

# Missiv till rapport om dataskyddsbudens förutsättningar

## Inledning

Dataskyddsbuden har i sitt uppdrag att övervaka efterlevnaden rörande dataskyddet där främst GDPR utgör grundförutsättningarna hos de personuppgiftsansvariga myndigheter som faller under samverkansavtalet. Rapporten om dataskyddsbudets förutsättningar tar sikte på artiklarna 37, 38 och 39 i GDPR som rör dataskyddsbudets förutsättningar och ställning i förhållande till den personuppgiftsansvariga samt samverkansavtalet som ligger till grund för dataskyddsbuden för de 8 kommuner som valt att organisera sina dataskyddsbud gemensamt.

## Rapportens syfte

Syftet med rapporten är att synliggöra de fördelar och utmaningar som följer med att gemensamt samverka kring tjänsten dataskyddsbud. Rapporten är tänkt att ge varje enskild personuppgiftsansvarig en bild av de förutsättningar som ligger till grund för dataskyddsbudens uppdrag samt ge råd om eventuella åtgärder som den personuppgiftsansvarige kan vidta för att stärka förutsättningarna för dataskyddsbuden. Att samverka kring tjänsten dataskyddsbud har många fördelar och kommunerna inom GR som valt att organisera sig på detta vis har genom åren med framgång fått en effektiv tjänst och samlad kompetens inom området. Dataskyddsbuden har genom samverkan fått många konkreta goda exempel på att det går att lösa uppgifterna på många olika sätt och genom olika strategier. Dataskyddsbuden har mycket tack vare samverkan kunnat förmedla många goda råd och gemensamma insatser som både sparat kommunerna tid, resurser och med högre kvalitet. Rapporten tar enbart sikte på dataskyddsbudens upplevda efterlevnad av artiklarna 37, 38 och 39 GDPR i förhållande med nuvarande samverkansavtal och upplevda verkliga förutsättningar.

## Hjälp till tolkning av resultat

GR är arbetsgivare åt dataskyddsbuden och ska med jämna mellanrum utvärdera och revidera styrdokumentet kopplade till tjänsten. Resultatet av denna rapport ersätter inte detta arbete men resultatet kan med fördel användas som underlag vid detta arbete. Respektive personuppgiftsansvarig kan använda materialet för att öka sin egen kunskap och förståelse kring dataskyddsbudens arbete och hur de effektivt kan utnyttja dessa resurser för

sin egen verksamhet i förhållande till sin egen dataskyddsorganisation.  
Förhoppningen är också att rapporten kan ge en verklighetsbild för de personuppgiftsansvariga och råd som kan användas för att eventuellt komplettera med egna resurser om så krävs för att stärka sin egen förmåga att leva upp till GDPR och annan lagstiftning relevant för uppdragen som åligger respektive myndighet.

Med vänlig hälsning

Johan Bergström

Dataskyddsombud Göteborgsregionens kommunalförbund enligt  
samverkansavtal

[johan.bergstrom@goteborgsregionen.se](mailto:johan.bergstrom@goteborgsregionen.se)



# Dataskyddsombudens förutsättningar utifrån nuvarande samverkansavtal

# Innehåll

Sammanfattning.....	3
1. Dataskyddsbudens arbetsuppgifter.....	6
1.1 Dataskyddsbudens ställning .....	6
1.2 Dataskyddsbudens arbetsuppgifter .....	8
1.2.1 Ge råd och bevaka efterlevnaden .....	8
1.2.2 Dataskyddsbudens roll vid konsekvensbedömningar .....	8
1.2.3 Vara kontaktperson och inta en riskbaserad arbetsmetod.....	9
1.2.4 Rollen utöver det obligatoriska vid behov.....	9
2. Samverkansavtalet .....	10
2.1 Bakgrund och syfte med samverkansavtalet.....	10
2.2 Arbetsuppgifter enligt samverkansavtalet.....	11
2.3 Fördelning av resurser enligt samverkansavtalet.....	12
3. Kommunernas interna dataskyddsorganisation .....	12
3.1 Sammanfattning av dataskyddsbudets kontroll 2021 om dataskyddsorganisationer i samverkanskommunerna .....	13
4. Förutsättningar för samverkan.....	14
4.1 Digitala förutsättningar för samverkan .....	17
5. Identifierade risker utifrån nuvarande förutsättningar .....	19
5.1 Risk att dataskyddsbuden inte är tillgängliga i tillräcklig utsträckning vilket leder till dataskyddsbuden inte hinner fullgöra sitt uppdrag .....	19
5.2 Risk att dataskyddsorganisationerna inte är försedda med tillräckliga resurser utefter vald samverkansform som leder till otydlighet i ansvar och roller .....	21
5.3 Risk att samverkansavtalet ger en felaktig bild av dataskyddsbudens uppdrag som leder till otydliga förväntningar på dataskyddsbudens leveranser .....	22
5.4 Risk att information blandas om olika personuppgiftsansvariga om de hanteras genom samma mailinkorg som kan leda till att sekretessgränser bryts .....	23
5.5 Risk att personuppgiftsansvariga inte på ett korrekt sätt och i god tid ser till att dataskyddsbuden deltar i alla frågor som rör skyddet av personuppgifter. .....	24
Bilagor .....	26
Referenser .....	26

# Sammanfattning

Ale, Alingsås, Härryda, Lerum, Lilla Edet, Partille, Stenungsund och Öckerö kommun har idag ett samverkansavtal om att gemensamt ha två dataskyddsbud som ska verka för kommunernas olika personuppgiftsansvariga myndigheter (undantaget är kommunala bolag som har egna dataskyddsbud). Att samverka kring tjänsten dataskyddsbud har många fördelar och kommunerna inom GR som valt att organisera sig på detta vis har genom åren med framgång fått en effektiv tjänst och samlad kompetens inom området.

Dataskyddsbuden har genom samverkan fått många konkreta goda exempel på att det går att lösa uppgifterna på många olika sätt och genom olika strategier. Dataskyddsbuden har mycket tack vare samverkan kunnat förmedla många goda råd och gemensamma insatser som både sparat kommunerna tid, resurser och med högre kvalitet. Rapporten tar enbart sikte på dataskyddsbudens upplevda efterlevnad av artiklarna 37, 38 och 39 GDPR i förhållande med nuvarande samverkansavtal och upplevda verkliga förutsättningar. Rapporten syftar till att utvärdera och synliggöra risker med nuvarande samverkansavtal och med de faktiska förutsättningar som idag finns på plats för att dataskyddsbuden ska kunna utöva sina uppdrag utifrån GDPRs definition. Rekommendationerna är riktade till samtliga samverkansparter och rapporten är skriven på en generisk nivå oberoende av kommunernas eventuella organisatoriska skillnader. Under denna rubrik sammanfattas de viktigaste slutsatser och risker som identifierats.

- **Risk att dataskyddsbuden inte är tillgängliga i tillräcklig utsträckning vilket leder till att dataskyddsbuden inte hinner fullgöra sitt uppdrag.**

Kort kommentar: Det är viktigt att dataskyddsbuden ges tid och är tillgängliga på ett sätt som möter behovet hos respektive samverkanspart. Om många parter samverkar om ett och samma dataskyddsbud växer behovet av en stark egen dataskyddsorganisation som aktivt driver dataskyddsarbetet lokalt. Det behöver också förtydligas hur kommunikation mellan dataskyddsbuden och de lokala organisationerna ska gå till för att stärka tillgängligheten och kännedom om dataskyddsbudens existens och roll. Se fördjupad kommentar under kapitel 5.1.

- **Risk att dataskyddsorganisationerna inte är försedda med tillräckliga resurser utefter vald samverkansform som leder till otydlighet i ansvar och roller.**

Kort kommentar: I dagsläget sker stora delar av dataskyddsbudens

kommunikation med personer centralt placerade i kommunerna som är utsedda kontaktpersoner. Detta kan vara en medveten strategi om kommunerna har en central dataskyddsorganisation som håller samman hela kommunens dataskyddsarbete. Varje samverkanspart bör dock beakta risken och bedöma om det finns anledning att respektive personuppgiftsansvarig utser en kontaktperson till dataskyddsombuden samt ser över behovet av en egen dataskyddsorganisation om dataskyddsarbete bör ske lokalt på förvaltningsnivå. Se fördjupad kommentar under kapitel 5.2.

- **Risk att samverkansavtalet ger en felaktig bild av dataskyddsombudens uppdrag som leder till otydliga förväntningar på dataskyddsombudens leveranser.**

Kort kommentar: Nuvarande samverkansavtal beskriver dataskyddsombudens uppdrag på kommunnivå. Kommunerna i sin helhet är dock aldrig personuppgiftsansvariga utan respektive nämnd ansvarar för sina ansvarsområden. Samverkansavtalet skulle behöva revideras utifrån faktiska förutsättningar så det blir tydligt vilka personuppgiftsansvariga som ingår i samverkansavtalet och hur stora resurser som respektive part är i behov utav. Se fördjupad kommentar under kapitel 5.3.

- **Risk att information blandas om olika personuppgiftsansvariga om de hanteras genom samma mailinkorg som kan leda till att sekretessgränser bryts.**

Kort kommentar: Dataskyddsombuden har idag en mailinkorg som varje samverkanspart använder i kommunikation med dataskyddsombuden. Ärenden blandas och det finns risk att sekretessgränser bryts. Uppdraget sker i stora delar på distans och det behöver vidare utredas hur inkomna ärenden ska flöda för att undvika att sekretessgränser bryts på ett otillbörligt sätt. Se fördjupad kommentar under kapitel 5.4.

- **Risk att personuppgiftsansvariga inte på ett korrekt sätt och i god tid ser till att dataskyddsombuden deltar i alla frågor som rör skyddet av personuppgifter vilket leder till att den personuppgiftsansvariga inte lever upp till GDPRs definition av vad ett dataskyddsombuds uppdrag ska innefatta.**

Kort kommentar: Enligt GDPR ska dataskyddsombuden ges chans att yttra sig i alla frågor som rör skyddet av personuppgifter och detta är en skyldighet som vilar på respektive personuppgiftsansvarig. När dataskyddsombuden verkar på distans och för flera olika verksamheter är det extra viktigt att hitta en arbetsmetod som möjliggör delaktighet. Samverkan i nuvarande form kräver också lokal kompetens och en förmåga att driva dessa frågor och veta när och hur dataskyddsombudet ska göras delaktig. Dessa arbetsmetoder och förutsättningar behöver beskrivas och bedömas så att dataskyddsombuden i

större utsträckning än i dag görs delaktiga i frågor rörande skyddet av personuppgifter. Se fördjupad kommentar under kapitel 5.5

Johan Bergström, dataskyddsombud  
Göteborg 2022

# 1. Dataskyddsombudens arbetsuppgifter

**Dataskyddsombudets övergripande arbetsuppgift är att övervaka så att organisationen följer dataskyddsförordningen (GDPR). Arbetsuppgifterna finns definierade i artikel 39 GDPR.**

Organisationer som behandlar personuppgifter i sin verksamhet ska i enlighet med artikel 37 GDPR utse ett dataskyddsombud. Utnämmandet är obligatoriskt för myndigheter och ska anmälas till Integritetsskyddsmyndigheten enligt deras instruktioner på [imy.se](https://imy.se). Dataskyddsombudet ska ha en särskild ställning i förhållande till verksamhet och detta regleras i artikel 38 GDPR.

## 1.1 Dataskyddsombudens ställning

Enligt artikel 38 GDPR ska den personuppgiftsansvariga säkerställa att dataskyddsombuden på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter. Detta kan genomföras på flera sätt. Antingen att dataskyddsombuden alltid bjuds in eller att myndigheten har en upparbetad dataskyddsorganisation som värnar om den personliga integriteten och som har en naturlig del i verksamhetens samtliga processer som behandlar personuppgifter. Dataskyddsombudens särskilda ställning gör dock det viktigt att denne ges chans att yttra sig i samband med personuppgiftsbehandlingar om myndigheten väljer att arbeta nära sin interna dataskyddsorganisation. EDPB eller dåvarande artikel 29-arbetsgruppen har tagit fram riktlinjer som beskriver detta mer och riktlinjen anger att om personuppgiftsansvariga ”kan säkerställa att dataskyddsombudet informeras och rådfrågas redan från början underlättar efterlevnaden av förordningen och främjar en strategi för inbyggt dataskydd och bör därför vara en standardrutin i organisationens styrning” (Artikel 29-arbetsgruppen för skydd av personuppgifter, Riktlinjer om dataskyddsombud, 2016)

Ur samma riktlinje går att utläsa att organisationen bör säkerställa att:

- Dataskyddsombudet ska regelbundet inbjudas att delta i möten på högsta och mellanliggande förvaltningsnivå,
- Dataskyddsombudet rekommenderas delta när beslut med följder för dataskyddet fattas. All relevant information ska i god tid förmedlas till dataskyddsombudet så att han eller hon kan ge lämpliga råd.
- Dataskyddsombudets åsikt måste alltid ges tillbörlig vikt. I händelse av oenighet rekommenderar artikel 29-arbetsgruppen att organisationen som god praxis dokumenterar skälen till att dataskyddsombudets råd inte har följts.
- Dataskyddsombudet ska rådfrågas omedelbart när en personuppgiftsincident eller annan incident har inträffat.



Organisationen ska också enligt artikel 38.2 GDPR stödja sitt dataskyddsombud genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dataskyddsombudens sakkunskap. EDPBs riktlinje anger följande att beakta som en förutsättning för att leva upp till detta krav:

- Högsta ledningen bör aktivt stödja dataskyddsombudets arbete (t.ex. på styrelsenivå).
- Dataskyddsombudet bör ha tillräckligt med tid på sig för att fullgöra sina uppgifter. Detta är särskilt viktigt när ett internt dataskyddsombud utnämns på deltid eller om ett externt 33 Artikel 35.2. 17 dataskyddsombud arbetar med dataskydd vid sidan om andra uppgifter. Annars kan motstridiga prioriteringar leda till att dataskyddsombudet försummar sitt uppdrag. Det är mycket viktigt att dataskyddsombudet har tillräckligt med tid för att ägna sig åt sina dataskyddsuppgifter. Det är god praxis att fastställa en procentandel för den tid som behövs för dataskyddsombudsfunktionen om det inte är en heltidstjänst. Det är även god praxis att bestämma hur mycket tid som behövs för att utföra dataskyddsuppgifterna, att fastställa en lämplig prioritetsnivå för dataskyddsombudets uppgifter och att dataskyddsombudet (eller organisationen) tar fram en arbetsplan.
- Lämpligt stöd i form av ekonomiska resurser, infrastruktur (lokaler, hjälpmedel, utrustning) och personal i förekommande fall.
- Utnämningen av dataskyddsombudet bör officiellt meddelas till all personal för att säkerställa att personalen vet att det finns ett dataskyddsombud inom organisationen och vilka uppgifter dataskyddsombudet utför.
- Nödvändig tillgång till andra avdelningar, t.ex. personalavdelningen, den juridiska avdelningen, it-avdelningen, säkerhetsavdelningen och så vidare, så att dataskyddsombudet får viktig hjälp och information från dessa andra avdelningar.
- Fortbildning. Dataskyddsombud måste ges möjlighet att hålla sig uppdaterade om utveckling på dataskyddsområdet. Målet bör vara att ständigt öka dataskyddsombudens sakkunskap, och de bör uppmuntras att delta i fortbildningskurser om dataskydd och andra yrkesutvecklingskurser, t.ex. genom att delta i forum och seminarier om integritetsfrågor.
- Alltefter organisationens storlek och struktur kan det vara nödvändigt att upprätta en dataskyddsgrupp (ett dataskyddsombud och hans/hennes personal). I sådana fall bör gruppens interna struktur och varje medlems uppgifter och ansvar tydligt fastställas. När dataskyddsombudet är en extern tjänsteleverantör kan en grupp av enskilda personer som arbetar för denna enhet även utföra dataskyddsombudets uppgifter som en grupp, under ansvar av en utsedd huvudkontakt för kunden.

Generellt sett gäller att ju mer komplex och/eller känslig behandlingen är desto mer resurser bör anslås till dataskyddsombudet. Dataskyddsfunktionen måste vara effektiv och ha tillräckligt med resurser i förhållande till den uppgiftsbehandling som utförs.

Organisationen ska också tillse att dataskyddsombuden kan utföra sina uppgifter på ett oberoende sätt, tillse så att dataskyddsombuden inte kan bli avsatta eller få sanktioner för att ha utfört dataskyddsombudens uppgifter samt se till så att det inte förekommer intressekonflikter i dataskyddsombudets uppdrag.

## 1.2 Dataskyddsombudens arbetsuppgifter

Dataskyddsombudens arbetsuppgifter definieras i artikel 39 GDPR och innehåller en rad olika uppgifter. Sammanfattningsvis så ska dataskyddsombuden inta ett dataskyddsperspektiv och arbeta riskbaserat utifrån verksamheternas komplexitet och känslighet.

### 1.2.1 Ge råd och bevaka efterlevnaden

Dataskyddsombuden ska enligt artikel 39.1 b GDPR samt skäl 97 bistå den personuppgiftsansvarige för att övervaka den interna efterlevnaden. Det vill säga:

- Samla in information för att identifiera hur behandling av personuppgifter sker,
- analysera och kontrollera huruvida bestämmelser om behandling efterlevs, och
- informera samt ge råd och utfärda rekommendationer till den personuppgiftsansvarige.

Viktigt att poängtera i sammanhanget är att det är den personuppgiftsansvarige, inte dataskyddsombudet, som ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med GDPR. Detta förtydligas i artikel 24.1 GDPR. Det är alltså den personuppgiftsansvariges organisation som har ansvaret för att uppgiftsskyddet efterlevs, inte dataskyddsombudet.

### 1.2.2 Dataskyddsombudens roll vid konsekvensbedömningar

Dataskyddsombudet ska också på begäran av personuppgiftsansvarig ge råd vad gäller konsekvensbedömningar avseende dataskydd och övervaka genomförandet av dem. Detta står beskrivet i artikel 35.1 GDPR. Viktigt att poängtera är att ansvaret åligger den personuppgiftsansvarige att genomföra konsekvensbedömningar. Dataskyddsombudet ska rådfrågas och kunna bistå i följande frågor:

- Huruvida en konsekvensbedömning avseende dataskydd bör göras.
- Vilken metod som ska användas för konsekvensbedömningen avseende dataskydd.

- Huruvida konsekvensbedömningen avseende dataskydd bör göras internt eller läggas ut på en extern part.
- Vilka skyddsåtgärder (inbegripet tekniska och organisatoriska åtgärder) som bör vidtas för att begränsa eventuella risker för de registrerades rättigheter och intressen.
- Huruvida konsekvensbedömningen avseende dataskydd har utförts korrekt och om dess slutsatser (om behandlingen ska fortsätta eller ej och vilka skyddsåtgärder som ska vidtas) överensstämmer med den allmänna dataskyddsförordningen.

### 1.2.3 Vara kontaktperson och inta en riskbaserad arbetsmetod

Dataskyddsombuden ska också verka som kontaktperson gentemot registrerade och tillsynsmyndigheten exempelvis vid förhandssamråd eller samråda i andra frågor rörande dataskydd.

Dataskyddsombuden ska arbeta utifrån en riskbaserad metod vilket innebär att ta vederbörlig hänsyn till de risker som förknippas med behandling, med beaktande av behandlingens art, omfattning, sammanhang och syften enligt artikel 39.2 GDPR. Detta kan sammanfattas med att arbeta utifrån sunt förnuft och dataskyddsombuden ska prioritera sin verksamhet och inrikta sitt arbete på behandlingar som medför högre risk för den personliga integriteten. Behandlingar som innebär lägre risk ska dock inte försummas utan bör också övervakas på lämpligt sätt men fokus bör ligga på behandlingar som medför högre risker om dataskyddsombudet tvingas prioritera.

### 1.2.4 Rollen utöver det obligatoriska vid behov

Artikel 39.1 GDPR anger vilka arbetsuppgifter som dataskyddsombuden minst ska ha och beskriver de uppgifter som är obligatoriska i rollen som dataskyddsombud. Det finns dock inget hinder för att ett dataskyddsombud kan ha fler arbetsuppgifter där utöver så vida inte detta medför en intressekonflikt med de obligatoriska uppdragen.

Arbetet med behandlingsregistret är ett sådant exempel. Enligt artikel 30.1 och 30.2 beskriver GDPR att det är den personuppgiftsansvarige eller personuppgiftsbiträdet som ska föra register över behandling som utförs under dess ansvar eller föra ett register över alla kategorier av behandling som utförs för den personuppgiftsansvariges räkning. Detta ansvar vilar inte på dataskyddsombuden.

Dataskyddsombudets roll i sammanhanget har diskuterats och det är vanligt förekommande att dataskyddsombud i sin roll i praktiken skapar dessa förteckningar som baseras på uppgifter de får från olika avdelningar inom en organisation. Detta är inte en arbetsuppgift som listas som en av de uppgifter som ett dataskyddsombud minst ska inneha. Men samtidigt är det just så det är formulerat. Vad ett dataskyddsombud **minst** ska ha som arbetsuppgifter. En personuppgiftsansvarig kan tilldela dataskyddsombudet uppgiften att föra register över behandling under den

personuppgiftsansvariges eller för den delen biträdets ansvar. Det är dock viktigt att detta kommuniceras, bedöms och planeras så dataskyddsombudet har tid och resurser att samtidigt utföra sina obligatoriska arbetsuppgifter. Då detta arbete både är tidskrävande och i grunden ett ansvar som åligger den personuppgiftsansvarige. Därför är det viktigt att bedöma om det är rimligt utifrån rådande förhållanden att ålägga fler än de obligatoriska arbetsuppgifterna på dataskyddsombuden beroende på dataskyddsombudens arbetsbelastning och ansvarsområden.

## 2. Samverkansavtalet

**Enligt artikel 37.2 får en koncern utnämna ett enda dataskyddsombud om det på varje etableringsort är lätt att nå dataskyddsombudet både som kontaktpunkt internt och externt. Detta speciellt med beaktande av dataskyddsombudets uppdrag att informera och ge råd till den personuppgiftsansvarige eller biträdet och de anställda som behandlar deras personuppgifter om deras skyldigheter enligt GDPR. Detta har Göteborgsregionens egen organisation tillsammans med 8 kommuner inom GR gjort. Genom ett samverkansavtal delar dessa parter på två dataskyddsombud som arbetar heltid i uppdraget.**

Att samverka och dela på resursen dataskyddsombud är ett effektivt sätt att möta kravet att utse ett verksamt dataskyddsombud för organisationer med liknande verksamhet och som själva inte har resurser eller behov att tillhanda hålla ett eget dataskyddsombud. Då blir denna typ av samverkan som flera kommuner inom Göteborgsregionen gjort ett kostnadseffektivt alternativ att arbeta på. Det finns också fördelar genom att samla kompetens och låta två eller flera dataskyddsombud arbeta i ett nära samarbete. Det stärker kompetensen i arbetsgruppen och motverkar sårbarheter vid personalförändringar och ledigheter. Fenomenet är också vanligt förekommande i vår omvärld och det finns flera andra organisationer som verkar på ett liknande sätt. Exempelvis Boråsregionens kommunalförbund, Sydarkivera och i viss mån Göteborgs stad mfl.

### 2.1 Bakgrund och syfte med samverkansavtalet

Då det 2018 blev obligatoriskt för myndigheter att utse dataskyddsombud beslutade kommunerna Härryda, Lerum, Partille och Öckerö kommun att gemensamt gå samman och samverka om en gemensam resurs för att leva upp till kraven. Samverkan skede genom Göteborgsregionens kommunalförbund (GR) som antog uppdraget att anställa och upprätthålla en arbetsplats i Göteborgsregionens lokaler i Göteborg för ett dataskyddsombud vars uppdrag var för samtliga dessa kommuner och GR egna interna organisation. 2020 utökades antalet kommuner och Alingsås, Stenungssund, Ale och Lilla Edet anslöt och ett nytt samverkansavtal togs fram. I det avtalet bedömdes två dataskyddsombud behövas för att tillgodose behovet.

Syftet med samverkan är enligt samverkansavtalet att gemensamt etablera och anställa dataskyddsombud för att långsiktigt trygga behovet av stöd i respektive parts verksamhet och uppfyllande av tillämplig dataskyddslagstiftning på området.

## 2.2 Arbetsuppgifter enligt samverkansavtalet

Samverkansavtalet anger vilka arbetsuppgifter dataskyddsombudet ska ägna sig åt men är samtidigt något diffus med en inledande formulering som ”I rollen som dataskyddsombud ingår bland annat;” och sedan fortsätter en ganska detaljerad arbetsbeskrivning:

- a) vara ett kunskapsstöd, informera och ge råd till parterna om innehåll och tillämplighet av gällande dataskyddsskyddslagstiftning och angränsande regler som aktualiseras,
- b) fungera som kontaktpunkt för och mellan tillsynsmyndigheten, och vid behov genomföra förhandssamråd.
- c) rapportera till respektive kommuns ledning angående dataskyddsfrågor, organisatoriska brister och utvecklingsbehov och liknande frågor, när så är påkallat,
- d) arbeta för organisatoriska säkerhetsskyddsåtgärder,
- e) identifiera kompetensutvecklingsbehov, planera och genomföra utbildningar avseende dataskyddslagstiftningen samt övervaka den interna efterlevnaden av organisationens strategi för dataskydd,
- f) bistå i utredningen av misstänkta dataintrång,
- g) ge råd vid genomförande av konsekvensbedömning av dataskydd och övervaka genomförande av denna,
- h) omvärldsbevaka frågor rörande dataskyddslagstiftningen
- i) övervaka den interna efterlevnaden av dataskyddslagstiftningen hos de kommuner som ingått Avtalet.

Dessa formuleringar stämmer ganska väl överens med definitionen i artikel 39.1 GDPR som anger vad ett dataskyddsombud minst ska ha för arbetsuppgifter.

För att jämföra med GDPRs beskrivning i artikel 39.1 där det framgår att dataskyddsombudet minst ska ha följande uppgifter:

- a) Att informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar personuppgifter om deras skyldigheter enligt denna förordning och andra av unionens eller medlemsstaternas dataskyddsbestämmelser.
- b) Att övervaka efterlevnaden av denna förordning, av andra av unionens eller medlemsstaternas dataskyddsbestämmelser och av den personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.
- c) Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den enligt artikel 35 GDPR.

d) Att samarbeta med tillsynsmyndigheten

e) Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, inbegripet det förhandssamråd som avses i artikel 36 GDPR, och vid behov samråda i alla andra frågor. (Integritetsskyddsmyndigheten, 2022)

## 2.3 Fördelning av resurser enligt samverkansavtalet

Resursfördelningen i samverkansavtalet är på kommunnivå och beskriver att varje kommun som delar på dataskyddsombuden har rätt till 24% av ett dataskyddsombuds arbetstid. Ända skillnaden är GRs interna organisation som har 8%. Denna tidsåtgång loggas i dagsläget inte och dataskyddsombuden arbetar utefter en riskbaserad arbetsmetod och är lyhörda för verksamheternas utmaningar och behov och genomför kontroller och insatser beroende på risk och efterfrågan. En del insatser sker också samordnat där exempelvis en större utbildningsinsats upptog en del tid för dataskyddsombuden hösten 2021. Denna utbildning riktade sig till samtliga verksamheter som hade ett intresse eller behov av att stärka sin egen dataskyddskunskap.

Det specificeras inte mer i detalj vilka och antalet nämnder som faller under dataskyddsombudens uppdrag. Så det får betraktas som underförstått att uppdraget inbegriper samtliga nämnder då varje enskild nämnd är personuppgiftsansvarig för de behandlingar som sker under nämndens ansvarsområde och har en skyldighet att anmäla dataskyddsombudet till Integritetsskyddsmyndigheten. Muntligen har dataskyddsombuden också fått information om att de kommunala bolagen ska utse och anmäla egna dataskyddsombud så dessa är undantagna samverkansavtalet. Det saknas dock en beskrivning om det i samverkansavtalet.

## 3. Kommunernas interna dataskyddsorganisation

**Alla kommuner har utöver sitt samverkande dataskyddsombud också en egen form av dataskyddsorganisation som ska verka operativt för att stärka dataskyddsarbetet i organisationen. Hur denna ska organiseras lämnar lagstiftaren till verksamheten själv att bedöma efter behov och komplexitet.**

Inför att GDPR trädde i kraft 2018 så kämpade verksamheter runt om i Sverige med att förbereda sig inför de krav och utmaningar som förordningen ställer. Vissa saker var enklare att förbereda sig inför medan andra var svårare. Att skatta behovet, insatserna och hur man skulle organisera sig för att nå upp till en godtagbar nivå i sitt dataskyddsarbete var svårt att bedöma initialt. Under de fyra åren som passerat sedan GDPRs startskott så har dock behovet av en stark dataskyddsorganisation klarnat. En kommuns verksamhet är komplex och hanterar stora mängder personuppgifter dagligen i näst intill samtliga processer. Att då ha ett proaktivt dataskyddsarbete som drivs av en stabil dataskyddsorganisation med en tydlig strategi där dataskyddsfrågor lyfts och hanteras i tidiga skeden är en förutsättning för

att bibehålla fart i sitt utvecklingsarbete och tillse att man följer GDPR och annan dataskyddslagstiftning.

### 3.1 Sammanfattning av dataskyddsombudets kontroll 2021 om dataskyddsorganisationer i samverkanskommunerna

Våren 2021 genomförde dataskyddsombudet en övergripande efterlevnadskontroll på flertalet områden kopplat till GDPR och hur kommunerna förberett sig för att möta de olika krav som GDPR ställer på kommunen. Den granskningen berörde följande områden som är exempel på väsentliga delar som en dataskyddsorganisation kan arbeta med.

**Dataskyddsorganisation** – Organisationskarta, Rollbeskrivningar, Ansvarsfördelning, Beslutsgångar i dataskyddsarbetet, Styrande dokument kopplat till dataskydd.

**Personuppgiftsregister** – Kopia på ert personuppgiftsregister samt en kommentar från kontaktperson hur ni anser att ni ligger till i arbetet.

**Integritetspolicy** – Vilka informationsinsatser ges till registrerade. Både allmänhet/invånare, internt anställda, konsulter och politiker. Hur synliggörs informationen. Skicka med de informationstexter ni har eller länka till dem om de finns publicerade.

**Registrerades rättigheter** – Vilka rutiner finns på plats för att tillmötesgå de registrerades rättigheter i form av begäran av registerutdrag etc. Hur många fall har ni fått in under 2020 där registrerade velat utnyttja sina rättigheter.

**Personuppgiftsincidenter** – Rutin vid personuppgiftsincidenter. Hur många incidenter rapporterades under 2020 och hur många av dem rapporterades till Datainspektionen (nuvarande IMY). Vem beslutar om en incident ska rapporteras till tillsynsmyndigheten IMY.

**Utbildningsinsatser** – Har ni genomfört utbildningsinsatser inom dataskydd till anställda? När och i vilken omfattning?

**Personuppgiftsbiträdesavtal** – Hur många avtal har ni? Har ni någon mall ni utgår ifrån? och gärna en kopia på ett befintligt avtal.

**Konsekvensbedömningar** – Hur många konsekvensbedömningar har ni och har ni någon mall ni utgår ifrån? Bifoga ett exempel på genomförd konsekvensbedömning om ni har det.

**Uppföljningsarbete** – Hur arbetar ni med att följa upp incidenter, Pubavtal och säkerställande av uppdaterat register och informationstexter?

**Dataskydd som design och standard** – Beskriv hur ni arbetar med detta, Exempelvis har ni kopplat dataskyddsarbetet med angränsande områden som Informationssäkerhet, It säkerhet etc Har ni något ledningssystem ni arbetar efter eller någon säkerhetsstandard. Har ni byggt in dataskydd i befintliga processer, upphandling, rekrytering etc.

**Övrigt** – Har ni ytterligare information om ert dataskyddsarbete som inte ryms inom mina frågeställningar får ni gärna beskriva och bifoga dessa med.

Återkopplingen i sin tur innehöll en hel del praktiska råd på hur verksamheterna kan stärka sin interna dataskyddsorganisation där de gemensamma slutsatserna kan

summeras med att dataskyddsarbetet som sker i kommunerna inte är tillräckligt tydligt definierat när det kommer till roller och ansvar. I GDPR faller ansvaret på den nämnd som är personuppgiftsansvarig för behandlingarna och där respektive förvaltning ska ta ansvar för de personuppgiftsbehandlingar som sker i den egna verksamheten. Många gånger är dataskyddsorganisationen placerad centralt i kommunerna med tyngdpunkt på att hantera kommunövergripande dataskyddsfrågor och med uppdraget att bistå förvaltningarna/sektorerna med råd och riktlinjer i hur de ska tänka när de behandlar personuppgifter. Ofta hanteras dessa frågor av kommunjurist, nämndsekreterare eller informationssäkerhetssamordnare i samverkan med motsvarande kanslichef eller IT-chef.

En utmaning som behöver tydliggöras är att förvaltningarna/sektorerna många gånger förväntar sig att den centrala dataskyddsorganisationen ska genomföra merparten av dataskyddsarbetet för hela kommunen. Den centrala organisationen upplever i sin tur att tiden inte räcker till eller att de har tillräckliga resurser för att hantera komplexa dataskyddsfrågor. Personerna som arbetar i dataskyddsorganisationen har i regel andra arbetsuppgifter som behöver prioriteras och det är svårt att få fart i dataskyddsarbetet.

Viktigt att beakta är att det inte finns några rätt eller fel här. Kommunen kan organisera sig med en stark central dataskyddsorganisation som bedömer och tar fram ställningstaganden som blir gällande för samtliga verksamheter men detta behöver tydliggöras med att dataskyddsorganisationen får ett tydligare uppdrag och där man ser till att man har tillräckligt med resurser för att proaktivt arbeta med dataskydd. Ansvaret kan dock aldrig lämnas över utan följer med den som är personuppgiftsansvarig. Därför finns det ett behov av att det finns personal utsedd från respektive förvaltning/sector som kan värna om och signalera om särskilda behov kopplade till deras uppdrag.

Resultatet visade också att kommunerna generellt ändå kommit igång förhållandevis väl med sitt dataskyddsarbete. Dock finns det många utvecklingsområden särskilt för att möta arbetsuppgifterna proaktivt och systematiskt.

Kontaktpersonerna till dataskyddsombuden kommer i regel från den centrala dataskyddsorganisationen i respektive kommun. På förvaltning/sektors nivå finns inte samma tydliga kontaktvägar för dataskyddsombuden och det är svårt att få en generell helhetsbild om hur förutsättningarna ser ut på lokal nivå. Det som står klart är dock att respektive personuppgiftsansvarig nämnd har dataskyddsombuden utsedda och bör rimligen kunna nyttja dataskyddsombuden utefter GDPRs definition. Frågan blir här då finns det förutsättningar för det och hur ser förväntansbilderna ut.

## 4. Förutsättningar för samverkan



**GDPR anger att flera olika aktörer kan gå samman och anlita dataskyddsombud som verkar för flera olika verksamheter. Detta har gjorts på flera håll runt om i Europa och i Sverige har mindre kommuner gjort så i många fall exempelvis vissa kommuner i Göteborgsregionen och Boråsregionen. Det faller ju dock på de personuppgiftsansvariga som väljer att samverka att säkerställa så att dataskyddsombudet har rätt förutsättningar för att lyckas i rollen och att belastningen är viktad så att samtliga verksamheter kan nyttja dataskyddsombudets tjänster så som rollen är tänkt minst enligt förordningens direktiv.**

Enligt artikel 37.3 får ett enda dataskyddsombud utnämnas för flera offentliga myndigheter, med hänsyn till deras organisationsstruktur och storlek. Personuppgiftsansvarige ska med beaktande av dataskyddsombudets olika arbetsuppgifter säkerställa att ett enda dataskyddsombud, vid behov med hjälp av en grupp, kan fullgöra dessa uppgifter på ett effektivt sätt trots att de har utnämnts för flera offentliga myndigheter. (Artikel 29-arbetsgruppen för skydd av personuppgifter, Riktlinjer om dataskyddsombud, 2016)

Då dataskyddsombuden är utsedda för kommunernas olika nämnder är det viktigt att se till att varje nämnd eller nämnds organisation får det stöd som de är i behov av. I samverkansavtalet framgår att de två dataskyddsombuden ska verka för 8 kommuner och GRs egna organisation. Det saknas dock en behovsanalys om hur förutsättningarna i kommunernas olika förvaltningar/sektorer ser ut samt vilka förutsättningar som ska säkras och tillhandahållas i egenskap av intern dataskyddsorganisation både på kommunal och förvaltningsnivå. Det finns inte heller någon bedömning om tidsåtgång för respektive förvaltning/sektor. För att ge en bild av antalet nämnder och förvaltningar/ sektorer i förhållande till dataskyddsombudets uppdrag följer här en sammanställning efter vad som beskrivs på respektive kommuns hemsida både politisk och förvaltningsorganisation.

Ale	Sektor kommunstyrelse	Kommunstyrelse
Ale	Sektor samhällsbyggnad	Samhällsbyggnadsnämnd
Ale	Sektor service	Servicekommitté
Ale	Sektor utbildning	Utbildningsnämnd
Ale	Sektor kultur	Kultur- och fritidsnämnd
Ale		Valnämnd
Ale		Jävsnämnd
Ale		Överförmyndarnämnd
Ale		Revisorerna
Alingsås	Kommunledningskontoret	Kommunstyrelsen + jävsutskott
Alingsås	Kommunledningskontoret	Krisledningsnämnden
Alingsås	Kommunledningskontoret	Överförmyndarnämnden
Alingsås	Kommunledningskontoret	Valnämnden
Alingsås	Barn- och ungdomsförvaltningen	Barn- och ungdomsnämnden

Alingsås	Kultur- och utbildningsförvaltningen	Kultur- och utbildningsnämnden
Alingsås	Samhällsbyggnadsförvaltningen	Miljöskyddsnämnden
Alingsås	Samhällsbyggnadsförvaltningen	Samhällsbyggnadsnämnden
Alingsås	Socialförvaltningen	Socialnämnden
Alingsås	Vård- och omsorgsförvaltningen	Vård- och omsorgsnämnden
Alingsås		Revisorerna
Göteborgsregionens kommunalförbund	Förvaltning	Förbundsstyrelsen
Göteborgsregionens kommunalförbund	Förvaltning	Utbildningsgruppen
Härryda	Sektorn för teknik och förvaltningsstöd, TOF	Kommunstyrelsen
Härryda		Valnämnd
Härryda	Sektorn för utbildning, kultur och fritid. UKF	Välfärdsnämnd
Härryda	Sektorn för socialtjänst, SOC	Välfärdsnämnd
Härryda	Sektorn för samhällsbyggnad, SHB	Miljö- och bygglovsnämnd
Härryda		Överförmyndarnämnd i samverkan
Härryda		Revisorerna
Lerum	Sektor lärande + övriga	Kommunstyrelsen
Lerum	Sektor samhällsbyggnad	Miljö och byggnadsnämnden
Lerum	Sektor stöd och omsorg	Individnämnden
Lerum		Valnämnden
Lerum		Krisledningsnämnden
Lerum		Överförmyndarnämnden
Lerum		Revisorerna
Lilla Edet	Sektor kommunledning	Kommunstyrelsen
Lilla Edet		Krisledningsnämnd
Lilla Edet		Valnämnd
Lilla Edet		Överförmyndarnämnd
Lilla Edet		Revisorerna
Lilla Edet	Sektor bildning	Bildningsnämnd
Lilla Edet	Sektor samhälle	Samhällsnämnd
Lilla Edet	Sektor socialtjänst	Socialnämnd
Partille	Kommunstyrelseförvaltningen	Kommunstyrelsen
Partille		Valnämnd
Partille		Överförmyndarnämnd
Partille	Utbildningsförvaltningen	Utbildningsnämnden
Partille	Kultur- och fritidsförvaltningen	Kultur- och fritidsnämnden
Partille	Bygg- och Miljöförvaltningen	Bygg- och miljönämnden
Partille	Social- och arbetsförvaltningen	Social- och arbetsnämnden
Partille	Vård- och omsorgsförvaltningen	Vård- och omsorgsnämnden
Partille		Revisorerna/

Stenungsund	Sektor Stödfunktioner	Kommunstyrelsen
Stenungsund		Valnämnden
Stenungsund		Överförmyndarnämnden
Stenungsund	Sektor socialtjänst	Sociala myndighetsnämnd
Stenungsund	Sektor samhällsbyggnad	Tekniska myndighetsnämnden
Stenungsund	Sektor utbildning	Kommunstyrelsen
Stenungsund		Revisionerna
Öckerö	Kommunstyrelsens förvaltning	Kommunstyrelsen
Öckerö	Utbildnings-, kultur- och fritidsförvaltningen	Utbildnings-, kultur- och fritidsnämnden
Öckerö	Kommunstyrelsens förvaltning	Bygg- och miljönämnd
Öckerö		Krisledningsnämnd
Öckerö	Socialförvaltningen	Socialnämnd
Öckerö		Valnämnd
Öckerö		Överförmyndarnämnd
Öckerö		Revisorerna

Om ovanstående stämmer finns det 68 nämnder som i sig är egna personuppgiftsansvariga för de personuppgiftsbehandlingar som sker inom respektive verksamhetsområde. Dessa 68 nämnder delar på 2 dataskyddsombud. Förvaltningsorganisationen är inte alltid kopplad till nämnd och vissa nämnder delar förvaltningsorganisation. Vissa nämnder är också väldigt specifika, små och som exempelvis valnämnderna blir aktiva i samband med val men är i övrigt vilande. Så behovet av dataskyddsombudets stöd ser högst troligt olika ut beroende på storlek, antal behandlingar och känslighet. Varje nämnd är dock att betrakta som egen personuppgiftsansvarig och dataskyddsombuden ska finnas tillgängliga och ha goda förutsättningar att följa upp även dessa verksamheter.

De olika nämnderna i kommunerna har ju likartade uppdrag, processer och regler som styr och detta underlättar vid rådgivning och i efterlevnadskontrollerna. Dock väcks frågan hur dataskyddsombuden ska vara lättillgängliga, synliga och kontinuerligt följa upp varje enskild personuppgiftsansvarig.

När dataskyddsombuden reser mellan kommunerna idag sker transport enligt GRs styrdokument för resor i tjänsten där anställda i huvudsak ska resa kollektivt. Regionens kommunala förbindelser ser olika ut och ibland kan restiden för att transportera sig till ytterkommunerna vara lång. Även möjligheter att resa mitt på dagen kan vara begränsad då kollektivtrafiken i regel har tätare turer under rusningstiderna.

## 4.1 Digitala förutsättningar för samverkan

För att dataskyddsombuden ska kunna verka effektivt och vara lättillgängliga behöver viss rådgivning och möten kunna ske på distans genom telefon, mail och videomöten. Dessa kontaktkanaler behöver vara tydliga och kommuniceras på ett effektivt sätt så

förutsättningarna för uppdraget är bra. I dagsläget har dataskyddsbuden en funktionsbrevlåda dit alla kommuner kan vända sig för rådgivning. Denna mail är också den som kommuniceras ut till invånare om de behöver komma i kontakt med dataskyddsbuden. Dataskyddsbuden har också personliga mailadresser. Utöver det har dataskyddsbuden också mobiltelefoner och tillgång till Office 365 för kommunikation. Dataskyddsbudens dokumentation lagras i GRs RDS lösning i G: katalogen. Dokumentationen kan vara stödmaterial, rapporter, rättsutredningar, kommunernas styrande dokument, utbildningsmaterial, omvärldsbevakning etc.

I samverkansavtalet regleras inte i vilken utsträckning dataskyddsbuden ska finnas tillgängliga på plats i respektive kommun utan detta ska bedömas och ske utefter behov. Det som framgår är att GR ska tillhandahålla en hemvist för dataskyddsbuden. Inför granskningen så kontaktades Sydarkivera som har en liknande organisering för att jämföra arbetssätt och den stora skillnaden är att deras dataskyddsbud arbetar uteslutande på distans.

### **E-post**

I dagsläget så inkommer frågor både från kommunernas anställda och registrerade som vill nå dataskyddsbudet till antingen en gemensam funktionsbrevlåda eller till dataskyddsbudens personliga GR mail i Outlook. Frågorna besvaras skyndsamt där brådskande ärenden prioriteras. Majoriteten av frågorna som kommer till dataskyddsbuden kommer från anställda inom kommunerna i samverkan samt GRs interna förvaltning. Frågorna kan handla om allmän rådgivning i tolkningsfrågor, Incidentbeskrivningar, mötesförfrågningar och utbildningsförfrågningar etc. Dataskyddsbuden prenumererar också på en del nyhetsbrev i sin omvärldsbevakning som kommer in denna väg.

### **Teams**

Dataskyddsbuden använder också Teams som videotjänst för att kunna bjuda in och delta i distansmöten. Då dataskyddsbuden verkar på distans finns ett stort behov av effektiva och säkra videosamtal för att kunna finnas lättillgängliga för kommunerna. Nätverken för kontaktpersonerna har i regel också skett på distans genom Teams. Anledningen att Teams används är för att det är det verktyg som Göteborgsregionens kommunalförbund beslutat att de anställda ska nyttja vid videomöten.

### **Telefon**

Dataskyddsbuden har också mobiltelefoner med både ett fast anknytningsnummer och mobilnummer dit verksamhet, registrerade och tillsynsmyndigheten kan nå dem på. Detta behövs också för att dataskyddsbudet ska vara lättillgängliga.

## **Office 365**

Dataskyddsbuden har liksom övriga anställda på GR tillgång till Office 365 som stöd för sitt dagliga arbete. Word och Powerpoint används mest frekvent. Arbetsmaterial lagras i Onedrive och färdiga dokument lagras lokalt inom GR i G: katalogen.

Överlämning av dokumentation så som rapporter och övriga skrivelser från dataskyddsbuden skickas per mail till kommunerna enligt överenskommelse men i regel skickas materialet till kommunbrevlådan och till berörd utsedd kontaktperson.

# **5. Identifierade risker utifrån nuvarande förutsättningar**

Under detta kapitel så redogör dataskyddsbuden för identifierade risker med nuvarande organisationsform och rekommendationer som kan stärka dataskyddsbudens förutsättningar att utöva sitt uppdrag inför framtiden med samverkansavtalet i grunden.

## **5.1 Risk att dataskyddsbuden inte är tillgängliga i tillräcklig utsträckning vilket leder till dataskyddsbuden inte hinner fullgöra sitt uppdrag**

Med dagens organisationsform verkar dataskyddsbuden nästan uteslutande utanför den interna organisationen då arbetsplatsen enligt samverkansavtalet är belägen i Göteborgsregionens kommunalförbunds lokaler i Göteborg. Detta kan leda till att verksamheten inte känner till att dataskyddsbuden finns till förfogande speciellt på förvaltningsnivå. Det blir också svårare för dataskyddsbuden att själva göra sig kända i organisationen. För att arbetet ska fungera och att dataskyddsarbetet ska integreras i kommunernas verksamhet uppstår här ett behov av en egen tydlig och stark intern dataskyddsorganisation. Som kan fånga upp och förmedla vidare information till dataskyddsbuden men också bjuda in dataskyddsbuden när så är lämpligt.

I samverkansavtalet framgår att dataskyddsbuden är utsedda för de åtta kommunerna som valt att ingå i samverkansavtalet för dataskyddsbud. En kommun är i sin helhet aldrig personuppgiftsansvarig utan det är det respektive nämnd som är för de behandlingar som sker inom nämndens ansvarsområde och uppdrag. Dataskyddsbuden har därför 68 olika personuppgiftsansvariga att både ge råd till och bevaka efterlevnaden för. Då dataskyddsbuden ska och har intagit en riskbaserad arbetsmetod så har kommunernas socialtjänstförvaltningar och skolförvaltningar haft efterlevnadskontroller under 2020 och 2021 medan de övriga förvaltningarna och nämnderna har blivit utan. Dataskyddsbuden prioriterade alltså på kommunnivå och fokuserade på kommunernas verksamhetsdelar som bedömdes hantera de mest integritetskänsliga personuppgifterna. Varje myndighet är

dock skyldig att utse och ge dataskyddsbudet goda förutsättningar att utöva sitt uppdrag och frågan är om det är lämpligt och tillräckligt att två dataskyddsbud delar på så många personuppgiftsansvariga. Slår man ut det blir det ca: 3 % av tiden på respektive förvaltning/nämnd. Nu är ju inte varje förvaltning/nämnd unik utan kommunernas verksamheter liknar varandra i stora drag om dock i olika organisationsformer. Kommunernas nämnder och förvaltningar står ofta inför liknande utmaningar vilket underlättar rådgivningsarbetet för dataskyddsbuden och detta leder till att dataskyddsbuden kan anpassa insatserna och fånga upp fokusområden att prioritera.

### **Förslag till Åtgärd:**

- Samverkansparterna bör var för sig utreda vilket behov respektive nämnd har av dataskyddsbudets tjänster och vilken egen intern dataskyddsorganisation som finns eller behöver tillsättas som kan stötta upp och bistå dataskyddsbuden i deras arbete med bland annat efterlevnadskontroller. Resonera om möjliga arbetssätt som inkluderar dataskyddsbuden, exempelvis att dataskyddsbuden ges möjlighet att lämna kommentarer eller bjuds in i specifika skeden av utvecklings eller inköpsprocesser, hålls uppdaterade om incidenthantering etc.
- Samverkansavtalet bör kompletteras med en skrivelse om organisatoriska förutsättningar hos respektive samverkanspart/ personuppgiftsansvarig om vad som är minimikrav på en lokal dataskyddsorganisation för att träda in i samverkansavtalet. En lämplig dataskyddsorganisation som kan driva dataskyddsarbetet hos respektive myndighet och som kan bistå dataskyddsbuden med information och vara stöd till den egna verksamheten parallellt med dataskyddsbuden.
- Samverkansparterna bör också bedöma och beskriva om och i vilken utsträckning de önskar ha dataskyddsbuden på plats ute i kommunerna för att dessa ska bli kända och tillgängliga för respektive personuppgiftsansvarigs verksamhet eller om de bedömer att det räcker med att ha dem på distans. I nuvarande samverkansavtal framgår endast att dataskyddsbuden ska ha sin hemvist i GRs lokaler men då uppdraget i majoritet utförs gentemot kommunerna så bör respektive part resonera kring tillgängligheten och behovet av att ha dataskyddsbudet på plats och om det i så fall finns tillräckliga resurser i form av arbetsplatser etc, så dataskyddsbuden har en god arbetsmiljö.
- Restiden är också en faktor att beakta och hur dataskyddsbuden smidigast reser inom regionen om behovet av att ha dataskyddsbuden på plats ökar.

## **5.2 Risk att dataskyddsorganisationerna inte är försedda med tillräckliga resurser utefter vald samverkansform som leder till otydlighet i ansvar och roller**

I dagsläget har respektive kommun försett dataskyddsombuden med en, två eller tre kontaktpersoner. Dessa är ofta placerade centralt i kommunen under en kansliförvaltning eller administrativ avdelning vilket är bra. Dessa personer kan på så vis hålla samman dataskyddsarbetet för kommunen. Dessa personer har också en bra översikt bild av förutsättningarna som finns ute i den egna kommunen. De blir en första kontaktväg för lokala dataskyddsorganisationer i kommunens övriga förvaltningar/sektorer.

Dataskyddsombuden är ju dock anmälda för respektive personuppgiftsansvarig inom kommunerna och det bör bli tydligare hur kommunerna styr sitt dataskyddsarbete och vem som är representant och driver dataskyddsarbetet på respektive myndighet inom kommunen. Dessa kontaktvägar saknas för dataskyddsombuden till respektive nämnds förvaltning och det medför att dataskyddsombuden har en god dialog med den centrala organisationen men saknar kontinuerlig dialog med lokala verksamheter på förvaltnings-/sektorsnivå. Märk väl att det kan finnas skäl för detta och GDPR reglerar inte hur enskilda myndigheter strukturerar sin dataskyddsorganisation eller var bedömningar och utredningar sker. Det bör dock vara tydligt hur organisationen valt att organisera sig dels för att verksamheterna själva ska veta vem som hanterar vilka frågor och var i organisationen det strategiska och operativa dataskyddsarbetet ska ske och dels för att dataskyddsombudet ska ges goda förutsättningar att fullgöra uppdraget enligt GDPRs definition.

### **Förslag till Åtgärd:**

- Varje samverkanspart bör bedöma om det räcker med utsedda kontaktpersoner från den centrala dataskyddsorganisationen eller om den ska kompletteras med kontaktpersoner till respektive förvaltning/sector/nämnd. Dataskyddsombuden skulle gärna se att respektive nämnds förvaltning/ sektor utser en kontaktperson ur den lokala dataskyddsorganisationen. Detta skulle underlätta kommunikationen mellan dataskyddsombuden och respektive förvaltning/sector när det uppkommer specifika frågor rörande specifik verksamhet.
- Om denna förändring skulle till skulle det dock behöva finnas en inre styrning så det blir tydligt hur respektive samverkanspart önskar att kommunikation sker. Det är inte helt ovanligt att en central dataskyddsorganisation håller ihop arbetet i kommunen i stort för att skapa en enhetlig hantering inom kommunen. Resurserna och kompetensen kan också göra det nödvändigt att ha en central organisation som utför merparten av dataskyddsarbetet. Organisationsformen bör främja så att relevant information sprids till kommunens berörda delar.

### **5.3 Risk att samverkansavtalet ger en felaktig bild av dataskyddsbudens uppdrag som leder till otydliga förväntningar på dataskyddsbudens leveranser**

I första kapitlet i denna rapport så beskrivs dataskyddsbudens uppdrag ur GDPRs definition. Förenklat kan GDPRs definition av dataskyddsbudens uppdrag sammanfattas genom dessa punkter. Kontinuerlig rådgivning, Bevakande av efterlevnaden, kontaktperson till tillsynsmyndigheten samt de registrerade och bistå vid konsekvensbedömningar. Detta ska ske för varje personuppgiftsansvarig som har ett utsett dataskyddsbud. Om flera personuppgiftsansvariga ska dela på ett dataskyddsbud bör en bedömning av dataskyddsbudens förutsättningar att fullgöra detta uppdrag upprättas. Detta för att klargöra i vilken utsträckning dataskyddsbuden ska bistå med rådgivning och rapporter kopplat till dataskyddsarbetet. Är det många personuppgiftsansvariga som delar på ett dataskyddsbud bör det även finnas en stark intern organisation på plats som kan bistå med egen internkontroll av dataskyddsarbetet på regelbunden basis som dataskyddsbudet ges möjlighet att lämna synpunkter på. Under rådande läge så är bedömningen att dataskyddsbuden inte hinner med att följa upp samtliga verksamheter som faller under deras ansvarsområde varje år och detta skapar en risk att dataskyddsarbetet släpar efter och att de olika verksamheterna inte får den stöttning som de är i behov av för att leva upp till dataskyddslagstiftningens krav.

Samverkansavtalet beskriver i nuvarande version att 8 kommuner och GRs egna organisation nyttjar dataskyddsbudens tjänster. De unika personuppgiftsansvariga listas inte vilket skapar förvirring vid tolkning av dataskyddsbudens uppdrag. Det nämns heller inget i samverkansavtalet att de kommunala bolagen är undantagna och förväntas bedöma behovet och utse egna dataskyddsbud. Önskvärt vore att respektive personuppgiftsansvarig listas och att de görs uppmärksammade på att samverkansavtalet finns. Dessutom vore det önskvärt om samverkansparterna skattade utefter varje förvaltning/sektors behov med beaktande av komplexitet, antal behandlingar, registrerade och andel känsliga personuppgifter i samverkansavtalet. Inför framtida revidering bör också samverkansparterna resonera om de kan samverka mer i dataskyddsarbetet och hur det i så fall skulle kunna fungera. Nuvarande samverkansavtal har medfört att dataskyddsbuden har intagit en riskbaserad arbetsmetod efter kommunernas verksamhet i sin helhet i linje med det samverkansavtal som finns upprättat. Då kommunerna inte är att betrakta som personuppgiftsansvariga i sin helhet så kan detta leda till att respektive nämnd som personuppgiftsansvarig inte lever upp till GDPRs krav kopplat till att dataskyddsbudet ska ha goda förutsättningar att utföra sitt uppdrag som ska ske gentemot varje personuppgiftsansvarig.

#### **Förslag till Åtgärd:**

- Faktum är att samverkansavtalet rör ganska många unika personuppgiftsansvariga. Utifrån det så bör samverkansparterna också bedöma om de anser att det är tillräckligt med den bemanning som idag finns



och klargöra vilka behov och förväntansbilder respektive personuppgiftsansvarig har på tjänsteleveransen. Denna bedömning bör utgå från dataskyddsombudsrollen så som den beskrivs GDPR. Denna bedömning bör dokumenteras och motiveras då det faller på respektive personuppgiftsansvarig att visa att man även lever upp till att ha ett utsett dataskyddsombud som verkar enligt GDPRs definition och har tillräcklig tid och resurser för att klara av uppdraget. Dessa bedömningar bör sedan delas med GR som bär anställningsansvaret så de kan planera och utforma tjänsten utifrån samverkansparternas behov, förväntningar och egna förutsättningar.

- Samverkansavtalet behöver revideras och tydliggöras så förutsättningarna tydliggörs.
- Samverkansparterna bör också kommunicera till de kommunala bolagen inom kommunen att de behöver bedöma om de behöver ett dataskyddsombud och i så fall se till att utse ett eget dataskyddsombud. Detta i de fall detta inte redan har genomförts. Alternativt bedöma om även de kommunala bolagen ska ingå i samverkansavtalet.

## **5.4 Risk att information blandas om olika personuppgiftsansvariga om de hanteras genom samma mailinkorg som kan leda till att sekretessgränser bryts**

Idag hanteras inkommande e-post till dataskyddsombuden genom en och samma e-postadress [dso@goteborgsregionen.se](mailto:dso@goteborgsregionen.se). Därför inkommer olika typer av ärenden och frågor från flera olika kommuner och förvaltningar/sektorer till samma inkorg. Detta blir problematiskt då flera olika kommuners och personuppgiftsansvarigas information blandas samman i en annan myndighet. Beroende på hur man ser på dataskyddsombudets ställning under tiden denne verkar för respektive kommun finns anledning att dela upp inkorgarna. Dels för att säkerställa så att ingen sekretess riskerar att lämna en myndighet på ett otillåtet sätt. Värt att beakta är att det inte är säkert att sekretesskyddet kan föras över om informationen byter myndighet. Dels också för att det ska bli tydligt vilken information som hör till vilken kommun/förvaltning. På så vis blir det enklare att argumentera för att informationen i dataskyddsombudens inkorg tillhör den organisation som initierat ärendet och behörigheten och innehållet till inkorgen blir begränsad till kommunen/förvaltningen beroende på vilken nivå som anses nödvändig. Dataskyddsombuden företräder ju flertalet personuppgiftsansvariga och hanterar och ges tillgång till stora mängder av kommunernas information efter behov för att kunna fullgöra uppdraget. Det är av vikt att strukturera under vilka förutsättningar som dataskyddsombuden ska verka och hur de ses i förhållande till respektive kommun. Är dataskyddsombuden en del av kommunens organisation under den tid de handlägger ärenden från kommunen eller ses informationen som expedierad när den skickas till

dataskyddsbuden som har sina anställningar i Göteborgsregionens kommunalförbund? Enligt skäl 97 till GDPR får Dataskyddsbudet ingå i den personuppgiftsansvariges eller personuppgiftsbiträdets personal, eller utföra uppgifterna på grundval av ett tjänsteavtal. Ur denna formulering bör det kunna antas att dataskyddsbuden får lov att verka å respektive personuppgiftsansvariges vägnar när respektive personuppgiftsansvarig myndighet köper tjänsten av Göteborgsregionens kommunalförbund. Det bör dock regleras så att dataskyddsbuden hanterar sina olika kunders uppgifter/ information separat.

### **Förslag till Åtgärd:**

- Samverkansparterna bör utreda hur dataskyddsbudens kommunikationskanaler kan styras för att undvika att sekretesskyddet slutar att fungera om information delas med dataskyddsbuden och att kommunikationen och åtkomsten begränsas till enbart dataskyddsbudet och berörd myndighet. Detta kan innebära flera olika scenarion där en möjlig åtgärd kan vara att exempelvis dataskyddsbuden får en funktionsbrevlåda hos respektive myndighet och att de får en signal till GRs mail när ett mail kommer in så de blir varse om att det har uppkommit ett ärende att hantera. Hur detta i praktiken ska struktureras bör samverkansparterna utreda och rusta för.
- Vidare kan också diskuteras lämpligheten i att dataskyddsbuden använder Office 365 som skrivbordsstöd i sitt arbete. GR liksom de flesta av samverkanskommunerna använder idag Office 365 i sin förvaltning. GR är enligt samverkansavtalet anställande myndighet för dataskyddsbuden och bär ansvaret att de har systemstöd som täcker deras behov av att kunna fullgöra sina uppdrag som dataskyddsbud. Kopplat till detta är rekommendationen att GR och de samverkanskommuner som beslutat att fortsätta använda Office 365 gör de bedömningar som krävs för att visa på lagligheten att nyttja tjänsten i sin ordinarie verksamhet.

## **5.5 Risk att personuppgiftsansvariga inte på ett korrekt sätt och i god tid ser till att dataskyddsbuden deltar i alla frågor som rör skyddet av personuppgifter.**

Nuvarande organisatoriska förutsättningar med dataskyddsbud i samverkan ställer höga krav på verksamheterna att tillse och bjuda in dataskyddsbuden i god tid och på ett korrekt sätt. Med så många personuppgiftsansvariga inblandade är det viktigt att det klargörs hur dataskyddsbuden ska ges god kännedom om personuppgiftsbehandlingarna, på vilket sätt de behandlas i verksamheten samt de motiveringar kring varför de behandlas som de gör och hur den personuppgiftsansvarige bedömt att detta samspelar med dataskyddslagstiftningen. Då dataskyddsbuden har ett brett ansvarsområde är det viktigt att respektive

personuppgiftsansvarig har en god förmåga att driva på dataskyddsarbetet på strategisk och operativ nivå och bereda ett gott underlag för dataskyddsombuden att lämna synpunkter på och ge råd utifrån. Med beaktan av nuvarande samverkansavtal och det faktum att dataskyddsombuden ska verka för så pass många personuppgiftsansvariga får det antas att respektive personuppgiftsansvariga ska ha förmåga att uppmärksamma dataskyddsombuden när frågor som rör skyddet av personuppgifter dyker upp och att man har upprättade strategier och rutiner för hur dataskyddsaspekten ska interageras i det dagliga arbetet i verksamhetens processer. Det är inte rimligt att anta att dataskyddsombuden utifrån nuvarande samverkansavtal ska ha detaljkunskap om respektive personuppgiftsansvarigs samtliga processer inte heller att dataskyddsombuden uppsökande själva ska skaffa sig kunskap om organisatoriska förändringar som berör skyddet av personuppgifter när de verkar på distans. Detta bör respektive personuppgiftsansvarig bistå dataskyddsombudet med i form av kompetens och resurser som kan samverka med dataskyddsombudet för att nå ett framgångsrikt och inkluderande arbetssätt. Om denna risk försummas kan det leda till att personuppgiftsansvariga inte lever upp till de förutsättningar som GDPR deklarerar att dataskyddsombuden ska ha i utövandet av sitt uppdrag. Arbetsmetoden bör också ta hänsyn till dataskyddsombudens tidsåtgång för att utföra de uppgifter som är kopplade till detta arbete i förhållande till övriga uppgifter som är ålagda dataskyddsombuden.

### **Förslag till åtgärder:**

- Samverkansparterna bör gemensamt resonera kring frågan och utreda hur dataskyddsombuden och respektive personuppgiftsansvarig ska verka och kan inkluderas för att gemensamt möta de krav som GDPR ställer på respektive nämnd i egenskap av personuppgiftsansvarig. Reda ut vilka arbetssätt som är lämpliga när man väljer att anlita ett dataskyddsombud på distans.
- Ta fram beskrivningar som tydliggör respektive personuppgiftsansvariges dataskyddsorganisation. Vilka förutsättningar, behov och ambitioner respektive personuppgiftsansvarig har i sitt dataskyddsarbete. Dessutom utreda vilka grundförutsättningar som respektive part behöver tillgodoses för att arbetet ska fungera i enlighet med samverkansavtalet och för att tillse att dataskyddsombuden ges goda förutsättningar att utöva sina uppdrag och på var och när i de olika processerna dataskyddsombuden ska kopplas in eller informeras.
- Respektive samverkanskommun bör bedöma och resonera hur de ser på personuppgiftsansvaret kopplat till respektive nämnd i förhållande till samverkansavtalet och om de bedömer det rimligt att dataskyddsombuden kan leva upp till deras skyldighet att utse ett verksamt dataskyddsombud och allt vad det innebär.

## Bilagor

1. Samverkansavtal Regionalt dataskyddsombud (senaste versionen)

## Referenser

Artikel 29-arbetsgruppen för skydd av personuppgifter, Riktlinjer om dataskyddsombud. (den 13 December 2016). Riktlinjer om dataskyddsombud. *Riktlinjer om dataskyddsombud*. Bryssel, Belgien: EDPB.

Integritetsskyddsmyndigheten. (den 09 03 2022). *www.imy.se*. Hämtat från imy.se: <https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/dataskyddsombud/om-dataskyddsombud-i-dataskyddsförordningen/>