Granskning av förberedelser inför införandet av GDPR

Revisionsrapport

Arboga kommun, Kungsör kommun, Köping kommun, Surahammar kommun och VMKF

KPMG AB

2018-02-07

Antal sidor 20

Arboga kommun, Kungsör kommun, Köping kommun, Surahammar kommun och VMKF
Granskning av förberedelser inför införandet av GDPR

2018-02-07

Innehållsförteckning

1 Sammanfattning

Vi har av revisorerna i Arboga, Kungsör, Köping och Surahammar samt Västra Mälardalens kommunalförbund fått i uppdrag att granska hur organisationerna förberett sig inför införandet av Dataskyddsförordningen. Uppdraget ingår i revisionsplanen för år 2017.

EU har i april 2016 beslutat om ett nytt regelverk för behandling av personuppgifter som ska börja tillämpas i medlemsstaterna i maj 2018. Den nya dataskyddsförordningen kommer att gälla som lag i samtliga medlemsstaterna och ersätter då tidigare nationell lagstiftning.

Revisorerna har bedömt att det föreligger *risk* att verksamheterna inte har kommit tillräckligt långt i sina förberedelser, och ser det som *väsentligt* att detta område granskas.

Syftet är att granska hur kommunen och kommunalförbundet har förberett sig inför införandet av dataskyddsförordningen i maj 2018.

Granskningen har genomförts genom dokumentstudier och intervjuer med berörda tjänstemän och politiker i medlemskommunerna och förbundet.

Efter genomförd granskning har vi de gemensamma rekommendationerna att:

- medlemskommunerna och förbundet måste klargöra ansvarsfördelningen avseende arbetsuppgifter i samband med införandet av dataskyddsförordningen.
- kommunerna och förbundet måste klargöra resursåtgång, personell och ekonomisk, för de identifierade åtgärderna.

2 Inledning/bakgrund

Vi har av revisorerna i Arboga, Kungsör, Köping och Surahammar samt Västra Mälardalens kommunalförbund fått i uppdrag att granska hur organisationerna förberett sig inför införandet av Dataskyddsförordningen. Uppdraget ingår i revisionsplanen för år 2017.

EU har i april 2016 beslutat om ett nytt regelverk för behandling av personuppgifter som ska börja tillämpas i medlemsstaterna i maj 2018. Den nya dataskyddsförordningen kommer att gälla som lag i samtliga medlemsstaterna och ersätter då tidigare nationell lagstiftning.

Mycket i dataskyddsförordningen liknar de regler som finns i personuppgiftslagen, men det är viktigt att poängtera att dataskyddsförordningen även innehåller stora förändringar och vissa helt nya bestämmelser. Den personuppgiftsansvariges ansvar och skyldigheter förtydligas och utökas och de registrerades rättigheter förstärks. De nya kraven kan komma att medföra stora förändringar i kommunernas verksamhet.

Det är viktigt att organisationerna redan påbörjat arbetet med hur de ska anpassa sig till dataskyddsförordningen. Det kan handla om att införa rutiner för att tillmötesgå dataskyddsförordningens utökade krav på öppenhet och de registrerades rättigheter. Dataskyddsförordningen lägger stor vikt vid den personuppgiftsansvariges skyldighet att kunna visa att förordningen följs, vilket kan medföra ökade krav på dokumentation. En anpassning till dataskyddsförordningen kommer att kräva att kommunerna ser över sin interna styrning och riktlinjer för hur personuppgifter hanteras.

Revisorerna har bedömt att det föreligger *risk* att verksamheterna inte har kommit tillräckligt långt i sina förberedelser, och ser det som *väsentligt* att detta område granskas.

2.1 Syfte och revisionsfråga

Syftet är att granska hur kommunen och kommunalförbundet har förberett sig inför införandet av dataskyddsförordningen i maj 2018.

Granskningen ska besvara följande revisionsfrågor:

- Har kommunen/kommunalförbundet identifierat vilka åtgärder som ska vidtas inför införandet av Dataskyddsförordningen?
- Finns en plan som på ett tillfredsställande sätt fastslår vilka åtgärder som ska vidtas?
- Finns ansvariga för införandeprocessen utsedda i kommunerna och kommunalförbundet?
- Är ekonomisk och personell resursåtgång identifierad?
- Är ansvarsfördelningen mellan kommunerna och kommunalförbundet klargjord på ett tydligt sätt?
- Utövar kommunstyrelsen i respektive kommun samt direktionen i kommunalförbundet uppsikt över införandeprocessen?

2.2 Avgränsningar

Granskningen omfattar kommunstyrelsens övergripande tillsyn i respektive kommun samt direktionens i Västra Mälardalens kommunalförbund och dess ansvar avseende anpassning till Dataskyddsförordningen.

2.3 Revisionskriterier

De kriterier som kommer att ligga till grund för bedömning och rekommendationer är:

- Kommunallagen 6 kap. 7 §
- Reglemente för intern kontroll
- Övriga tillämpbara interna beslut och arbetsordningar.

2.4 Ansvarig nämnd

Granskningen avser kommunstyrelsen i A

2.5 Projektorganisation/granskningsansvarig

Granskningen har genomförts av Jesper Wigh, med stöd av Karin Helin-Lindqvist, certifierad kommunal revisor.

Rapporten har saklighetsgranskats av kanslichef i Köpings och Arboga kommuner, utredare och ansvariga för förberedelsearbetet i Surahammars och Kungsörs kommuner och administrativ chef i Västra Mälardalens Kommunalförbund

2.6 Metod

Granskningen har genomförts via dokumentstudier och intervjuer med berörda tjänstemän och politiker.

3 Resultat av granskningen

3.1 Lagstiftningen

EU:s dataskyddslag utgjorde från 1995 en gemensam grund inom unionen, men som direktiv var det upp till varje land att realisera regelverket och tolka det. Den 25 maj 2018 får Sverige och övriga EU-medlemsländerna en ny gemensam lagstiftning, som ska ersätta den nuvarande personuppgiftslagen (PUL) i Sverige. Den nya lagstiftningen ska namnges dataskyddsförordningen (inom EU – GDPR – General Data Protection Regulation), och kommer bland annat att innebära nya och skarpare regler om hur företag, myndigheter och organisationer får behandla personuppgifter1. Förordningen kommer att ställa ytterligare och särskilda krav på organisationers hantering av personuppgifter samt att det kommer att bli betydligt mer kostsamt att bryta mot den nya lagstiftningen. I Sverige är det datainspektionen som ska se till att myndigheter, kommuner, företag och andra organisationer följer dataskyddsförordningen. Förordningen innehåller i allt 99 artiklar och Datainspektionen rekommenderar att man läser dessa tillsammans med de beaktandesatser (skäl) som hör till artikeln. I motsats till personuppgiftslagen måste företag i enlighet med dataskyddsförordningen meddela om den rättsliga grunden för behandling av personuppgifter och möjligheten att lämna klagomål till Datainspektionen om den registrerade menar att fel har begåtts.

Ett av syftena med dataskyddsförordningen är att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Förordningen har även mål om att frambringa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU så att det fria flödet av uppgifter inom unionen inte hindras. Detta uppfylls då genom att förordningen är direkt tillämplig i de skilda medlemsstaterna och att samma regler gäller inom hela unionen. Andra syften med att ta fram en ny dataskyddsförordning har varit att modernisera dataskyddsdirektivets regler från 1995 och att tillämpa dessa till det nya digitala samhället.

Myndigheter som inte sköter sig och som inte lever upp till förordningens krav kommer att bemöta större konsekvenser. Det kommer att införas möjligheter för tillsynsmyndigheten (Datainspektionen) att i vissa fall döma ut administrativa sanktionsavgifter. Hur sanktionsavgifterna kommer att se ut för myndigheter och den offentliga sektorn är upp till varje medlemsland att bedöma. I Sverige har Dataskyddsutredningen föreslagit att myndigheter ska kunna påläggas sanktionsavgifter som ska ligga mellan 10 och 20 miljoner kronor när en myndighet missköter sin behandling av personuppgifter. För företag gäller andra sanktionsavgifter (se dataskyddsförordningen art 83.4 och 83.6).

Som komplement till dataskyddsförordningen kommer medlemsstaterna att komplettera förordningen med nationell lagstiftning, bland annat Dataskyddslagen (SOU 2017:39).

[1] Med personuppgifter avses varje upplysning som avser en identifierad eller identifierbar fysisk person. Avgörande är att uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person.

Roller

Dataskyddsförordningen får en i vissa delar förändrad nomenklatur för de personer och organisationer som hanterar personuppgifter.

- Personuppgiftsansvarig – den organisation som bestämmer för vilka ändamål de registrerade uppgifterna ska behandlas och för vilket ändamål, exempelvis en nämnd. Den personuppgiftsansvarige måste se till att behandlingen sker i enlighet med dataskyddsförordningens samtliga bestämmelser. Dess personal får enbart behandla personuppgifter enligt de instruktioner som getts av den personuppgiftsansvarige.
- Personuppgiftsbiträde – är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den egna organisationen och får endast behandla personuppgifter enligt instruktioner från den personuppgiftsansvarige.
- Dataskyddsombud – myndigheter måste enligt dataskyddsförordningen utse ett dataskyddsombud. Dataskyddsombudets roll är att övervaka att organisationen följer dataskyddsförordningen samt att vara kontaktperson för de registrerade, personalen inom organisationen och datainspektionen. Ombudet har inget eget ansvar att organisationen följer förordningen.

3.2 Organisation

Arboga, Kungsör, Köping och Surahammars kommuner ingår i ett gemensamt kommunalförbund – Västra Mälardalens Kommunalförbund (VMKF). Förbundet ansvarar enligt förbundsordningen för de ingående kommunernas räddningstjänst. Surahammars kommun ingår dock inte i VMKF avseende räddningstjänsten. Förbundet ansvarar även för driftsfrågor, administrativ service samt konsultativ stödverksamhet inom följande områden:

- IT-drift och support, förvaltning
- Telefoni
- Löne- och pensionsadministration
- Ekonomiadministration
- Skanning
- Inköp och upphandling
- Arkiv
- Krisberedskap
- Personuppgiftsombud
- Bostadsanpassning och parkeringstillstånd

Surahammars kommun har endast lämnat över ansvaret för IT-drift och support, telefoni och inköp och upphandling och ansvarar därmed själv för övriga frågor.

VMKF har en IT avdelning som driftar, d.v.s. ser till att maskinvara, nätverk och program fungerar, medlemskommunernas IT-verksamhet.

Arboga, Kungsör och Köpings kommuner har anställt en gemensam IT-strateg med placering i Köping som kartlägger kommunernas system. I denna kartläggning ingår till viss del att se vilka system och register som hanterar personuppgifter. Enligt IT-

strategen har han bra kontroll på förekommande system och de personuppgifter som hanteras där, men sämre kontroll över register som upprättas i kommunerna och däri ingående personuppgifter.

3.2.1 Tjänstebilaga: PUL

Arboga, Kungsör och Köpings kommuner har enligt förbundsordningen avtal med förbundet avseende personuppgiftsombud. Förbundets lönechef har rollen som personuppgiftsombud för de tre kommunerna omfattande ca 10 % av en tjänst. PuL-ombudets roll och ansvar gentemot kommunerna regleras skriftligt. Av dokumentet framgår att personuppgiftsombudet ska vara kommunens resurs och stöd i arbetet med behandling av personuppgifter i enlighet med personuppgiftslagen och att Västra Mälardalens Kommunalförbund förbinder sig att tillhandahålla ett personuppgiftsombud. Det framgår även klart att respektive kommunal nämnd eller bolag fortfarande är personuppgiftsansvarig.

Av dokumentet framgår vilka som är kontaktpersoner från förbundets respektive kommunens, en kort beskrivning av den överenskomna tjänsten samt finansieringsprincip för tjänsten.

Av överenskommelsen framgår exempel på ombudets uppgifter, uppdrag och roll:

- Granska rutiner för behandling av personuppgifter
- Anmäla brister till personuppgiftsansvarig
- Föra förteckning över behandlingar (system och register)
- Utarbeta rutiner för den interna kontrollen och granskningen
- Se till att det finns administrativa och tekniska åtgärder för IT-säkerheten

Det fastslås särskilt att kommunen och VMKF under första kvartalet 2017 ska diskutera och besluta om åtgärder i samband med Dataskyddsförordningens ikraftträdande 2018.

3.2.2 Gemensam insats

VMKF har tillsammans med Arboga, Kungsör och Köpings kommuner enats om en gemensam insats för att förbereda kommunerna inför införandet av Dataskyddsförordningen.

Som ett led i förberedelserna inför införandet av Dataskyddsförordningen träffades VMKF och kommunerna samt en inbjuden specialist i maj 2017 för att ”få en ökad kunskap om den nya lagstiftningen, en gemensam nulägesbild vart vi befinner oss i arbetet, aktiviteter som bör genomföras innan lagstiftningen träder i kraft … skapa en tydlig rollfördelning inklusive ansvar och arbetsuppgifter för kommunerna och VMKF.”

Enligt minnesanteckningarna skickade VMKF under hösten 2016 ut personuppgiftsförteckningar, d.v.s. inventeringslistor över de IT-system och register som innehåller personuppgifter, till alla personuppgiftsansvariga för ifyllande. Dessa ska skickas tillbaka till VMKF. Vid mötestillfället hade häften av de personuppgiftsansvariga svarat.

I minnesanteckningarna anges att man bedömer att det kommer att krävas en heltidstjänst under perioden augusti -17 till maj -18 för att klara av det extra arbete som uppstår under införandet. Under förvaltningsfas efter införandet görs bedömningen att

det kommer att krävas mer än de 10 % av tjänst som finns avsatt i nuläget. Frågan om extra finansiering har inte lösts.

De medverkande kommunerna och kommunalförbundet enas om att skapa ett antal roller och att använda en gemensam terminologi för dessa.

- Personuppgiftsansvarig (styrelse/nämnd)
- Företrädare för personuppgiftsansvarig (förvaltningschef/VD)
- Dataskyddsombud KAK (f.d. PuL-ombud VMKF)
- Dataskyddssamordnare (inom resp. kommun)
- Dataskyddshandläggare inom resp. styrelse/nämnd (f.d. PuL-handläggare)

Vidare konstateras ett antal arbetsuppgifter som dataskyddsombudet respektive övriga roller ska ansvara för. På dataskyddsombudets roll ligger bland annat:

- Samordnar kommunernas arbete via kanslichefer
- Ta fram förslag på riktlinjer och rutiner/instruktioner
- Tar fram mallar
- Genomför enkäter, uppföljning, utvärdering
- Sammanställer register

Slutligen presenteras en lista över aktiviteter som bör genomföras för att uppnå en lägsta nivå, motsvarande dagens krav enligt PuL, samt vilken funktion som ansvarar för aktiviteten.

Intervjuer med företrädare för kommunerna respektive förbundet visar på en otydlighet var ansvaret för att de lista åtgärderna genomförs ligger. Förbundet anser sig oförmögna att leverera det som angetts i minnesanteckningarna om de inte får ytterligare medel. Kommunerna anser å sin sida att ansvarsfördelningen är tydlig och räknar med att förbundet levererar det de åtagit sig att göra.

3.3 Kommentar

Vi noterar att ansvaret för flertalet av de aktiviteter som listas i minnesanteckningarna från mötet i maj 2017 ligger på VMKF.

Frågan om finansiering av det extraarbete förberedelserna inför införandet har inte lösts. Detta leder till att del av arbetet i kommunerna avstannat i väntan på förbundets insatser.

Vi rekommenderar att frågan om behov av extra resurser löses snarast och att ansvaret för respektive åtgärd enligt åtgärdslistan klargörs.

4 Kommunernas/förbundets förberedelser inför införandet av Dataskyddsförordningen

4.1 Arboga kommun

Arboga kommun har i sina förberedelser utgått från minnesanteckningarna från mötet i maj 20170.

Enligt kanslichefen i Arboga kommun kommer man att använda sig av de roller och benämningar som beslutats om vid det tidigare nämnda mötet. Man har dock ännu inte genomfört själva namnbytet på rollerna. Kanslichefen har i kommunen utsetts till ansvarig från kommunens sida för förberedelser och implementering av de åtgärder som bedöms nödvändiga för att leva upp till de krav dataskyddsförordningen ställer.

Kommunen har i stora drag identifierat de åtgärder som kommer att krävas inför införandet av Dataskyddsförordningen. Denna kartläggning följer de aktiviteter som listades vid mötet i maj 2017. Exempelvis har en uppdatering av registerförteckningen gjorts och skickats till förbundet. Man har däremot inte tagit fram en plan för dessa åtgärder.

Kanslichefen anser att ansvarsfördelningen mellan kommunen och förbundet är klargjord i och med den dokumentation och de beslut som finns. Kommunen har inte fortsatt arbetet med förberedelser utan avvaktar förbundets fortsatta arbete. Frågan hålls levande och kommunen tar del av den information som publiceras, framförallt av SKL.

Information om det pågående arbetet har lämnats till kommunstyrelsen i de ekonomiska rapporter som lämnats, d.v.s. delårsrapporter, bokslut och budget. Ingen protokollförd information har lämnats till kommunstyrelsen, men uppfattningen hos de intervjuade är att kommunstyrelsen är informerad om att arbetet pågår.

4.1.1 Svar på revisionsfrågorna

Har kommunen identifierat vilka åtgärder som ska vidtas inför införandet av Dataskyddsförordningen?

Vår bedömning är att kommunen på ett övergripande plan har kartlagt de åtgärder som måste vidtas inför införandet av dataskyddsförordningen, men att mer detaljerade åtgärder kommer att behöva identifieras.

Finns en plan som på ett tillfredsställande sätt fastslår vilka åtgärder som ska vidtas?

Vår bedömning är att det inte finns en plan för åtgärderna. Den gemensamma aktivitetslistan anger varken prioriteringsordning eller tidsordning för aktiviteterna.

Finns ansvariga för införandeprocessen utsedda i kommunen?

Vår bedömning är att kommunen har utsett ansvariga för införandet och att dataskyddsombudet ska tillhandahållas av förbundet. Övriga roller i enlighet med minnesanteckningar är utsedda i kommunen.

Är ekonomisk och personell resursåtgång identifierad?

Vår bedömning är att kommunen inte har identifierat resursåtgång, vare sig för personella resurser eller ekonomiska resurser.

Är ansvarsfördelningen mellan kommunerna och kommunalförbundet klargjord på ett tydligt sätt?

Vår bedömning är att ansvarsfördelningen mellan förbundet och kommunerna formellt sätt är tydlig, men att tolkningen av fattade beslut skiljer sig åt. Vissa aspekter behöver klargöras ytterligare, ex. vis behovet av personuppgiftsbiträdesavtal mellan kommunen och förbundet.

Utövar kommunstyrelsen uppsikt över införandeprocessen?

Vår bedömning är att kommunstyrelsen inte utövar någon aktiv uppsikt över införandeprocessen. Kommunstyrelsen är informerad om att arbetet pågår och att politiska beslut kan komma behöva fattas.

4.1.2 Slutsats och bedömning

Vår sammanfattande bedömning är att Arboga kommun har brister i sina förberedelser inför införandet av dataskyddsförordningen.

Kommunen har inte fortsatt arbetet med att kartlägga nödvändiga åtgärder utan stannat vid den sammanställning som utförts gemensamt med förbundet och övriga kommuner.

Det finns inte heller någon plan för när åtgärderna ska vidtas, vem som är ansvarig eller resursåtgång.

Vår bedömning är att ansvarsfördelningen internt i kommunen är klargjord. Dock behöver ansvarsfördelningen mellan kommunen och förbundet klargöras ytterligare.

Utifrån vår granskning rekommenderar vi kommunstyrelsen att:

- Klargöra ansvarsfördelningen mellan kommunen och Västra Mälardalens Kommunalförbund avseende arbetsuppgifter i samband med införandet av dataskyddsförordningen.
- Säkerställa att arbetet med att kartlägga och implementera kommunens specifika åtgärder i samband med införandet av dataskyddsförordningen fortsätter.
- Klargöra resursåtgång, personell och ekonomisk, för de identifierade åtgärderna.
- Säkerställa att styrelsen håller sig informerad rörande det pågående arbetet kring införandeprocessen

4.2 Kungsörs kommun

Kungsörs kommun har satt samman en arbetsgrupp som dels ska arbeta inför införandet dataskyddsförordningen, men även arbeta mer långsiktigt för att öka kunskapen i hela kommunen. Arbetsgruppen samordnas av en central dataskyddssamordnare som även är kontaktperson gentemot dataskyddsombudet. Dataskyddssamordnaren utses av kommunchefen. Respektive förvaltning och bolag har dataskyddshandläggare vilka utsetts av förvaltningschef/VD och ingår i arbetsgruppen.

Arbetsgruppen har kartlagt aktiviteter och åtgärder som ska utföras av kommunen. Uppfattningen är att de gemensamma minnesanteckningarna mer tar sikte på gemensamma aktiviteter så dessa behöver kompletteras med kommunspecifika aktiviteter. En viktig åtgärd som kommunen identifierat är att kartlägga de system som *inte* driftas av IT-avdelningen. Viktiga frågor att besvara gäller frågor kring intrång och hur de ska hanteras.

Kartläggningen av åtgärder och aktiviteter har skett utifrån nuläget och anger utöver kommunens aktiviteter även förbundets åtgärder enligt minnesanteckningarna. Efter fortsatt arbete och kartläggning av medarbetarnas medvetenhet kring frågan kan nya åtgärder identifieras och planen behöva uppdateras.

Kommunen har inte full kontroll över kostnader för införandet. Det arbete som bedrivs i nuläget ligger inom verksamhetens ram, men extrainsatser kan kräva ytterligare resurser framgent.

Kungsörs dataskyddssamordnare anger att ansvarsfördelningen mellan kommunen och förbundet är tydligt angiven utifrån förbundsordningen och att dataskyddsombudets ansvar är tydligt fastlagt.

4.2.1 Svar på revisionsfrågorna

Har kommunen identifierat vilka åtgärder som ska vidtas inför införandet av Dataskyddsförordningen?

Vår bedömning är att kommunen på ett övergripande plan har kartlagt aktiviteter utifrån nuläget. Ytterligare arbete kommer att tillföra åtgärder.

Finns en plan som på ett tillfredsställande sätt fastslår vilka åtgärder som ska vidtas?

Enligt vår bedömning finns en plan där åtgärderna är översiktligt tidsatta.

Finns ansvariga för införandeprocessen utsedda i kommunen?

Vår bedömning är att kommunen har utsett ansvariga för införandeprocessen, både på kommuncentral och förvaltningsnivå.

Är ekonomisk och personell resursåtgång identifierad?

Enligt vår bedömning har inte kommunen identifierat vare sig ekonomisk eller personalmässig resursåtgång.

Är ansvarsfördelningen mellan kommunerna och kommunalförbundet klargjord på ett tydligt sätt?

Vår bedömning är att ansvarsfördelningen mellan förbundet och kommunen formellt sett är tydlig, men att tolkningen av fattade beslut skiljer sig åt. Vissa aspekter behöver klargöras ytterligare, ex. vis behovet av personuppgiftsbiträdesavtal mellan kommunen och förbundet.

Utövar kommunstyrelsen i kommunen uppsikt över införandeprocessen?

Vår bedömning är att kommunstyrelsen inte utövar någon aktiv uppsikt över införandeprocessen. Kommunstyrelsen är informerad om att arbetet pågår och att politiska beslut kan komma behöva fattas.

4.2.2 Slutsats och bedömning

Vår sammanfattande bedömning är att Kungsörs kommun har en relativt god kontroll över förberedelserna inför införandet av dataskyddsförordningen.

Kommunens arbetsgrupp har identifierat åtgärder som måste vidtas och tilldelat dessa en ansvarig. Vi ser dock att det saknas bedömning av personell och ekonomisk resursåtgång.

Vår bedömning är att ansvarsfördelningen internt i kommunen är klargjord. Dock behöver ansvarsfördelningen mellan kommunen och förbundet klargöras ytterligare.

Utifrån vår granskning rekommenderar vi kommunstyrelsen att:

- Klargöra resursåtgång, personell och ekonomisk, för de identifierade åtgärderna.
- Klargöra ansvarsfördelningen mellan kommunen och Västra Mälardalens Kommunalförbund avseende arbetsuppgifter i samband med införandet av dataskyddsförordningen.
- Säkerställa att styrelsen håller sig informerad rörande det pågående arbetet kring införandeprocessen

4.3 Köpings kommun

I Köpings kommun är kanslichefen ansvarig för kontakten mellan kommunen och VMKF.

Köping kommun köper tjänsten PuL-ombud av förbundet, reglerat i förbundsordning och basavtal.

Arbetet lokalt i kommunen med införandet av Dataskyddsförordningen påbörjades tidigt 2017. Kommunen har gjort en genomgång av samtliga system som hanterar personuppgifter. Vid genomgången uppdaterades informationen vid behov avseende exempelvis systemansvariga, om system har tillkommit etc. Den uppdaterade informationen lämnades sedan till VMKF.

Kommunen har skapat en lokal organisation i enlighet med minnesanteckningarna från mötet med VMKF i maj 2017, d.v.s. utsett dataskyddssamordnare och dataskyddshandläggare, samt klarlagt deras respektive roller och uppgifter. Man har även sammanställt en lista på övergripande nivå för kommunens respektive förbundets kommande arbete. Kanslichefen har informerat anställda i kommunen, bland andra nämndsekreterargruppen och vård- och omsorgsförvaltningen. Köpings kommun planerar en utbildning i egen regi för kommunens dataskyddshandläggare i slutet av februari. Enligt kommunen har en dialog förts med VMKF kring behovet av utbildning, men då återkoppling inte har skett genomför de utbildning på egen hand.

Information kring dataskyddsförordningen och den nya lagstiftningen lämnades till kommunens ledningsgrupp den 19 januari, där kommunens fortsatta krav på VMKF även diskuterades.

Kanslichefen har en dialog med kommunalrådet kring frågan om anpassning till dataskyddsförordningen. Det har inte kommit någon formell begäran från kommunstyrelsen att bli informerad i frågan och det har inte heller ännu fattats några beslut på politisk nivå. Kanslichefens uppfattning är att kommunstyrelsen vet att det pågår ett arbete inför införandet och att VMKF deltar i detta arbete.

4.3.1 Svar på revisionsfrågorna

Har kommunen identifierat vilka åtgärder som ska vidtas inför införandet av Dataskyddsförordningen?

Vår bedömning är att kommunen inte har identifierat ytterligare åtgärder utöver den aktivitetslista som togs fram vid mötet den 18 maj 2017.

Finns en plan som på ett tillfredsställande sätt fastslår vilka åtgärder som ska vidtas?

Vår bedömning är att kommunen inte har tagit fram en åtgärdslista för kommunens specifika åtgärder.

Finns ansvariga för införandeprocessen utsedda i kommunen?

Kommunen har utsedda ansvariga för det egna arbetet i kommunen. Organisationen följer det som gemensamt med VMKF och övriga kommuner fastlades i maj 2017.

Är ekonomisk och personell resursåtgång identifierad?

Vår bedömning är att vare sig ekonomisk eller personell resursåtgång är identifierad.

Är ansvarsfördelningen mellan kommunerna och kommunalförbundet klargjord på ett tydligt sätt?

Vår bedömning är att ansvarsfördelningen mellan förbundet och kommunerna formellt sätt är tydlig, men att tolkningen av fattade beslut skiljer sig åt. Kommunens uppfattning är att det gemensamma personuppgiftsombudet ska hålla samman arbetet för kommunerna och att förbundet har det största ansvaret.

Utövar kommunstyrelsen i kommunen uppsikt över införandeprocessen?

Vår bedömning är att kommunstyrelsen inte utövar någon aktiv uppsikt över införandeprocessen. Kommunstyrelsen är informerad om att arbetet pågår och att politiska beslut kan komma behöva fattas.

4.3.2 Slutsats och bedömning

Vår sammanfattande bedömning är att Köpings kommun brister i sina förberedelser inför införandet av dataskyddsförordningen.

Kommunen har inte identifierat kommunspecifika åtgärder inför införandet utan endast utgått från den gemensamma åtgärdslista som tagits fram. De identifierade åtgärderna har inte heller tidsatts, tilldelats en ansvarig eller resursbedömts.

Vår bedömning är att ansvarsfördelningen internt i kommunen är klargjord. Dock behöver ansvarsfördelningen mellan kommunen och förbundet klargöras ytterligare.

Utifrån vår granskning rekommenderar vi kommunstyrelsen att:

- Klargöra ansvarsfördelningen mellan kommunen och Västra Mälardalens Kommunalförbund avseende arbetsuppgifter i samband med införandet av dataskyddsförordningen.
- Säkerställa att arbetet med att kartlägga och implementera kommunens specifika åtgärder i samband med införandet av dataskyddsförordningen fortsätter.
- Klargöra resursåtgång, personell och ekonomisk, för de identifierade åtgärderna.
- Säkerställa att styrelsen håller sig informerad rörande det pågående arbetet kring införandeprocessen

4.4 Surahammars kommun

Surahammars kommun står utanför det gemensamma arbetet kring PuL-frågor i kommunalförbundet.

Kommunen har utsett en projektledare för införandet av Dataskyddsförordningen som arbetar med frågan på 50 %. Projektet har en tydlig ägare i kommunchefen samt en styrgrupp som utgörs av kommunledningsgruppen.

I projektet finns en projektgrupp där kommunens 4 nämnder samt kommunstyrelsen representeras av 13 personer.

Enligt planeringen kommer projektledaren att ta över ansvaret som dataskyddsombud för hela kommunen. I nuläget har tre nämnder samt kommunstyrelsen beslutat att projektledaren ska ta rollen som dataskyddsombud. Övriga projektdeltagare kommer att gå in i rollen som dataskyddssamordnare för sina respektive verksamheter. Projektledarens/dataskyddsombudets respektive projektdeltagarnas/dataskyddssamordnarnas ansvar och uppgifter har fastslagits.

Identifierade åtgärder har listats utifrån vilket område frågan gäller, vad som måste göras, hur det ska göras samt vem/vilka som är ansvariga. En omfattande projektplan har tagits fram som beskriver mål, förutsättningar, projektorganisation samt projektets faser.

Projektledaren anger att man i nuläget är i en kartläggningsfas för att skaffa sig en övergripande bild av de system och register som innehåller personuppgifter samt de behandlingar kommunen utför. Kartläggningen pågår och resultaten hanteras i systemet Draftit.

4.4.1 Svar på revisionsfrågorna

Har kommunen identifierat vilka åtgärder som ska vidtas inför införandet av Dataskyddsförordningen?

Vår bedömning är att kommunen har identifierat de åtgärder som måste vidtas för att kommunen ska leva upp till de krav som ställs i och med införandet av Dataskyddsförordningen. När nulägesbilden är klar ska åtgärder tas fram utifrån identifierade brister gentemot lagstiftningen.

Finns en plan som på ett tillfredsställande sätt fastslår vilka åtgärder som ska vidtas?

Vår bedömning är att projektet har tagit fram en tidsplan för inledningsfasen samt en grov tidsplanering för en ”åtgärdsfas” samt en ”Förankringsfas”/Implementering.

Åtgärder utifrån kartläggningen tas fram efter hand projektet fortskrider samt efter att kartläggningsfasen är färdig.

Finns ansvariga för införandeprocessen utsedda i kommunen?

Vår bedömning är att kommunen har tydligt utsedda ansvariga för införandeprocessen. Kommunen har en beslutad projektorganisation med projektägare, styrgrupp, projektledare samt projektgrupp.

Projektledarens respektive projektdeltagarnas ansvar i projektet är tydligt angivet i den dokumentation vi tagit del av.

Kommunövergripande delprojekt kan komma att sättas upp för vissa åtgärder som identifieras i kartläggningsfasen.

Är ekonomisk och personell resursåtgång identifierad?

Vår bedömning är att kommunen identifierat del av resursåtgången. Projektet har övergripande identifierat personell resursåtgång för kartläggningsfasen, men inte för de senare faserna i projektet. I och med att en åtgärdsplan tas fram efter kartläggningen kan en mer precis bedömning av resursåtgång göras.

Är ansvarsfördelningen mellan kommunerna och kommunalförbundet klargjord på ett tydligt sätt?

Vår bedömning är att ansvarsfördelningen mellan förbundet och kommunerna formellt sätt är tydlig, men att tolkningen av fattade beslut skiljer sig åt. Projektledaren anser att ansvarsfördelningen mellan förbundet och kommunen måste klargöras. Ett flertal frågor har redan dykt upp och kvarstår att lösa, exempelvis om personuppgiftsbiträdesavtal måste tecknas mellan kommunen och förbundet.

Utövar kommunstyrelsen i kommunen uppsikt över införandeprocessen?

Vår bedömning är att kommunstyrelsen inte utövar någon aktiv uppsikt över införandeprocessen. Kommunstyrelsen är informerad om att arbetet pågår och att politiska beslut kan komma behöva fattas.

4.4.2 Slutsats och bedömning

Vår sammanfattande bedömning är att Surahammars kommun har en god kontroll över förberedelserna inför införandet av Dataskyddsförordningen. En organisation med klart uttalade roller och ansvarsområden är satt på plats och arbetar aktivt med frågan.

Vissa frågor kring ansvarsfördelning mellan kommunen och förbundet kvarstår att reda ut, exempelvis frågan om personuppgiftsbiträdesavtal.

Utifrån vår granskning rekommenderar vi kommunstyrelsen att:

- Klargöra ansvarsfördelningen mellan kommunen och Västra Mälardalens Kommunalförbund avseende arbetsuppgifter i samband med införandet av dataskyddsförordningen.
- Säkerställa att styrelsen håller sig informerad rörande det pågående arbetet kring införandeprocessen

4.5 Västra Mälardalens Kommunalförbund

VMKF har utöver sin roll som utförare av delar av medlemskommunernas IT-verksamhet även eget ansvar som personuppgiftsansvarig för de personuppgifter man hanterar i den egna verksamheten.

Ansvaret för att förbereda verksamheterna inför införandet av Dataskyddsförordningen ligger i förbundet på respektive chef. Förbundets ledningsgrupp används som samordnande gruppering för arbetet där förberedelsearbetet är en stående punkt på ledningsgruppsmötena.

Förbundets lönechef är personuppgiftsombud för förbundet men även Arboga, Köping och Kungsörs kommuner. Diskussioner har förts kring hennes roll i det nya regelverket och om den är förenlig med kravet på dataskyddsombudets oberoende ställning.

Förbundet har kartlagt sin egen verksamhet och samtliga system och register där personuppgifter förekommer. Uppgifterna har lagts in i samma SharePoint register där kommunernas registerförteckningar finns. Det nuvarande registret följer Datainspektionens mall för hur registerförteckningar ska vara utformade. Ett nytt system för hantering av registerförteckningarna har upphandlats.

Utöver kartläggning av register har förbundet följt de åtgärder som listats i minnesanteckningarna från maj 2017. Man är fortfarande i en kartläggningsfas, men börjar få klarhet i vad som måste göras. En åtgärdsplan, som bygger på minnesanteckningarna, har tagits fram där respektive chef ansvarar för att åtgärderna genomförs.

Förbundets tjänstemän har konstaterat att förberedelserna och de nya reglerna kommer att medföra extrakostnader samt att det tar tid från övriga arbetsuppgifter. De intervjuade anser att förbundet genom minnesanteckningarna från maj 2017 äskat extramedel för att finansiera arbetet inför införandet. Kommuncheferna ska även vara informerade om behovet av extramedel, men att frågan inte är löst. Förbundet har alltså inte fått någon extrafinansiering utan måste lösa uppgifterna inom befintlig ram.

De intervjuade tjänstemännen från förbundet anser inte att ansvarsfördelningen mellan kommunerna och förbundet är klarlagd. Ansvarsfrågan avseende ”vem som driver vad” är enligt dem oklar i och med att kommunerna inte finansierat en heltidstjänst för att arbeta med frågan.

Direktionen har informerats om det pågående arbetet och kring innebörden av den nya lagstiftningen.

4.5.1 Svar på revisionsfrågorna

Har förbundet identifierat vilka åtgärder som ska vidtas inför införandet av Dataskyddsförordningen?

Vår bedömning är att förbundet på grundläggande plan identifierat de åtgärder som måste vidtas. Arbetet är i en kartläggningsfas vilket innebär att ytterligare åtgärder kan identifieras vartefter arbetet fortskrider.

Finns en plan som på ett tillfredsställande sätt fastslår vilka åtgärder som ska vidtas?

Vi bedömer att förbundets plan endast på ett övergripande plan fastslår vilka åtgärder som ska vidtas.

Finns ansvariga för införandeprocessen utsedda i kommunen?

Vår bedömning är att förbundet har tydligt utsedda ansvariga för arbetet.

Är ekonomisk och personell resursåtgång identifierad?

Den plan över åtgärder som krävs av förbundet inför införandet är inte tillräckligt detaljerad för att beskriva personell och ekonomisk resursåtgång.

Är ansvarsfördelningen mellan kommunerna och kommunalförbundet klargjord på ett tydligt sätt?

Vår bedömning är att ansvarsfördelningen mellan förbundet och kommunerna formellt sätt är tydlig, men att tolkningen av fattade beslut skiljer sig åt. Förbundet har inte signalerat att de inte haft möjlighet att utföra sina arbetsuppgifter enligt överenskommelserna på grund av bristande resurser, vilket medför oklarheter kring vem som i realiteten ansvarar för respektive åtgärd.

Utövar direktionen i förbundet uppsikt över införandeprocessen?

Vår bedömning är att direktionen inte utövar någon aktiv uppsikt över införandeprocessen. Direktionen är informerad om att arbetet pågår och att politiska beslut kan komma behöva fattas.

4.5.2 Slutsats och bedömning

Vår sammanfattande bedömning är att VMKF har en relativt god kontroll över förberedelserna inför införandet av dataskyddsförordningen. Förbundet har utsett ansvariga för arbetet och identifierat åtgärder.

Ansvarsfördelningen mellan medlemskommunerna och förbundet avseende gemensamma system och förbundets övergripande roll som ansvarig för IT-drift och personuppgiftsombud är däremot inte tydligt klargjord.

Utifrån vår granskning rekommenderar vi förbundsdirektionen att:

- Klargöra ansvarsfördelningen mellan Västra Mälardalens Kommunalförbund och medlemskommunerna avseende arbetsuppgifter i samband med införandet av dataskyddsförordningen.
- Säkerställa att arbetet med att kartlägga och implementera förbundets specifika åtgärder i samband med införandet av dataskyddsförordningen fortsätter.
- Klargöra resursåtgång, personell och ekonomisk, för de identifierade åtgärderna.
- Säkerställa att direktionen håller sig informerad rörande det pågående arbetet kring införandeprocessen

Arboga kommun, Kungsör kommun, Köping kommun, Surahammar kommun och VMKF
Granskning av förberedelser inför införandet av GDPR

2018-02-07

Jesper Wigh

Revisor/konsult

2018-02-07

KPMG AB

Karin Helin Lindkvist

Certifierad kommunal revisor