Revisionsrapport -Granskning av införande av dataskyddsförordningen - Yttrande
Ärende 12
KS 2018/185

2018-06-0511 | Dnr: KS 2018/185

Kommunstyrelsen

Svar på revisionsrapport: införandet av nya Dataskyddsförordningen

Förslag till beslut

Kommunstyrelsens beslut

Kommunstyrelsen beslutar att godkänna svaret på granskningsrapporten, enligt förslag.

Ärendebeskrivning

Under våren 2018 gjordes en granskning av kommunens införandearbete av den nya Dataskyddsförordningen, GDPR. Granskningen, som gjordes drygt två månader innan GDPRs ikraftträdande den 25 maj, fokuserade främst på tydliggörande av ansvarsfördelning och identifiering av nödvändiga insatser.

Redan vid granskningstillfället stod det klart att mycket av det som revisionen ställde frågor om skulle bli svårt att svara på, då de nationella riktlinjerna för hur GDPR ska tolkas inte var färdiga vid granskningstillfället. Dessutom var mycket kommunalt arbete redan påbörjat men, av naturliga skäl, inte färdigställt vid tiden för granskningen.

Trots dessa bakgrundsfaktorer har nu ett så tydligt svar som möjligt tagits fram avseende revisionens betänkligheter. Kommunens GDPR-projektgrupp vill dock understryka att kommunen har bedrivit ett bra införandearbete, där lagstiftningen uppfylldes mer än väl den 25 maj. Självklart är arbetet ännu inte färdigt, men den grundplattform som tagits fram under våren är mycket stabil och kommer underlätta kommunens fortsatta arbete med GDPR.

Revisionen identifierade vid granskningstillfället (daterat 16 april 2018) tre punkter där de önskade att kommunen förbättrade sitt införandearbete:

1. Säkerställa att nödvändiga anpassningar identifieras och genomförs inom ramen för alla verksamheters ansvarsområden och att dessa framgår av nämndernas riktlinjer

Att identifiera och genomföra nödvändiga anpassningar inom alla verksamheters ansvarsområden innan GDPR börjar gälla är nära på omöjligt, då många lagstiftningar (särskilt inom skolans och socialtjänstens områden) fortfarande väntar på anpassning i enlighet med dataskyddslagstiftningen. Detta innebär att nämndernas riktlinjer fortfarande är under uppbyggnad: inför ikraftträdandet av GDPR valde projektgruppen istället att ”punktmarkera” de områden där nödvändiga anpassningar krävdes akut, och att ta fram rutiner och stöddokument

Kommunstyrelsen
Hanna Sandberg
• Hanna.Sandberg@kavlinge.se

Kävlinge kommun
Kullagatan 2, 244 80 Kävlinge
046 - 73 90 00 • kommunen@kavlinge.se • www.kavlinge.se

för dessa.
Dessa rutiner och stöddokument innefattar bland annat rutin för mejlhantering, rutin för informering till registrerad, rutin för samtycken, rutin för behörighetskontroll, rutin för check and control, rutin för hantering av dokument inom skolans värld, rutin för hantering av personalärenden, samt rutin för utlämnande av handlingar med personuppgifter inom olika verksamheter. Efter framtagande har projektgruppen arbetat för att dessa rutiner och stöddokument ska bli kända och användas inom samtliga, berörda verksamheter.
Ambitionen är att under hösten inkorporera dessa rutiner/stöddokument i de övergripande riktlinjedokumenten, och att då förhoppningsvis kunna komplettera med de första nationella ”GDPR-standardiseringarna” som bör börja dyka upp ganska snart.
Sammanfattningsvis kan alltså sägas att nödvändiga anpassningar har identifierats, men att arbetet med att genomföra dessa – av naturliga skäl – inte kommer att vara färdigt inom det närmaste året.

2. Säkerställa att det genomförs regelbundna GDPR-kontroller på såväl övergripande som verksamhetskritisk nivå

Även detta arbete är svårt att säkerställa innan GDPR börjar gälla, av samma anledning som presenterades i svaret ovan: det är fortfarande oklart hur GDPR ska appliceras – och kontrolleras – inom många områden, varför det är svårt att sätta upp rutiner för regelbundna GDPR-kontroller.
Vissa kommunövergripande kontroller har dock redan fastställts: exempelvis kommer samtliga anställda som registerfört en behandling att få en begäran om granskning en gång om året, där de ska säkerställa att deras registerföring fortfarande stämmer. Denna kontroll sker automatiskt genom kommunens registerföringssystem.
Vidare kommer det också att skickas ut en påminnelse minst en gång om året per mejl (från Säkerhetsenhetens funktionsmejl), där de anställda uppmuntras att rensa mappar och mejlkorgar.
Kontroller på verksamhetsnivå är dock inte fastställda, även om alla verksamheter starkt uppmuntras att upprätta GDPR-kontrollrutiner. Verksamheterna är, såsom det ser ut idag, ganska ojämna i sina informationssäkerhetskontroller, där exempelvis Socialtjänsten redan har ett väletablerat kontrollförfarande i enlighet med Patientdatalagen, medan Miljö- och teknik inte är lika vana vid den här typen av kontroller. Medvetenhet om behovet av att öka mängden informationssäkerhetskontroller generellt finns dock både hos de anställda och hos deras chefer, vilket främst märks genom ett ökat antal frågor och diskussioner inom kommunen. I kommunens antagna GDPR-strategi finns också ett krav på att verksamheterna ska genomföra intern kontroll avseende GDPR/informationssäkerhet minst en gång vartannat år, gärna med fokus på den praktiska hanteringen av personuppgifter (exempelvis inkomna personuppgifter).

3. Säkerställa att ledamöterna får tillräcklig kunskap inom området

Det är svårt att definiera begreppet ”tillräckligt”, men projektgruppen har varit mycket transparanta gentemot politiken och regelbundet informerat om det arbete som pågått kring GDPR. Exempelvis har samtliga nämnder haft besök minst en gång av någon från projektgruppen, och alla förtroendevalda har fått två informationsmejl plus en länk till kommunens e-utbildning. Det har dessutom lagts upp information om kommunens hantering av personuppgifter på de förtroendevaldas sidor på Kavlinge.se. Således anser projektgruppen att de förtroendevalda har fått tillräcklig kunskap inom området.

Kommunkansliet

Elektroniskt godkänd av:
Mats Svedberg, kanslichef, 2018-08-21
Mikael Persson, kommundirektör, 2018-08-22

Beslutet ska skickas till
För kännedom

För verkställighet

Svar på Revisionsrapport: införandet av Dataskyddsförordningen

Ernst and Young identifierade vid granskningen (daterad 16 april 2018) tre punkter där de önskade att kommunen förbättrade sitt införandearbete för att säkerställa en tillräcklig beredskap den 25 maj:

1. Säkerställa att nödvändiga anpassningar identifieras och genomförs inom ramen för alla verksamheters ansvarsområden och att dessa framgår av nämndernas riktlinjer

Att identifiera och genomföra nödvändiga anpassningar inom alla verksamheters ansvarsområden *innan* GDPR börjar gälla och har gällt ett tag är nära på omöjligt, då många lagstiftningar (särskilt inom skolans och socialtjänstens områden) fortfarande väntar på anpassning i enlighet med dataskyddslagstiftningen. Detta innebär att nämndernas riktlinjer fortfarande är under uppbyggnad: inför ikraftträdandet av GDPR valde projektgruppen istället att ”punktmarkera” de områden där nödvändiga anpassningar krävdes akut, och att ta fram rutiner och stöddokument för dessa.

Dessa rutiner och stöddokument innefattar bland annat rutin för mejlhantering, rutin för informering till registrerad, rutin för samtycken, rutin för behörighetskontroll, rutin för check and control, rutin för hantering av dokument inom skolans värld, rutin för hantering av personalärenden, samt rutin för utlämnande av handlingar med personuppgifter inom olika verksamheter. Efter framtagande har projektgruppen arbetat för att dessa rutiner och stöddokument ska bli kända och använda inom samtliga, berörda verksamheter.

Ambitionen är att under hösten inkorporera dessa rutiner/stöddokument i de övergripande riktlinjedokumenten, och att då förhoppningsvis kunna komplettera med de första tydliga och nationella ”GDPR-standardiseringarna” som bör dyka upp ganska snart.

Sammanfattningsvis kan alltså sägas att nödvändiga anpassningar har identifierats, men att arbetet med att genomföra dessa – av naturliga skäl – inte kommer att vara färdigt inom det närmaste året.

2. Säkerställa att det genomförs regelbundna GDPR-kontroller på såväl övergripande som verksamhetskritisk nivå

Även detta arbete är svårt att säkerställa innan GDPR börjar gälla, av samma anledning som presenterades i svaret ovan: det är fortfarande oklart hur GDPR ska appliceras – och kontrolleras – inom många områden, varför det är svårt att sätta upp rutiner för regelbundna GDPR-kontroller.

Vissa kommunövergripande kontroller är dock redan fastställda: exempelvis kommer samtliga anställda som registerfört en behandling att få en begäran om granskning en gång om året, där de ska se till så att deras registerföring fortfarande stämmer. Detta sker automatiskt genom kommunens registerföringssystem.

Vidare kommer det också att skickas ut en påminnelse minst en gång om året per mejl (från Säkerhetsenhetens funktionsmejl), där de anställda uppmuntras att rensa mappar och mejlkorgar.

Kontroller på verksamhetsnivå är dock oklarare, även om alla verksamheter starkt uppmuntras att upprätta GDPR-kontrollrutiner. Verksamheterna är, såsom det ser ut idag, ganska ojämna i sina informationssäkerhetskontroller, där exempelvis Socialtjänsten redan har ett väletablerat kontrollförfarande i enlighet med Patientdatalagen, medan Miljö- och teknik inte är lika vana vid den här typen av kontroller. Medvetenhet finns dock både bland de anställda och hos deras chefer gällande att öka kontrollerna avseende informationssäkerhet generellt, vilket främst märks via ett ökat antal frågor och diskussioner. I kommunens antagna GDPR-strategi finns också ett krav att verksamheterna ska genomföra intern kontroll avseende GDPR/informationssäkerhet minst en gång vartannat år, vilket rimligtvis kommer efterlevas.

3. Säkerställa att ledamöterna får tillräcklig kunskap inom området

Det är svårt att definiera begreppet ”tillräckligt”, men projektgruppen har varit mycket transparanta gentemot politiken och regelbundet informerat om det arbete som pågått gällande GDPR: samtliga nämnder har haft besök minst en gång av någon från projektgruppen, alla förtroendevalda har fått två informationsmejl plus en länk till kommunens e-utbildning. Det har dessutom lagts upp information om kommunens hantering av personuppgifter på de förtroendevaldas sidor på Kävlinge.se. Således anser projektgruppen att de förtroendevalda har fått tillräcklig kunskap inom området – vad de sedan valt att ta till sig, är svårare att svara på.

Revisionsrapport 2018
Genomförd på uppdrag av revisorerna
April 2018

Kävlinge kommun

Granskning av införandet av dataskyddsförordningen

Building a better working world

Innehåll

1. Inledning

1.1. Bakgrund

Den 25 maj 2018 kommer den nya europeiska dataskyddsförordningen att ersätta den svenska personuppgiftslagen (PUL) och bli lag i Sverige. Förordningen innehåller regler om hur personuppgifter får behandlas av myndigheter. Det nya regelverket kan innebära stora förändringar för den kommunala verksamheten, vilket gör det angeläget med noggrann planering och förberedelse för anpassning till det nya regelverket. Det finns annars en risk att den enskildes personliga integritet kränks eller att kommunen tvingas betala sanktionsavgifter, om reglerna inte följs.

1.2. Syfte och revisionsfrågor

Granskningens syfte är att bedöma om kommunstyrelsen och nämnderna arbetar på ett ändamålsenligt sätt med planering och anpassningar inför införandet av den nya dataskyddsförordningen.

I granskningen besvaras följande revisionsfrågor:

- Har styrelsen/nämnden tydliggjort ansvaret? (T.ex. ansvar för förändringsarbete samt att utse dataskyddsombud och tydliggjort dennes roll och uppgifter).
- Har nödvändiga förändringar med anledning av införande av förordningen identifierats?
- Har nödvändiga anpassningar påbörjats i rimlig omfattning?
- Finns aktuella och ändamålsenliga rutinbeskrivningar för hur personuppgifter ska hanteras i verksamheterna?
- Har styrelsen/nämnderna informerat nyckelpersoner i verksamheterna om förändringarna och dess innebörd på ett tillräckligt sätt?

1.3. Genomförande

Granskningen grundas på intervjuer och dokumentstudier (se bilaga 1). Intervjuer har skett med kanslichef, säkerhetschef, säkerhetshandläggare och involverade tjänstemän från förvaltningsdelarna. Samtliga intervjuade har beretts tillfälle att sakgranska rapporten. Granskningen är genomförd februari – mars 2018.

2. Revisionskriterier

2.1. Dataskyddsförordningen

Dataskyddsförordningen blir, efter beslut i EU, svensk lag den 25 maj 2018 och ersätter därmed personuppgiftslagen (PUL) i Sverige. Dataskyddsförordningen reglerar, i likhet med PUL, grundläggande bestämmelser om enskildas rätt till skydd av personuppgifter. Att skydda enskildas grundläggande rättigheter och friheter kopplat till personuppgiftshantering är således ett av syftena med dataskyddsförordningen.

En stor del av bestämmelserna i dataskyddsförordningen överensstämmer med tidigare bestämmelser enligt PUL, men några viktiga förändringar finns. Nedan sammanfattas de huvudsakliga förändringarna för organisationer[1] i korthet.

- **Samtycke -** Dataskyddsförordningen bygger i stor utsträckning på aktivt samtycke till registrering. I förordningen ställs särskilda krav på hur samtycke ska lämnas, i synnerhet vid behandling av känsliga personuppgifter (såsom uppgifter om hälsa eller religiös åskådning). Den som behandlar personuppgifter måste kunna visa att giltigt samtycke har lämnats av den som har registrerats.

- **Ökade rättigheter -** Enligt dataskyddsförordningen har den registrerade rätt att när som helst begära att få sina uppgifter raderade, med undantag för om det föreligger någon rättslig grund för behandlingen. Undantagsfall kan uppstå i de fall organisationen som hanterar personuppgifter behöver dessa för exempelvis bokföringsändamål. Med tanke på de ökade kraven som ställs på att de registrerade enkelt ska kunna få sina uppgifter raderade bör organisationen enligt Datainspektionen se över rutiner gällande hur en sådan begäran hanteras.

- **Dataportabilitet** – när uppgifter behandlas med stöd av samtycke eller för att uppfylla ett avtal, ska den registrerade ha rätt att få ut de uppgifter som lämnats för att överföra dem till en annan tjänst.

- **Konsekvensbedömning** – innan man planerar en ny personuppgiftsbehandling, vilken innebär särskilda risker för den registrerade, ska en bedömning göras av vilka konsekvenser behandlingen kan få och vilka åtgärder som behövs för att minska risker för den enskilde.

- **Anmälan om personuppgiftsincident** – vid händelse av säkerhetsincident, exempelvis dataintrång eller oavsiktlig förlust av uppgifter, måste det anmälas till Datainspektionen inom 72 timmar. Vid risk för exempelvis id-stöld eller bedrägeri kan de personer vars personuppgifter berörs behöva informeras.

- **Dataskyddsombud** – vissa organisationer, myndigheter eller andra former som behandlar känsliga uppgifter, eller är involverade i särskilt riskfylld behandling av personuppgifter, måste utse en person i organisationen som har som särskild uppgift

[1] Dataskyddsförordningen gäller i princip inom all slags verksamhet och oavsett vem som utför personuppgiftsbehandlingen. Den gäller således för företag, föreningar, organisationer, myndigheter och privatpersoner. I detta avsnitt används begreppet organisation, vilket även innefattar kommuner.

att bevaka dataskyddsfrågor – ett dataskyddsombud. Ombudet har bland annat till uppgift att utföra kontroller och informationsinsatser. Ombudet ska vara väl insatt i de lagar som gäller för personuppgiftsbehandling.

- **”Missbruksregeln” försvinner** – När dataskyddsförordningen träder ikraft kommer den så kallade missbruksregeln inte längre finnas kvar. Missbruksregeln innebär att man idag kan använda enklare regler för personuppgifter i ostrukturerat material, exempelvis information om personer i e-post, på internet eller i en enkel lista som man har i datorn. När missbruksregeln försvinner innebär det att samma regler som gäller för personuppgifter i databaser och ärendehanteringssystem, också ska användas för det som skrivs om personer i exempelvis e-post och på webbplatser.

- **Sanktionsavgift** – vid brytande mot förordningens regler kan Datainspektionen ålägga en sanktionsavgift. Avgiftens storlek är bland annat beroende av hur allvarlig överträdelsen är, om det skett avsiktligt eller inte samt vilka åtgärder som vidtagits för att minska skadan. Vid mindre förseelser riskerar den som bryter mot förordningen ett påpekande eller föreläggande om eventuella brister. Anses brottet däremot vara allvarligare, eller om organisationen anses ovillig att vidta nödvändiga åtgärder, riskeras böter upp till 20 miljoner euro eller 4 % av företagets/organisationens eller moderbolagets globala omsättning.

2.2. Datainspektionens vägledning

Datainspektionen är tillsynsmyndighet när det gäller kommunernas hantering av personuppgifter. Enligt Datainspektionens vägledning behöver kommunerna bl.a. förbereda sig inför Dataskyddsförordningens ikraftträdande på följande vis:

- Försäkra sig om att beslutsfattare och nyckelpersoner inom organisationen är medvetna om att personuppgiftslagen kommer att ersättas av dataskyddsförordningen. Undersöka hur organisationen kommer att påverkas av förordningen och identifiera de områden som de måste arbeta särskilt med.

- Inventera och dokumentera vilka personuppgifter som hanteras, hur de samlas in och till vem uppgifterna lämnas ut. Göra en bred översyn för att ta reda på vilka uppgifter som hanteras inom de olika delarna av organisationen.

- Undersöka om verksamheten har utnyttjat personuppgiftslagens undantag för att behandla personuppgifter i ostrukturerat material, den så kallade missbruksregeln. Denna regel kommer inte att finnas kvar i förordningen. Undersöka särskilt om behandling som idag stödjer sig på missbruksregeln är förenlig med dataskyddsförordningens bestämmelser.

- Granska den information som lämnas till de registrerade och fundera över vilka förändringar av den informationen som kan bli nödvändig att göra.

- Se över rutiner för att säkerställa att alla rättigheter som de registrerade har enligt dataskyddsförordningen kan uppfyllas, som exempelvis hur personuppgifter raderas och hur uppgifter lämnas ut elektroniskt i ett allmänt använt format.

- Undersöka vilka olika typer av uppgifter som behandlas och med vilket rättsligt stöd detta görs. Dokumentera slutsatserna.

- Undersöka på vilket sätt samtycke inhämtas, vilken information som lämnas och hur uppgiften om att samtycke har lämnats av den registrerade sparas.

- Fundera på hur kontroll av en persons ålder ska göras och hur vårdnadshavares samtycke inhämtas i samband med behandling av barns personuppgifter online.

- Se till att det finns tillräckliga rutiner på plats för att upptäcka, rapportera och utreda personuppgiftsincidenter.

- Fundera på om personuppgiftsbehandlingen är förenad med särskilda risker för enskildas fri- och rättigheter och om det i så fall behöver göras en konsekvensbedömning avseende dataskydd.

- Ta hänsyn till dataskyddsförordningens regler när nya IT-system tas fram eller befintliga förändras. Det ger en större möjlighet att följa reglerna, höja säkerheten och förhindra onödiga framtida kostnader.

- Bestämma var i organisationen som ansvaret för dataskyddsfrågor ska ligga. Utse ett dataskyddsombud.

3. Granskningsresultat

3.1. Ansvar och roller

Kommunstyrelsen och nämnderna har utsett en central projektgrupp som består av sex tjänstemän från kommunkansliet och förvaltningsdelarna. Projektgruppen ansvarar för den övergripande implementeringen av förändringsarbetet som ska göras inför dataskyddsförordningens ikraftträdande. Det finns en struktur för hur arbetet ska genomföras som bygger på de tre delarna; dokument, utbildning och struktur i organisationen.

- Dokument: strategi för hantering, riktlinjer och stöddokument
- Utbildning: fysiska utbildningar, obligatorisk e-learning, besöka alla verksamheters arbetsplatsträffar
- Struktur: dataskyddsombud, informationssäkerhetssamordnare, implementera visionen om ”inbyggt dataskydd” på verksamhetsnivå

Kommunens säkerhetschef har förordnats till dataskyddsombud av kommunstyrelsen och samtliga nämnder vid deras sammanträden under februari och mars 2018. Av intervjuerna framkom att informationssäkerhetssamordnare ska utses inom varje nämnd och kommunstyrelsen. Detta ska ske vid deras sammanträden under april 2018. Informationssäkerhetssamordnaren ska ansvara för att alla verksamheter inventerar och anmäler sina behandlingar av personuppgifter.

Kommunstyrelsen, genom säkerhetsenheten, ansvarar för att ta fram strategier, rutiner och mallar för arbetet. Varje nämnd ansvarar för att genomföra inventering och registrering av personuppgifter samt att de ska upprätta egna styr- och/eller stöddokument som de anser att de är i behov av. Enligt de intervjuade finns det inom varje nämnd egna projektgrupper med representanter från de olika delverksamheterna. Arbetet som sker i nämnderna följs upp i den centrala projektgruppen.

Det framkom vid intervju att projektgruppen försöker ta höjd för den annalkande politiska omorganisationen. Det pågående arbetet inför lagens ikraftträdande utgår dock från den befintliga organisationen.

3.2. Strategi för hantering av dataskyddsförordningen

Kommunen har tagit fram en strategi för hantering av dataskyddsförordningen, dokumentet är daterat 8 februari 2018. Enligt tidplanen ska strategin antas i kommunstyrelsen den 25 april 2018. Dokumentet fastställer att alla verksamheter där kommunen har ett huvudmannaansvar är bundna av strategin. Strategins syfte är att ange hur kommunen ska säkerställa allmänna dataskyddsförordningens krav och villkor. Strategins mål är att alla verksamheter där kommunen har ett huvudmannaansvar ska ha förståelse för hur förordningen ska implementeras i den specifika verksamheten. Strategin beskriver vad den nya förordningen kommer att innebära för kommunen, t.ex. att konsekvensbedömningar måste göras innan nya behandlingar av personuppgifter sker, samt att ”missbruksregeln” försvinner. Den beskriver de allmänna säkerhetskraven som ställs på kommunen att utforma sina IT-system, sin IT-användning och sina rutiner enligt principen om inbyggt dataskydd och dataskydd som standard.

Strategin anger att kommunstyrelsen och nämnderna är fristående personuppgiftsansvariga. Detta innebär att kommunstyrelsen och nämnderna ansvarar för att säkerställa att behandling av personuppgifter inom den egna nämnden sker i enlighet med lagstiftningen och

kommunens styrdokument. Det anges också att det är personuppgiftsansvarig som ansvarar för att meddela tillsynsmyndigheten vid personuppgiftsincident. Enligt strategin ska varje nämnd upprätta Riktlinjer för hantering av Allmänna Dataskyddsförordningen, som beskriver den praktiska implementeringen. Strategin fastställer att samtliga nämnder ska utse minst en informationssäkerhetssamordnare, samt vilken roll och ansvar samordnaren ska ha. Dataskyddsombudets roll och ansvar är också formulerat. Dataskyddsombudet ska agera rådgivande åt nämnderna, hjälpa till vid konsekvensbedömningar, på ett övergripande plan övervaka efterlevnaden av dataskyddsförordningen samt vara kontaktperson mot tillsynsmyndigheten.

Enligt strategin ska personer vars personuppgifter blir behandlade av kommunen få information om var personuppgifterna finns lagrade, vilka personuppgifter som avses, hur personuppgifterna lagras, samt vem den registrerade kan kontakta för frågor gällande lagringen av personuppgifter. Informationen ska förmedlas på ett sätt att den registrerade förstår och den registrerade ska få information om vilka rättigheter den enskilde har gentemot kommunen. Strategin klargör allmänna principer för behandling av personuppgifter och skäl för behandling av personuppgifter. Därtill anges hur utlämnade av personuppgifter ska ske och att vid en ny behandling av personuppgifter som innebär hög risk[2] för de registrerade ska den föregås av en konsekvensbedömning. I strategin beskrivs även vad konsekvensbedömningen ska innehålla.

Av strategin framgår även när anmälan om personuppgiftsincident ska ske till tillsyns-myndigheten och vad anmälan ska innehålla. Vidare anges att kommunen har ett gemensamt registerföringssystem för att registerföra behandling av personuppgifter men att det är varje personuppgiftsansvarigs ansvar att registerföra de behandlingar som förekommer inom varje nämnd. Personuppgiftsansvarige ansvarar för att kunna göra registret tillgängligt för tillsynsmyndigheten.

Strategin tar upp de tre verksamheter som kommunen delar med andra kommuner och därmed har kommungemensamma behandlingar av personuppgifter. För att säkerställa att personuppgifter hanteras på ett korrekt sätt inom dessa verksamheter ska personuppgiftsbiträdesavtal upprättas mellan kommunernas kommunstyrelser. Strategin hanterar även frågan om personuppgiftsbiträden i övrigt och att avtal ska upprättas med dessa parter.

Uppföljning och kontroll regleras också i strategin. Uppföljning ska ske av det interna arbetet och vilka rutiner som ska följas upp i verksamheterna ska beskrivas i nämndernas egna riktlinjer. I strategin anges att specifik uppföljning av ett område inom förordningen kan göras genom intern kontroll, samt att denna form av intern kontroll bör göras minst vartannat år. I strategin anges att kommunrevisionen regelbundet bör följa upp kommunens efterlevnad av dataskyddsförordningen, minst vart femte år, på en kommunövergripande nivå.

Enligt strategin ska alla nyanställda i kommunen genomgå en utbildning samt genomföra ett test vid anställningen, som säkerställer att den anställda förstått kommunens ansvar enligt

[2] Hög risk är definierat som:

a) En stor mängd personuppgifter behandlas, och då särskilt om dessa är känsliga personuppgifter
b) Många olika typer av personuppgifter behandlas, och då särskilt om dessa är känsliga personuppgifter
c) Flera olika personer har tillgång till personuppgifterna
d) Personuppgifterna berörs av delvis eller helt automatiserad behandling (exempelvis systematisk kamera/övervakning, samkörning av register eller bakgrundsgranskning)
e) Personuppgifterna rör personer som av något skäl befinner sig i underläge eller beroendeställning

dataskyddsförordningen. Samtliga kommunanställda ska därefter regelbundet uppdatera sina kunskaper genom ett liknande test, fortbildningen ska ske minst en gång vartannat år. Dataskyddsombudet och informationssäkerhetssamordnarna ska fortbildas minst en gång varje år eller vid behov.

Systemägarna ska säkerställa att IT-systemet följer principerna om inbyggt dataskydd och dataskydd som standard även efter utveckling/inköp av system. Det framgår av strategin att det till stor del är upp till alla anställda att se till att förhålla sig till dataskyddsförordningen i det operativa arbetet. Exempelvis att anställda som använder IT-system ska uppmärksamma om något inom IT-systemet verkar bryta mot förordningen och principerna om inbyggt dataskydd och dataskydd som standard samt att samtliga anställda ansvarar för att regelbundet och konsekvent radera den information som inte längre uppfyller sitt syfte.

Kommunens strategi ska följas upp vid behov men minst en gång vartannat år. Ansvarig för uppföljning är säkerhetsenheten.

3.3. Riktlinjer, rutiner och mallar

Nedanstående dokument har arbetats fram av kommunkansliet som ska användas av samtliga nämnder:

- **Riktlinjer för hantering: Allmänna dataskyddsförordningen**

  Dokumentet följer i stort strategins struktur, men ska göras nämndspecifik för att passa varje nämnds egna verksamheter, system och kontroller som behöver göras. Vid granskningens genomförande har ingen nämnd ännu fastställt sin riktlinje. Enligt tidplanen ska samtliga nämnder ha antagit sin riktlinje senast 4 april 2018.

- **Rutin för hantering av personuppgiftsincidenter**

  Rutinen anger att personuppgiftsincidenter ska anmälas till Datainspektionen inom 72 timmar. Rutinen beskriver tillvägagångssättet samt att den/de registrerade som har blivit drabbade av personuppgiftsincidenten ska informeras så snart som möjligt efter att personuppgiftsincidenten är upptäckt.

- **Incidentrapporteringsmall för personuppgiftsincidenter**

  Mallen är till för samtliga verksamheter att använda vid rapportering av personuppgiftsincidenter. I rapporten ska bland annat incidenten beskrivas, hur incidenten upptäcktes, vad den berodde på, vilka åtgärder som har vidtagits för att motverka negativa konsekvenser, hur många registrerade som är drabbade. Rapporten ska lämnas till nämndens informationssäkerhetssamordnare som därefter skickar den vidare till dataskyddsombudet.

- **Rutin för inventering**

  Rutinen beskriver hur inventeringar ska genomföras. Inventeringarna avser behandlingar av personuppgifter inför registrering i iFacts[3], ostrukturerat material[4], avtal och arbetsplatsen och dess IT-system. I inventeringsarbetet ska medarbetarna också fundera över säkerheten i behandlingen, hur denna kan förbättras av dem själva och av verksamheten i stort. Säkerheten innefattar både IT-säkerheten (den tekniska) och den organisatoriska säkerheten (exempelvis rutiner för att låsa in material, gallringsrutiner med mera).

- **Registerförteckningsguide – GDPR**

  En guide som ska bistå medarbetare när de ska fylla i registerföringsformuläret för personuppgiftsbehandlingar enligt dataskyddsförordningen. Guiden består av frågor och är indelade i fem delar; allmänt, om personuppgifterna, säkerhetsåtgärder, personuppgiftsincidenter och personuppgiftbiträde.

Av intervjuerna framkom att det finns ett par dokument som är planerade att upprättas på central nivå som ska gälla för all verksamhet. Dessa är:

- Hjälp vid konsekvensbedömning
- Mall för personuppgiftsbiträdesavtal

3.4. System och information på hemsidan

Det framkom även att två system är inköpta för att fungera som stöd i arbetet, det ena är iFacts och det andra är Draftit[5]. Alla personuppgiftsbehandlingar ska vara i registerföringssystemet innan den 25 maj. Dataskyddsombudet och informationssäkerhetssamordnarna kommer att vara primära användare i systemen, övriga medarbetare ska genom en e-tjänst inkomma med de behandlingar som ska registerföras.

Vidare framkom att arbetet med att ta fram information om dataskyddsförordningen till hemsidan har påbörjats, och ska vara publicerat den 24 maj enligt tidplanen. Informationen ska ge medborgare vägledning om processen samt deras möjligheter att få fram uppgifter som kommunen behandlar.

3.5. Utbildning

Utbildningar sker på olika sätt. Två fysiska utbildningstillfällen är planerade att genomföras, ett i mars och ett i april, för medarbetare som kontinuerligt kommer i kontakt med personuppgifter. Enligt de intervjuade kommer cirka 200 av kommunens anställda delta vid dessa tillfällen. Därtill ska samtliga anställda genomföra ett obligatoriskt e-learningtillfälle mellan den 16 mars och 18 maj. Utbildningen nås via kommunens intranät, och efter genomförd kurs ska ett test genomföras varefter medarbetaren får ett diplom som intygar att hen har klarat av kursen. Kursen ska också genomföras av samtliga nyanställda under introduktionstiden. Det framkom av intervjuerna att vid behov kommer även spetsutbildningar för vissa yrkeskategorier att

[3] iFacts är ett informationshanteringssystem som bl.a. kan användas för inventering och mappning av GDPR datakällor, processorer och IT-resurser inklusive GDPR klassificering och kategorisering.
[4] Ostrukturerad behandling av personuppgifter innefattar alla behandlingar som görs slentrianmässigt eller i form av extra arbetsstöd; det vill säga i listor, löptexter, minnesanteckningar och liknande.
[5] Draftit är ett system som stötta verksamheter med regelefterlevnaden av dataskyddslagstiftningen på både svensk och EU-nivå (GDPR). Verktygen i Draftit kan användas för att kartlägga, registrera och administrera behandlingar av personuppgifter i en så kallad registerförteckning.

genomföras under samma period som e-learningen. Dessa utbildningstillfällen är dock inte planerade vid granskningens genomförande.

Kunskapsöverföring ska utöver utbildningstillfällena ske genom att representanter från projektgruppen – både den kommuncentrala och de nämndcentrala – besöker samtliga verksamheter och ledningsgrupper för att berätta om den nya dataskyddsförordningen och vad den innebär för kommunen.

Av intervjuerna framkom också att det finns vissa verksamheter som är i behov av extra stöd. Verksamheter som lyftes fram är HR, IT och vissa verksamheter inom socialtjänsten och skolan. Utmaningarna för dessa verksamheter är dels att det finns olika typer av personuppgiftsbehandling dels att de även påverkas av speciallagstiftning som styr verksamheterna. I detta avseende finns ett fortsatt behov av att identifiera vad som behöver kompletteras kompetensmässigt. Genom leverantören Draftit har kommunen tillgång till en juristfunktion som kan bistå med rådgivning till exempelvis dessa verksamheter.

Ledamöter i kommunstyrelsen och nämnderna har informerats om den nya förordningen via e-post. De har även erbjudits att delta i e-utbildningen som är obligatorisk för medarbetarna. En informationsfilm som är framtagen av Sundsvalls kommun kommer att visas vid sammanträdena i april, då även informationssäkerhetssamordnarna ska antas.

4. Bedömning

Vår bedömning är att ansvarsfördelningen är tydlig. Det framgår av strategin att respektive verksamhet är fristående personuppgiftsansvarig, vilket innebär att kommunstyrelsen och nämnderna ansvarar för att säkerställa att behandling av personuppgifter inom den egna nämnden sker i enlighet med lagstiftningen och kommunens styrdokument. Vidare anser vi att det är ändamålsenligt att en central projektgrupp har tillsatts för att bedriva förändringsarbetet som krävs inför lagens ikraftträdande. Projektgruppen har arbetat fram en strategi som vi anser beskriver de nödvändiga förändringarna med anledning av införandet av förordningen, även om den till stor del avser den kommunövergripande nivån.

Vidare bedömer vi att nödvändiga anpassningar har påbörjats på kommunövergripande nivå. Vi grundar bedömningen på att ett dataskyddsombud har utsetts av respektive nämnd och därtill planeras att respektive nämnd ska utse en informationssäkerhetssamordnare. Förutsatt att nödvändiga anpassningar identifieras i verksamheterna, att arbetet med att ta fram samt fastställa nämndspecifika riktlinjer färdigställs enligt tidplanen, bedömer vi även detta som ändamålsenligt.

Vi har också tagit del av rutinbeskrivningar för hur personuppgifter ska hanteras i verksamheterna, vilka vi anser vara tillräckliga. Det är även positivt att rutiner, guider och mallar har upprättats på central nivå och ska gälla för hela den kommunala organisationen.

Vi kan konstatera att styrelsen och nämnderna har planerat för att informera nyckelpersoner och övriga medarbetare i verksamheterna om förändringarna och dess innebörd inför ikraftträdandet. Vi kan även konstatera att styrelsen/nämnderna har informerats via e-post samt blivit erbjudna att delta i e-utbildningen. Ett sätt att säkerställa att ledamöterna tillskansar sig tillräcklig kunskap om dataskyddsförordningen skulle vara att göra e-utbildningen obligatorisk även för dem.

Den sammantagna bedömningen är att kommunstyrelsen och nämnderna arbetar på ett ändamålsenligt sätt med planeringen inför införandet av den nya dataskyddsförordningen. Vår bedömning grundar sig på att de har identifierat nödvändiga förändringar, vilka framgår av strategin, samt att upprättandet av riktlinjer, rutiner och mallar till stor del har påbörjats.

Kommunen har dock inte påbörjat det praktiska arbetet, som exempelvis avser att registerföra behandling av personuppgifter och gallra befintligt material som innehåller personuppgifter, vilket kan leda till tidspress då arbetet ska vara klart vid förordningens ikraftträdande. Även om det finns en tidplan som anger att arbetet ska vara klart till den 25 maj, framgår det inte vilka personalresurser som ska genomföra arbetet.

Revisionsfrågor	Svar
Har styrelsen och nämnderna tydliggjort ansvaret?	Ja, kommunstyrelsen och nämnderna har utsett ett dataskyddsombud. Dataskyddsombudet är kommunens säkerhetschef. Dataskyddsombudet roll och ansvar är reglerat i strategin som avser den nya förordningen.
Har nödvändiga förändringar med anledning av införande av förordningen identifierats?	Ja, det framgår av strategin och tidplanen för implementeringen att nödvändiga åtgärder har identifierats.
Har nödvändiga anpassningar påbörjats i rimlig omfattning?	Delvis, strategin är klar men ännu inte fastställd politiskt, riktlinjerna är under framtagande och utbildningar har påbörjats. Vidare är en mall för personuppgiftsbiträdesavtal under framtagning och

	register för behandling ska påbörjas. Arbetet med att uppdatera informationen på hemsidan ska också ha påbörjats. Det har framgått att strukturen för arbetet är under uppbyggnad men att det praktiska arbetet har påbörjats i liten utsträckning vilket leda till tidspress för att kommunen ska hinna klart med verkställandet av åtgärderna till den 25 maj.
Finns aktuella och ändamålsenliga rutinbeskrivningar för hur personuppgifter ska hanteras i verksamheterna?	Delvis, arbetet kring rutiner har påbörjats men de framtagna rutinerna är på kommunövergripande nivå. Det finns ett fortsatt behov av att ta fram rutiner på verksamhetsnivå.
Har styrelsen/nämnderna informerat nyckelpersoner i verksamheterna om förändringarna och dess innebörd på ett tillräckligt sätt?	Delvis, en e-learningkurs ska genomföras av samtliga medarbetare och två fysiska utbildningstillfällen har planerats in. Det finns verksamheter som behöver extra stöd i arbetet, och i detta avseende saknas en plan för hur de ska få det stöd som behövs.

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen och nämnderna att:

- säkerställa att nödvändiga anpassningar identifieras och genomförs inom sina respektive verksamheter och att dessa framgår av riktlinjerna som ska antas politiskt,
- säkerställa att det genomförs regelbundna kontroller på såväl övergripande som verksamhetsnivå inom ramen för GDPR, samt
- säkerställa att ledamöterna får tillräcklig kunskap inom området.

Kävlinge den 16 april 2018

Negin Nazari
EY

Sara Shamekhi
EY

Bilaga 1: **Källförteckning**

Intervjuade:

- Mats Svedberg, kanslichef
- Björn Andersson, säkerhetschef tillika dataskyddsombud
- Hanna Sandberg, säkerhetshandläggare tillika informationssäkerhetssamordnare för kommunstyrelsen
- Rolf Perleij, administrativ chef tillika informationssäkerhetssamordnare för miljö & teknik
- Anna Hyberg, IT-strateg tillika informationssäkerhetssamordnare för bildningsnämnden

Medverkat vid intervjuerna:

- Fernando Dinis Viseu, förtroendevald revisor
- Dietmar Olbrich, förtroendevald revisor
- John Axel Persson, förtroendevald revisor

Dokument:

- Strategi för hantering: Allmänna dataskyddsförordningen
- Riktlinjer för hantering: Allmänna dataskyddsförordningen (mall för verksamheten)
- Rutin för hantering av personuppgiftsincidenter
- Incidentrapporteringsmall för personuppgiftsincidenter
- Rutin för inventering
- Registerförteckningsguide- GDPR
- Tidplan