig på flera områden. Vissa verksamheter har angett att överföringar sker, men inte till vilka länder, eller bara i undantagsfall angett vilka länder som avses. Andra har, som nämnts ovan, i princip uteslutande angett USA som tredjeland, trots att det i många fall inte alls är säkert att överföringen av uppgifter är begränsad till USA, eller ens sker till USA över huvud taget. Medan andra verksamheter har angett att det eventuellt förekommer en tredjelandsöverföring på grund av ett personuppgiftsbiträdes juridiska hemvist. Det förekommer också verksamheter som inte angett att en enda tredjelandsöverföring sker, en uppgift som dataskyddsombudet på goda grunder betvivlar riktigheten av.

Dataskyddsombudet vill därför sammanfattningsvis ånyo poängtera att det är de faktiska omständigheterna som Stadens verksamheter måste kunna redogöra för, för att kunna uppfylla kraven i artikel 30.1e. Det räcker till exempel att någon del av behandlingen, hur ringa den än är, genomförs med hjälp av ett biträde eller underbiträde i tredje land för att tredjelandsöverföringen ska dokumenteras i behandlingsregistret. Likväl så ska samtliga överföringar dokumenteras, det vill säga det räcker inte att till exempel bara ange ett personuppgiftsbiträdes tredjeland om det samtidigt överförs personuppgifter till underbiträden i andra tredjeländer.

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”.[28] 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 att ha granskat de kontrollerade verksamheternas behandlingsregister vill dataskyddsombudet särskilt förtydliga att artikel 30.1f föreskriver att det är tidsfristerna som ska anges. Dataskyddsombudet anser inte att det är tillräckligt

[28] 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”.*

att ange att gallringsbeslut finns, eller att det framgår av en dokumenthanteringsplan hur länge uppgifterna kommer sparas. Detta helt enkelt eftersom ett sådant förfarande inte uppfyller kravet om att ange tidsfrister i registret, utan endast informerar om att tidsfrister finns. 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 artikeln. Av de europeiska dataskyddsmyndigheterna EDPB[29] och EDPS[30] register framgår de faktiska tidsfristerna direkt i registret, detsamma gäller för IMY:s eget register.[31]

En av GDPR:s grundläggande principer är den om lagringsminimering (artikel 5.1e i GDPR), vilket innebär att personuppgifter inte får:

förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter.

Detta innebär att det som utgångspunkt bara är tillåtet att behandla personuppgifterna för det ursprungliga ändamålet så länge det är nödvändigt för det ursprungliga ändamålet. GDPR medger dock vidarebehandling av uppgifter för just arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 (artikel 5.1b och 5.1e i GDPR).

Dataskyddsombudet anser att för att registret ska bli funktionellt och transparent så bör tidsfristerna för radering för de enskilda kategorierna av personuppgifter som ingår i behandlingen spegla personuppgifternas hela livscykel. Om en specifik kategori av personuppgift kommer vidarebehandlas för exempelvis arkivändamål så ska även tidsfristen för detta ändamål anges trots att vidarebehandlingen egentligen utgör en eller flera separata behandlingar. Det är också så som EDPB valt att göra, med hänvisningar till bevarandeplaner och historiska värden inom ramen för den enskilda behandlingen, trots att detta alltså i sak utgör andra ändamål.[32] Det betyder att om kategorierna av personuppgifterna ska behandlas för det ursprungliga ändamålet i 5 år hos den aktuella verksamheten och sedan bevaras för arkivändamål, så rekommenderas verksamheten, att ange att uppgifterna sparas i 5 år för det ursprungliga

[29] Se exempel i EDPB:s behandlingsregister EDPB records of processing activities - Access to documents request (hämtad 2024-11-27).
[30] Se exempel i EDPS:s behandlingsregister EDPS record of processing activity - Whistleblowing procedure (hämtad 2024-11-27).
[31] Se IMY:s förteckning över personuppgiftsbehandlingar (aktuell version från 2024-10-23).
[32] Se exempel i EDPB:s behandlingsregister EDPB records of processing activities - Access to documents request (hämtad 2024-11-27).

ändamålet och att de därefter bevaras för arkivändamål, precis som EDPB gör i sitt behandlingsregister.

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 Stadens förvaltningar och bolag att ge en allmän beskrivning av säkerhetsåtgärder.[33] Att beskrivningen ska vara allmän betyder att det inte finns något krav om att återge en detaljerad beskrivning av alla säkerhetsåtgärder.[34]

Dataskyddsombudets samlade bedömning efter genomförd granskning av de utvalda verksamheterna är att beskrivningen av tekniska och organisatoriska säkerhetsåtgärder genomgående är bristfällig. I många fall saknas beskrivningen helt. I andra fall beskrivs endast tekniska, men inte organisatoriska säkerhetsåtgärder. Många gånger beskrivs också samma säkerhetsåtgärder som genomgående återkommer i registret, även om det kan vara i olika konstellationer. Trots att de säkerhetsåtgärder som anges kan vara relevanta, såsom backup, kryptering, behörighetsbegränsningar, rutiner och så vidare, så är beskrivningarna många gånger kortfattade och behöver utvecklas. Beskrivningen ska utgå från hur åtgärderna relaterar till, och säkerställer, en lämplig säkerhetsnivå utifrån kraven i artikel 32.1 i GDPR. Dataskyddsombudet vill därför särskilt påtala att uppgiften om säkerhetsåtgärder är obligatorisk i enlighet med artikel 30.1g i GDPR och att regleringen avser både tekniska och organisatoriska säkerhetsåtgärder. Artikeln hänvisar explicit till de säkerhetsåtgärder som beskrivs i artikel 32.1 i GDPR. Att, som en del verksamheter, enbart hänvisa till att man följer principerna om inbyggt dataskydd och dataskydd som standard i artikel 25.1 och 25.2 i GDPR, är inte tillräckligt eftersom dessa principer är just principer för att säkerställa att säkerhetsåtgärder finns på plats, men inte säger något om säkerhetsåtgärderna, och därför inte kan anses utgöra en beskrivning av dessa.

Samtliga åtgärder i den allmänna beskrivningen hänför sig alltså till de säkerhetsåtgärder som beskrivs i artikel 32.1:

a) pseudonymisering och kryptering av personuppgifter,
b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,

[33] Se Article 29 Working Party Guidelines on transparency under Regulation 2016/679 s. 29, pt 59.
[34] 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).

d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Det är således inte nödvändigt att återge alla rutiner eller åtgärder som tagits fram för att säkerställa att behandlingen genomförs enligt plan, utan bara de som hänför sig till behandlingens säkerhet i enlighet med kriterierna i artikel 32.1. För de rutiner som en verksamhet hänvisar till i sin allmänna beskrivning ska det alltid framgå vad rutinerna syftar till. Om rutinerna avser behörighetsstyrning eller tilldelning, eller något annat, så bör det framgå av beskrivningen och inte bara beskrivas som ”rutiner”.

2.8 Rättslig grund och motivering

Dokumentation av uppgift om en behandlings rättsliga grund, motivering av den rättsliga grunden och hänvisning till stödet för 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. Dataskyddsombudet rekommenderar därför att samtliga verksamheter anger rättslig grund, motivering och hänvisning till stöd för den rättsliga grunden i sitt behandlingsregister. Det som menas med motivering och hänvisning är att exempelvis ange att ”enligt 1 § i lag XX är bolaget skyldigt att YY vilket utgör en rättslig förpliktelse”, ”behandlingen är nödvändig för att uppfylla villkoren i avtalet ZZ”, eller ”enligt reglementet § 3 har förvaltningen till uppdrag att göra XX vilket utgör en uppgift av allmänt intresse”.

Den personuppgiftsansvarige behöver, innan en behandling påbörjas, ha klart för sig vilken rättslig grund som tillämpas för det eller de ändamål som behandlingen innefattar. Som dataskyddsombudet redogjort för under avsnitt 2.1.1.2 kan en behandling 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 utforma behandlingar som innehåller flera närliggande ändamål, om det är motiverat. I sådana fall kan flera rättsliga grunder anges. En förutsättning för det är dock att varje enskilt ändamål uppfyller kraven om att vara särskilda, uttryckligt angivna och berättigade och går att knyta till en (enda) rättslig grund per ändamål, enligt kravet att personuppgifter bara kan behandlas för ett ändamål med stöd av en (enda) rättslig grund.[35] Ett sådant

[35] EDPB, 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.”* och s. 25 pt 121. 1. “*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.*

upplägg kräver, enligt dataskyddsombudets mening, att de enskilda delarna av behandlingen måste preciseras på en sådan nivå att de ändå hade kunnat utgöra en egen post/rad i behandlingsregistret. Att bygga mycket komplexa behandlingar med flera deländamål riskerar snabbt att bli väldigt rörigt, vilket dataskyddsombudet redogjort för under avsnitt 2.1.1.2. Det är därför betydligt enklare att hålla reda på vad de olika behandlingarna faktiskt innefattar om varje ändamål också utgör egna poster i behandlingsregistret. Med detta sagt kan det i vissa fall vara motiverat med ett upplägg där en behandling innehåller flera olika ändamål.

Den personuppgiftsansvarige behöver även ha i åtanke att komplexa behandlingsprocesser med flera rättsliga grunder kan göra det svårt att informera de registrerade på ett korrekt sätt. Informationsskyldigheten i artikel 13.1c och 14.1c i GDPR kräver att den personuppgiftsansvarige tydligt informerar den registrerade om ändamålen med behandlingen och den rättsliga grunden. Även möjligheten att på ett korrekt sätt hantera de registrerades rätt till radering i artikel 17 i GDPR, och rätten att göra invändningar enligt artikel 21 i GDPR kräver att den personuppgiftsansvarige har klart för sig på uppgiftsnivå vilken den rättsliga grunden är för en behandling. Dataskyddsombudet vill i sammanhanget också särskilt poängtera att den rättsliga grunden likväl som ändamålet, ska vara knuten till den faktiska behandlingen, det vill säga det kan *inte* finnas en behandlingsindelning för hur den personuppgiftsansvarige informerar de registrerade, en för behandlingsregistret, en tredje för de konsekvensbedömningar som genomförs och en fjärde för att ta ställning till en begäran från de registrerade om att utöva sina rättigheter.

Bland de verksamheter som dataskyddsombudet granskat inom ramen för den fördjupade kontrollen har flera angett mer än en rättslig grund för behandlingar i sina behandlingsregister, i vissa fall upp till fyra olika rättsliga grunder. Detta trots att behandlingarna endast utgörs av ett ändamål. Detta är inte i överensstämmelse med kraven i GDPR, eftersom ett ändamål alltså bara kan stödja sig på en (enda) rättslig grund. Efter genomförd granskning kan dataskyddsombudet konstatera att ingen av de verksamheter som hänvisat till flera rättsliga grunder för en behandling har gjort det på ett sådant sätt att det lever upp till kraven i GDPR.

Dataskyddsombudet uppfattar också att många verksamheter slarvar med motiveringen av och hänvisningarna till stödet för den rättsliga grund som man valt att hänvisa till. En absolut grundläggande förutsättning är att den rättsliga grund som dokumenteras i behandlingsregistret, och som verksamheterna hänvisar till, faktiskt är korrekt och tillämpbar för de ändamål man angett som grund för behandlingen av personuppgifter.

3 Dataskyddsombudets sammanfattade bedömning

Att förstå och tillämpa de olika leden i artikel 30.1 GDPR är inte så enkelt som det kan uppfattas vid en första anblick, något som blivit tydligt i samband med genomförd granskning. Trots tydliga krav i GDPR på vad ett behandlingsregister ska innehålla, finns det betydande brister i Stadens verksamheters dokumentation av behandlingar. Dataskyddsombudet bedömer att det finns ett omfattande arbete att göra för att leva upp till kraven i artikel 30 i GDPR. Det gäller för det första att ha kännedom om verksamhetens personuppgiftsbehandlingar, för att därefter kunna omvandla dessa till tydliga, konkreta och specifika ändamål. Varje ändamål behöver avgränsas på en nivå som gör att verksamheten kan arbeta på ett funktionellt sätt med GDPR:s samtliga delar, alltså på ett sådant sätt som möjliggör att informera registrerade, att genomföra konsekvensbedömningar, att hantera begäran från de registrerade om att utöva sina rättigheter samt att hantera alla andra delar av GDPR. Detta kräver god kännedom om den egna organisationen och om de lagar och regler som styr verksamhetens arbete. Av den anledningen är det osannolikt att en enda person klarar av att ta fram en verksamhets hela behandlingsregister på egen hand. Det krävs resurser, kunskap och deltagande från de personer som direkt arbetar i kärnverksamheten inom respektive verksamhetsområde i den egna organisationen. Utöver den kunskap som kärnverksamheten har, krävs även kunskaper i GDPR. Därtill krävs ett arbete för att gå igenom befintliga avtal, för att kunna bedöma om det förekommer någon tredjelandsöverföring, genomgång av gallringsbeslut för att kunna precisera lagringstiderna på ett sätt som uppfyller kraven, förtydliga vilka de registrerade är och vilka personuppgifter som behandlas om respektive kategori registrerade i en behandling, samt identifiera faktiska mottagare, både internt och externt. Utifrån detta är det tydligt för dataskyddsombudet att arbetet med behandlingsregistret kräver både resurser och tid.

Med ledning från de granskade verksamheterna kan dataskyddsombudet konstatera att arbetet med behandlingsregister inte är en uppgift som utförts på det omfattande sätt som GDPR kräver. Ett behandlingsregister som uppfyller kraven är däremot en förutsättning för att kunna bedriva ett systematiskt dataskyddsarbete. Ett komplett behandlingsregister ska spegla hur verksamheten behandlar personuppgifter. Om behandlingsregistret är komplett innebär det också att verksamheten har fullgod översikt över de personuppgifter som behandlas, att samtliga behandlingar har berättigade särskilda, uttryckliga och berättigade ändamål, vilka mottagare som verksamheten delar uppgifter med och varför, samt när de olika uppgifterna ska raderas. Det är således en förutsättning för att utifrån ansvarsskyldigheten kunna påvisa att GDPR följs.

För att en verksamhet i praktiken ska kunna ha ett systematiskt dataskyddsarbete behöver det finnas ett korrekt dokumenterat register för att kunna uppfylla informationsplikten och behandla personuppgifter på ett öppet sätt gentemot de registrerade, för att kunna hantera de registrerades rättigheter, såsom rätten till tillgång, rätten till radering och rätten att göra invändningar,

samt veta vilka behandlingar som kräver en konsekvensbedömning, men också utifrån ett riskperspektiv kunna prioritera dessa. Det är också viktigt, utifrån efterlevnaden av GDPR, att personalen har kännedom om vilka personuppgiftsbehandlingar som är tillåtna i verksamheten.

Dataskyddsombudet rekommenderar samtliga verksamheter i Staden att gå igenom sitt behandlingsregister utifrån de rekommendationer som framgår i denna rapport. För att kunna omhänderta rekommendationerna är det viktigt att verksamheterna tillser att tillräckliga resurser avsätts i form av tid och personal. Då ett fullständigt och funktionellt behandlingsregister är en förutsättning för att verksamheterna ska kunna fullgöra sina skyldigheter enligt GDPR bör arbetet med behandlingsregistret ha hög prioritet inom samtliga bolag och förvaltningar under 2025.

Rapport framtagen av dataskyddsenheten
Telefon: 031-365 00 00 (kontaktcenter)
E-post: dso@intraservice.goteborg.se

Göteborgs Stad