Granskning av rutiner för efterlevnad av dataskyddsförordningen

Revisionsrapport
Tranemo kommun

KPMG AB

2021-07-08

Antal sidor 24

Tranemo kommun
Granskning av rutiner för efterlevnad av dataskyddsförordningen

2021-07-08

Innehållsförteckning

1 Sammanfattning

Vi har av Tranemo kommuns revisorer fått i uppdrag att granska kommunens rutiner för efterlevnad av dataskyddsförordningen. Dataskyddsförordningen trädde ikraft den 25 maj 2018 och är gällande ramverk för behandling av personuppgifter. Den nya lagstiftningen syftar bl.a. till ett starkare skydd för individers integritet och större makt till att kunna bestämma över sina personuppgifter.

Bristande hantering samt överträdelser kan innebära betydande sanktionsavgifter till skillnad från tidigare lagstiftning. En bristande hantering av personuppgifter riskerar också leda till förtroendeskador för kommunen.

Sammanfattningsvis kan konstateras att det finns väsentliga brister vad avser efterlevnaden av dataskyddsförordningen. Utifrån ett tydligt behov av stödjande insatser har rapporten utformats på ett vägledande sätt i vissa delar.

Vi bedömer det som positivt att kommunstyrelsen samt kommunstyrelseförvaltningen har varit lyhörda för genomförd granskning och har påbörjat ett förbättringsarbete efter genomförd granskning.

Mot bakgrund av vår granskning bedömer vi att följande delar bör ses över:

- Kommunstyrelsen har inom ramen för sin uppsiktsplikt ett ansvar att följa upp huruvida verksamheterna inom nämnder och kommunala bolag efterlever dataskyddsförordningen. I syfte att uppnå en enhetlig kunskapsnivå samt en enhetlig hantering inom kommunen erfordras en central styrning från kommunstyrelsens sida vada avser utbildningsinsatser samt framtagande av ändamålsenliga styrdokument.

- Dokumentation av personuppgiftsincidenter är obligatorisk, där samtliga incidenter ska dokumenteras samt risk- och konsekvensbedömas **oaktat allvarlighetsgrad**. Vi bedömer att dokumentationen av personuppgiftsincidenter inte är på en tillfredställande nivå.

- Sannolikheten att flertalet sektioner/nämnder inte har haft någon form av person-uppgiftsincident alternativt har endast 1-2 fall sedan lagens ikraftträdande är låg, där vi bedömer att bristande kunskapsnivå i kombinationen med avsaknad av centrala rutiner samt en central styrning är bakomliggande faktorer. Vi anser att det finns ett behov av kunskapshöjande insatser inom förvaltningarna samt personal ute i verksamheterna vad avser **identifiering, risk- och konsekvensbedömning** och **dokumentation** av personuppgiftsincidenter.

- Vi anser att kommunövergripande styrdokument i form av rutinbeskrivningar av större vikt för verksamheterna samt av juridisk betydelse, bör utöver återgivning på intranätet, även finnas i en formaliserad form med angivet datum för upprättande samt beslutsinstans.

- Vi bedömer att den kommunövergripande rutinen avseende hantering av person-uppgiftsincidenter behöver revideras vad avser den praktiska hanteringen vid upptäckt av en incident. Detta i syfte att förmedla en korrekt hantering samt underlätta för medarbetarna genom en samlad och distinkt tillvägagångsbeskrivning, (se sid. 14).

- Efter genomförd granskning har en mall arbetats fram för dokumentation av personuppgiftsincidenter. Vi har i samband med faktagenomgången granskat framtagen mall där det finns en del brister. Mallen behöver revideras samt kompletteras i syfte att uppfylla lagens krav samt säkerställa en ändamålsenlighet (se avsnitt 3.7 för närmare vägledning).
Utifrån erfarenheten att viktiga delar kan utebli när interna mallar upprättas, rekommenderar vi kommunstyrelsen att använda sig av tillsynsmyndighetens dokumentationsmall i sin helhet. Detta säkerställer att samtliga nödvändiga delar enligt lagstiftningen upptas. Vidare leder det till en effektivisering i form av minskad administration, där dokumentation av en incident inte behöver ske två gånger vid de tillfällen där en incident behöver skickas vidare till Integritetsskyddsmyndigheten.

- Vi bedömer att det är centralt att dataskyddsombuden genomför **interna granskningar** av kommunstyrelsens, nämndernas samt de kommunala bolagens arbete med dataskyddsförordningen i syfte att få fram åtgärdsbehoven.

- Resultatet av dataskyddsombudens granskningar ska återkopplas till berörd sektion, nämnd eller bolagsstyrelse. Granskad sektion, nämnd, bolag bör efter genomförd granskning återkomma med en åtgärds-/handlingsplan till dataskyddsombuden inom fastställd tidsram. Vidare bör resultatet av granskningarna redogöras för kommunstyrelsen utifrån styrelsens uppsiktsplikt.

- Vi anser att dataskyddsombuden bör sammanställa en **årlig lägesrapport** över statusen av styrelsers och nämndernas arbete vad avser efterlevnad av dataskyddsförordningen. Denna redogörelse görs lämpligen i samband med årsbokslutet och delges kommunstyrelsen och kommunfullmäktige.

- Utifrån befintliga risker rekommenderar vi att ett urval av kontrollmål med sikte på efterlevnad av dataskyddsförordningen tillförs de årliga internkontrollplanerna. Exempel på aktuella kontrolmål är dokumentation av personuppgiftsincidenter, risk- och konsekvensbedömningar, korrekt upprättade registerförteckningar, de registrerades rättigheter mm.

- Vi bedömer att det finns ett behov av ett krafttag vad avser upprättande av registerförteckningar, där det idag finns brister. Vi anser att nämnderna bör utse ansvariga för upprättande och underhåll av registerförteckningar följt av riktade utbildningar för denna kategori av personal. Alternativt att det inrättas centrala funktioner som hanterar registerförteckningarna.

- Vi bedömer antalet registerförteckningar vara för få i förhållande till de verksamhetsområden som hanteras, framförallt vad gäller omsorgssektionen samt lärandesektionen. Härigenom bör samtliga verksamheter genomföra en inventering, där det säkerställs att förteckningar upprättas för samtliga personuppgiftsbehandlingar.

-Förbättringsarbetet avseende registerförteckningarna behöver komma igång snarast då det har flutit alltför lång tid sedan lagens ikraftträdande. Det bör framhållas att oaktat den praktiska/organisatoriska hanteringen är det respektive nämnd/ styrelse som ansvarar för att säkerställa att det finns registerförteckningar för samtliga personuppgiftsbehandlingar samt att dessa är korrekt upprättade. Kommunstyrelsen har dock inom ramen för sin uppsiktplikt ett ansvar att följa upp samtliga nämnders och bolagens arbete vad avser efterlevnaden av dataskyddsförordningen.

- Kommunstyrelsen bör upprätta en kommunövergripande rutinbeskrivning avseende hanteringen av inkomna begäran om rättelse, radering och begränsning.

2 Inledning

Vi har av Tranemo kommuns revisorer fått i uppdrag att granska kommunens rutiner för efterlevnad av dataskyddsförordningen.

Dataskyddsförordningen trädde ikraft den 25 maj 2018 och är gällande ramverk för behandling av personuppgifter. I och med ikraftträdandet av dataskyddsförordningen, (GDPR), upphävdes personuppgiftslagstiftningen, (PuL 1998:204). Den nya lagstiftningen syftar bl.a. till ett starkare skydd för individers integritet och större makt till att kunna bestämma över sina personuppgifter. Härigenom ska både offentliga och privata verksamheter anpassa hanteringen av personuppgifter till gällande regler inom ramen för Dataskyddsförordningen.

Bristande hantering samt överträdelser kan innebära betydande **sanktionsavgifter** till skillnad från tidigare lagstiftning. Likaså riskerar en bristande hantering av person-uppgifter leda till **förtroendeskador** för kommunen som helhet samt personuppgiftsansvariga nämnder och styrelser.

Med anledning av ovanstående har kommunens revisorer dragit slutsatsen i sin riskanalys, att kommunens rutiner avseende efterlevnad av dataskyddsförordningen behöver granskas.

2.1 Syfte och revisionsfråga

Rapporten syftar till att granska kommunens övergripande rutiner för efterlevnad av dataskyddsförordningen. Följande avser rapporten besvara:

- Finns det ett centralt utsett dataskyddsombud?
- Befinner sig dataskyddsombudet i en oberoendeposition?
- Har samtliga nämnder beslutat om att utse ett dataskyddsombud?
- Har kommunstyrelsen säkerställt att det finns registerförteckningar över personuppgiftsbehandlingar i enlighet med artikel 30.1, dataskydds-förordningen?
- Har dataskyddsombudet genomfört kontroller av registerförteckningarna?
- Är registerförteckningarna korrekt upprättade utifrån dataskydds-förordningens grundläggande principer? (Ändamålsbeskrivning, rättslig grund för behandling, personuppgiftsansvarig, kategorier av personuppgifter, förekomst av känsliga personuppgifter, mottagare intern och externt, dokumentation om förekomst av överföring av personuppgifter sker till tredje land, personuppgiftsbiträden, tidsfrister för radering, beskrivning av tekniska och organisatoriska säkerhetsåtgärder m.m.)
- Finns rutiner för incidentrapporteringar?

- Hur många incidentrapporter har inkommit sedan lagens ikraftträdande?
- Har det genomförts någon riskbedömning av incidenterna och hur många har kategoriserats som allvarliga?
- Har incidenter som bedömts medföra allvarliga risker för den registrerades integritet anmälts till Integritetsskyddsmyndigheten (f.d. Datainspektionen)?
- Finns dokumenterade rutiner för begäran om registerutdrag?
- Finns dokumenterade rutiner för rättelse av uppgifter?
- Finns dokumenterade rutiner för radering av uppgifter?
- Är dataskyddsförordningens olika delar samt efterlevnad av dessa upptagits i den årliga internkontrollplanen i form av kontrollmål?

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

- Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.
- Riktlinjer från European Data Protection Board, (Europeiska dataskyddsstyrelsen)
- Interna riktlinjer/policys.

2.3 Metod

Granskningen har genomförts genom:

- Studium och genomgång av relevanta styrdokument och beslutsunderlag.
- Granskning och analys av registerförteckningar avseende personuppgifts-behandlingar.
- Intervjuer och avstämningar med t.f. kanslichef tillika planeringschef, ordinarie kanslichef tillika kommunjurist, dataskyddsombud samt kommunstyrelsens ordförande.

Rapporten har faktakontrollerats av kanslichefen.

3 Resultat av granskningen

Nedan följer resultatet av granskningen. I ett vägledande syfte samt tydliggörande de kriterier som vi har granskat mot, föregås avsnitten av sammanfattande beskrivningar av gällande lagstiftning.

3.1 EU-rättslig lagstiftning

Dataskyddsförordningen trädde ikraft den 25 maj 2018 och är gällande ramverk för behandling av personuppgifter. I och med ikraftträdandet av dataskyddsförordningen, (GDPR), upphävdes personuppgiftslagstiftningen, (PuL 1998:204). Den nya lagstiftningen syftar bl.a. till ett starkare skydd för individers integritet och större makt till att kunna bestämma över sina personuppgifter. Härigenom ska både offentliga och privata verksamheter anpassa hanteringen av personuppgifter till gällande regler inom ramen för dataskyddsförordningen.

Bristande hantering samt överträdelser kan innebära betydande **sanktionsavgifter** till skillnad från tidigare lagstiftning. Likaså riskerar en bristande hantering av person- uppgifter leda till **förtroendeskador** för kommunen som helhet samt personuppgifts- ansvariga nämnder och styrelser.

Hantering av personuppgifter ska ske utifrån förordningens grundläggande principer enligt följande:

- Laglighet
- Korrekthet
- Öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Riktighet
- Lagringsminimering
- Integritet och konfidentialitet
- Ansvarsskyldighet

Vid behandling av personuppgifter måste verksamheterna stödja sig på en så kallad ”**rättslig grund**”. Utan en rättslig grund är personuppgiftsbehandling ej laglig.

Vidare ska styrelsen och nämnderna utse ett dataskyddsombud, (DSO), som bl.a. har till uppgift att övervaka efterlevnaden av dataskyddsförordningen.

3.2 Dataskyddsombud

Dataskyddsförordningen, artikel 37.1, fastställer att ett dataskyddsombud, (DSO) ska utses i följande tre fall:

a) Behandlingen genomförs av en myndighet eller ett offentligt organ.

b) Den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning.

c) Den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter och personuppgifter som rör fällande domar i brottmål och överträdelser.

3.3 Dataskyddsombudets uppdrag

Enligt dataskyddsförordningen, artikel 39 ska dataskyddsombudet ha minst följande uppgifter:

- Att **informera och ge råd** till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar skyldigheter enligt dataskyddsförordningen.

- Att **övervaka och kontrollera efterlevnaden** av dataskyddsförordningen.

- Att **övervaka och kontrollera efterlevnaden** av den personuppgiftsansvariges eller personuppgiftsbiträdets **strategi för skydd** av personuppgifter, inbegripen ansvarstilldelning, **information till och utbildning av personal** som deltar i behandling och **tillhörande granskning.**

- Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den.

- Att samarbeta med tillsynsmyndigheten.

- Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, och vid behov samråda i alla andra frågor.

Det framhålls samtidigt att arbetet som dataskyddsombud ställer höga krav vad avser **integritet** och **hög yrkesetik**.

Vad gäller erforderlig kompetens fastställer dataskyddsförordningen att ett dataskyddsombud ska utses på grundval av **yrkesmässiga kvalifikationer** och i synnerhet sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra ovan nämnda uppgifter.

3.4 Dataskyddsombud och oberoende, Tranemo kommun

Dataskyddsombudets främsta uppdrag är att **systematiskt arbeta och övervaka efterlevnaden** av dataskyddsförordningen samt agera **rådgivande.**

Det är av vikt att dataskyddsombudet befinner sig i en **oberoendeposition**, där vederbörande ska kunna arbeta självständigt och fullgöra sina uppgifter på ett oberoende sätt. Detta innebär att personuppgiftsansvariga eller personuppgifts-biträden exempelvis inte får instruera dataskyddsombudet om vilka resultat som bör uppnås, hur ett klagomål ska hanteras eller att inta en viss ståndpunkt i ärenden som rör dataskyddslagstiftningen. Som exempel kan nämnas att det inte är lämpligt att ett dataskyddsombud sitter i organisationens ledning eller är delaktig i att fatta strategiska beslut om kärnverksamheten.

Iakttagelser

Tranemo kommun ingår i en samverkan vad avser tjänsten som dataskyddsombud. Aktuell tjänst köps av Boråsregionen Sjuhärads kommunalförbund. Vid tid för granskningen finns två dataskyddsombud som hanterar sju kommuner inom ramen för samverkan.

3.4.1 Kommentarer och bedömning

Vid tid för granskningen befinner sig dataskyddombuden organisatoriskt sett i en oberoendeposition.

3.5 Utnämning av dataskyddsombud

Samtliga personuppgiftsansvariga[1] ska utse ett dataskyddsombud. Beslutet ska dokumenteras och vara protokollfört.

Iakttagelser

Vi har tagit del av samtliga nämnders beslut avseende utnämning av dataskyddsombud förutom krisledningsnämnden.

3.4.1 Kommentarer och bedömning

Granskningen visar att samtliga nämnder förutom krisledningsnämnden formellt har utsett ett dataskyddsombud.

3.6 Personuppgiftsincidenter, risk- och konsekvensbedömning, dokumentation och anmälan

En **personuppgiftsincident är** en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna innebär närmare att individer:

[1] Personuppgiftsansvarig är respektive nämnd och styrelse.

Dataskyddsförordningen, (artikel 33, punkt 1), fastställer att vid en personuppgifts-incident ska den personuppgiftsansvarige utan onödigt dröjsmål och inte senare än **72 timmar** efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig. I Sverige är det Integritetsskyddsmyndigheten (f.d. Datainspektionen) som är behörig tillsynsmyndighet.

Den **registrerade ska informeras** om personuppgiftsincidenten **utan onödigt dröjsmål**, om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter (artikel 34, punkt 1).

De personuppgiftsincidenter som **inte bedöms medföra risker** för individers rättigheter och friheter behöver ej anmälas till tillsynsmyndigheten. Därav är det av vikt att ansvarig nämnd/styrelse genomför en **konsekvensanalys** vid eventuella incidenter i syfte att bedöma allvarlighetsgraden.

Samtliga personuppgiftsincidenter ska **dokumenteras oaktat allvarlighetsgrad**.

EU-rätten fastställer vidare att i de fall där organisationen har anlitat ett personuppgiftsbiträde, (PuB), ska personuppgiftsbiträdet underrätta den personuppgiftsansvarige (dvs. nämnd/styrelse), utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident, (artikel 33, punkt 2).

Iakttagelser

Vi har delgivits en kommunövergripande rutinbeskrivning vad avser hantering av av personuppgiftsincidenter i form av ett urklipp från kommunens intranät. Vid tid för granskningen finns ingen kommunövergripande mall för dokumentation av person-uppgiftsincidenter.

Vi har begärt in en redogörelse för antal upptäckta personuppgiftsincidenter samt dokumentation kopplad till respektive incident inom samtliga nämnder. Nedan redogörs för antal personuppgiftsincidenter per nämnd.

Figur 3.5.1

Kommunstyrelsen	Antal incidenter 2018	Varav anmälda till DI	Antal incidenter 2019	Varav anmälda till DI	Antal incidenter 2020	Varav anmälda till DI	Antal incidenter t.o.m. juni 2021	Varav anmälda till IMY
Omsorgssektionen	0	0	2	1	2	1	0	0
Lärandesektionen	0	0	2	0	2	0	1	0
Tekniska sektionen	0	0	0	0	1	0	0	0
Samhällsutvecklings-sektionen	0	0	0	0	0	0	1	0
Servicesektionen (Ekonomi, personal, medborgarservice, KLK)	0	0	0	0	1	0	1	1
Nämnder								
Överförmyndarnämnd	0	0	0	0	0	0	0	0
Valnämnd	0	0	0	0	0	0	0	0
Krisledningsnämnd	0	0	0	0	0	0	0	0
Samverkansnämnd personal	0	0	0	0	0	0	0	0

3.6.1 Kommentarer och bedömning

Dokumentation av personuppgiftsincidenter är obligatorisk, där den personuppgiftsansvarige ska dokumentera samtliga personuppgiftsincidenter inbegripet:

- **omständigheterna** kring incidenten,
- **risker och effekter** samt
- de **korrigerande åtgärder** som har vidtagits.

Detta innebär att respektive personuppgiftsansvarig ska genomföra en risk- och konsekvensbedömning följt av en tydlig dokumentation. Det bör noteras att en hantering som strider mot dataskyddsförordningen kan leda till **sanktionsavgifter** samt **förtroendeskador** för Tranemo kommun.

Vi anser att kommunövergripande styrdokument i form av rutinbeskrivningar av större vikt för verksamheterna samt av juridisk betydelse, bör utöver återgivning på intranätet, även finnas i en formaliserad form med angivet datum för upprättande samt beslutsinstans.

Vid tid för granskningen saknas en kommunövergripande dokumentationsmall för personuppgiftsincidenter, vilket vi bedömer vara en väsentlig brist. Som tidigare nämnts är dokumentation av samtliga incidenter obligatorisk. Dokumentationen ska bl.a. göra det möjligt för tillsynsmyndigheten att vid behov kontrollera efterlevnaden av hantering av personuppgiftsincidenter. Kommunstyrelsen har ett ansvar för framtagande av kommunövergripande styrdokument i syfte att bl.a. skapa en **enhetlig hantering** inom kommunen vad avser efterlevnad av dataskydds-förordningen.

Vi har vid tid för granskningen föreslagit att tillsynsmyndighetens dokumentations-mall används i sin helhet. Detta säkerställer att samtliga nödvändiga delar enligt lagstiftningen upptas. Vidare leder det till en effektivisering i form av minskad administration, där dokumentation av en incident inte behöver ske två gånger vid de tillfällen där en incident behöver skickas vidare till Integritetsskyddsmyndigheten. Minimering av antalet mallar underlättar för medarbetarna samt leder till en ökad verkställighet.

Vi bedömer att den kommunövergripande rutinen avseende hantering av person-uppgiftsincidenter behöver revideras vad avser den praktiska hanteringen vid upptäckt av en incident. Detta i syfte att förmedla en korrekt hantering samt underlätta för medarbetarna genom en samlad och distinkt tillvägagångsbeskrivning. Idag är beskrivningen spretig och inte ändamålsenlig till sin struktur, vilket kan skapa viss förvirring hos medarbetarna och som i sin tur riskerar leda till en minskad verkställighetsgrad.

Rutinbeskrivningen bör ange en tydlig **roll- och ansvarsfördelning** i syfte att på ett enkelt sätt konkretisera ”**vem gör vad**” vid upptäckt av en incident. Här bör funktioner/ titlar klargöras vad avser ansvaret för ifyllande av dokumentations-/anmälningsmallen. Det är av vikt att klargöra huruvida det är närmaste chef eller eventuell utsedd GDPR-samordnare/informationssäkerhetshandläggare inom förvaltningen som ska kontaktas i ett första steg när en anställd upptäckter en incident.
Vidare bör det framgå att dokumentationsmallen bör ifyllas tillsammans med utsedd ansvarig inom sektionen/nämnden. Detta i syfte att minimera riskerna för **inkonsekventa bedömningar** samt **intressekonflikter** i samband med risk- och konsekvensbedömningar som i sin tur avgör huruvida incidenten ska till tillsyns-myndigheten samt huruvida incidenten ska rapporteras till den registrerade (i det här fallet den drabbade).

Det bör framhållas att det är personuppgiftsansvarig nämnd som ansvarar för bedömning och hantering av personuppgiftsincidenter, men vi rekommenderar att samråd alltid sker med dataskyddsombudet i de fall det råder en osäkerhet kring risk- och konsekvensbedömningen. Vidare rekommenderar vi att samtliga incidenter kommer till dataskyddsombudets kännedom.

Vi rekommenderar att redan i början av rutinbeskrivningen klargöra att samtliga ska **dokumenteras oaktats allvarlighetsgrad** och **oaktat om incidenten ska anmälas till IMY eller ej**. På så sätt uppstår inga tveksamheter avseende dokumentationskravet.

Vidare bör det i rutinbeskrivningen finnas en hänvisning samt länk till en fastställd kommunövergripande mall för dokumentation av inträffade incidenter.

Rutinbeskrivningen kan den med fördel klargöra **vilken information som ska ges till den registrerade** vid en incident som medför en hög risk för de registrerades rättigheter och friheter. Väsentliga delar är:

- en klar och tydlig beskrivning av incidenteten,
- kontaktuppgifter till dataskyddsombudet samt den person som är insatt i ärendet,
- beskrivning av sannolika konsekvenser av incidenteten samt
- åtgärder som har vidtagits följt av beskrivning av insatser som har genomförts för att mildra konsekvenserna.

Denna information som en del i det kommunövergripande styrdokumentet minimerar riskerna med olikartade tillämpningar i verksamheterna vid de fall där den registrerade ska informeras.

3.7 Kommunövergripande dokumentationsmall, personuppgifts-incidenter

Iakttagelser

I samband med faktaavstämningen har det framkommit att kommunstyrelseförvaltningen har efter vår granskning arbetat fram en kommunövergripande dokumentationsmall för personuppgiftsincidenter. Detta bedöms som positivt. Vi har begärt in den framtagna dokumentationsmallen, där vi har noterat vissa brister. Med anledning av detta har ett nytt avsnitt (3.7), tillförts granskningen i syfte att vägleda kommunstyrelsen, där mallen behöver revideras samt kompletteras.

3.7.1 Kommentarer och bedömning

Vi bedömer att framarbetad mall behöver revideras samt utvecklas enligt nedanstående punkter, i syfte att säkerställa en ändamålsenlighet samt uppfylla gällande föreskrifter vad avser hantering av personuppgiftsincidenter.

- Av mallen ska personuppgiftsansvarig nämnd/styrelse framgå.

- I mallen efterfrågas vilken kategori av personuppgifter som incidenten avser, vilket är korrekt och ska finnas med i en incidentsdokumentation. Dock finns en rubrik med benämningen ”**Harmlösa personuppgifter**”, där rubriken **behöver tas bort**, då det inte är förrän en genomförd risk- och konsekvensbedömning som en viktning samt bedömning av effekt och påverkan kan göras. En sådan rubrik kan leda till misstolkningar samt felbedömningar som kan leda till allvarliga konsekvenser för de registrerade.

- frågan om ”*vilken säkerhet det fans för personuppgifterna*” bör kompletteras med flera svarsalternativ som på ett tydligt sätt klargör huruvida uppgifterna i **sin helhet** eller i **vissa delar var krypterade** alternativt **inte var krypterade** vid tid för incidenten.

- **Beskrivning av incidenten** är obligatorisk, där incidenten och omständigheterna ska återges på ett tydligt sätt. Detta framgår inte av framtagen mall.

- **Beskrivning av vidtagna åtgärder** är obligatorisk, där åtgärderna ska beskrivas på ett tydligt sätt. Detta framgår inte av framtagen mall.

- Tillsynsmyndighetens sex svarsalternativ vad avser förtydligande av **typ av incident** bör tillföras mallen (obehörigt röjande genom felaktigt utskicka av mail/brev/sms, övriga typer av obehörigt röjande, obehörig åtkomst, förlust, förstöring, ändring.)

- en fråga om ”*varför har incidenten inträffat*” bör tillföras mallen. Detta i syfte att kunna kartlägga behov av att förändra arbetssätt, rutiner mm., agera förebyggande samt vidta lämpliga åtgärder.

- vid förekomst av en incident som hanteras av ett **personuppgiftsbiträde** ska uppgifterna till berörd leverantör anges.

- som tidigare nämnts ska **samtliga inträffade incidenter genomgå en risk- och konsekvensbedömning**. Denna del är central för bedömning av incidentens allvarlighetsgrad och därmed dess påverkan och effekt på den registrerade. Det är genom en risk- och konsekvensbedömning som personuppgiftsansvarig nämnd/ styrelse kan avgöra huruvida incidenten ska inrapporteras till tillsynsmyndigheten samt huruvida den registrerade ska informeras. Dokumentation avseende denna del saknas och bör tillföras till mallen omgående.

En incident ska bedömas utifrån följande allvarlighetsgrader kopplad till den registrerades integritet:

1. Obetydlig
2. Begränsad
3. Betydande
4. Mycket allvarligt

- Ytterligare central del som saknas i mallen är huruvida den registrerade ska informeras om incidenten. Den **registrerade ska informeras** om en person-uppgiftsincident **utan onödigt dröjsmål**, om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Av dokumentations-underlaget ska det framgå **huruvida den registrerade har informerats** samt **när i tid**. Likaså ska bedömningen att **inte informera den registrerade motiveras**. Denna del bör tillföras mallen omgående.

Som vägledning kan delar av den nationella tillsynsmyndighetens mall redogöras:

Följande frågor ska besvarats i en anmälan till IMY:

1. Har ni informerat de registrerade om incidenten?

2. När informerade ni de registrerade?

Vid ett ”Nej-svar” på ovanstående frågor behöver följande redogöras:

3. Kommer ni att informera de registrerade?

4. När kommer ni att informera de registrerade?

Vid ett ”Nej-svar” på ovanstående frågor behöver följande fråga besvaras:

5. Varför kommer ni inte att informera de registrerade?

Utifrån erfarenheten att viktiga delar kan utebli när interna mallar upprättas, rekommenderade vi kommunstyrelsen i samband med intervjuerna att använda sig av tillsynsmyndighetens dokumentationsmall i sin helhet. Vår tidigare rekommendation kvarstår.

3.8 Antal personuppgiftsincidenter

Iakttagelser

Som tidigare nämnts i avsnitt 3.5 har vi begärt in en redogörelse för antal upptäckta personuppgiftsincidenter sedan lagens ikraftträdande, inom samtliga nämnder, (se tabell sid. 12).

3.8.1 Kommentarer och bedömning

Vad avser omfattningen av incidenter, bedömer vi antalet incidenter vara för lågt i förhållande till verksamheternas omfattning, där sannolikheten att det finns ett mörkertal är stor. Vår bedömning är att sannolikheten att flertalet sektioner/nämnder inte har haft någon form av personuppgiftsincident under flera år alternativt har endast 1-2 fall, är låg. Vi tror att detta beror på en låg kunskapsnivå inom verksamheterna om vad personuppgiftsincident är och vad som ska klassas som en incident. Likaså har centrala rutiner saknats.

Det råder enighet bland de intervjuade att kunskapsbrist är en grundläggande orsak.

Vi anser att det finns ett behov av en central styrning från kommunstyrelsen sida vad avser utbildningsnivån inom verksamheterna. Vi anser att det finns ett behov av kunskapshöjande insatser inom förvaltningarna samt personal ute i verksamheterna vad avser identifiering, hantering och risk- och konsekvensbedömning av person-uppgiftsincidenter.

I samband med faktagenomgången har det framkommit att kommunstyrelsen har agerat utifrån revisonens rekommendation, där utbildningsinsatser har ägt rum. Detta bedöms som positivt. Utbildningen har upplevts som svår ut i verksamheterna, där också frågor har lyfts vad avser nyttan. Dataskyddsförordningen är en omfattande och komplex lagstiftning, vilket ställer krav på riktade utbildningar.

3.9 Intern kontroll och kunskapsnivå

Iakttagelser

Av granskningen framgår att det råder en allmän låg kunskapsnivå inom

verksamheterna vad avser dataskyddsförordningen. Denna bild bekräftas av de intervjuade. Likaså uttrycks att det inte finns erforderlig kompetens ut i verksamheterna, där befintlig resurs är i egenskap av kommunjurist på kommunledningskontoret, vilket inte är tillräckligt.

Av intervju med dataskyddsombudet delas granskningens iakttagelser vad avser befintliga brister inom ramen för efterlevnad av dataskyddsförordningen, där det råder enighet att den främsta utmaningen är bristande kunskap och kompetens samt att verksamheterna behöver inse vikten av ett fungerande dataskyddsarbete. Vidare påpekas att verksamheterna behöver också inse allvarlighetsgraden i avsteg från dataskyddsförordningen.

Vad avser att använda dataskyddsombuden till rådgivning och utbildningsinsatser framgår att dataskyddsombuden är tillgängliga och har resurser till att stödja och utbilda men att nämnder och styrelser inte har efterfrågat något stöd. Sammatget har stöd och hjälp efterfrågats i mycket begränsad omfattning.

Vid tid för granskningen har dataskyddsombuden genomfört en intern kontroll i form av en enkät med 18 frågor med ett urval av frågor avseende efterlevnad av dataskyddsförordningen. Därefter har granskningsprotokoll upprättats där antal ja/delvis/nej svar följd av antal nödvändiga åtgärder redogörs. Den interna kontrollen har avsett de sektioner som lyder under kommunstyrelsen. Planen har varit att efter ifylld enkät ha en genomgång om de delar som behöver åtgärdas. Dock framgår att endast lärandesektionen samt kanslifunktionen inom servicesektionen deltog vid genomgångarna. Vid tid för granskningen har kontroller inte genomförts av nämnderna.

3.9.1 Kommentarer och bedömningar

Vi bedömer att det är centralt att dataskyddsombuden genomför interna granskningar av kommunstyrelsens, nämndernas samt de kommunala bolagens arbete med dataskyddsförordningen i syfte att få fram åtgärdsbehoven. Vi bedömer att granskningarna behöver vara av mer uttömmande karaktär i syfte att skapa nytta, effekt och resultat. Frågor i enkätform är en bra start. Därefter erfordras fördjupade granskningar med sikte på olika områden. Ett första fördjupat område bör vara granskning av **registerförteckningarna** som vid tid för granskningen är väsentligt bristfälliga (se avsnitt 3.9). Andra områden är exempelvis hantering av personuppgiftsincidenter, ostrukturerad data, personuppgiftsbiträdesavtal, hantering av känsliga personuppgifter mm. Utifrån dataskyddsförordningens omfattande karaktär finns flertalet områden som bör granskas internt.

Granskningarna bör dokumenteras i rapportform för respektive sektion, nämnd och bolagsstyrelse i syfte att tydliggöra åtgärdsbehoven. Det är vidare av vikt att eventuella utvecklingsområden och brister framgår på ett tydligt sätt följd av

åtgärder. Utifrån rådande kunskapsnivå samt lagstiftningens komplexitet är det av vikt med vägledande åtgärder i syfte att verksamheterna ska kunna komma vidare.

Resultatet av granskningarna ska återkopplas till berörd sektion, nämnd eller bolagsstyrelse. Granskad sektion, nämnd, bolag bör efter genomförd granskning återkomma med en åtgärds-/handlingsplan till dataskyddsombuden inom fastställd

tidsram. Vidare bör resultatet av granskningarna redogöras för kommunstyrelsen utifrån styrelsens uppsiktsplikt.

Vidare anser vi att dataskyddsombuden bör sammanställa en **årlig lägesrapport** över statusen av styrelsers och nämndernas arbete vad avser efterlevnad av dataskyddsförordningen. Denna redogörelse görs lämpligen i samband med årsbokslutet och delges kommunstyrelsen och kommunfullmäktige.

Kommunstyrelsen har inom ramen för sin uppsiktsplikt ett ansvar att följa upp huruvida verksamheterna efterlever dataskyddsförordningen. I syfte att uppnå en enhetlig kunskapsnivå samt en enhetlig hantering inom kommunen erfordras en central styrning från kommunstyrelsens sida vada avser utbildningsinsatser samt centrala kommunövergripande styrdokument, (se kommande avsnitt vad avser styrdokument).

Vi vill också framhålla att det är nämnder och styrelser i egenskap av personuppgiftsansvariga som är juridiskt sett ytterst ansvariga för att uppnå en tillfredställande nivå vad avser efterlevnaden av dataskyddsförordningen. Kommunstyrelsen kan inte inta rollen som personuppgiftsansvarig för någon annan nämnd eller styrelse. Dock ansvarar kommunstyrelsen för att säkerställa en tillfredställande kunskapsnivå samt hantering av personuppgifter inom kommunens verksamheter.

Det är vidare av vikt att sektioner och nämnder använder sig av dataskyddsombuden vad avser rådgivning och stöd. Utifrån granskningens resultat noterar vi att det finns ett tydligt behov av vägledning vad avser efterlevnad av dataskyddsförordningen.

Vad avser nämndernas årliga internkontrollplaner finns vid tid för granskningen inga kontrollmål upptagna med sikte på efterlevnad av dataskyddsförordningen. Utifrån befintliga förbättringsområden samt risker rekommenderar vi att ett urval av kontrollmål med sikte på efterlevnad av dataskyddsförordningen tillförs de årliga internkontrollplanerna. Exempel på aktuella kontrolmål är dokumentation av personuppgiftsincidenter, risk- och konsekvensbedömningar, korrekt upprättade registerförteckningar, de registrerades rättigheter mm.

Förbättringsarbete efter genomförd revison

I samband med faktagenomgången har det framkommit att dataskyddsombudsorganisationen har efter genomförd revision genomfört ytterligare interna granskningar. Vidare har vi delgivits att en informationssäkerhetssamordnare kommer att anställas under våren 2022. Ytterligare åtgärder som har ägt rum efter genomförd revision är att ansvarsfördelningen har förtydligats, där GDPR-handläggare finns utsedda inom respektive sektion. Det framgår att sektionerna har börjat förstå att det krävs ett krafttag samt omtag vad avser efterlevnad av dataskyddsförordningen. Vi bedömer genomförda och planerade insatser som positiva.

3.10 Registerförteckningar

All behandling av personuppgifter ska uppfylla de grundläggande principerna i enlighet med dataskyddsförordningen.

- Laglighet
- Korrekthet
- Öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Riktighet
- Lagringsminimering
- Integritet och konfidentialitet
- Ansvarsskyldighet

Dataskyddsförordningen fastställer för att påvisa att förordningen följs ska peron-uppgiftsansvariga föra register över behandling som sker under deras ansvar, (s.k. registerförteckningar). Registerförteckningarna ska på begäran redovisas för tillsynsmyndigheten, dvs. Integritetsskyddsmyndigheten, där registren ska utgöra en grund för övervakning av behandling av personuppgifter.

Iakttagelser

Vi har tagit del av upprättade registerförteckningar, där vi har noterat en del centrala brister. Av intervjuerna med tjänstepersonerna samt dataskyddsombudet framgår en medvetenhet kring att det finns brister vad avser registerförteckningarna. Det framgår att kunskapen är låg inom verksamheterna vad avser hantering av registerförteckningar. Vid tid för granskningen anges att en modul har inköpts till det befintliga styrverktyget Stratsys, inom ramen för ledningssystem för informations-säkerhet, som ska bidra till att förbättra dataskyddsarbetet. Ambitionen vid tid för granskningen är att inkludera registerförteckningarna i denna modul, där det uttrycks att ett omtag och förbättringsarbete kommer att ske under hösten 2020.

Vi har genomfört en granskning av registerförteckningarna där bl.a. följande brister har noterats:

- Avsaknad av kontaktuppgifter till den personuppgiftsansvariga nämndens förvaltning.

- Avsaknad av kontaktuppgifter till dataskyddsombudets samt avsaknad av data-skyddsombudets fullständiga namnuppgift.

- Blanka rutor där frågorna är obesvarade i sin helhet.

- Avsaknad av angivelse av tidsfrist för gallring/radering.

- Förekomst av ”vet-ej-svar” vad avser tidsfrister för gallring/radering.

- Som svar på tidsfrist avseende gallring/radering förekommer svar i form av ”i enlighet med dokumenthanteringsplanen” eller ”så länge det är nödvändigt…”. Det bör framhållas att vad avser angivande av tidsfrister ska dessa anges uttryckligen, dvs. det räcker inte med en hänvisning till nämndens dokument-hanteringsplan. Denna punkt berör dataskyddsförordningens grundläggande princip om ”lagringsminimering”.

- Avsaknad av angivelse av laglig/rättslig grund för registreringen.

- Angivande av svar i form av ”rättslig grund” på frågan om vilken rättslig grund som används som stöd för behandlingen.

- Förekomst av svar där ”dokumenthanteringsplanen” eller ”styrdokument” anges som rättslig grund.

- Benämningen ”*myndighetsutövning*” förekommer som svar på efterfrågat lagstöd. All myndighetsutövning ska grundas på lagar inom EU-rätten eller nationell rätt. Därmed ska aktuell författning och lagrum anges i samband med angivande av myndighetsutövning som rättslig grund.

- Uppgifter av ”*allmänt intresse*” anges som rättslig grund utan hänvisning till lagstöd. För att uppgifter av allmänt intresse ska kunna nyttjas krävs stöd i lagstiftningen eller beslut som har meddelats med stöd av gällande lagstiftning.

- Vad avser ”känsliga personuppgifter” är utgångspunkten att det är förbjudet att behandla dessa. Det finns dock undantag. Det bör framhållas att vad gäller behandling av känsliga personuppgifter finns specificerade krav enligt artikel 9 i data-skyddsförordningen följt av krav på konsekvensbedömningar i enlighet med artikel 35. Detta ställer krav på att behandling av känsliga personuppgifter ska vara väl motiverade och välgrundade samt stödjas av gällande lagstiftning. Samtliga nämnder bör se över huruvida detta krav har uppfyllts.
Det förekommer att ”allmänt intresse” eller ”myndighetsutövning” anges som stöd för behandling av känsliga personuppgifter utan hänvisning till aktuell lagstiftning och lagrum.

- Förekomst av att det anges att samtliga kategorier av känsliga personuppgifter behandlas i en och samma behandling, (exempelvis ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska uppgifter och biometriska uppgifter för att entydigt identifiera en fysisk persons uppgifter om hälsa, uppgifter om en fysisk persons sexualliv eller sexuella läggning mm.), där också relevansen av vissa uppgifter kan ifrågasättas.

- På frågan ”vilka kategorier av registrerade personer som behandlingen avser”, har det i vissa fall skett en misstolkning, där funktioner/titlar i kommunen har angivits. Likaså förekommer svar som ”behöriga medarbetare”.

- vad avser frågan om huruvida personuppgiftsbiträde anlitas förekommer svar i form av endast personnamn. Här erfordras namn på leverantören, där också kontaktuppgifter till

företrädare kan anges. Vi rekommenderar att en kolumn tillförs i mallen där det framgår huruvida det finns ett personuppgiftsbiträdeavtal i de fall där ett personuppgiftsbiträde anlitas. Det är centralt att det finns ett aktuellt avtal mellan personuppgiftsansvarig och personuppgiftsbiträden.

- Varje personuppgiftsbehandling inom ramen för olika system/verktyg ska anges självständig följt av separata svar vad avser exempelvis: ändamål, rättslig grund, kategorier av registrerade, typer av personuppgifter, samtycke, personuppgiftsbiträde, personuppgiftsbiträdesavtal, överföring till tredje land, förekomst av känsliga personuppgifter, tidsfrist för radering, tekniska och organisatoriska säkerhetsåtgärder mm. Dock förekommer fall där flera system/verktyg har slagits samman, vilket strider mot gällande lagstiftning.

- vi har noterat att det är **alltför få personuppgiftsbehandlingar** som har registrerats i förhållande till ansvarsområden och verksamhetsomfattningar. Detta gäller framförallt omsorgssektionen samt lärandesektionen.

3.10.1 Kommentarer och bedömning

Vi bedömer att det finns ett behov av ett grundligt kraft- samt omtag vad avser upprättande av registerförteckningar, där det idag finns centrala brister. Vi anser att nämnderna bör utse ansvariga för upprättande och underhåll av register-förteckningar följt av riktade utbildningar för denna kategori av personal. Alternativt att det inrättas centrala funktioner som hanterar registerförteckningarna. Det bör dock framhållas att oaktat den praktiska organiseringen av hantering av register-förteckningar, är det respektive nämnd/styrelse som ansvarar för att tillse att det finns korrekt upprättade förteckningar över nämndens/styrelsens behandlingar.

Vi bedömer vidare att antalet registerförteckningar vara för få i förhållande till de verksamhetsområden som hanteras, framförallt vad gäller omsorgssektionen samt lärandesektionen. Härigenom bör verksamheterna genomföra en inventering, där det säkerställs att förteckningar upprättas för samtliga personuppgiftsbehandlingar.

I samband med faktagenomgången har det framkommit att arbetet med att se över registerförteckningarna har ännu inte påbörjats, vilket bedöms som bristfälligt. Vi har delgivits att ett projekt har satts igång tillsammans med Ulricehamn med sikt på dataskydd och informationssäkerhet, där registerförteckningarna kommer att ingå.

Vi bedömer att förbättringsarbetet avseende registerförteckningarna behöver komma igång snarast då det har flutit alltför lång tid sedan lagens ikraftträdande. Som tidigare nämnts ska respektive nämnd/styrelse säkerställa att det finns registerförteckningar för samtliga personuppgiftsbehandlingar samt att dessa är korrekt upprättade. Detta innebär att oaktat den praktiska/organisatoriska hanteringen är det respektive nämnd/styrelse som bär ansvaret. Kommunstyrelsen har dock inom ramen för sin uppsiktplikt ett ansvar att följa upp samtliga nämnders (inkl. gemensamma nämnder) och styrelsers arbete vad avser efterlevnaden av dataskyddsförordningen.

3.11 Registerutdrag, rättelse, radering och begränsning

I enlighet med dataskyddsförordningen har den registrerade rätt att begära ut ett så kallat registerutdrag från offentliga och privata organisationer. Ett registerutdrag ska redogöra för de personuppgifter som en myndighet eller ett företag behandlar om en person samt på vilket sätt uppgifterna behandlas.

Likaså har den registrerade rätt till att utan dröjsmål få felaktiga uppgifter rättade. På samma sätt finns rättigheten att utan onödigt dröjsmål få sina personuppgifter raderade om de exempelvis inte längre är nödvändiga för de ändamål för vilka de samlats in eller att den registrerade återkallar sitt samtycke som behandlingen grundar sig på. Den registrerade kan också invända mot registreringen utifrån att det saknas en laglig grund för behandlingen.

Ytterligare rättigheter avser begränsning av behandling av personuppgifter, där den registrerade under visa omständigheter kan kräva att personuppgifter behandlas endast för vissa avgränsade syften.

Iakttagelser

Vi har tagit del av en rutinbeskrivning i form av urklipp från intranätet avseende registerförfrågan.

Vi saknar en rutinbeskrivning för hanteringen av en inkommen begäran avseende rättelse, radering och begränsning.

3.11.1 Kommentarer och bedömning

Vi bedömer att det finns tydliga rutiner för begäran av registerutdrag. Av rutinbeskrivningen bör beslutsinstans samt fastställelsedatum framgå.

Vi bedömer att kommunstyrelsen bör upprätta en rutinbeskrivning avseende hanteringen av inkomna begäran om rättelse, radering och begränsning.

4 Slutsats och rekommendationer

Sammanfattningsvis kan konstateras att det finns väsentliga brister vad avser efterlevnaden av dataskyddsförordningen. Utifrån ett tydligt behov av stödjande insatser har rapporten utformats på ett vägledande sätt i vissa delar.

Vi bedömer det som positivt att kommunstyrelsen samt kommunstyrelseförvaltningen har varit lyhörda för genomförd granskning och har påbörjat ett förbättringsarbete efter genomförd granskning.

Mot bakgrund av vår granskning bedömer vi att följande delar bör ses över:

- Kommunstyrelsen har inom ramen för sin uppsiktsplikt ett ansvar att följa upp huruvida verksamheterna inom nämnder och kommunala bolag efterlever dataskyddsförordningen. I syfte att uppnå en enhetlig kunskapsnivå samt en enhetlig hantering inom kommunen erfordras en central styrning från kommunstyrelsens sida vada avser utbildningsinsatser samt framtagande av ändamålsenliga styrdokument.

- Dokumentation av personuppgiftsincidenter är obligatorisk, där samtliga incidenter ska dokumenteras samt risk- och konsekvensbedömas **oaktat allvarlighetsgrad**. Vi bedömer att dokumentationen av personuppgiftsincidenter inte är på en tillfredställande nivå.

- Sannolikheten att flertalet sektioner/nämnder inte har haft någon form av person-uppgiftsincident alternativt har endast 1-2 fall sedan lagens ikraftträdande är låg, där vi bedömer att bristande kunskapsnivå i kombinationen med avsaknad av centrala rutiner samt en central styrning är bakomliggande faktorer. Vi anser att det finns ett behov av kunskapshöjande insatser inom förvaltningarna samt personal ute i verksamheterna vad avser **identifiering, risk- och konsekvensbedömning** och **dokumentation** av personuppgiftsincidenter.

- Vi anser att kommunövergripande styrdokument i form av rutinbeskrivningar av större vikt för verksamheterna samt av juridisk betydelse, bör utöver återgivning på intranätet, även finnas i en formaliserad form med angivet datum för upprättande samt beslutsinstans.

- Vi bedömer att den kommunövergripande rutinen avseende hantering av person-uppgiftsincidenter behöver revideras vad avser den praktiska hanteringen vid upptäckt av en incident. Detta i syfte att förmedla en korrekt hantering samt underlätta för medarbetarna genom en samlad och distinkt tillvägagångsbeskrivning, (se sid. 14).

- Efter genomförd granskning har en mall arbetats fram för dokumentation av person-uppgiftsincidenter. Vi har i samband med faktagenomgången granskat framtagen mall där det finns en del brister. Mallen behöver revideras samt kompletteras i syfte att uppfylla lagens krav samt säkerställa en ändamålsenlighet (se avsnitt 3.7 för närmare vägledning).
Utifrån erfarenheten att viktiga delar kan utebli när interna mallar upprättas, rekommenderar vi kommunstyrelsen att använda sig av tillsynsmyndighetens dokumentationsmall i sin helhet. Detta säkerställer att samtliga nödvändiga delar enligt lagstiftningen upptas. Vidare leder det till en effektivisering i form av minskad administration, där dokumentation av en incident inte behöver ske två gånger vid de tillfällen där en incident behöver skickas vidare till Integritetsskyddsmyndigheten.

- Vi bedömer att det är centralt att dataskyddsombuden genomför **interna granskningar** av kommunstyrelsens, nämndernas samt de kommunala bolagens arbete med dataskyddsförordningen i syfte att få fram åtgärdsbehoven.

- Resultatet av dataskyddsombudens granskningar ska återkopplas till berörd sektion, nämnd eller bolagsstyrelse. Granskad sektion, nämnd, bolag bör efter genomförd granskning återkomma med en åtgärds-/handlingsplan till dataskyddsombuden inom fastställd tidsram. Vidare bör resultatet av granskningarna redogöras för kommunstyrelsen utifrån styrelsens uppsiktsplikt.

- Vi anser att dataskyddsombuden bör sammanställa en **årlig lägesrapport** över statusen av styrelsers och nämndernas arbete vad avser efterlevnad av dataskyddsförordningen. Denna redogörelse görs lämpligen i samband med årsbokslutet och delges kommunstyrelsen och kommunfullmäktige.

- Utifrån befintliga risker rekommenderar vi att ett urval av kontrollmål med sikte på efterlevnad av dataskyddsförordningen tillförs de årliga internkontrollplanerna. Exempel på aktuella kontrolmål är dokumentation av personuppgiftsincidenter, risk- och konsekvensbedömningar, korrekt upprättade registerförteckningar, de registrerades rättigheter mm.

- Vi bedömer att det finns ett behov av ett krafttag vad avser upprättande av registerförteckningar, där det idag finns brister. Vi anser att nämnderna bör utse ansvariga för upprättande och underhåll av registerförteckningar följt av riktade utbildningar för denna kategori av personal. Alternativt att det inrättas centrala funktioner som hanterar registerförteckningarna.

- Vi bedömer antalet registerförteckningar vara för få i förhållande till de verksamhetsområden som hanteras, framförallt vad gäller omsorgssektionen samt lärande- sektionen. Härigenom bör samtliga verksamheter genomföra en inventering, där det säkerställs att förteckningar upprättas för samtliga personuppgiftsbehandlingar.

-Förbättringsarbetet avseende registerförteckningarna behöver komma igång snarast då det har flutit alltför lång tid sedan lagens ikraftträdande. Det bör framhållas att oaktat den praktiska/organisatoriska hanteringen är det respektive nämnd/ styrelse som ansvarar för att säkerställa att det finns registerförteckningar för samtliga personuppgiftsbehandlingar samt att dessa är korrekt upprättade. Kommunstyrelsen har dock inom ramen för sin uppsiktplikt ett ansvar att följa upp samtliga nämnders och bolagens arbete vad avser efterlevnaden av dataskyddsförordningen.

- Kommunstyrelsen bör upprätta en kommunövergripande rutinbeskrivning avseende hanteringen av inkomna begäran om rättelse, radering och begränsning.

KPMG AB

Viktoria Berstam
Sakkunnig/Certifierad kommunal revisor

Tranemo kommun
Granskning av rutiner för efterlevnad av dataskyddsförordningen

2021-07-08