2024-01-26

Analys av personuppgiftsansvar och personuppgiftsbehandling inom Energirådgivningen i Stockholms län

Av Christer Hjert
Kommunakuten AB

Innehåll

Sammanfattning

- Styrgruppen fastställer årligen inriktningsbeslut och verksamhetsplan med utgångspunkt i de samverkande parternas prioriteringar och de av staten angivna förutsättningarna för statsbidraget. Vidare framgår av verksamhetsbeskrivningen att styrgruppen ansvarar för verksamhetens operativa arbete och bl.a. ska fastställa riktlinjer för GDPR. Eftersom styrgruppen dessutom måste betraktas som ett gemensamt beslutsorgan som representerar samtliga samarbetspartners är bedömningen att parterna gemensamt fastställer ändamål och medel för behandlingen och att de därför har ett gemensamt personuppgiftsansvar.
- Med nuvarande samarbetsorganisation och beslutsgång synes det vara svårt att komma runt frågan om ett gemensamt personuppgiftsansvar. För att ändra det gemensamma personuppgiftsansvaret till ett personuppgiftsansvar för t.ex. värdkommunerna så behöver förutsättningarna för samarbetet förändras.
- Med beaktande av den trots allt begränsade behandlingen av personuppgifter, som dessutom i princip bara innefattar vad som skulle kunna sägas vara harmlösa uppgifter och som i princip alltid bygger på samtycke av de behandlade så synes en sådan förändring inte vara vare sig rimlig eller nödvändig.
- I princip kan dessutom samma effekter uppnås med gemensamt personuppgiftsansvar som med ett personuppgiftsansvar som ligger på personuppgiftsbehandlande kommun.
- I artikel 26.1 i dataskyddsförordningen anges att gemensamt personuppgiftsansvariga på ett öppet sätt ska fastställa och komma överens om sina respektive ansvarsområden för efterlevnad av förordningens krav.
- Gemensamt personuppgiftsansvariga måste alltså klargöra ”vem som gör vad” genom att själva bestämma vem som ska utföra vilka uppgifter för att säkerställa att behandlingen uppfyller de tillämpliga kraven enligt GDPR i förhållande till den gemensamma behandlingen. Detta sker i ett avtal mellan parterna.
- Det behövs alltså ett tydligt dokument som anger vem som gör vad. Att upprätta ett sådant dokument bör inte vara särskilt svårt i det här fallet. Utgångspunkterna för en sådan överenskommelse kan utgöras av samverkansöverenskommelsen och verksamhetsbeskrivningen eftersom dessa dokument beskriver vem som gör vad samt av artikel 30 registret där de olika behandlingarna beskrivs. Ett enkelt sätt är då att

utgå från artikel 30 registret och fylla på med information om vem som i olika situationer ansvarar för behandlingen och vad det innebär.

- Genom en sådan här lösning kan också ansvaret för att säkerställa att behandlingarna sker på ett korrekt sätt avtalsvägen fördelas på den som genomför behandlingen.
- En fördel med det är att samtliga samarbetsparter som behandlar personuppgifter också får ett ansvar för att det behandlas korrekt. Det här är en viktig och praktisk lösning eftersom det är svårt för alla att ha koll på alla. Det innebär att samtliga krav som följer på behandlingarna ska hanteras av den som faktiskt utför behandlingen.
- Det gör det också enklare när det kommer till krav på säkerhet etc. Varje ansvarig får då det fulla ansvaret för att säkerställa säkerhet och konfidentialitet i de respektive behandlingar de utför samt att göra konsekvensanalyser och andra åtgärder.
- För att säkerställa en tydlig fördelning av ansvar/uppgifter behöver styrgruppen fastställa riktlinjer (policy) för GDPR hanteringen, dessutom behövs ett avtal som reglerar fördelningen av ansvar i det gemensamma personuppgiftsansvaret.
- En fördelning av ansvaret på detta sätt leder förmodligen till den säkraste lösningen. Ansvar och kontroll kring efterlevnaden av behandlingen av personuppgifter flyttas till respektive behandlande kommun och hamnar på så sätt så nära utföraren som möjligt. Detta bör påtagligt öka förutsättningarna för regelefterlevnad och inte minst kontrollen över densamma enligt närhetsprincipen.
- I nuläget är framtagande av riktlinjer och avtal för fördelning av det gemensamma personuppgiftsansvaret det mest prioriterade. Så fort det är på plats kan respektive part som behandlar uppgifter säkerställa behandlingen i sin respektive verksamhet.
- När avtalet enligt artikel 26 är på plats ankommer det enligt den föreslagna lösningen på respektive behandlande kommun att utföra respektive åtgärder som dessa har ansvar för. Det innebär att bl.a. risk- och sårbarhetsanalyser, eventuella konsekvensbedömningar, behandlingsregister, rutiner för hantering av incidenter etc. ska utföras av respektive behandlande kommun.
- Sammantaget innebär den valda lösningen den förmodligen enklaste lösningen där ansvaret läggs så nära den som behandlar som är möjligt. Det är också den behandlande aktören som har bäst möjligheter att säkerställa att de behandlingar de utför sker på ett sätt som är förenligt med gällande regelverk.

1. Inledning och frågeställningar

1.1. Inledning

Energirådgivningen i Stockholms län bygger på en samverkansöverenskommelse och bedrivs inom ramen för Energikontoret Storstockholm (EKR). Med beaktande av att det är många aktörer som genom samverkansöverenskommelsen är inblandade energirådgivningen uppkommer många frågeställningar avseende såväl personuppgiftsansvar som personuppgiftsbehandling. Som en följd av detta önskar EKR och kommunerna att frågorna om personuppgiftsbehandling i verksamheten utreds och klargörs.

EKR har i offertförfrågan ställt upp ett antal frågor som utgör utgångspunkt för personuppgiftsutredningen. I det här stadiet görs en genomgång och analys av de olika frågeställningarna för att beskriva lösningsmodeller och möjliga tillvägagångssätt och de utmaningar som detta innebär. Vi kommer att mer eller mindre redogöra för de respektive frågeställningarna var för sig nedan.

1.2. Frågeställningarna

1. Tydlig beskrivning av personuppgiftsansvaret för respektive personuppgiftsansvarig samt utreda vilka valmöjligheter det finns beträffande uppdelningen av personuppgiftsansvaret för den regionala energi- och klimatrådgivningen (EKR). Går det att undvika situationen med gemensamt personuppgiftsansvar och vad krävs i så fall för det?
    a. Vi tittar på behandlingen av personuppgifter i verksamheten och med det som utgångspunkt gör vi en bedömning av hur personuppgiftsansvaret är fördelat. Vi kommer dessutom, om möjligheten finns, att analysera eventuella alternativa lösningar för fördelning av personuppgiftsansvaret med utgångspunkt i samverkansöverenskommelsen för att med det som grund se om det finns lösningar som är enklare, tydligare och säkrare.

2. Utredning av huruvida PUB-avtal eller annat styrande dokument behöver ingås mellan personuppgiftsansvarig och personuppgiftsbiträde med anledning av verksamhetens samverkansöverenskommelse. För att göra denna bedömning kommer vi att behöva

granska samverkansöverenskommelsen och verksamhetsplanen som är tänkt att beskriva organisationen kring hur EKR rent praktiskt jobbar.

   a. Vi gör en genomgång av verksamheten och flödet av personuppgifter i de olika processerna och med det som utgångspunkt gör vi en analys av behovet av personuppgiftsbiträdesavtal. Vi kommer i den här delen att behöva titta på samverkansöverenskommelsen och verksamhetsplanen men det mest avgörande är ändå verksamhetens processer för att se om och hur personuppgifter faktiskt behandlas och med det som utgångspunkt göra en bedömning av behovet av PUB-avtal.

3. Omfattning av det administrativa arbetet, dvs. beskrivning av vilka dokument och rutiner som behöver tas fram (både ur GDPR-synpunkt och andra eventuella administrativa påföljder).
   a. När vi har svaret på ovanstående frågor (1 och 2) och har analyserat organisation, verksamhetsplan och processer utgör det utgångspunkt för en sammanställning av behovet av styrande dokument i verksamheten. Frågan rör sig i ett gränsland där harmoni också måste finnas i förhållande till styr och ledningssystem i verksamheten, till frågor om intern kontroll osv.

4. Estimerade tidsintervall för en konsult att ”etablera” organisationen på ett GDPR-efterlevande sätt enligt de olika alternativen.
   a. Vi gör en uppskattning av tidsintervallet. Det kan eventuellt bli fråga om flera olika tidsintervall om det finns flera alternativa lösningar.

5. En huvudsaklig konsekvensbedömning bör göras för vart och ett av alternativen med inriktning på vilka risker som behöver hanteras inom ramen för respektive alternativ, vilket då innebär att göra en kartläggning av aktuella risker för respektive alternativ, kategorisering av riskerna i juridiska respektive tekniska risker (eventuellt värdering av riskerna i termer av impact/likelihood men det skulle kunna vänta till ett kommande steg). Även vad som krävs för att hantera riskerna i de olika alternativen med inriktning på vilken kompetensnivå som krävs av personalen inom ramen för respektive alternativ (något av alternativen kräver säkert väsentligt högre kompetens än andra p.g.a. högre juridisk komplexitet och fler stora risker).

   a. Vi gör en riskanalys med utgångspunkt i den personuppgiftsbehandling som analyserats i stegen ovan. Inom ramen för riskanalysen kommer vi särskilt att svara på ovan angivna frågor. Vår bedömning är att det kan nödvändigt att göra en värdering av riskerna i termer av impact/likelihood redan här eftersom det är avgörande för prioriteringen inom ramen för ett åtgärdsprogram/arbetsplan (se punkt 6).

6. Ta fram en arbetsplan för hur de olika riskerna i de olika alternativen bör hanteras och rekommendera hur de bör prioriteras av tjänstemännen under t.ex. de första 12 månaderna, för att få en indikation på hur mycket ”extra admin” det kommer att innebära för tjänstemännen att jobba enligt respektive alternativ. Kommer något av alternativen med fördelning av personuppgiftsansvar att kräva mycket mer admin i vardagen än de andra alternativen?
   a. Det här handlar i stor utsträckning om slutsatser av vad som framkommit under de ovan redovisade punkterna. Vi gör en sammanställning med det som utgångspunkt där vi redogör för åtgärdsförslag. Inom ramen för de olika åtgärdsförslagen gör vi en bedömning av tidsåtgång och en uppskattning av kostnader. Vi kommer också att bedöma hur olika förslag och åtgärder påverkar det dagliga arbete i form av administrativa insatser.

2. Energirådgivningens organisation

2.1. Samarbetets reglering

Som nämnts inledningsvis bygger Energirådgivningen i Stockholms län på en samverkansöverenskommelse och bedrivs inom ramen för EKR. En central utgångspunkt för analysen av ansvaret för och rollerna i personuppgiftsbehandlingen är just denna samverkansöverenskommelse och vad den innebär. Samverkansöverenskommelsen reglerar syfte och mål med samarbetet, parternas inbördes förhållanden till varandra, vilka roller de har, hur delaktiga de är i verksamheten och hur delaktiga de är i det övergripande beslutsfattandet.

Samverkansöverenskommelsen kompletteras av en verksamhetsbeskrivning som anger organisationsstrukturen, vilka roller (organ) som finns, de olika rollernas ansvar och befogenheter. Utöver samverkansöverenskommelsen och beskrivningen antas dessutom

verksamhetsplaner och projektplaner med närmare beskrivning av vad de samverkande parterna ska åstadkomma.

Syftet med granskning av dessa dokument som reglerar samarbetet i energirådgivningen är att klargöra hur personuppgiftsansvaret fördelar sig mellan de samverkande perterna. För att kunna göra det måste det klargöras vem (vilket organ) som med stöd av dessa styrdokument bestämmer för vilka ändamål personuppgifter ska behandlas och hur behandlingen ska gå till.

2.2 Samverkansöverenskommelsen och verksamhetsbeskrivningen

2.2.1. Samverkansöverenskommelsens mål, syfte och finansiering

Syftet med samverkansöverenskommelsen är enligt 2 § att stödja en fungerande och kostnadseffektiv kommunal energi- och klimatrådgivning inom Stockholms län. Målsättningen är att skapa förutsättningar för en effektiv användning av de resurser som tillfaller kommunerna i Stockholms län för EKR:s verksamhet via statsbidrag. Samarbetet ska sträva efter att skapa förutsättningar för insatser som bidrar till att minska regionens negativa klimatpåverkan mer än vad som skulle kunna åstadkommas utan mellankommunalt samarbete.

Vidare är målet för verksamheten enligt 3 § att genom rådgivning och projektverksamhet främja:

1. en effektiv och miljöanpassad användning av energi,
2. en minskad klimatpåverkan från energianvändningen,
3. att riksdagens energi- och klimatpolitiska mål nås,
4. att de samverkande parternas mål för energi- och klimatområdet nås.

Enligt 6 § ska kommunerna erlägga en andel av det statliga bidraget som avgift till den regionala samverkan. Avgiften för avtalsperioden 2022-2025 är 23 procent av respektive samverkande kommuns totala bidrag för energi- och klimatrådgivning från Energimyndigheten, med undantag för Stockholms stad som erlägger 16 procent med anledning av att Stockholms stad når bidragets maxbelopp och därmed erhåller en lägre bidragsnivå per målgrupp.

2.2.3. Organisation och styrning

Av 7 § samverkansöverenskommelsen följer att det operativa arbetet som bedrivs inom samarbetet leds av en styrgrupp utsedd av Storsthlms styrelse. Ledamöterna till styrgruppen ska nomineras av kommundirektörerna i de kommuner som anslutit sig till denna samverkansöverenskommelse. Vidare framgår av 8 § att ledamöter som nomineras till styrgruppen ska vara en chef eller nyckelperson med beslutsmandat i sin hemkommun. Den nominerade ska även ha ansvar för genomförandet av det lokala energi- och klimatarbetet. Slutligen anges i 9 § att styrgruppen ska bestå av sju ledamöter från de samverkande kommunerna. Storsthlm representeras av en ledamot i styrgruppen och värdkommunerna ska var och en för sig ges möjlighet till representation i styrgruppen. En ordförande för styrgruppen ska utses av Storsthlms styrelse på förslag av kommundirektörerna i de samverkande kommunerna.

2.2.4. Styrgruppen

Styrgruppens uppgifter och ansvar regleras i 15 – 18 §§ i samverkansöverenskommelsen, där det bl.a. framgår att styrgruppen årligen fastslår inriktningsbeslut och verksamhetsplan med utgångspunkt i de samverkande parternas prioriteringar och de av staten angivna förutsättningarna för statsbidraget. Av verksamhetsbeskrivningen framgår dessutom att styrgruppen även leder det operativa arbetet som bedrivs inom samarbetet. Av den punktlista som återfinns under punkten 1.3.2 i verksamhetsbeskrivningen och närmare definierar styrgruppens uppgifter framgår att styrgruppen beslutar om strategiska dokument, t.ex. om kommunikation och GDPR.

2.2.5. Värdkommunerna

De kommuner som åtar sig att vara värdkommuner har enligt 14 § samverkansöverens-kommelsen ansvar för samarbetets gemensamma resurser och utgör projektledare och rådgivare för verksamheten. Tillsammans ansvarar värdkommunerna för planering, genomförande, uppföljning och rapportering av den gemensamma verksamheten. Värdkommunernas åtaganden specificeras i den årliga verksamhetsplanen. Av avsnitt 1.3.3. i verksamhetsbeskrivningen framgår att för den operativa driften av det gemensamma arbetet har styrgruppen ett flertal projektledare och rådgivare baserade i värdkommunerna (VK) till sitt förfogande.

2.3. De samverkande kommunerna

De samverkande kommunernas roll är inte särskilt utförligt beskriven i vare sig samverkansöverenskommelsen eller i verksamhetsbeskrivningen. Det framgår emellertid att det ytterst är dessa som ansvarar för verksamheten och att de fattar gemensamma beslut i styrgruppen. Av 16 § samverkansöverenskommelsen framgår att styrgruppen årligen fastslår inriktningsbeslut och verksamhetsplan med utgångspunkt i de samverkande parternas prioriteringar och de av staten angivna förutsättningarna för statsbidraget. Även om inte alla samverkande parterna samtidigt är representerade i styrgruppen så måste styrgruppen ändå betraktas som gemensamt beslutsorgan för samtliga samverkande kommuner då dess ledamöter nomineras av kommundirektörerna i de samverkande kommunerna.

3. Personuppgiftsansvar

3.1. Personuppgiftsansvar

Kvalificeringen som gemensamt personuppgiftsansvariga kan uppstå när mer än en aktör är involverad i behandlingen. Personuppgiftsansvarig är enligt 4.7 dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt. I den kommunala organisationen betraktas varje nämnd som personuppgiftsansvarig avseende sina behandlingar.

Av artikel 26 dataskyddsförordningen följer att om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga.

Den eller de som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till är alltså personuppgiftsansvariga. Den som är personuppgiftsansvarig kan överlåta den faktiska behandlingen av personuppgifter men personuppgiftsansvaret kan aldrig överlåtas.

Det är den personuppgiftsansvarige som ansvarar för att principerna för personuppgifts-behandling enligt artikel 5 dataskyddsförordningen är uppfyllda, samt att lämpliga och effektiva åtgärder införs avseende densamma. I vissa fall är det tydligt vem som har rollen som personuppgiftsansvarig. Det kan exempelvis följa av lag, såsom när en myndighet i sitt myndighetsutövande har att behandla personuppgifter. Andra gånger är personuppgiftsbehandlingen naturligt knuten till en parts funktion. Exempelvis en arbetsgivare som ansvarar för behandlingen av sina anställdas personuppgifter.

I de allra flesta fall krävs emellertid en analys av de faktiska omständigheterna för att identifiera vem eller vilka som bär personuppgiftsansvaret för vilken behandling. Personuppgiftsansvaret kan avse en enskild behandling eller en serie behandlingar. Samma part kan även samtidigt fungera som ett personuppgiftsbiträde för andra behandlingar. Varje enskild behandling måste därför övervägas noga. Villkoren i ett avtal kan vara vägvisande, men det är i slutändan parternas faktiska aktiviteter och förhållande till varandra som avgör rollfördelningen, och således inte hur de har valt att definiera sin roll.

3.1.1. Gemensamt personuppgiftsansvar

Det övergripande kriteriet för att gemensamt personuppgiftsansvar ska föreligga är gemensamt deltagande av två eller flera enheter i fastställandet av behandlingsändamål och behandlingssätt. Gemensamt deltagande kan ske i form av ett gemensamt beslut som fattas av två eller flera enheter eller som är ett resultat av konvergerande beslut av två eller flera enheter där besluten kompletterar varandra och är nödvändiga för att behandlingen ska kunna ske på ett sådant sätt att de har en påtaglig inverkan på fastställandet av behandlingsändamål och behandlingssätt. Ett viktigt kriterium är att behandlingen inte skulle vara möjlig utan båda parternas deltagande i betydelsen att behandlingen från varje part är oskiljbar, dvs. den är oupplösligt sammanflätad. Det gemensamma deltagandet måste inkludera fastställandet av behandlingsändamålet å ena sidan och fastställandet av behandlingssättet å andra sidan.

3.1.2. Bedömning av gemensamt deltagande

Gemensamt deltagande i fastställandet av ändamål och medel innebär att mer än en enhet har ett avgörande inflytande över huruvida och hur behandlingen sker. I praktiken kan gemensamt

deltagande ske på flera olika sätt. Till exempel kan gemensamt deltagande anta formen av ett gemensamt beslut som fattas av två eller flera enheter eller härrör från konvergerande beslut från två eller flera enheter angående ändamål och väsentliga medel.

Gemensamt deltagande via ett gemensamt beslut, vilket är innebär att besluta tillsammans och innebär en gemensam avsikt i enlighet med den vanligaste förståelsen av termen ”gemensamt” som avses i artikel 26 i dataskyddsförordningen (se EDPB, Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, punkt 55).

3.1.3 Gemensamt fastställande av ändamål

Gemensamt personuppgiftsansvar kräver även att två eller flera enheter har haft inflytande över behandlingssätten. Detta innebär inte att varje involverad enhet alltid måste besluta alla behandlingssätt för att gemensamt personuppgiftsansvar ska föreligga. Som klargörs av EU-domstolen kan olika enheter vara involverade i olika skeden av behandlingen och i olika grad. Olika gemensamt personuppgiftsansvariga kan därför definiera behandlingsmedlen i olika omfattning, beroende på vem som effektivt kan göra detta.

Det kan också vara så att en av de inblandade enheterna tillhandahåller medlen för behandlingen och gör dem tillgängliga för behandling av personuppgifter av andra enheter. Enheten som beslutar att använda dessa medel så att personuppgifter kan behandlas för ett visst ändamål deltar också i fastställandet av behandlingsmedlen (se EDPB, Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, punkt 63-64).

Av de exempel som EDPB redovisar i Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, sid 24 ff. synes sådana samarbetssituationer som liknar Energirådgivnings samarbete regelmässigt leda till gemensamt personuppgiftsansvar.

3.2. Personuppgiftsansvaret inom Energirådgivningen

Som redogjort för i avsnitt 2 ovan är det styrgruppen som årligen fastslår inriktningsbeslut och verksamhetsplan med utgångspunkt i de samverkande parternas prioriteringar och de av

staten angivna förutsättningarna för statsbidraget. Vidare framgår av verksamhetsbeskrivningen att styrgruppen ansvarar för verksamhetens operativa arbete och bl.a. ska fastställa riktlinjer för GDPR. Eftersom styrgruppen dessutom måste betraktas som ett gemensamt beslutsorgan som representerar samtliga samarbetspartners är bedömningen att parterna gemensamt fastställer ändamål och medel för behandlingen och att de därför har ett gemensamt personuppgiftsansvar.

För att ändra det gemensamma personuppgiftsansvaret till ett personuppgiftsansvar för t.ex. värdkommunerna så behöver förutsättningarna för samarbetet förändras. I princip måste alla beslut om ändamål och medel för behandlingen överlämnas till värdkommunerna. En sådan förändring skulle innebära att de övriga parterna i samarbetet inte skulle ha något reellt inflytande över verksamheten annat än att beställa ett ”resultat” och låta värdkommunerna helt besluta om hur de ska uppnå resultatet.

Med beaktande av den trots allt begränsade behandlingen av personuppgifter, som dessutom i princip bara innefattar vad som skulle kunna sägas vara harmlösa uppgifter och som alltid bygger på samtycke av de behandlade så synes en sådan förändring inte vara vare sig rimlig eller nödvändig.

4. Behovet av personuppgiftsbiträdesavtal eller annan skriftlig reglering av personuppgiftsbehandlingen

4.1. Personuppgiftsbiträdesavtal

Ett personuppgiftsbiträde definieras enligt artikel 4.8 dataskyddsförordningen som en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Av artikel 28.3 dataskyddsförordningen ska, när uppgifter behandlas av ett personuppgiftsbiträde, hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige och i vilken föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och

kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges.

Eftersom bedömningen ovan leder till att det är fråga om ett gemensamt personuppgiftsansvar i energirådgivningens verksamhet finns det inget personuppgiftsbiträde att avtala med.

4.2. Annan skriftlig reglering av personuppgiftsbehandlingen

I artikel 26.1 i dataskyddsförordningen anges att gemensamt personuppgiftsansvariga på ett öppet sätt ska fastställa och komma överens om sina respektive ansvarsområden för efterlevnad av förordningens krav.

Gemensamt personuppgiftsansvariga måste alltså klargöra ”vem som gör vad” genom att själva bestämma vem som ska utföra vilka uppgifter för att säkerställa att behandlingen uppfyller de tillämpliga kraven enligt GDPR i förhållande till den gemensamma behandlingen som saken gäller. Med andra ord ska ansvarsfördelningen för efterlevnad göras genom användning av termen ”respektive” i artikel 26.1. (se EDPB, Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, punkt 162).

Syftet med dessa regler är att säkerställa att ansvaret för efterlevnad av dataskyddsreglerna när flera aktörer är involverade, särskilt i komplexa databehandlingsmiljöer, tydligt fördelas för att undvika att skyddet av personuppgifter reduceras eller att en negativ kompetenskonflikt leder till kryphål där vissa skyldigheter inte efterlevs av någon av parterna som är involverade i behandlingen. Det bör klargöras här att allt ansvar måste fördelas enligt de faktiska omständigheterna för att uppnå ett operativt avtal (se EDPB, Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, punkt 163).

Av det ovan sagda följer att det behövs ett dokument som tydligt anger vem som gör vad. Att upprätta ett sådant bör inte vara särskilt svårt i det här fallet. Utgångspunkterna för en sådan överenskommelse utgörs av samverkansöverenskommelsen och verksamhetsbeskrivningen som beskriver vem som gör vad och av artikel 30 registret där de olika behandlingarna beskrivs. Ett enkelt sätt är alltså att utgå från artikel 30 registret och fylla på med information om vem (av de samarbetande parterna) som i olika situationer ansvarar för behandlingen och

vad det innebär. Inom ramen för detta dokument regleras också ansvaret sinsemellan för de parter som ingår i energirådgivningen.

En avtalsreglering enligt ovan påminner i många stycken ett personuppgiftsbiträdesavtal och effekterna kan till stora delar bli desamma i fråga om ansvar, beroende på hur det regleras mellan parterna.

5. Vilka dokument och rutiner som behöver tas fram m.m.

5.1. Inledning

En del i uppdraget är att beskriva omfattning av det administrativa arbetet, dvs. beskrivning av vilka dokument och rutiner som behöver tas fram (både ur GDPR-synpunkt och andra eventuella administrativa påföljder).

5.2. Dokument och rutiner

Med de ställningstaganden som gjorts och de slutsatser som detta föranlett är det i princip två huvuddokument som behöver upprättas. Det ena dokumentet som behöver upprättas är det ovan redovisade skriftliga dokumentet om vem som gör vad. Det andra dokumentet är riktlinjer för hanteringen av personuppgiftsbehandling. Till riktlinjerna bör även kopplas en beskrivning av behandlingarna som bl.a. redogör för ändamålen med dessa och som fastställs av styrgruppen. Till stora delar motsvaras det av det artikel 30 register som redan är upprättat.

Vad gäller ”vem gör vad” dokumentet så har innehållet i ett sådant redovisats under punkten 4.2. ovan. När det gäller riktlinjer så anges i den punktlista som återfinns under punkten 1.3.2 i verksamhetsbeskrivningen och som närmare definierar styrgruppens uppgifter att styrgruppen beslutar om strategiska dokument, t.ex. GDPR. Några sådana dokument synes inte finnas och bör därför snarast upprättas. Riktlinjerna bör ta sin utgångspunkt i det gemensamma personuppgiftsansvaret och i ”vem gör vad” dokumentet. Med denna grundinställning som utgångspunkt bör anges att varje samarbetspart ansvarar för den personuppgiftsbehandling som denne vidtar inom ramen för samarbetet och att den personuppgiftsbehandlingen ska ske i enlighet med respektive behandlande parts ansvar för personuppgiftsbehandling.

Genom en lösning i enlighet med ovan görs på ett öppet sätt en redovisning av respektive parts ansvarsområden och hur de ska säkerställa en personuppgiftsbehandling som är förenligt med gällande regler, inte minst kravet i artikel 26.1 dataskyddsförordningen.

En lösning som den föreslagna innebär dessutom minsta möjliga administrativa belastning inom ramen för samarbetet.

5.3. Estimerade tidsintervall

Att ta fram nödvändiga dokument för föreslagna åtgärder (”vem gör vad” dokumentet och GDPR policyn) bör inte innebära mer arbete än uppskattningsvis 50 timmar för Energirådgivningen. Det finns redan idag ett artikel 30 register, en verksamhetsbeskrivning där de olika organens roller definieras, årliga verksamhetsplaner samt projektplaner för både basprojekt och verksamhetsprojekt.

Det mesta arbetet är förmodligen redan gjort eftersom dessa dokument ger en god bild över vilka personuppgifter som behandlas i verksamheten, varför de behandlas och av vem de behandlas. Arbetet med dessa två dokument måste påbörjas omgående eftersom de är styrande för övriga åtgärder.

Eftersom utgångspunkten är att varje kommun inom ramen för sin respektive verksamhet ska hantera övriga frågor med utgångpunkt i vilket ansvar de tilldelas enligt ”vem gör vad” dokumentet är det svårt att bedöma vad detta innebär i tidsåtgång. För Energirådgivningen innebär det inget merarbete men för vissa kommuner som utför och kommer att tilldelas ett ansvar enligt ”vem gör vad” dokumentet kommer det att innebära visst merarbete kring kartläggning, risk- och sårbarhetsanalyser och eventuella konsekvensbedömningar, behandlingsregister, rutiner för hantering av incidenter etc. Såvitt kan bedömas innebär det dock ingen egentlig skillnad och inte heller något merarbete i förhållande till om dessa skulle vara personuppgiftsansvariga eller personuppgiftsbiträden för de behandlingar de gör.

6. Konsekvensbedömning

6.1. Inledning

Ibland är det ett krav att göra en konsekvensbedömning. Detta gäller om personuppgifts-behandlingen sannolikt leder till hög risk för de registrerades fri- och rättigheter. Av ordalydelsen i artikel 35.1 och skäl 76 i GDPR följer att det krävs en riskbedömning för att avgöra frågan om en konsekvensbedömning behöver göras. Detta innebär att den personuppgiftsansvarige först måste bedöma vilka risker behandlingen innebär. Detta görs genom en dataskyddsrättslig riskanalys, ett övervägande om konsekvensbedömning.

Enligt artikel 35.1. GDPR ska om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.

Med beaktande av den personuppgiftsbehandling som görs inom ramen för energirådgivningen framstår det som mindre sannolikt att en konsekvensbedömning enligt artikel 35 i GDPR behöver göras. Det bör emellertid göras en risk- och sårbarhetsanalys över verksamhetens olika behandlingar. Den risk och sårbarhetsanalysen bör dock göras av den respektive samarbetspart som gör den faktiska behandlingen av personuppgifter och ske inom ramen för den aktörens systematiska dataskyddsarbete.

6.2. Konsekvensbedömning av respektive personuppgiftsbehandlande part

Mot bakgrund av ställningstagandet om gemensamt personuppgiftsansvar och den uppgiftsfördelning som ska fastställas enligt artikel 26.1 ska detta regleras inom ramen för det s.k ”vem gör vad” dokumentet om ansvaret inom ramen för det gemensamma personuppgiftsansvaret. Risk- och sårbarhetsanalyserna kommer således att utföras av varje kommun som behandlar uppgifter inom ramen för energirådgivningssamarbetet. Det blir också varje behandlande kommun som kommer att ansvara för bedömningen av om en konsekvensbedömning måste upprättas eller inte.

Att reglera detta i ”vem gör vad” dokumentet så att varje behandlande kommun blir ansvarig för risk och sårbarhetsanalyser och konsekvensbedömningar innebär att ansvaret hamnar så nära den faktiska behandlingen som möjligt. Det innebär också att den som är ansvarig är den som har bäst kunskaper om vad som faktiskt behandlas och hur det behandlas, i vilken teknisk miljö behandlingen sker och vilka eventuella personuppgiftsbiträden som finns.

7. Vad måste göras nu?

7.1. Inledning

Med utgångspunkt i ovan gjorda ställningstaganden måste en arbetsplan tas fram där de nu nödvändiga åtgärderna hanteras. Arbetsplanen är främst fråga om en prioritering och en fördelning av uppgifter. Ett problem i sammanhanget är att det ännu inte finns någon ansvars- och uppgiftsfördelning, dvs ett ”vem gör vad” dokument enligt artikel 26 i GDPR. Eftersom det inte finns något sådant dokument finns inte heller något fastställt innehåll att ta ställning till. Detta till trots finns det några prioriterade och nödvändiga uppgifter att snarast ta tag i. Vissa åtgärder som med nödvändighet kommer att regleras inom ramen för ”vem gör vad” dokumentet kan också planeras även om det dokumentet ännu inte är framtaget och beslutat.

7.2. Åtgärder och prioritering

Nedan listas åtgärder och prioriteringar som behöver göras och i vilken ordning det bör ske.

1. Den absolut mest prioriterade uppgiften är att ta fram ”vem som gör vad” dokumentet. Detta är ett krav enligt artikel 26 i GDPR och är också det dokument som kommer att styra den fortsatta hanteringen. Detta bör påbörjas snarast då det dels är ett direkt rättsligt krav dels ska beslutas av samtliga i energirådgivningen samverkande parter. Innan det läggs fram för de samverkande parterna för beslut/undertecknande bör det fastställas av styrgruppen.
2. I samband med att ”vem gör vad” dokumentet tas fram bör även en GDPR-policy för energirådgivningen tas fram och fastställas av styrgruppen. Det är lämpligt att dessa båda dokument tas fram samtidigt så att de dels harmonierar dels att rätt sak hamnar i rätt dokument.
3. Eftersom utgångspunkten föreslås vara att uppgifter och ansvar ska fördelas så att den kommun som faktiskt behandlar en uppgift också är den kommun som ska ”ha personuppgiftsansvaret” kring denna behandling kan, framförallt, värdkommunerna

påbörja ett arbete i enlighet med detta förslag. Det ligger dessutom i deras eget intresse att få detta gjort snarast eftersom det är en uppgift som redan borde ha gjorts tidigare.

4. En ytterligare fråga som är viktig är återrapportering. Styrgruppen bör hållas informerad om status kring personuppgiftsbehandlingar som ske, om eventuella problem, förändringar, utmaningar och incidenter. Detta får dock delvis bedömas ligga i ett nästa steg men kommer samtidigt att delvis beröras i både GDPR- policyn och i ”vem gör vad” dokumentet. Det främsta skälet för detta är att det faktiskt handlar om gemensamt personuppgiftsansvar och då bör parterna vara informerade av sådant som är av vikt även om ansvaret är reglerat i ”vem gör vad” dokumentet och det är styrgruppen som representerar samtliga personuppgiftsansvariga.