Boråsregionen Sjuhärads Kommunalförbund

Granskning av samordnad funktion för dataskyddsombud

REVISIONSRAPPORT

2023-03-15
Antal sidor: 35

Erik Österberg, jurist
Mats Herling, jurist

Insatt AB
Kyrkogatan 4
553 16 Jönköping
www.insatt.com

Jerker Stenqvist, auktoriserad revisor och certifierad kommunal revisor

SQ Revision & Rådgivning AB
Hörngatan 1
573 42 Tranås

Innehåll

1. Inledning 4
1.1 Bakgrund 4
1.2 Syfte och revisionsfrågor 5
1.3 Metod 6
1.4 Avgränsning och disposition 6
2. Allmän juridisk utgångpunkt – dataskyddsombud 7
3. Resultatet av granskningen 8
3.1 Vilka förväntningar, uppdrag eller mål finns från anslutna kommuner? 8
3.1.1 Utgångspunkter 8
3.1.2 Förväntningar, uppdrag och mål hos anslutna kommuner 9
3.1.3 Iakttagelser och bedömning 10
3.2 Vilka avtal/överenskommelser finns upprättade med respektive kommun? 10
3.2.1 Utgångspunkter 10
3.2.2 Upprättade avtal/överenskommelser 11
3.2.3 Iakttagelser och bedömning 11
3.3 Tydlig ansvarsfördelningen mellan dataskyddsombuden och kommunerna? 11
3.3.1 Utgångspunkter 11
3.3.2 Ansvarsfördelningen mellan dataskyddsombuden och kommunerna 12
3.3.3 Iakttagelser och bedömning 13
3.4 I vilken utsträckning uppfyller granskningsverksamheten de lagkrav som finns inom området? 14
3.4.1 Utgångspunkter 14
3.4.2 Dataskyddsombudens granskningsverksamhet 15
3.4.3 Iakttagelser och bedömning 18
3.5 Är prioriteringen i granskningsarbetet lämplig med hänsyn till granskningsområde och typen av granskningsobjekt? 20
3.5.1 Utgångspunkter 20
3.5.2 Prioriteringen i granskningsarbetet utifrån granskningsområde och granskningsobjekt 20
3.5.3 Iakttagelser och bedömning 21

3.6 Är bemanningen och resurser för dataskyddsombuden tillräckliga för verksamhetens uppgift? 21
3.6.1 Utgångspunkter 21
3.6.2 Dataskyddsombudens bemanning och resurser 22
3.6.3 Iakttagelser och bedömning 25
3.7 Är dataskyddsombudens rådgivning och utbildningsinsatser tillräckliga? 26
3.8 Om dataskyddsombudens rådgivning är tillräcklig 26
3.8.1 Utgångspunkter 26
3.8.2 Dataskyddsombudens rådgivning 27
3.8.3 Iakttagelser och bedömning 28
3.9 Om utbildningen ombuden tillhandahåller verksamheterna är tillräcklig 29
3.9.1 Utgångspunkter 29
3.9.2 Utbildning som dataskyddsombuden tillhandahåller verksamheterna 30
3.9.3 Iakttagelser och bedömning 30
4. Sammanfattande slutsatser och rekommendationer 32

1. Inledning

Vi har av revisorerna i Sjuhärads kommunalförbund fått i uppdrag att granska hur kommunalförbundets dataskyddsombud verkar inom förbundet och gentemot de medlemskommuner som deltar i samverkan.

1.1 Bakgrund

Allmänna dataskyddsförordningen EU 2016/679[1] (härefter ”GDPR”, ”dataskydds-förordningen” eller ”förordningen”) trädde i kraft den 25 maj 2018, gäller i hela EU och ersatte i Sverige den äldre Personuppgiftslagen (1998:204) (PUL) från 1998. Det främsta syftet med dataskyddsförordningen är att bidra till starkare skydd för individers integritet och större makt för enskilda att kunna bestämma över sina personuppgifter. Andra syften med dataskyddsförordningen är att modernisera dataskyddsdirektivets regler från 1995 och att anpassa dessa till det nya digitala samhället. Såväl offentliga som privata verksamheter behöver anpassa hanteringen av personuppgifter så att den uppfyller gällande regler i dataskyddsförordningen och kompletterande nationell lagstiftning[2]. Förordningen kräver att vissa verksamheter utser ett dataskyddsombud. I de fall personuppgiftsbehandling utförs av en myndighet eller ett offentligt organ ska personuppgiftsansvarig utse dataskyddsombud. Eftersom de kommunala nämnderna är personuppgiftsansvariga och offentliga organ behöver de utse dataskyddsombud.

I februari 2018 beslutades att inrätta en delregional funktion för dataskyddsombud inom Boråsregionen Sjuhärads Kommunalförbund (härefter ”samverkan”). Funktionen innebär att dataskyddsombud verkar och är organiserade inom kommunalförbundet och agerar dataskyddsombud till de kommuner som önskar delta i samverkan. Kostnaden fördelas mellan deltagande kommuner.

Den utredning som föregick beslutet anger följande fördelar med en samverkansorganisation inom kommunalförbundet;

- Kommunalförbundet erbjuder en befintlig samverkansorganisation med styrning från respektive kommun.
- Dataskyddsombuden erbjuds en självständig roll i förhållande till kommunerna som ligger väl i linje med intentionerna i den nya dataskyddsförordningen.
- Samverkan kring dataskyddsombud skapar förutsättningar för en robust bemanning.
- Samverkan kring dataskyddsombud ger goda förutsättningar att erbjuda kommunerna den kompetensbredd som förordningen föreskriver.

[1] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

[2] Se bl.a. lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (Kompletteringslagen).

Sedan 2018 har dataskyddsombuden verkat som dataskyddsombud åt kommunerna Bollebygd, Borås stad, Herrljunga, Svenljunga, Tranemo, Ulricehamn och Vårgårda, ett antal kommunala bolag samt Södra Älvsborgs Räddningsförbund (SÄRF) och Sjuhärads Samordningsförbund (härefter ”deltagande/anslutna kommuner”). Verksamheten finansieras genom en fast avgift per deltagande kommun samt en rörlig del baserad på kommunens antal invånare.

Sedan den 1 januari 2022, då även Marks kommun anslöt sig till samverkan, har både grundkostnaden och den kommuninvånarbaserade kostnaden räknats om för att den totala budgeten för verksamheten inte skulle öka. På så vis har uppdragets omfång utökats utan att funktionens resurser ökat.

På uppdrag av revisorerna i Sjuhärads kommunalförbund genomförde revisionskontoret i Borås Stad 2021 en förstudie som syftade till att undersöka hur kommunalförbundets dataskyddsombud verkar inom förbundet och gentemot de medlemskommuner som deltar i samverkan. Revisionskontorets övergripande slutsats var att det fanns förutsättningar för vidare fördjupad granskning inom området. Innevarande syfte tar avstamp i slutsatserna från förstudien.

1.2 Syfte och revisionsfrågor

Granskningen syftar, i enlighet med kraven i upphandlingsunderlagen, till att undersöka de förutsättningar kommunalförbundets dataskyddsombud har för att verka inom förbundet och gentemot de medlemskommuner som deltar i samverkan. Projektet innefattar även en granskning av funktionens arbetssätt med fokus på följsamhet mot lagar och prioritering av tillsynsarbetet med hänsyn till granskningsobjekten.

Granskningen avser besvara följande revisionsfrågor:

- Vilka förväntningar, uppdrag eller mål finns från anslutna kommuner?
- Vilka avtal/överenskommelser finns upprättade med respektive kommun?
- Är ansvarsfördelningen tydlig mellan dataskyddsombuden och kommunerna?
- I vilken utsträckning uppfyller dataskyddsombudens granskningsverksamhet de lagkrav som finns inom området?
- Är prioriteringen hos granskningsarbetet lämpligt med hänsyn till granskningsområde och typen av granskningsobjekt?
- Är bemanningen och resurser för dataskyddsombuden tillräckliga för verksamhetens uppgift?
- Är dataskyddsombudens rådgivning och utbildningsinsatser tillräckliga?

1.3 Metod

Granskningen har genomförts genom:

- Studium och genomgång av relevanta styrdokument, granskningsunderlag och andra underlag, samt
- Intervjuer och avstämningar med dataskyddsombuden Magnus Blomqvist och Dan Bodin samt dataskyddssamordnare i tre kommuner av olika storlek (Borås stad, Ulricehamn och Vårgårda).

Intervjuanteckningarna har faktakontrollerats av respektive intervjuperson. Rapporten har faktakontrollerats av granskningsledare Samuel Kaufman och granskningsmedarbetare Anna Duong vid revisionskontoret i Borås Stad för revisorerna i Sjuhärads Kommunalförbunds räkning.

1.4 Avgränsning och disposition

Granskningen har avgränsats till att omfatta verksamhetsorganisationen för Sjuhärads kommunalförbund och de revisionsfrågor som uppställts i förfrågningsunderlaget för den offentliga upphandling (och i syftet ovan) genom vilken Insatt tilldelades uppdraget.

Uppdragets omfång har inte tillåtit intervjuer med företrädare för samtliga anslutna kommuner, varför det avgränsats till tre kommuner av olika storlek.

Kapitel 2 innehåller en allmän juridisk utgångspunkt med genomgång av lagkraven i främst artikel 37 - 39 i förordningen.

I Kapitel 3 följer själva resultatet av granskningen. För att besvara syftet och revisionsfrågorna samt för att på ett tydligt och övergripande sätt presentera resultatet delas kapitel 3 (i regel) in i ett avsnitt per revisionsfråga. I syfte att ge vägledning och för tydliggörandet av de kriterier som vi har granskat mot, inleds avsnitten med sammanfattande beskrivningar av krav i gällande rätt, styrdokument eller i vissa fall andra föresatser. Därefter innehåller avsnittet en sammanfattning av vad som framkommit i intervjuerna och i begärda underlag. I slutet av varje avsnitt sammanfattas våra iakttagelser, bedömningar och identifierade brister samt i vissa fall förslag på förbättringsåtgärder. Även om genomförda intervjuer utgått ifrån de fasta revisionsfrågorna har vi försökt hålla dem öppna och ganska fria, med förhoppningen om att ett öppet samtalsklimat medför fler och bättre synpunkter. Detta har gett ytterligare intressanta iakttagelser, uppslag och synpunkter som egentligen ligger utanför revisionsfrågorna. Eftersom vi tror att såväl kommunalförbundet, de anslutna kommunerna som dataskyddsombuden kan ha nytta av dessa iakttagelser har dessa inkluderats i rapporten och under de avsnitt de passat bäst.

I Kapitel 4 sammanfattar vi våra slutsatser.

2. Allmän juridisk utgångpunkt – dataskyddsombud

Om den personuppgiftsansvarige eller personuppgiftsbiträdet (härefter benämnt ”den personuppgiftsansvarige”) är en myndighet eller ett offentligt organ, får ett enda dataskyddsombud utnämnas för flera sådana myndigheter eller organ, med hänsyn till deras organisationsstruktur och storlek. Dataskyddsombudet får agera för sådana sammanslutningar och andra organ som företräder personuppgiftsansvariga. Dataskyddsombudet ska utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i artikel 39. Dataskyddsombudet får ingå i den personuppgiftsansvariges personal, eller utföra uppgifterna på grundval av ett tjänsteavtal. Det är alltså tillåtet att anlita en utomstående uppdragstagare. Den personuppgiftsansvarige ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten.

Av artikel 39 dataskyddsförordningen framgår att dataskyddsombudet ska ha *minst* följande uppgifter:

A. informera och ge råd till den personuppgiftsansvarige, och de anställda som behandlar personuppgifter om vilka skyldigheter de har enligt dataskyddsförordningen och andra dataskyddsbestämmelser;
B. övervaka efterlevnaden
    1. av denna förordning,
    2. av andra av unionens eller medlemsstaternas dataskyddsbestämmelser och
    3. av den personuppgiftsansvariges strategi för skydd av personuppgifter, inbegripet
        - ansvarstilldelning,
        - information till och utbildning av personal som deltar i behandling och tillhörande granskning.

Dataskyddsombudet har även vissa anknytande skyldigheter:

C. på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd;
D. samarbeta och vara kontaktperson för tillsynsmyndigheten i frågor som rör behandling, inbegripet förhandssamråd, samt
E. vara kontaktbar för registrerade som vill utöva sina rättigheter eller som har frågor om personuppgiftsbehandlingen.

Dataskyddsombudet ska, när det gäller dennes genomförande av sina uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt.

Av förordningen följer även krav på den personuppgiftsansvarige att bland annat säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter. Dessutom ska den personuppgiftsansvarige stödja dataskyddsombudet i

dennes arbete genom att tillhandahålla de resurser som krävs för genomförandet av ombudets uppgifter samt ge tillgång till personuppgifter och behandlingsförfaranden. Därtill ska den personuppgiftsansvarige bidra till upprätthållandet av dataskyddsombudets sakkunskap, till exempel genom att vid behov erbjuda utbildning inom området. Den personuppgiftsansvarige ska säkerställa att dataskyddsombudet inte tar emot instruktioner som gäller utförandet av dataskyddsombudets uppgifter ovan. Dataskyddsombudet får fullgöra andra uppgifter och uppdrag. Den personuppgiftsansvarige ska se till att sådana uppgifter och uppdrag inte leder till en intressekonflikt.[3]

3. Resultatet av granskningen

3.1 Vilka förväntningar, uppdrag eller mål finns från anslutna kommuner?

3.1.1 Utgångspunkter

Dataskyddsverksamheten inom Boråsregionen Sjuhärads kommunalförbund inklusive den samordnade dataskyddsombudensfunktionens uppdrag, syften och mål kan sammanfattas enligt följande. Dataskyddsverksamheten inom kommunalförbundet är en samverkan som syftar till att (kostnads)effektivt ge medlemskommunerna kunskap och erfarenhet i dataskyddsfrågor. Kommunalförbundet ska erbjuda en samverkansorganisation med styrning från respektive kommun. Dataskyddsombuden erbjuds en självständig och oberoende roll i förhållande till de personansvariga verksamheterna på kommunerna i enlighet med intentionerna i dataskyddsförordningen. Samverkan kring dataskyddsombud ämnar skapa förutsättningar för en robust bemanning.

Samverkan kring dataskyddsombud ger goda förutsättningar att erbjuda kommunerna den kompetensbredd som förordningen föreskriver. Medlemmarna i Boråsregionen Sjuhärads kommunalförbund ska känna att de har bra tillgänglighet till dataskyddsombuden och därmed känna trygghet gällande hur den personliga integriteten hanteras inom den egna organisationens olika verksamheter.

Samverkansformens övergripande målsättning är att säkerställa ett gott skydd av den personliga integriteten genom att ge medlemskommunerna möjlighet att skaffa sig kontroll över de vitala delarna i dataskyddsförordningen och ge dem verktyg att motverka och minska antalet personuppgiftsincidenter.

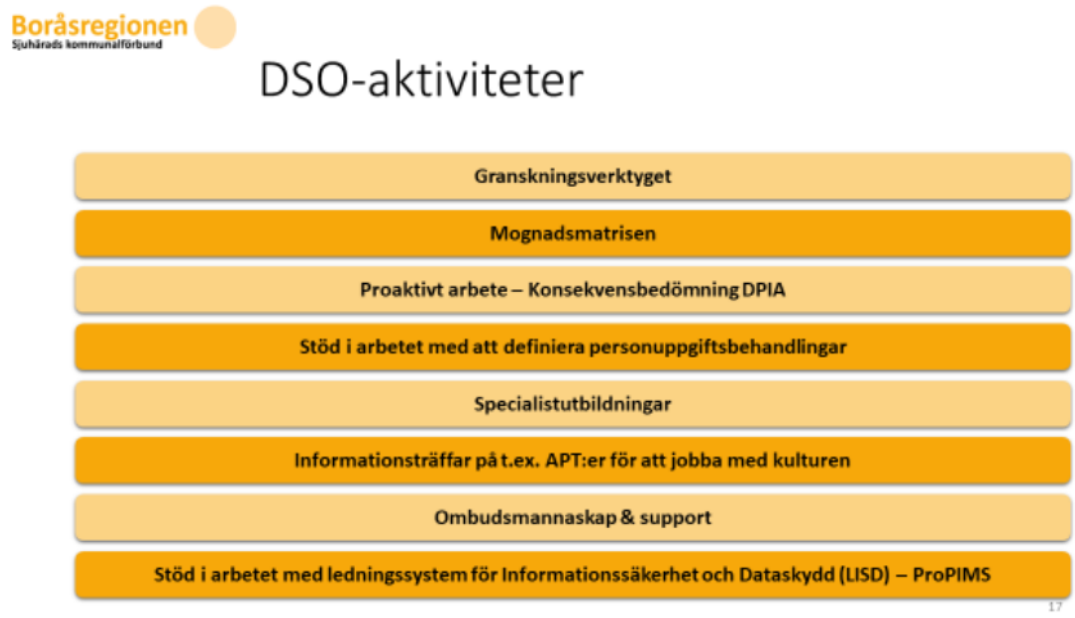
Dataskyddsombuden erbjuder sin kompetens och ger service åt verksamheterna, dess personal samt kommunmedlemmar genom rådgivning, information, utredningar och

[3] Artikel 38.6 dataskyddsförordningen.

utbildningsinsatser. I de fall det behövs, ges också stöd och hjälp i att bedöma hur personuppgiftsincidenter ska hanteras.[4]

I Figur 1 illustreras dataskyddsombudens årliga aktiviteter som ingår i deras uppdrag.

Figur 1



3.1.2 Förväntningar, uppdrag och mål hos anslutna kommuner

Det har under granskningen framkommit att anslutna kommuner i huvudsak har följande förväntningar, uppdrag och mål på dataskyddsombudsfunktionen och dataskyddsombuden. Mot bakgrund av att funktionen inrättats för att de anslutna kommunerna ska få dataskyddsombud som är lättillgängliga, vilket i sin tur motiverat att två dataskyddsombud anställts på heltid av kommunalförbundet, förväntar sig de anslutna kommunerna att dataskyddsombuden är just lätta att nå, att de besitter expertkunskap samt att de enbart sysslar med dataskydd och strikt angränsade frågor. I slutänden handlar förväntningarna om att få valuta för avsatta kommunmedel. Mer specifikt förväntar sig de anslutna kommunerna att dataskyddsombuden

- besitter spetskunskap inom området så att deras dataskyddskontakter kan vända sig till dem vid svårare frågor för att få korrekta, välavvägda och verksamhetsnära svar och vägledning,
- ska kunna hålla generella utbildningar inom dataskydd och

[4] Budget 2021 för Sjuhäradskommunalförbund.

- tar fram och utformar vissa rutindokument.

Hos dataskyddsombuden finns en medvetenhet om att de anslutna kommunerna vill ha valuta för pengarna och därigenom att dataskyddsombuden ska synas och höras ute i kommunerna och deras olika verksamheter. Eftersom dataskyddsarbetet inte utgör kärnverksamheten och därför kan förbises av vissa enheter eller i vissa situationer jobbar dataskyddsombuden behovsbaserat och försöker ta större kontakt med de enheter där de ser behoven. Utifrån kraven i rollen dataskyddsombud avseende dels ombudets oberoende, dels den granskning av verksamheten som behöver utföras, kan de inte bistå de olika enheterna med att skriva dokument och rutiner, eftersom effekten skulle bli att de i förlängningen granskar sig själva.

3.1.3 Iakttagelser och bedömning

Vår bedömning är att de anslutna kommunerna till övervägande del har rimliga förväntningar på samverkansfunktionen och dataskyddsombuden utifrån kommunalförbundets uppdrag och mål för samverkan. Dataskyddsombuden är i sin tur väl införstådda med dessa förväntningar tillika på vilket sätt de kan och inte kan bistå de olika enheterna utifrån rollens begränsningar (främst vad gäller oberoende). Mot bakgrund av samverkansfunktionens utformning och att två tjänster tillsatts för att tillse samtliga kommuners behov av tillgängliga dataskyddsombud delar vi kommunernas uppfattning om att de ska kunna förvänta sig att dataskyddsombuden är lätta att nå samt syns och hörs i verksamheten.

Eftersom kommunernas förväntningar och mål på dels dataskyddsamverkan, dels dataskyddsombuden samt vår bedömning av hur dessa förväntningar och mål uppfylls genomsyrar resterande revisionsfrågor har vi valt att lägga våra ytterligare iakttagelser och bedömningar efter att dessa frågor besvarats i de sammanfattande slutsatserna under Kapitel 4.

3.2 Vilka avtal/överenskommelser finns upprättade med respektive kommun?

3.2.1 Utgångspunkter

Uppdraget är personligt och ska beslutas av varje nämnd som ombudet arbetar för. Dataskyddsombudet får ingå i den personuppgiftsansvariges personal, eller utföra uppgifterna på grundval av ett tjänsteavtal. Det är alltså tillåtet att anlita en utomstående uppdragstagare. Den personuppgiftsansvarige ska säkerställa att dataskyddsombudet inte tar emot instruktioner som gäller utförandet av dataskyddsombudets uppgifter.[5]

Vid tiden för förstudien (från september 2022) som föranledde innevarande granskning fanns inte (uppdaterade) avtal eller överenskommelse med respektive kommun upprättade. Det

[5] Artikel 38.3 dataskyddsförordningen.

som fanns var den överenskommelse som upprättats i kommunchefsgruppen. Förbundet hade tagit fram ett avtalsutkast för vid tidpunkten nyligen anslutna Marks kommun och skulle ingå avtal med respektive ansluten kommun med utgångspunkt i nämnda avtalsutkast.

3.2.2 Upprättade avtal/överenskommelser

Vid tiden för vår granskning har de intervjuade uppgett att avtal finns på plats med de anslutna kommuner samt att dessa bygger på samma avtalsstruktur och mall. Det står inte något i kommunalförbundsordningen om dataskyddsombudens arbete. Det är dataskyddsombudens verksamhetsplan som styr deras arbete. Alla personuppgiftsansvariga enheter ska ha utsett dataskyddsombud, vilket dataskyddsombuden har kontrollerat genom att begära ut uppgifter från tillsynsmyndigheten Integritetskyddsmyndigheten (IMY). Vidare har de intervjuade uppgett att avtalen är relativt kortfattade och att de mer eller mindre klargör att samverkan och dataskyddsombud tillhandahålls men utan detaljer om hur uppdraget ska utföras mot bakgrund av förordningens krav på dataskyddsombudets oberoende ställning. Vi har begärt och fått ta del av ett sådant avtal.

3.2.3 Iakttagelser och bedömning

De intervjuade har uppgett att de avtal som saknades/inte var uppdaterade (efter att Marks kommun anslutit sig) vid tiden för förstudien nu har upprättats, vilket självklart ses som positivt. En av de anslutna kommunernas företrädare var dock osäker på om något avtal finns upprättat. Avtalsinnehållet och att avtalslydelsen undviker att beskriva hur dataskyddsombudsuppdraget ska utföras ligger väl i linje med förordningen och att den personuppgiftsansvarige ska säkerställa att dataskyddsombudet inte tar emot instruktioner som gäller utförandet av dennes uppgifter. Vi har inget att anmärka på innehållet vad gäller det upprättade avtal vi tagit del av. Vårt uppdrag har inte medgett tiden att kontrollera att alla anslutna kommuner verkligen har avtal med kommunalförbundet. Med tanke på det och osäkerheten i en av de intervjuade kommunerna rekommenderar vi att man säkerställer att avtal med respektive kommun finns upprättat.

3.3 Tydlig ansvarsfördelningen mellan dataskyddsombuden och kommunerna?

3.3.1 Utgångspunkter

Personuppgiftsansvariga nämnder i varje kommun ansvarar för att förordningens regler följs. Det är alltså organisationen och inte dataskyddsombudet som ansvarar för regelefterlevnaden. Därför måste organisationen ha rutiner och arbeta på ett sådant sätt att krav efterföljs. Om en organisation inte har följt reglerna är det organisationen som bär ansvaret, inte ombudet.

Dataskyddsombudet ska kunna agera självständigt och oberoende i organisationen. De personuppgiftsansvariga nämnderna inom kommunen ansvarar för att ombudet får det stöd, de befogenheter och tillräckliga resurser som krävs för att kunna utföra sitt uppdrag på ett effektivt och oberoende sätt. Ombudet ska också ges möjlighet att delta i alla frågor som rör dataskydd och rapportera direkt till högsta förvaltningsnivå. I uppdraget ingår även den rådgivande rollen - dataskyddsombudet ska informera och ge råd till dels den personuppgiftsansvarige, dels de anställda som behandlar personuppgifter, om vilka skyldigheter de har enligt dataskyddsförordningen och andra dataskyddsbestämmelser.[6]

3.3.2 Ansvarsfördelningen mellan dataskyddsombuden och kommunerna

Inledningsvis ska sägas att dataskyddsombuden är anställda av kommunalförbundet och är således formellt sett självständiga gentemot de anslutna kommunerna.

Granskningen visar att alla intervjuade är medvetna om att det är verksamheterna som ska sköta det löpande dataskyddsarbetet och att dataskyddsombuden mer agerar som stöd i denna del. Detta hänger även ihop med dataskyddsombudets oberoende och granskande roll. Angående rollen har en ansluten kommun uppfattat en viss otydlighet. Den har tagit exemplet att dataskyddsombuden velat vara med på återkommande möten i ett större digitaliseringsprojekt, men samtidigt undanbett sig att upprätta enklare rutiner för dataskydd. Kommunen har uppgett att dataskyddombuden inte borde sitta med på varje sådant möte utifrån dels deras oberoende roll, dels att de bjudit in sig till mötena i digitaliseringsprojektet för att snarare bidra med sin digitaliseringskompetens (från genomgången digitaliseringsutbildning) än sin dataskyddkompetens. Kommunen har upplevt en viss dubbeltydighet från dataskyddsombudens sida beträffande hur de förhåller sig till den oberoende rollen, genom att de i ena stunden vill delta i det löpande arbetet (genom att delta i möten), men inte vill upprätta rutindokument i den andra. Det råder konsensus mellan de intervjuade kommunerna att de vill kunna vända sig till och nyttja dataskyddsombuden som experter på dataskydd, när de själva kör fast i en fråga. En ansluten kommun har uttryckt det som att de vill kunna ställa en fråga till dataskyddsombuden, få ett svar och sedan gå vidare själva, utan att ombuden erbjuder sig att löpande sitta med på möten. I varje fall ska dataskyddsombuden inte delta i möten för att bidra med kompetens de råkar ha vid sidan av den strikt dataskyddsmässiga. En annan kommun tycker dock att ansvarsfördelningen är mycket otydlig, den har inte förstått vad dataskyddsombudens uppdrag är och vad de kan förvänta sig från dem. Ombuden visar sig inte i kommunen förutom i samband med granskning och mognadsmatris.

Dataskyddsombuden har uppgett att de möts av uppskattning när de väl besöker de anslutna kommunerna och dess enheter. Folk ställer upp och hjälper till att boka möten med mera varför mottagligheten på kommunerna är god. Någon enhet har uttryckt att

[6] Artikel 38.3 dataskyddsförordningen.

dataskyddsombuden inspirerar dem att fortsätta med dataskyddsarbetet. De flesta av verksamheterna har visat uppskattning i att dataskyddsombuden har varit tydliga men att verksamheterna själva har fått ta ansvar för att bygga upp sitt dataskyddsarbete utifrån ombudens framtagna processer och strukturer. Däremot skiljer det sig markant hur de olika enheterna klarat av att sköta dataskyddsarbetet under eget ansvar. ”Det kan beskrivas som att många är gröna, en del gula och flera röda”. De enheter som inte tagit tag i dataskyddsarbetet förstår egentligen inte att det är de som har ansvaret och att de är personuppgiftsansvariga. De har varken intresse eller fokus. Det är framför allt en enhet där både dataskyddsombuden och omgivande förvaltningar påpekat brister år efter år. Vad dataskyddsombuden fått till svar är att enheten inte kan området och att den varken har budget eller personal. I det fallet har dataskyddsombuden känt sig tvingade att lyfta bristerna för nämnden. Bristerna har varit tydliga i varje års granskning. Angående ”de röda” enheterna önskar dataskyddsombuden, eftersom processer och strukturer redan är satta, att dessa enheter börjar förstå och ta sitt ansvar. De ser fördelar med en uppstart med en metodledare som går in och ”får i gång” dessa enheter och att det avsätts resurser så att enheterna får administration att ta till sig vad dataskyddsombuden säger. De på enheterna vet inte hur formulären ombuden tagit fram fungerar och klarar för tillfället inte av systematiskt dataskyddsarbete.

3.3.3 Iakttagelser och bedömning

Dataskyddsombuden har byggt upp ett ramverk för kommunernas och dessas organisatoriska enheternas dataskyddsarbete. Det löpande datsskyddsarbetet ska alltså bedrivas på de organisatoriska enheterna och ombuden ska arbeta med regelbunden tillsyn och rådgivning, vilket ligger i linje med syftet bakom regelverket och dess bestämmelser för dataskyddsombudsrollen. Eftersom det är varje nämnd som är personuppgiftsansvarig och dataskyddsombudets roll inbegriper kontrollverksamhet är det ändamålsenligt att ombuden undviker för stor inblandning i det fortlöpande dataskyddsarbetet. Även ett resursfördelningsperspektiv kräver en avvägning av dataskyddsombudens deltagande i det dagliga dataskyddsarbetet. Antalet registrerade i kommunerna som de är dataskyddsombud för och effektivitetsaspekten motiverar ytterligare att det inte är dataskyddsombuden som utför det daglig dataskyddsarbetet.

Ansvarsfördelningen kräver även att samtliga enheter tar sitt ansvar och verkligen utför sitt dataskyddsarbete. Granskningen visar att nivån och intresset för dataskyddsfrågor skiljer sig stort mellan olika kommuner och olika enheter. Anledningar som nämns till att vissa enheter inte bedriver ett aktivt arbete är bland andra brist på resurser, kunskap eller vilja. Det formella ansvaret är korrekt fördelat, men samtliga enheter måste utföra sin del. Vi vill påminna samtliga enheter om deras respektive ansvar och uppmana verksamhetsledningar och personuppgiftsansvariga nämnder att tillsätta resurser och prioritera dataskyddsarbetet. Häri ingår även att involvera dataskyddsombuden i besluts- och arbetsprocesser med påverkan på dataskyddsarbetet, vilket krävs enligt artikel 38 dataskyddsförordningen.

Av vad som framgår ovan under avsnitt 3.3.1 ska ombudet ha en oberoende roll men samtidigt ges möjlighet att delta i alla frågor som rör dataskydd. Vidare får dataskyddsombudet fullgöra andra uppgifter och uppdrag. Den personuppgiftsansvarige ska se till att sådana uppgifter och uppdrag inte leder till en intressekonflikt.

Mer konkret kan vi se fördelar med att dataskyddsombuden deltar på vissa möten och i synnerhet ges möjlighet att komma med dataskyddsperspektivet i alla frågor där personuppgiftsbehandling förekommer (inbegripet digitaliseringsprojekt). Det finns inte heller något formellt som hindrar att dataskyddsombudet, utöver dataskydd, fullgör andra uppgifter och uppdrag. Vi kan även förstå kommunens upplevelse av tvetydighet att dataskyddsombuden ska ges möjlighet att delta i alla frågor som rör dataskydd men inte bör upprätta rutiner och riktlinjer utifrån den oberoende rollen. Förordningens ramar för dataskyddsombud förmedlar dock en ganska komplicerad rollbeskrivning som innehåller dels en granskande-, dels en stöttande och rådgivande del. Det är denna rollbeskrivning vi har att förhålla oss till och granska mot. Med det sagt och även om dataskydd, informationssäkerhet och digitalisering är områden som ofta överlappar varandra, delar vi kommunens syn på fördelarna med om dataskyddsombudens roll vore mer renodlad. Ombuden borde således syssla med dataskydd så långt det är möjligt, speciellt eftersom de har så pass många registrerade att vara dataskyddsombud för[7]. Att då delta i återkommande möten för att bidra med andra kompetenser de råkar ha ligger enligt vår bedömning utanför kommunalförbundets dataskyddsombuds uppdrag. Detta speciellt sett i ljuset av att vissa kommuner upplever att dataskyddsombuden sällan visar sig hos dem.

3.4 I vilken utsträckning uppfyller granskningsverksamheten de lagkrav som finns inom området?

3.4.1 Utgångspunkter

De lagkrav som finns för dataskyddsombudets granskningsverksamhet är som följer. Av artikel 39.1 b) GDPR framgår att dataskyddsombudet ska granska efterlevnaden

- av förordningen,
- av andra dataskyddsbestämmelser och
- av den personuppgiftsansvariges övergripande strategi för skydd av personuppgifter, (inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning).

Några mer specifika detaljer eller någon ledning för hur, hur ofta eller vad som ska granskas ges inte.

[7] Se avsnitt 3.6.2, s. 25, i denna rapport.

Däremot framgår av artikel 39.2 att dataskyddsombudet vid utförandet av sina arbetsuppgifter, inbegripet granskning, ska ta vederbörlig hänsyn till de risker som är förknippade med behandling av personuppgifter, med beaktande av behandlingens

- art,
- omfattning,
- sammanhang och
- syften.

Bestämmelsen innebär enligt Artikel 29-gruppen att dataskyddsombudet ska prioritera sin verksamhet och inrikta sitt arbete på eventuella problem som utgör en högre risk för dataskyddet.[8]

I skäl 75 berörs vilka riskerna för fysiska personers rättigheter och friheter kan vara. Sannolikhetsgraden och allvaret för riskerna för fysiska personers rättigheter och friheter kan sammanfattas till personuppgiftsbehandling som skulle kunna medföra

- fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till
    - diskriminering,
    - identitetsstöld eller bedrägeri,
    - ekonomisk förlust, skadat anseende,
    - förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt,
    - obehörigt hävande av pseudonymisering
    - eller annan betydande ekonomisk eller social nackdel,
- om registrerade kan berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter,
- om känsliga personuppgifter behandlas,
- om personliga aspekter bedöms i syfte att skapa eller använda personliga profiler (profilering),
- om det sker behandling av personuppgifter rörande sårbara fysiska personer, framför allt barn, eller
- om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.[9]

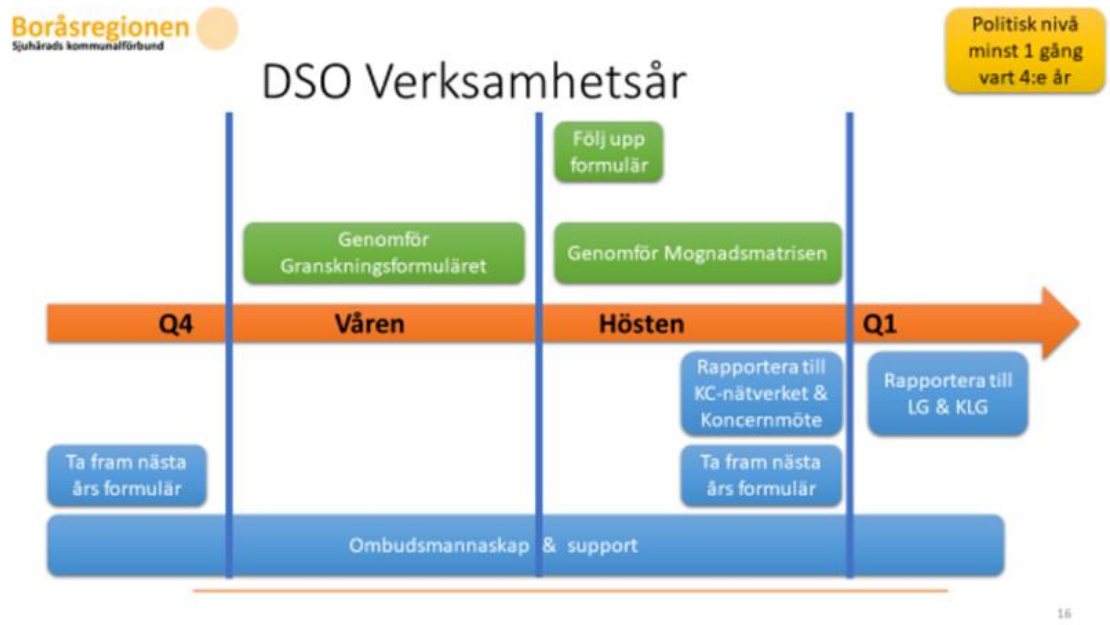
3.4.2 Dataskyddsombudens granskningsverksamhet

Av de underlag vi tagit del av och intervjun med dataskyddsombuden framgår i huvudsak följande om granskningsverksamheten. Granskningsverksamheten består av två fasta delar;

[8] s.22 Artikel 29-gruppens riktlinjer om dataskyddsombud antagna den 13 december 2016, senast granskade och antagna den 5 april 2017 (Artikel 29-gruppens riktlinjer om dataskyddsombud).
[9] Beaktandeskäl 75 till dataskyddsförordningen.

ett granskningsformulär som enheterna fyller i varje vår och en mognadsmatris som enheterna fyller i varje höst.

I Figur 2 beskrivs dataskyddsombudens verksamhet utifrån en årlig planering, där granskningsverksamheten utgör en betydande del.



Figur 2

Granskningsformuläret på våren

Granskningsverksamheten är dels baserad på nödvändigheten av att bygga strukturer i rätt ordning (att först ha övergripande rutiner på plats innan man börjar ta fram detaljerade dokument för specifika delar av sin verksamhet), dels riskbaserad (i första hand de förvaltningar som har stora risker och i andra hand de högriskområden som finns). Härutöver kan man sammanfatta granskningsverksamhetens syften i två delar.

1. Generell granskning – för att säkerställa att vissa organisationer finns på plats.
2. Förflyttningsgranskning – för att höja nivån på arbetet.

De största frågorna tas först och byggs år för år på vilket leder till bättre och bättre nivå. Dataskyddsombuden höjer nivån genom att exempelvis år 1 fråga om enheterna har en utbildningsplan och år 2 fråga om de följer upp att medarbetarna går utbildningarna och att planen följs. Varje enhet får sedan, med dataskyddsombudens hjälp, ta fram en egen åtgärdslista för hur de ska komma upp i ”Ja”.

Granskningsformuläret innehåller två moment, dels det generella (håller enheten takten i det fortlöpande dataskyddsarbetet?), dels ett specifikt årligt granskningstema. Deras granskningar genomlyser inte allt och de skriver inte några 75 sidors rapporter (som vissa revisionsbyråer). De tar i stället med 18 påståenden i sitt granskningsformulär. De generella påståendena ska bidra till dataskyddsombudens kunskap om verksamheten på enheten samt enhetens insikt om dess egen verksamhet. De flesta påståendena är generella och tar sikte på takten i det fortlöpande arbetet, medan 4–5 frågor av de 18 vigs åt årets tema. Exempelvis hade de temat arkivering vid tidpunkten för e-Arkivs införande. Första påståendet är alltid om förra årets åtgärdslista åtgärdats. Och för de generella påståendena brukar alltid frågor om utbildning och incidenthantering vara med. Anledningen till att många enheter inte arbetar tillräckligt aktivt med åtgärdslistan handlar ytterst om att de inte prioriterar arbetet. Efter att granskningsformuläret skickats ut, besvarats och dataskyddsombuden gått igenom svaren bokas ett uppföljningsmöte. Under mötet får enheten, med dataskyddsombudens hjälp, ta fram de åtgärder som behöver vidtas för att enheten ska kunna anses uppfylla påståendena i granskningsformuläret. Första frågan under uppföljningsmötet är alltid hur det går med föregående punkter på åtgärdslistan. I ett fall hade åtgärdslistan blivit ”rödare och rödare” och dataskyddsombuden tvingades underrätta nämnden, vilket ledde till förbättringar. Kanske borde de ha tätare uppföljningar med de enheter där de ser att åtgärdslistan inte sköts och underrätta nämnderna i ett tidigare skede. Annars blir det i regel långt mellan mötena med respektive enhet.

Dataskyddsombuden ser inte att det finns utrymme att genomföra fler granskningar under ett kalenderår. Eftersom dataskyddsombuden har cirka 80 enheter att granska upplever de att det varken finns tid eller möjlighet för djupare, mer kvalitativa spetsgranskningar. De skulle vilja ha tiden att utföra djupare analyser inom specifika områden för att kunna komma med mer skarpa rekommendationer, vilket skulle bidra till höjd kunskapsnivå. De upplever samtidigt att de inte kan släppa nuvarande granskningsupplägg eftersom deras granskningsverksamhet dels styrs av verksamhetsplanen och årshjulet (som de inte vill ändra), dels för att de då skulle missa uppföljning av de stora grundläggande områdena (som utbildning, artikel 30 osv.) vilket skulle leda till sänkt kvalitet i dessa delar. Ett uppslag är dock att ett enklare förfarande/underhållsarbete för nuvarande granskning skulle kunna frigöra en större möjlighet för dataskyddsombuden att arbeta mer proaktivt.

Mognadsmatrisen på hösten

Varje höst skickar de ut ”Mognadsmatrisen” där enheterna genom att svara på frågor på strategisk nivå får självskatta sig och sin mognad av dataskyddsarbetet. Matrisen innehåller tio fasta delar, bland andra ”Kvaliteten på behandlingsregistret” och ”Uppfyllande av Rättigheter”. Ett annat exempel från mognadsmatrisen är om enheten har en robust incidenthanteringsprocess. Matrisen innehåller en definition för vad som krävs för att processen ska anses robust och en skala från 0 till 9 som enheten får placera in sin

verksamhet; 0 avser ”att man inte ens har börjat fundera på frågan” och 9 avser ”mycket hög kvalitet”.

De anslutna kommunerna

Av intervjuerna med de anslutna kommunerna framkommer i huvudsak följande. De är på det stora hela nöjda med dataskyddsombudens granskningar och nivån dessa ligger på. Granskningarna är inte för avancerade och dataskyddsombuden är bra på att identifiera relevanta frågor/påståenden.

På frågan om förutsättningar för djupare mer kvalitativa granskningar har någon kommun antytt att deras enheter inte är mogna för sådana. Någon kommun har uttryckt en önskan om att Excelmallarna, som genereras ur granskningarna dels skulle hålla högre kvalitet, dels tillfogas funktionen att enheterna skulle kunna jämföra nivån hos motsvarande verksamheter i de andra anslutna kommunerna. Det skulle i sin tur leda till att vissa kommuner/enheter/verksamheter höjer sin nivå för ”man vill inte vara sämre än grannen”. Granskningsformulär och sedan uppföljning är i grunden ett bra upplägg för granskningen. Däremot finns önskemål om snabbare och tätare uppföljning för att arbetet med åtgärdslistan inte ska glömmas bort. Nu har granskningsformulären skickats ut runt februari och uppföljning skett först framåt hösten. Skulle man kunna ha två eller tre träffar (i varje fall en innan sommar-semestern) för att se så att enheterna kommit i gång med arbetet eller om de behöver hjälp och i så fall kunna bistå?

3.4.3 Iakttagelser och bedömning

På våren försöker dataskyddsombuden höja nivån i dataskyddsarbetet genom att ställa högre och högre krav i granskningsformuläret och på hösten utgår ett fast mognadsschema. Det är självklart positivt att de försöker höja nivån i vår-granskningarna. Det kan konstateras att med utskick av både granskningsformulär och mognadsmatris, sammanställning och viss kvalitativ granskning av cirka 80 enheter följer en omfattande och tidskrävande administration. Tiden hade möjligen kunnat disponeras mer effektivt. Med tanke på att vår-granskningen blott innehåller 18 påståenden vore i varje fall ett övervägande om utskick av mognadsmatrisen vid samma tidpunkt som vårgranskningen (för att frigöra tid, kanske för tätare uppföljningsmöten eller en kompletterande spetsgranskning?) på sin plats.

Även om kommunerna till stor del är nöjda med nivån på granskningarna; att de inte är för avancerade och att vissa inte anser sig mogna för djupare, mer kvalitativa granskningar, delar vi dataskyddsombudens syn på att sådana lite djupare granskningar behövs. Just nu bygger granskningen på självskattning och vi saknar en granskningsdel som de facto synar några behandlingar i artikel 30-registret eller en informationstext i sömmarna. Nuvarande upplägg visar mest enheternas självupplevda kartläggning av om saker finns på plats och inget om kvaliteten på innehållet i exempelvis en informationstext. Det finns inga tydliga lagkrav för

ramarna i granskningsverksamheten. Vi ser dock utifrån Artikel 29-gruppens tolkning att dataskyddsombudet ska inrikta sitt arbete (däribland granskningsverksamheten) på eventuella problem som utgör en högre risk för dataskyddet, att viss del djupgranskning skulle ligga närmare att uppfylla lagkraven för granskning. Det gäller främst de enheter vars personuppgiftsbehandlingar utgör en högre risk för integriteten såsom personuppgifts-behandling i stor omfattning och behandling av känsliga personuppgifter. Vi tror att i varje fall sådana verksamheter samt de mer mogna enheterna skulle lära sig ytterligare och ta sitt dataskyddsarbete till nästa nivå med mer kvalitativ feedback. Risken med nuvarande upplägg är att dessa enheter stagnerar. Skulle en möjlig väg vara att genomföra en kvalitativ granskning för ”högriskenheter” samt mogna enheter och behålla nuvarande upplägg för de som inte kommit lika långt i sitt dataskyddsarbete? Det skulle i så fall kräva en större omdisponering och effektivisering av arbetet.

Beträffande åtgärdslistorna kan det finnas både för- och nackdelar med att verksamheterna själva tar fram dessa. Det kan styrka en enhet att de själva arbetar fram vilka åtgärder som behöver vidtas samtidigt som det befäster rollfördelningen - att det snarare är enheterna än ombuden som ska står för det löpande och operativa dataskyddsarbetet. Enheterna ökar tryggheten och utvecklas genom att driva sitt arbete fullt ut, samtidigt som det för enheter som ännu inte är mogna kan leda till att ribban blir för hög vilket kan leda till motsatt effekt. En annan fördel kan vara att enheterna blir mer självständiga och ökar lärandet när de själva får komma fram till åtgärderna. För mogna enheter kan det vara ett bra upplägg. En tydligare rådgivning från dataskyddsombuden hade samtidigt sparat tid för de mindre mogna enheterna, tid som hade kunnat läggas på att vidta åtgärderna i stället för att planera vilka åtgärder de behöver vidta. Med tanke på att granskningsformuläret är identiskt för samtliga enheter hade det varit relativt enkelt för dataskyddsombuden att även bistå med standardiserade rekommenderade åtgärder för dem som inte uppfyller påståendena fullt ut.

En annan iakttagelse är att tiden mellan att dataskyddsombuden identifierar att dataskyddsarbetet försummas (genom att åtgärdslistorna inte följs) på enhet till att förbättring sker (exempelvis genom att dataskyddsombuden lyfter det till nämnden) i vissa fall är för lång. Detta gäller särskilt i ljuset av nuvarande upplägg med ganska glesa uppföljningar, och långt mellan gångerna då dataskyddsombuden träffar respektive enhet. Risken är att en åtgärdslista tas fram, inga åtgärder vidtas under året och vid nästa möte är det dags för en ny åtgärdslista och enheten ligger snart två år av åtgärder efter. För sådana enheter ser vi behov av ytterligare stöd, kanske tätare uppföljning och om inte det hjälper ett snabbare förfarande att lyfta bristerna för nämnden. Även denna rekommendation ligger i linje med Artikel 29-gruppens tolkning om att ombuden ska prioritera sin verksamhet och inrikta sitt arbete på eventuella problem som utgör en högre risk för dataskyddet.

Sammanfattningsvis ska sägas att det inte finns några uttryckliga lagkrav för hur dataskyddsombudens granskningsverksamhets ska genomföras. Utifrån Artikel 29-gruppens tolkning om en riskbaserad inriktning på granskning rekommenderar vi någon form av

djupare spetsgranskning, vilken skulle kunna möjliggöras genom överväganden om att effektivisera

- upplägg och administration för utskick och insamling och nuvarande granskning,
- återkoppling och åtgärdsförslag för nuvarande granskning.

3.5 Är prioriteringen i granskningsarbetet lämplig med hänsyn till granskningsområde och typen av granskningsobjekt?

3.5.1 Utgångspunkter

Som ett led i skyldigheten att övervaka efterlevnaden av förordningen kan dataskyddsombuden

- samla in information för att identifiera hur behandling av personuppgifter sker,
- analysera och kontrollera huruvida bestämmelser om behandlingen efterlevs, och
- informera samt ge råd och utfärda rekommendationer till den personuppgiftsansvarige eller personuppgiftsbiträdet.[10]

3.5.2 Prioriteringen i granskningsarbetet utifrån granskningsområde och granskningsobjekt

Utöver vad som framkommer ovan under 3.4.2 om upplägget för granskningsarbetet har de anslutna kommunerna uppgett i huvudsak följande. En önskan är mer verksamhetsnära/områdesspecifika granskningar. Påståendena i granskningsformuläret är ofta på en generell nivå. En del påståenden gäller generellt för kommunen och sköts centralt men samma frågor skickas till varje enhet. Ett exempel är att temat för granskningen ett år var cookie-hantering för kommunens sida, vilket inte var speciellt relevant att svara på för dem ute i verksamheterna i och med att det sköttes centralt (av kommunikationsavdelningen) för kommunens hemsida. Ett förslag är att skicka ut ett generellt formulär för kommunstyrelsen och de centrala funktionerna och mer specifika versioner för verksamheterna. Någon kommun har även svårt att förstå syftet med mognadsmatrisen och vissa av påståendena i granskningsformuläret. Det har varit olika upplägg för mognadsmatrisen olika år. I den senaste skulle samtliga kommunens verksamheters svar slås samman i en mognadsmatris. Syftet försvann helt eftersom en verksamhet hade svarat 1 och en annan 6 gällande deras upplevda nivå av incidenthantering. Eftersom det skiljde sig mycket mellan de olika verksamheterna var det omöjligt och lönlöst att försöka slå ihop svaren. Ska mognadsmatrisen överhuvudtaget användas behöver svaren ges på verksamhetsnivå (även i en mindre kommun). Granskningsformulären (för våren) behöver vara mer verksamhetsspecifika. Det blir även svårt för verksamheterna att förstå varför vissa påståenden finns med och hur de ska ta ställning till dessa. ”Hur ska kultur och fritid förstå

[10] Artikel 39.1 b dataskyddsförordningen.

vad en mjuk process är?" och kommer påståendet från ett krav i förordningen eller från dataskyddsombuden? En kontextualisering av påståendena önskas.

3.5.3 Iakttagelser och bedömning

Vi förstår mot bakgrund av antalet enheter och den administration det medför samt den skiftande nivån och hur långt de olika enheterna kommit i dataskyddsarbetet dataskyddsombudens utmaningar i att bedriva en genomförbar, effektiv och samtidigt för alla enheter relevant granskningsverksamhet med hänsyn till såväl granskningsområde som typen av granskningsobjekt. Med det sagt rekommenderar vi, i linje med avsnitt 3.4.3 om hur granskningsverksamheten uppfyller lagkraven inom området och vad som framkommit i övrigt angående granskningsverksamheten, en översyn av granskningsupplägget för att utvärdera hur man kan förändra för att uppnå en mer verksamhetsanpassad, riskbaserad, kontextualiserad, effektiv och spetsig granskning som ger enheterna än mer handfasta åtgärder att vidta i sitt fortsatta dataskyddsarbete.

3.6 Är bemanningen och resurser för dataskyddsombuden tillräckliga för verksamhetens uppgift?

3.6.1 Utgångspunkter

Den personuppgiftsansvariga ska stödja dataskyddsombudet i utförandet av dennes uppgifter genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter.[11] Beroende på uppgiftsbehandlingens natur och organisationens verksamheter och storlek bör följande resurser tillhandahållas dataskyddsombudet:

- Aktivt stöd från högsta ledningen för dataskyddsombudets arbete.
- Tillräckligt med tid för att dataskyddsombudet ska kunna fullgöra sina uppgifter.
- Lämpligt stöd i form av ekonomiska resurser, infrastruktur (lokaler, hjälpmedel, utrustning) och personal i förekommande fall.
- Officiellt meddelande till all personal om att dataskyddsombudet utnämnts.
- Tillgång till andra avdelningar inom organisationen som kan ge det stöd, de bidrag och den information som dataskyddsombudet behöver i sitt arbete.
- Fortbildning.[12]

[11] Artikel 38.2 dataskyddsförordningen.
[12] s. 26 f. Artikel 29-gruppens riktlinjer om dataskyddsombud.

3.6.2 Dataskyddsombudens bemanning och resurser

Av Boråsregionen Sjuhärads kommunalförbunds årsredovisning för 2021 framgår att dataskyddsombudsverksamheten uppvisat positiva resultat såväl för 2020 som 2021, vilket tyder på erforderliga monetära resurser för nuvarande bemanning.

Vår resterande presentation av granskningsresultatet utgår från Artikel 29-gruppens tolkning av vilka resurser den personuppgiftsansvarige bör ställa till dataskyddsombudets förfogande enligt punktlistan ovan.

Aktivt stöd från högsta ledningen för dataskyddsombudets arbete

Dataskyddsombuden uppger att de inte har tillräckligt aktivt stöd från samtliga kommunledningar, vilket främst beror på att alla inte har kunskap/utbildning inom dataskydd. Enligt verksamhetsplanen ska dataskyddsombuden träffa alla ledningsgrupper. I dessa möten försöker de sälja in budskapet och trycka på vikten av att prioritera dataskyddsarbetet i budgeten osv. De upplever att det är enklare att få ledningens aktiva stöd i de större kommunerna, varför de även hållit chefsutbildningar i de mindre kommunerna, för att sprida kunskap och insikt om områdets vikt. Ett uppslag är kanske att ha ett årshjul eller annan kontinuitet för utbildning för cheferna, så att området prioriteras och kunskapen och relevansen inte glöms bort eller försvinner i och med byte av personal. Vissa enheter tar inte sitt ansvar när det kommer till dataskyddsarbetet. Anledningarna till att dessa enheter är ”röda” kan vara flera. I vissa saknas kunskapen och intresset. En del har fått det operativa ansvaret för dataskyddsarbetet ”i knät” och har inget större intresse. Andra enheter har uppgett att de inte får resurserna från sin kommun. Om de organisatoriska enheterna skulle ta sitt ansvar och få fler grundläggande rutiner och styrdokument på plats, hade dataskyddsombuden sluppit lägga mer tid på att upprepa sig och påminna om dessa och hade kunnat lägga mer tid på proaktivt arbete i stället.

Tillräckligt med tid för att dataskyddsombudet ska kunna fullgöra sina uppgifter

Denna punkt tar enligt vår bedömning mer sikte på dataskyddsombud som har en viss del av sin tjänst avsatt till att vara dataskyddsombud. I Boråsregionen Sjuhärads kommunalförbund finns två tillsatta heltidstjänster för dataskyddsombud. Vi hänvisar till punkten om lämpligt stöd och personal samt våra slutsatser nedan.

Lämpligt stöd i form av ekonomiska resurser, infrastruktur (lokaler, hjälpmedel, utrustning) och personal i förekommande fall.

Granskningen har inte åskådliggjort några brister vad gäller resurser i form av infrastruktur såsom lokaler, hjälpmedel och utrustning. När det kommer till personal är de två dataskyddsombuden registrerade dataskyddsombud för drygt 80 enheter och har drygt 50

stående kontaktytor i form av dataskyddssamordnare och dataskyddskontakter. Som tidigare nämnts medför detta en stor administration och därmed stor tidsåtgång vigd åt utskick och insamling av granskningsformulär, bokning av uppföljningsmöten och frågor om granskningsformulären med mera. Dataskyddsombuden har uttryckt att de känner att de är en person kort. Detta manifesteras i att bland annat granskningsarbetet är mer ingående nu än det var i början när de frågade om enheterna exempelvis hade ett artikel 30-register och nu ställer de mer ingående frågor om behandlingarna/säkerställer att samtliga behandlingar finns med. På ett sätt sväller dataskyddsombudens arbete i takt med att enheternas nivå på arbetet höjs – ju mer ingående frågor de ställer till enheterna, desto större rådgivning behöver de i nästa steg bidra med.

En annan omständighet är att Marks kommun även anslutit sig till samverkan. En utgångspunkt är att andra större kommuner har ungefär 70 000 invånare per heltidsanställt dataskyddsombud. Innan Marks kommun kom med låg samverkan på cirka 200 000 invånare sammanlagt (frånsett de kommunala bolagen), så redan då låg de i överkant. När fler kommuner ansluter sig får de en exponentiell tillväxt som de inte kommer klara av. Uppdraget har blivit kvantitativt större vilket det kvalitativa arbetet har fått stryka på foten för.

En tredje sak som kräver tid är till GDPR närbesläktade områden (där det kommer mycket förändringar och ny lagstiftning) som dataskyddsombuden känner ett behov av att bevaka och vara insatta i. I början fanns det ”luft i systemet”, men nu har de fått börja göra avkall bland annat på deras egna utbildningar/nätverk och får kämpa för att avsätta tid för dessa. Innan deltog de båda i nätverk, exempelvis var båda med i JUC. Nu har de fått dela på sig för att bevaka förändringar dels på det strikta dataskyddsområdet, dels på angränsande områden såsom digitalisering, informationssäkerhet, AI, Öppna data osv.

Dataskyddsombuden känner en oro för om eller när de behöver växla upp dataskyddsarbetet (exempelvis i granskningarna) ytterligare och hur de ska kunna hålla sig á jour i compliance-frågorna. Alla kommuner jobbar exempelvis med digitaliseringsstrategier men tappar bort integritetsskydds- och cybersäkerhetsperspektiven. Nu bevakar dataskyddsombuden dessa områden, men även Öppna data, E-tjänster, Data Act och AI med flera så gott det går eftersom dessa angränsar till dataskyddet och riskerar att inkräkta på integriteten. I bästa fall har kommunerna jurister, men dessa jobbar mer som ”helpdesk”. Kommunerna arbetar reaktivt och det är ingen på kommunerna som jobbar proaktivt med compliance-verksamhet. Dataskyddsombuden känner egentligen inte att det är deras ansvar, men i brist på någon som har den rollen har de känt sig tvingade att axla ansvaret vilket kräver en enorm kunskapsinhämtning eftersom det händer så mycket inom dessa områden. Av denna anledning finns en önskan från dataskyddsombuden att alla kommuner borde dela en compliance-person med koll på dessa angränsande områden. Dataskyddsombuden skulle då gärna jobba i tätt samarbete med en person med sådan tjänst. Att hänga med och ta ansvar inom ramen för dataskyddsombudsrollen känns dock övermäktigt. En sådan resurs skulle vara till nytta för e-tjänster, Öppna data, AI med flera - kanske i form av en delregional verksamhetsutvecklare; en sammankallande roll som framtidsspanar, sköter uppföljningar,

cybersäkerhet - det mer tekniktunga området. Denne skulle också kunna driva ett nätverk på kommunförbundsnivå och samordna aktioner. Oavsett om man utvecklar en e-tjänst eller upphandlar en färdigutvecklad tjänst, ska checklistan finnas där, för att uppnå privacy by design och cybersäkerhet med mera.

Officiellt meddelande till all personal om att dataskyddsombudet utnämnts.

De flesta kommuner har publicerat dataskyddsombudens namn och kontaktuppgifter på sina hemsidor. Det är oklart om även officiella meddelanden till all personal gick ut 2018.

Tillgång till andra avdelningar inom organisationen som kan ge det stöd, de bidrag och den information som dataskyddsombudet behöver i sitt arbete.

Granskningen visar att dataskyddsombuden möts av engagemang och ges tillgång till andra delar av organisationen. ”Folk ställer upp och hjälper till att boka möten, frigör tid med mera varför mottagligheten på kommunerna är god.”

Fortbildning[13]

Dataskyddsombudet ska utses på grundval av yrkesmässiga kvalifikationer och, särskilt, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra sina uppgifter. Den nödvändiga nivån på sakkunskapen bör fastställas i enlighet med den uppgiftsbehandling som utförs och det skydd som krävs för de personuppgifter som behandlas. Om behandlingen av personuppgifter är särskilt komplex eller omfattar en stor mängd känsliga uppgifter kan dataskyddsombudet till exempel behöva ha mer sakkunskap och mer stöd.

Följande kvalifikationer och sakkunskap är relevanta:

- Kunskap om dataskyddslagstiftning och praxis på nationell nivå och EU-nivå, inklusive djupgående kunskap om den allmänna dataskyddsförordningen.
- Förståelse av hur behandlingen av personuppgifter genomförs.
- Kunskap om olika typer av informationsteknik och datasäkerhet.
- Kunskap om affärssektorn och organisationen i fråga.
- Förmåga att främja en dataskyddskultur inom organisationen

Därtill ska den personuppgiftsansvarige bidra till upprätthållandet av dataskyddsombudets sakkunskap, till exempel genom att vid behov erbjuda utbildning inom området.

[13] s. 26 f. Artikel 29-gruppens riktlinjer om dataskyddsombud.

Dataskyddsombuden är med i flera nätverk både på dataskyddsidan (JUC, GDPR-Excellence och Dataskyddsombud inom offentlig sektor i Västra Sverige) och inom det mer tekniska området (AI Sweden och IoT Sweden). Det ena dataskyddsombudet är utbildad jurist och det andra projektledare i grunden. Det föreligger visserligen inget krav på juristexamen eller juridisk utbildning för att axla rollen som dataskyddsombud. Å andra sidan är det med tanke på rättsområdets komplexitet och kraven ovan på djupgående kunskap om förordningen en fördel att åtminstone ha den juridiska metoden med sig in i rollen. Det har mot denna bakgrund lyfts en del frågetecken beträffande icke-juristens kompetens inom området från en av de anslutna kommunerna. Det framgår även av dataskyddsombudens redogörelser att den ene lagt större vikt vid den tekniska sidan (AI, digitalisering och IoT). Han är å andra sidan med i GDPR-Excellence-nätverket.

Dataskyddsombuden deltar i kunskapsnätverk och utbildningar. Granskningen har inte visat att budgeten begränsar monetära resurser för att delta i sådana. Däremot har de på grund av tidsbrist fått göra avkall och inte delta bägge i vissa utbildningar/nätverk. De vill egentligen ha samma kunskapsnivå inom allt, så att enheterna ska kunna fråga vilken som och få likvärdiga svar. Numer finns dock inte tillräcklig tid för egen fortbildning/delta i utbildningar, vilket är en effekt av att arbetet tar mer tid nu jämfört med i början.

3.6.3 Iakttagelser och bedömning

Dataskyddsombuden har uppgett att andra större kommuner har förhållandet 70 000 invånare per heltidstjänst. Dataskyddsombuden är nu två heltidstjänster på 230 000 invånare inkl. Marks kommun, d.v.s. en heltidstjänst per 115 000 invånare och det är utan de kommunala bolagen. Mot bakgrund härav har uppdraget blivit kvantitativt större vilket kommer få eller har redan fått en negativ inverkan på det kvalitativa.

En del av dataskyddsombudens tid äts upp av de enheter som inte tar sitt ansvar, vilket gör att ombuden tvingas repetera och upprepa grundläggande saker för dessa ”röda” enheter. Oavsett om dessa enheters bristande dataskyddsarbete beror på brist på ansvarstagande, kunskap, resurser från sin kommun eller en kombination av dessa faktorer får det följden att dataskyddsombuden tvingas lägga tid och resurser på att upprepa sig över sådant som redan borde vara på plats.

Dataskyddsombuden har uppgett att det i början fanns ”luft i systemet”, vilket gjorde att bägge kunde vara med i samma nätverk och genomgå samma utbildningar. De ska visserligen inte behöva kämpa för att hinna med fortbildningen, men att de nu fått börja dela upp dem mellan sig behöver inte vara ett problem och att de kunde delta bägge tidigare var nog snarare ett kvitto på att arbetet inte helt fyllde två heltidstjänster. Att de nu har fått dela på sig och bevaka lite olika områden genom att delta i olika nätverk och utbildningar bedömer vi ligger bättre i linje med ett kostnads- och effektivitetsperspektiv. Så länge de överför den nya kunskapen mellan sig torde inte det utgöra ett problem. Dataskyddsombuden har själva lyft att de inte

vill ha olika kunskapsnivåer och att båda ska kunna svara likvärdigt på samma frågor (från verksamheterna). Med tanke på att viss kritik riktats från kommunerna mot den enes kunskaper inom dataskydd borde denne lämpligen prioritera dataskyddsnätverken.

Som vi varit inne på under avsnitt 3.3.3 förordar vi att dataskyddsombuden renodlas till att vara just hundra procent dataskyddsombud, vilket deras tjänster föreskriver. Det vill säga att dataskyddsombuden varken åtar sig ansvar/bevakning av områden som ligger utanför rollen som dataskyddsombud eller bevakning och compliance-arbete i angränsande områden.

Även om de ”röda” enheterna skulle börja ta större ansvar och vissa effektiviseringsåtgärder i dataskyddsombudens nuvarande verksamhetsplan vidtas, kan konstateras att två tjänster inte helt räcker till för att både sköta uppdraget i nuvarande form, kanske vidareutveckla vissa delar (enligt våra rekommendationer) samt därtill följa med i angränsande områdens rätts- och teknikutveckling. Vi rekommenderar därför Boråsregionen Sjuhärads kommunalförbund och kommunerna att dataskyddsombudens roll renodlas och att frågan om hur luckan i ett proaktivt compliance-arbete ska fyllas och vem som ansvarar för den utreds.

3.7 Är dataskyddsombudens rådgivning och utbildningsinsatser tillräckliga?

Vi har utifrån vad som framkommit i granskningen valt att dela upp denna revisionsfråga i två delfrågor;

- om dataskyddsombudens rådgivning är tillräcklig, se vidare avsnitt 3.8 samt
- om utbildningen dataskyddsombuden tillhandahåller verksamheterna är tillräcklig, se vidare avsnitt 3.9.

3.8 Om dataskyddsombudens rådgivning är tillräcklig

3.8.1 Utgångspunkter

En av dataskyddsombudets huvuduppgifter är att *informera* och *ge råd* till den personuppgiftsansvarige, och de anställda som behandlar personuppgifter om vilka skyldigheter de har enligt dataskyddsförordningen och andra dataskyddsbestämmelser[14].

Personen som utses till dataskyddsombud ska utses baserat på yrkesmässiga kvalifikationer, sakkunskap och förmåga att utföra uppgifterna och därmed ha kunskap om dataskydd.

I Sjuhäradskommunalförbunds budget för 2021 anges att;

”Dataskyddsverksamheten är en samverkan som syftar till att effektivt ge medlemskommunerna kunskap och erfarenhet i dataskyddsfrågor. Medlemmarna i

[14] Artikel 39.1 dataskyddsförordningen.

Boråsregionen ska känna att de har bra tillgänglighet till dataskyddsombuden och därmed känna trygghet gällande hur den personliga integriteten hanteras inom den egna organisationens olika verksamheter. Med verksamhet avses exempelvis förvaltningar, kluster av förvaltningar, avdelningar, sektorer, sektioner, kommunalförbund, kommunala bolag och nätverk. Personuppgiftsansvarig (PUA) är alltid respektive nämnd eller styrelse.

Samverkansformens övergripande målsättning är att ge medlemskommunerna möjlighet att skaffa sig kontroll över de vitala delarna i dataskyddsförordningen och ge dem verktyg att motverka och minska antalet incidenter; vars konsekvenser kan ge dålig publicitet vilket kan skada både varumärket och minska kommunens anseende hos allmänheten. Under 2021 är ambitionen att öka det proaktiva arbetet.

Dataskyddsombuden erbjuder sin kompetens och ger service åt verksamheterna, dess personal samt kommunmedlemmar genom rådgivning, information, utredningar och utbildningsinsatser. I de fall det behövs, ges också stöd och hjälp i att bedöma hur personuppgiftsincidenter ska hanteras."

3.8.2 Dataskyddsombudens rådgivning

De anslutna intervjuade kommunerna har uppgett i huvudsak följande. Dataskyddsombuden är lättillgängliga och ställer man en fråga får man ofta svar i samma samtal. Någon kommun upplever dock att svaret ibland kan vara lite "svart eller vitt" och inte så pragmatiskt. Kommunen skulle önska ett svar mer i stil med "som dataskyddsombud kan jag inte rekommendera denna åtgärd/detta system. Men om ni vidtar denna åtgärd, kommer vi att hjälpa till så att det blir så bra det kan bli. Genom riskanalyser eller vad det kan vara." Någon kommun upplever inte att dataskyddsombuden levererar den tid kommunen betalar för (speciellt inom rådgivningen), men det kan delvis bero på att kommunen skulle kunna ställa högre krav på ombudens närvaro. Samma kommun har uttryckt att man kanske skulle behöva omvärdera hur mycket tid kommunen verkligen behöver dataskyddsombuden nu jämfört med 2018 då avtalet skrevs – de är mer självgående nu. Merparten av kommunerna upplever ingen skillnad i rådgivningen beroende på vilket av dataskyddsombuden de ställer frågan till. Någon kommun upplever dock att de hellre frågar det ena dataskyddsombudet eftersom de upplever att de får bättre, mer pragmatiska och verksamhetsnära svar från denne. Samma kommun har uppgett att den andre kanske inte riktigt besitter kunskapen inom dataskydd. Denne anpassar sitt arbete och sina svar mer utifrån sin sidokompetens och inte utifrån sin roll som dataskyddsombud.

Angående deras rådgivningsinsatser har dataskyddsombuden uppgett i huvudsak följande. De ser att frågorna kommer in mer och mer - allt från korta frågor till längre utredningar. De har försökt sälja in att det inte kostar något att ställa frågor till dem. Mer eller mindre dagligen kommer löpande frågor in som dokumenteras i dataskyddsombudens ärendehanteringssystem. De försöker ta hand om frågorna en och en och genom loggningen kan de sedan utvärdera om de saknar kunskap inom vissa områden/frågor. Vissa frågor är

återkommande, bland annat om rollerna personuppgiftsansvarig/personuppgiftsbiträde. Frågorna kommer ofta från kontaktpersonerna, men ibland direkt från exempelvis socialhandläggare som på grund av sekretess eller uppgifter av känslig art inte vill gå via dataskyddskontakten. De deltar även i möten som referenspersoner och då bli det mer än enskilda frågor. Ett exempel var att de deltog i återkommande möten i ett projekt för införande av ett biblioteksystem. Sådant är givande men tar timmar och dagar i förlängningen. De har fått avsäga sig något projekt där de satt på möten varje vecka tidigare. Enligt budget ska rådgivningen utgöra 10–15 %, vilket faktisk nedlagd tid nog även motsvarar. De skulle sannolikt kunna effektivisera hantering av löpande frågor. De har redan öronmärkt tid för dessa, delat upp bevakningen av mailkorgen mellan sig samt i vissa fall bokat ett möte med alla inblandade och då även kunnat besvara kompletterande frågor direkt. De har inte tillräckligt tydliga nätverk/tydlig organisation genom kontaktpersoner på förvaltningsnivå i småkommunerna för att till exempel en gång i månaden samla alla kommuners socialförvaltningar och därigenom besvara vanligt förekommande frågor i sådan verksamhet och få en större spridning på rådgivningen. I så fall skulle man behöva organisera det.

I sin rådgivning och under informationsdelen av uppdraget[15] publicerar dataskyddsombuden nyhetsbrev med nyheter som rör dataskydd och informationssäkerhet. Målet med nyhetsbreven är att ”försöka bidra till informationsspridning av aktuella frågor. Ambitionen är inte att nyhetsbreven ska komma ut med någon jämn frekvens- utan de ska snarare komma ut när det finns nyheter som är relevanta att sprida.” Dataskyddsombuden har uppskattat, trots reservationen, att de brukar publicerar 3–4 nyhetsbrev per år. Vi har begärt och har fått ta del av ett sådant nyhetsbrev.

3.8.3 Iakttagelser och bedömning

Det finns krav i såväl förordningen som intern uppdragsbeskrivning om att dataskyddsombuden ska bistå verksamheten med rådgivning om dess skyldigheter enligt dataskyddsförordningen och andra dataskyddsbestämmelser. Vi ser rådgivningsdelen i uppdraget som i huvuddrag två delar; en för rådgivning i direkta frågor från verksamheten och en framåtsyftande angående att informera om ny praxis på området och hur rättsfall, tillsynsbeslut samt vägledningar påverkar verksamheten och om åtgärder behöver vidtas på grund av dessa (informationsdelen). Informationsdelen är även tätt sammankopplad med utbildning, se avsnitt 3.9 nedan.

Angående rådgivning i direkta frågor från verksamheten har dataskyddsombuden upprättat en relativt tydlig process för hur frågor ska mottas, loggas, besvaras och även för ansvarsfördelningen dataskyddsombuden emellan. Det verkar vara en effektiv process att frågorna går via dataskyddskontakterna som fungerar som ett ”filter” och skickar vidare endast de frågor som de inte kan besvara. Om dataskyddsombuden märker att det börjar

[15] Se vidare under avsnitt 3.8.3.

komma in fler ”enkla” frågor direkt från verksamheten som skulle kunna fångas upp av dataskyddskontakterna kan man överväga en rekommendation om interna riktlinjer/rutiner om att frågor just ska gå via dataskyddskontakterna. Vidare kan ombuden via ärendehanteringssystemet identifiera återkommande frågor och egna kunskapsluckor. Eftersom de delat upp bevakningen av mailkorgen mellan sig minimeras även omställningstider och fördröjd återkoppling vid den enes frånvaro med mera. En effektiv process manifesteras också i att majoriteten av kommunerna är nöjda med tillgänglighet och svaren på deras frågor. Även att rådgivningsdelen motsvarar i budget angivet omfång indikerar en fungerande rådgivningsdel. Angående de enstaka klagomål som inkommit beträffande det ena dataskyddsombudets dataskyddskompetens och rådgivning är det svårt för oss att avgöra om det ligger något i det eller om det mer handlar om att man föredrar det andra dataskyddsombudet. Vi kan endast förtydliga vår rekommendation om att dataskyddsombudens roll bör renodlas i enlighet med våra slutsatser och rekommendationer under avsnitt 3.3.3 och 3.6.3 och specifikt att dataskyddsombudens rådgivning inte bör tyngas för mycket av närbesläktade områden.

Vidare rekommenderar vi ett övervägande om att verka för ytterligare nätverk/tydlig organisation genom kontaktpersoner på förvaltningsnivå i framförallt småkommunerna för att till exempel en gång i månaden eller kvartalet samla exempelvis alla kommuners socialförvaltningar och därigenom besvara vanligt förekommande frågor i sådan verksamhet och på så sätt få en större spridning på rådgivningen.

Angående informationsdelen ser vi än större förbättringspotential. Enligt vår bedömning får dataskyddsombudens omvärldsbevakning inte fullt genomslag i verksamheten. Visserligen publicerar dataskyddsombuden 3–4 nyhetsbrev per år innehållandes nyheter på dataskydds- (och informationssäkerhets-) området. En av de intervjuade kommunsamordnarna har uttryckt det som att hen efter att hen fått nyhetsbreven får ”sålla” bland nyheterna innan hen vidareförmedlar till verksamheten, eftersom hen inte anser alla nyheter relevanta för varsamheten. För att nyhetsbreven och praxisändringar/förtydliganden ska få genomslag i verksamheten ser vi förbättringspotential i att förtydliga hur nyheterna är relevanta i det dagliga arbetet och om de exempelvis medför att kommunens rutiner och styrdokument behöver revideras. Dataskyddsombuden skulle i nästa steg behöva en rutin för att följa upp att sådana rekommendationer verkligen fått genomslag i berörda verksamheter.

3.9 Om utbildningen ombuden tillhandahåller verksamheterna är tillräcklig

3.9.1 Utgångspunkter

Enligt artikel 39 dataskyddsförordningen har dataskyddsombudet, bland annat, i uppgift att övervaka organisationens efterlevnad av dess strategi för information till och utbildning av personal som deltar i behandlingen. Härutöver framgår i Sjuhäradskommunalförbunds budget för 2021 att:

”Dataskyddsombuden erbjuder sin kompetens och ger service åt verksamheterna, dess personal samt kommunmedlemmar genom rådgivning, information, utredningar och utbildningsinsatser.”

3.9.2 Utbildning som dataskyddsombuden tillhandahåller verksamheterna

Granskningen har visat att det i dagsläget ligger på respektive kommun att försöka nå ut med grundläggande dataskyddsutbildningar till sina samtliga anställda. Detta har gjort att kommunerna, i bästa fall, har upphandlat någon av de webbaserade utbildningstjänster som finns på marknaden. Även dataskyddsombudens granskningsresultat visar att det är den vägen de anslutna kommunerna valt för att uppfylla det grundläggande utbildningsansvaret. Utöver detta har kommunerna uppgett att dataskyddsombuden bjudits in till vissa arbetsplatsträffar och hållit utbildning på fördjupande nivå. Det har uttryckts att dessa utbildningar präglats av mycket lagtext och en högre nivå än vad verksamheterna är mogna för. Samtidigt har en tydlig önskan om mer verksamhetsnära och anpassad utbildning uttryckts. Exempel som lyfts är att utbildningen borde vara anpassad så att även de som jobbar inom skolan eller vården förstår, med fokus på relevanta frågeställningar för just deras verksamhet. Ett annat önskemål har varit en utbildning för mellanchefer som står i kontakt med verksamheten och kan vidareförmedla kunskapen neråt i organisationen.

Dataskyddsombuden har i sin tur betonat att det grundläggande utbildningsansvaret ligger på respektive ansluten kommun eftersom kommunalförbundet inte är en driftsorganisation. De förväntar sig- och följer upp i granskningarna att enheterna tagit fram utbildningsplaner och rekommenderar e-learning-program. Kunskaps- och utbildningsnivån skiljer sig markant från olika kommuner och enheter. Vissa enheter införde en utbildningsplan vid förordningens ikraftträdande, men har sedermera lagt ner den. Sedan ikraftträdandet har vissa enheter identifierat 0 (noll) personuppgiftsincidenter och andra desto fler. Skulle dataskyddsombuden hålla grundutbildningarna, för många tusen medarbetare, skulle de behöva anställa pedagoger eller anlita något av de utbildningsföretag som erbjuder sådana tjänster. De håller däremot introduktionsutbildning för de medarbetare som utses till dataskyddskontakter samt utbildningar på bland annat specialist-, chef- och sektionsnivå. För dataskyddskontakterna/samordnarna rekommenderar de även den utbildning som tillhandahålls av Skövde Högskola. Inom ramen för kursen får deltagarna i uppgift att göra en GAP-analys av den egna kommunen. Dataskyddskontakterna får då en genomlysning/GAP-analys av sin kommun samt hela den kunskapsmässiga verktygslådan. De har hållit chefsutbildningar även i de mindre kommunerna för alla chefer. De kan se fördelar med ett årshjul eller på annat sätt en kontinuitet i utbildning för cheferna.

3.9.3 Iakttagelser och bedömning

Eftersom dels skrivningen om utbildning i artikel 39 är svårtolkad, dels att det av årsredovisningen 2021 framgår att dataskyddsombuden ska erbjuda sin kompetens och ge

service åt verksamheterna genom bland annat utbildningsinsatser, är det naturligt att de anslutna kommunerna förväntar sig just utbildning. Det råder i vissa kommuner förväntningar på dataskyddsombuden att tillhandahålla utbildningar i högre grad än vad som idag görs.

Att ansvaret för grundläggande dataskyddsutbildning idag ligger på respektive kommun kan vara en av förklaringarna till de skiftande kunskapsnivåer som finns mellan medarbetare i de olika kommunerna. Utifrån kostnadseffektivitet och begränsningen i dataskyddsombudens tid och resurser, delar vi kommunernas och dataskyddsombudens samsyn om att den grundläggande GDPR-utbildning (för samtliga anställda) bör ges digitalt. För att harmonisera den generella kunskapsnivån bland medarbetarna i samtliga anslutna kommuner ser vi fördelar med att inkludera grundläggande GDPR-utbildning i kommunalförbundets samverkan.

Granskningen har även åskådliggjort en skillnad mellan de anslutna kommunernas förväntningar och dataskyddsombudens inställning till för vilka målgrupper de senare ska tillhandahålla ytterligare (fördjupade) utbildningar. Mot bakgrund av dessa omständigheter rekommenderar vi en översyn av dels samordnad grundläggande utbildning, dels dataskyddsombudens fördjupande utbildningsansvar och vilka målgrupper detta ska riktas mot. Inom ramen för översynen rekomederar vi en avvägning mellan minst, men inte begränsat till, följande parametrar; kommunernas önskemål, de rätta målgrupperna för att få bäst vidarespridning i verksamheten och dataskyddsombudens resurser – med målsättningen *en effektiv, verksamhetsnära och målgruppsanpassad utbildning*.

Antalet identifierade personuppgiftsincidenter kan vara en indikator på utbildningsnivån bland de olika enheterna. Granskningen vittnar om en stor spridning från enheter där incidenter identifieras och anmäls till enheter som inte haft en incident sedan förordningens ikraftträdande, vilket i sin tur torde vara en indikation på alltför skiftande kunskapsnivå. En annan iakttagelse angående incidenthanteringen, som egentligen inte har med utbildning att göra men som är viktig att lyfta, är dataskyddsombudssamverkans målsättning och beskrivning i Sjuhäradskommunalförbunds budget för 2021. Där framgår följande angående incidenter:

”Samverkansformens övergripande målsättning är att ge medlemskommunerna möjlighet att skaffa sig kontroll över de vitala delarna i dataskyddsförordningen och ge dem verktyg att motverka och minska antalet incidenter; vars konsekvenser kan ge dålig publicitet vilket kan skada både varumärket och minska kommunens anseende hos allmänheten.”

Vi delar visserligen synen på att personuppgiftsincidenter kan medföra negativ publicitet som riskerar att skada såväl varumärke som anseende. Vi ställer oss däremot frågande till skrivningen ovan och befarar att den riskerar att motverka att incidenter lyfts upp och anmäls vilket i sin tur riskerar att hindra enheternas utveckling på dataskyddsområdet. I vår värld är skrivningen felriktad och riskerar leda till en ”tystnadskultur” och att incidenter inte eskaleras och anmäls. I dataskyddsombudens rollbeskrivning finns ett mått av att inspirera till

dataskyddsarbetet för att verksamheten ska kunna förbättras och då krävs snarare en kultur där medarbetarna uppmuntras att anmäla incidenter eller andra brister de uppmärksammar.

4. Sammanfattande slutsatser och rekommendationer

Trots att de anslutna kommunernas förväntningar på samverkansfunktionen och dataskyddsombuden utifrån kommunalförbundets uppdrag och mål för samverkan till övervägande del är rimliga och att dataskyddsombuden är i sin tur väl införstådda med dessa förväntningar, har granskningen åskådliggjort vissa till synes orimliga- och andra helt rimliga förväntningar som i dagsläget inte infrias. Att vissa kommuner förväntar sig att dataskyddsombuden ska ta fram riktlinjer ”åt” dem och på så vis utföra det löpande dataskyddsarbetet är orimligt ur såväl dataskyddsombudets oberoende roll som ur resursperspektivet. Ansvarsfördelningen enligt förordningen förutsätter även att det är de personuppgiftsansvariga, och inte dataskyddsombuden, som sköter, prioriterar och ger sina enheter resurser för det löpande dataskyddsarbetet. En helt rimlig förväntning är dock att dataskyddsombuden ska synas och höras, även i de mindre kommunerna, utöver då de genomför sin årliga granskning. När samverkan infördes skulle den skapa förutsättningar för en robust bemanning. I takt med att uppdraget blivit både kvantitativt större och mer omfattande vad gäller arbetsmängd för nuvarande dataskyddsombud står det klart att de inte helt räcker till. En övergripande slutsats är att dataskyddsombudens roll renodlas att omfatta just dataskydd och att Boråsregionen Sjuhärads kommunalförbund och kommunerna utreder frågan om hur luckan i ett proaktivt compliance-arbete ska fyllas och vem som ansvarar för den.

Här följer, utifrån revisionsfrågorna, våra sammanfattande slutsatser och rekommendationer i punktform.

- Angående vilka avtal som finns upprättade med respektive kommun. Avtal med respektive ansluten kommun, som tidigare saknats, har nu i regel upprättats. Vi har inget att anmärka på innehållet vad gäller det upprättade avtal vi tagit del av. Vårt uppdrag har inte medgett att kontrollera att alla anslutna kommuner har avtal med kommunalförbundet.
    - Vi rekommenderar, med tanke på osäkerheten i en av de intervjuade kommunerna, att man säkerställer avtal med respektive kommun finns upprättat.

- Angående ansvarsfördelningen mellan dataskyddsombuden och kommunerna. Dataskyddsombuden har byggt upp ett ramverk för kommunerna för att det löpande datsskyddsarbetet ska kunna bedrivas på de organisatoriska enheterna. Ombuden ska ägna sig åt regelbunden tillsyn och rådgivning i enlighet med syftet bakom

regelverket och dess föreskrivningar för dataskyddsombudsrollen. Eftersom det är varje nämnd som är personuppgiftsansvarig och dataskyddsombudets roll inbegriper kontrollverksamhet samt ur ett resursfördelningsperspektiv är det ändamålsenligt att ombuden undviker för stor inblandning i det fortlöpande dataskyddsarbetet. Vi vill påminna samtliga enheter om deras respektive ansvar och uppmana verksamhetsledningar och personuppgiftsansvariga nämnder att tillsätta resurser och prioritera dataskyddsarbetet. Häri ingår även att involvera dataskyddsombuden i besluts- och arbetsprocesser med påverkan på dataskyddsarbetet. Mot bakgrund av samverkansfunktionens utformning och att två tjänster tillsatts för att tillse samtliga kommuners behov av ett tillgängligt dataskyddsombud delar vi kommunernas uppfattning om att de ska kunna förvänta sig att dataskyddsombuden uteslutande arbetar med dataskydd. Ombuden bör således syssla med dataskydd så långt det är möjligt, speciellt eftersom de har så pass många registrerade att vara dataskyddsombud för. Att då delta i återkommande möten för att bidra med andra kompetenser de råkar ha ligger enligt vår bedömning utanför kommunalförbundets dataskyddsombuds uppdrag. Detta speciellt sett i ljuset av att vissa kommuner upplever att dataskyddsombuden sällan visar sig hos dem.

- Vi rekommenderar därför att åtgärder vidtas för att renodla dataskyddsombudens roll.

- Angående i vilken utsträckning granskningsverksamheten uppfyller lagkraven. Det finns inte några uttryckliga lagkrav för hur dataskyddsombudens granskningsverksamhets ska genomföras. Även om kommunerna till stor del är nöjda med nivån på granskningarna; att de inte är för avancerade och att vissa inte anser sig mogna för djupare, mer kvalitativa granskningar, delar vi dataskyddsombudens syn på att sådana lite djupare granskningar behövs. Just nu bygger granskningen på självskattning och vi saknar en granskningsdel som de facto synar några behandlingar i artikel 30-registret eller en informationstext i sömmarna. Nuvarande upplägg visar mest enheternas självupplevda kartläggning av om saker finns på plats och inte tillräckligt om kvaliteten på innehållet i artikel 30-registret och andra styrdokument.
  - Vi rekommenderar, utifrån Artikel 29-gruppens tolkning om en riskbaserad inriktning på granskning, någon form av djupare spetsgranskning, vilken skulle kunna möjliggöras genom överväganden om att effektivisera
    - upplägg och administration för utskick och insamling och nuvarande granskning,
    - återkoppling och åtgärdsförslag för nuvarande granskning.

- Angående om prioriteringen i granskningsarbetet är lämplig med hänsyn till granskningsområde och typen av granskningsobjekt. Trots tung administration och skiftande nivå för hur långt de olika enheterna kommit i dataskyddsarbetet är det av yttersta vikt att dataskyddsombuden kan bedriva en effektiv, relevant och

verksamhetsnära granskningsverksamhet med hänsyn till såväl granskningsområde som typen av granskningsobjekt.

- Vi rekommenderar en översyn av granskningsupplägget för att utvärdera hur man kan förändra för att uppnå en mer verksamhetsanpassad, riskbaserad, effektiv, kontextualiserad och spetsig granskning som ger enheterna än mer handfasta åtgärder att vidta i sitt fortsatta dataskyddsarbete.

- Angående om bemanningen och resurser för dataskyddsombuden är tillräckliga för verksamhetens uppgift. Förutom att uppdraget har blivit kvantitativt större vilket har eller kommer få en negativ inverkan på det kvalitativa äts en del av dataskyddsombudens tid upp av de enheter som inte tar sitt ansvar. Huruvida dataskyddsombuden åtar sig ansvar/bevakning av områden som ligger utanför rollen som dataskyddsombud eller om även bevakning och compliance-arbete i angränsande områden ska ligga på dem ligger utanför vår granskning. Det kan konstateras att två tjänster inte helt räcker till för att både sköta uppdraget i nuvarande form, kanske vidareutveckla vissa delar samt därtill följa med i angränsande områdens rätts- och teknikutveckling.
  - Vi rekommenderar därför Boråsregionen Sjuhärads kommunalförbund och kommunerna att renodla dataskyddsombudens roll och utreda om hur luckan i ett proaktivt compliance-arbete ska fyllas och vem som ansvarar för den.

- Angående huruvida dataskyddsombudens rådgivning är tillräcklig. Angående rådgivning i direkta frågor från verksamheten har dataskyddsombuden upprättat en relativt tydlig process för hur frågor ska mottas, loggas, besvaras och även för ansvarsfördelningen dataskyddsombuden emellan.
  - Vi rekommenderar, i syfte att effektivisera rådgivningen och informationsspridandet i verksamheterna, att
    - koppla informationsgivning i nyhetsbreven än mer till vad nyheterna innebär för verksamheterna i det dagliga arbetet
    - överväga om att verka för ytterligare nätverk genom kontaktpersoner på förvaltningsnivå inom liknande verksamhet och därigenom besvara vanligt förekommande frågor i just den verksamheten.

- Angående dataskyddsombudens utbildningsinsatser. Ansvaret för grundläggande dataskyddsutbildning ligger idag på respektive kommun. Utifrån kostnadseffektivitet och begränsningen i dataskyddsombudens tid och resurser, delar vi kommunernas och dataskyddsombudens samsyn om att den grundläggande GDPR-utbildning (för samtliga anställda) bör ges digitalt. Att inte alla kommuner verkar ta ansvaret för att tillhandahålla sina anställda den grundläggande dataskyddsutbildningen kan dels vara en av förklaringarna till de skiftande kunskapsnivåer som finns mellan medarbetare i

de olika kommunerna, dels en förklaring till att vissa enheter/kommuner inte har identifierat några personuppgiftsincidenter. För att harmonisera den generella kunskapsnivån bland medarbetarna i samtliga anslutna kommuner, ser vi fördelar med att inkludera grundläggande GDPR-utbildning i kommunalförbundets samverkan. Det råder i vissa kommuner förväntningar på dataskyddsombuden att tillhandahålla utbildningar i högre grad än vad som idag tillhandahålls. Granskningen har även åskådliggjort en skillnad mellan de anslutna kommunernas förväntningar och dataskyddsombudens inställning till för vilka målgrupper de senare ska tillhandahålla ytterligare (fördjupade) utbildningar.

- Mot bakgrund av dessa omständigheter rekommenderar vi en översyn av dels
  - samordnad grundläggande utbildning, dels
  - dataskyddsombudens fördjupande utbildningsansvar och vilka målgrupper detta ska riktas mot. Inom ramen för översynen rekommenderar vi en avvägning mellan minst, men inte begränsat till, följande parametrar; kommunernas önskemål, de rätta målgrupperna för att få bäst vidarespridning i verksamheten och dataskyddsombudens resurser – med målsättningen en *effektiv, verksamhetsnära och målgruppsanpassad utbildning*.

Granskningen har syftat till att undersöka de förutsättningar kommunalförbundets dataskyddsombud har för att verka inom förbundet och gentemot de medlemskommuner som deltar i samverkan. Projektet har även innefattat en granskning av funktionens arbetssätt med fokus på följsamhet mot lagar och prioritering av tillsynsarbetet med hänsyn till granskningsobjekten. Även om det finns goda förutsättningar för dataskyddsombuden att verka inom förbundet och gentemot de anslutna kommunerna samt upprätthålla ett lagenligt rätt prioriterat arbetssätt, står funktionen inför andra utmaningar nu jämfört med när de tillträdde. En stor mängd kontaktytor och tillkommande administration, som växer ju fler kommuner som ansluter sig, och generellt sett högre nivå och mer tidskrävande arbete gör att den ”luft” som tidigare fanns i systemet nu är borta. Flera kommuner upplever att dataskyddsombuden besöker dem för sällan samtidigt som dataskyddsombuden känner att de inte räcker till när de även känner att de behöver bevaka dataskyddets angränsande områden. Vår sammanfattande slutsats och rekommendation är att Boråsregionen Sjuhärads Kommunalförbund och kommunerna renodlar dataskyddsombudens roll och utreder frågan om hur luckan i ett proaktivt compliance-arbete ska fyllas och vem som ansvarar för den.

Erik Österberg, jurist

Mats Herling, jurist

Jerker Stenqvist, **auktoriserad revisor och certifierad kommunal revisor**

Missiv

Boråsregionen
Sjuhärads kommunalförbund

2023-03-22

Direktionen Sjuhärads kommunalförbund
Samtliga medlemskommuner i Sjuhärads kommunalförbund

GRANSKNING AV SAMORDNAD FUNKTION FÖR DATASKYDDSOMBUD

Insatt AB har på uppdrag av Revisorerna i Sjuhärads kommunalförbund genomfört en fördjupad granskning av dataskyddsombudens verksamhet inom Sjuhärads kommunalförbund. Det övergripande syftet med granskningen var att undersöka de förutsättningar kommunalförbundets dataskyddsombud har för att verka gentemot de medlemskommuner som deltar i samverkan och att granska dataskyddsombudens arbetssätt med fokus på följsamhet mot lagar och prioritering av granskningsarbetet.

Granskningen visar att det finns goda förutsättningar för dataskyddsombuden att verka inom förbundet, att arbeta mot de anslutna kommunerna och att upprätthålla ett lagenligt rätt prioriterat arbetssätt. Dock står funktionen inför andra utmaningar nu jämfört med när den inrättades. En stor mängd kontaktytor och tillkommande administration, som växer ju fler kommuner som ansluter sig, och generellt sett högre nivå och mer tidskrävande arbete gör att det tidsutrymme som tidigare fanns för dataskyddsombuden nu är borta.

Vi bedömer att de förutsättningar kommunalförbundets dataskyddsombud har för att verka inom förbundet och gentemot de medlemskommuner som deltar i samverkan i huvudsak är tillräckliga samt att verksamheten bedrivs på ett i huvudsak ändamålsenligt sätt. I granskningen framkommer dock flera utvecklingsområden och rekommendationer. Vi rekommenderar Sjuhärads kommunalförbund och kommunerna att bl.a. renodla dataskyddsombudens roll och utreda hur ett proaktivt arbete när det gäller efterlevnad av lagar och regler inom området kan genomföras och vem som ansvarar för det.

I övrigt hänvisar vi till granskningsresultat och rekommendationer i bilagd rapport.

Missiv med bilagd rapport tillställs Direktionen i Sjuhärads kommunalförbund. Svar från Direktionen med planerade åtgärder emotses senast 2023-06-22. Missivet med bilagd rapport tillställs även respektive medlemskommun och deras revisorer för kännedom.

Boris Preijde
Marijke Hallencreutz
Ingrid Isaksson
Weine Eriksson
Malin Myrman

Bilaga: *Rapport avseende granskning av samordnad funktion för dataskyddsombud, Boråsregionen Sjuhärads Kommunalförbund*

Borås Stads Revisionskontor
Besöksadress: Sturegatan 42
Postadress: Borås Stad, Revisionskontoret, 501 80 Borås
Webbplats: boras.se/revisionskontoret
Telefonnummer: 033-35 71 56
E-post: revisionskontoret@boras.se

§ 42 Revisionsrapport samordnad funktion för dataskyddsombud

Diarienummer: 2023/SKF0133

Beslut

Direktionen ger kansliet i uppdrag att återkomma med förslag på åtgärder utifrån granskningsrapporten till Direktionens sammanträde den 9 juni 2023

Sammanfattning

Insatt AB har på uppdrag av Revisorerna i Sjuhärads kommunalförbund genomfört en fördjupad granskning av dataskyddsombudens verksamhet inom Sjuhärads kommunalförbund. Det övergripande syftet med granskningen var att undersöka de förutsättningar kommunalförbundets dataskyddsombud har för att verka gentemot de medlemskommuner som deltar i samverkan och att granska dataskyddsombudens arbetssätt med fokus på följsamhet mot lagar och prioritering av granskningsarbetet.

Revisorerna bedömer att förutsättningarna i huvudsak är tillräckliga samt att verksamheten bedrivs på ett i huvudsak ändamålsenligt sätt. I granskningen framkommer dock flera utvecklingsområden och rekommendationer. Revisorerna rekommenderar Sjuhärads kommunalförbund och kommunerna att bl.a. renodla dataskyddsombudens roll och utreda hur ett proaktivt arbete när det gäller efterlevnad av lagar och regler inom området kan genomföras och vem som ansvarar för det.

Svar från Direktionen med planerade åtgärder ska vara revisorerna tillhanda senast 2023-06-22. Missivet med bilagd rapport ska även tillställas respektive medlemskommun och deras revisorer för kännedom.

Expedieras till

Medlemskommunerna