Ljungby kommun 2021-06-22

Revisorerna

Till

Kommunstyrelsen

(KF:s presidium för kännedom)

Granskning av efterlevnad av dataskyddsförordningen

KPMG har på vårt uppdrag utfört rubricerad granskning.

På revisionsmöte 2021-06-22 har KPMG presenterat granskningen för oss revisorer.

Vi överlämnar härmed rapporten till kommunstyrelsen för yttrande senast den 4 oktober 2021.

Ljungby som ovan

Annette Bjers Gustavsson

Ordförande

Christer Yngvesson

Vice ordförande

Granskning av rutiner för efterlevnad av dataskyddsförordningen

Revisionsrapport
Ljungby kommun

KPMG AB

2021-06-14

Antal sidor 23

Ljungby kommun
Granskning av rutiner för efterlevnad av dataskyddsförordningen

2021-06-14

Innehållsförteckning

1 Sammanfattning

Vi har av Ljungby 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 som helhet samt personuppgifts-ansvariga nämnder och styrelser.

Sammanfattningsvis kan konstateras att det finns väsentliga brister vad avser efterlevnaden av dataskyddsförordningen. Vi bedömer att det finns ett behov av en central styrning från kommunstyrelsens sida samt ett krafttag vad avser nämnders och styrelsens arbete med att uppfylla och efterleva dataskyddsförordningen. Likaså erfordras riktade utbildningsinsatser till samtliga nämnder, där kunskapsnivån är låg i dagsläget.

Vi bedömer det som positivt att kommunstyrelsen samt kommunstyrelseförvaltningen har varit lyhörda för genomförd granskning och har ambitioner att snarast påbörja ett förbättringsarbete.

Utifrån ett tydligt behov av stödjande insatser har rapporten utformats på ett vägledande sätt i vissa delar.

Mot bakgrund av vår granskning rekommenderar vi att följande:

- Kommunstyrelsen bör utöva en central styrning i syfte att öka graden av efterlevnad av dataskyddslagstiftningen.

- Dataskyddsombudet bör tillhandahålls erforderliga resurser och förutsättningar för att kunna genomföra ett systematiskt arbete och övervaka efterlevnaden av dataskyddsförordningen samt kunna utbilda och agera rådgivande. Likaså är kontinuitet i uppdraget av vikt.

- Vi anser att det är det är mycket viktigt att dataskyddsombudet genomför **interna granskningar** av styrelsens, nämndernas samt kommunala bolags arbete med dataskyddsförordningen. Uteblivna granskningar och kontroller leder till att verksamheterna inte får kännedom om de brister och risker som föreligger och som behöver åtgärdas. Granskningar och kontroller genomförda av dataskydds-ombudet ska dokumenteras med en återkoppling till ansvarig nämnd samt redogörelse för kommunstyrelsen inom ramen för styrelsens uppsiktsplikt.

- Granskad nämnd bör efter dataskyddsombudets granskningar inkomma med en åtgärds-/handlingsplan.

- Dataskyddsombudet bör sammanställa en **årlig lägesrapport** över styrelsers och

nämndernas lägesstatus vad avser efterlevnad av dataskyddsförordningen. Denna redogörelse görs lämpligen i samband med årsbokslutet och delges kommunstyrelsen och kommunfullmäktige.

- Det bör betonas att det är **personuppgiftsansvariga nämnder och styrelser** som är juridiskt sett ytterst ansvariga för att uppnå en tillfredställande nivå vad avser efterlevnaden av dataskyddsförordningen. Dock bör kommunstyrelsen inom ramen för sin uppsiktplikt följa upp nämndernas och de kommunala bolagens arbete.

- Kommunstyrelsen bör säkerställa att det finns fastställda, ändamålsenliga samt aktuella kommunövergripande styrdokument och riktlinjer i syfte att uppnå en enhetlig hantering samt säkerställa en tillfredställande samt homogen kunskapsnivå inom verksamheterna.

- Respektive styrelse och nämnd bör i sin årliga internkontrollplan uppta **ett eller flera kontrollmål** med sikte på efterlevnad av dataskyddsförordningen.

- Kommunstyrelsen bör snarast fastställa ett styrdokument för hantering och anmälan av personuppgiftsincidenter (se avsnitt 3.6 för vägledning). Utifrån avsaknad av rutiner och styrning i kombination med bristande kunskaper inom verksamheterna har inga personuppgiftsincidenter dokumenterats, konsekvensbedömts eller anmälts till tillsynsmyndigheten sedan lagens ikraftträdande. Dokumentation av personuppgiftsincidenter är obligatorisk, där samtliga incidenter ska dokumenteras oaktat allvarlighetsgrad. Likaså ska den registrerade (i det här fallet den drabbade) informeras om incidenten **utan onödigt dröjsmål**, om incidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.

- I syfte att uppnå ett ändamålsenligt styrdokument, rekommenderar vi att utkastet avseende "Rutin för anmälan av personuppgiftsincidenter" revideras i enlighet med angiven vägledning.

- Vi rekommenderar att IMY:s mall används för dokumentation av personuppgifts-incidenter, där kommunstyrelsen inte behöver upprätta en egen mall. På så sätt säkerställs att samtliga nödvändiga delar kommer med samt att riskerna för bortfall av information och att viktiga delar i processen inte genomförs minimeras. Ytterligare en fördel är effektivisering och minskad administration för medarbetarna genom att endast ett underlag behöver ifyllas. (I samband med faktagenomgången har det framkommit att kommunen kommer att använda IMY:s dokumentationsmall i enlighet med revisionens rekommendation)
- Kommunstyrelsens ledamöter bör årligen får ta del av statistik avseende samtliga inträffade personuppgiftsincidenter inom ramen för styrelsens uppsiktsplikt.
- Vi bedömer att det krävs riktade utbildningsinsatser avseende upptäckt, hantering, dokumentation och konsekvensbedömning av personuppgiftsincidenter, där generellt hållna utbildningar inte är lämpliga i dagsläget. Utbildningen behöver nå samtliga medarbetare.
- Vi bedömer att det krävs ett kraftigt omtag vad avser arbetet och underhåll av

registerförteckningar (se sid 18-20).

- Vi bedömer antalet registerförteckningar vara för få inom styrelsen samt nämnderna i förhållande till de verksamhetsområden som hanteras. Härigenom behöver styrelsen samt samtliga nämnder snarast genomföra en inventering och säkerställa att förteckningar upprättas för samtliga personuppgiftsbehandlingar.
- Vi bedömer att det erfordras en grundlig utbildning för att komma till rätta med befintliga brister vad avser registerförteckningar.
- Kommunstyrelsen bör upprätta en rutinbeskrivning avseende hanteringen av inkomna begäran om rättelse, radering och begränsning.

2 Inledning

Vi har av Ljungby 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?

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 kommunchef, kanslichef tillika säkerhetschef dataskyddsombud samt kommunstyrelsens ordförande.

Rapporten är faktakontrollerad av kommunchefen och 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 personuppgifter leda till **förtroendeskador** för kommunen som helhet samt personuppgiftsansvariga 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 dataskydds-förordningen 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 Dataskyddsorganisation, oberoende och intern kontroll, Ljungby 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 personuppgiftsbiträden 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

Styrelser och nämnder i Ljungby kommun utsåg ett dataskyddsombud fr.o.m. 25 maj 2018, där vederbörande avslutade sitt uppdrag under januari 2020. Därefter har det funnits en lucka där något nytt dataskyddsombud inte har utsetts av styrelser och nämnder. Fr.o.m. mitten på augusti 2020 inrättades en tjänst som krisberedskaps- och säkerhetssamordnare tillika dataskyddsombud, där 50% av tiden skulle ägnas krisberedskapsarbetet och resterande 50% skulle delas mellan informations-säkerhetsarbetet och rollen som dataskyddsombud.

I samband med introduktion av granskningen delgavs att dataskyddsombudet har sedan tidigare valt att lämna sitt uppdrag, där anställningen skulle upphöra den 16 maj 2021. Vi hann genomföra intervjuer och avstämningar med aktuellt dataskyddsombud innan anställningens upphörande.

Av intervju med dataskyddsombudet framgår att under perioden aug 2020 – maj 2021 har tiden ägnats till att samla en lägesbild samt få igång arbetet inom gruppen för GDPR-samordnarna. Under denna period har det inte genomförts några granskningar eller kontroller av styrelsens, nämndernas och de kommunala bolagens efterlevnad av dataskyddsförordningen.
Det framgår vidare att verksamheternas arbete med dataskyddsförordningen (GDPR), har varit bristfällig sedan tidigare och att läget försämrades i och med pandemin, där arbetet nedprioriterades ytterligare. Dataskyddsombudet uttrycker vidare att den största utmaningen i kommunen är bristande kunskap och kompetens vad avser arbetet med dataskyddsförordningen, där det finns ett påtagligt behov av stöd och vägledningsinsatser. Det uttrycks att det finns en acceptans för dataskyddsombudets roll och uppdrag inom förvaltningarna.

Vidare framkommer att avsedd tjänstomfattning gällande rollen som dataskydds-ombud inte är tillräcklig.

Vid tid för granskningen har kommunledningskontoret påbörjat rekryteringsarbetet av ett nytt dataskyddsombud.

3.3.1 Kommentarer och bedömning

Vi bedömer att det krävs en kontinuitet inom ramen för rollen som datakydds-ombud i syfte att kunna uppnå konkreta resultat samt mätbara effekter. Likaså är det av vikt att dataskyddsombudet tillhandahålls erforderliga resurser och förutsättningar för att kunna genomföra ett systematiskt arbete och övervaka efterlevnaden av dataskyddsförordningen samt kunna utbilda och agera rådgivande.
Vi bedömer att i ett läge som Ljungby kommun befinner sig i vad avser arbetet med GDPR, är det initialt inte tillräckligt med en tjänsteomfattning på ca 25%.

Vi anser att det är det är mycket viktigt att dataskyddsombudet genomför **interna granskningar** av styrelsens, nämndernas samt kommunala bolags arbete med dataskyddsförordningen. Detta i syfte att synliggöra statusen samt åtgärdsbehoven inom respektive verksamhet, där en **lägesrapport är centralt** för att nämnder och styrelser ska kunna komma vidare. Uteblivna granskningar och kontroller leder till att verksamheterna inte får kännedom om de brister och risker som föreligger och som behöver åtgärdas. Vi bedömer att interna årliga granskningar bör ske av respektive nämnd/styrelse. Granskningarna kan också med fördel delas upp per verksamhet-sområde inom samma nämnd i syfte att tydliggöra verksamhetsspecifika behov. Granskningar och kontroller genomförda av dataskyddsombudet ska dokumenteras med en återkoppling till ansvarig nämnd samt redogörelse för kommunstyrelsen inom ramen för styrelsens uppsiktsplikt. Granskad nämnd bör därefter inkomma med en åtgärds-/handlingsplan till dataskyddsombudet.

Ett första granskningsområde bör vara arbetet med registerförteckningarna (se avsnitt 3.7). Redan under 2019 konstaterades att förvaltningarna har påbörjat ett arbete med registerförteckningarna men hindras till viss del av resursbrist, där också interna rutiner behöver säkerställas. Vidare framgår behovet av utbildningsinsatser.

Vidare bör dataskyddsombudet sammanställa en **årlig lägesrapport** över styrelsers och nämndernas lägesstatus vad avser efterlevnad av dataskyddsförordningen. Denna redogörelse görs lämpligen i samband med årsbokslutet och delges kommunstyrelsen och kommunfullmäktige. En sammanfattande lägesrapport finns för år 2019 sammanställd av tidigare dataskyddsombud. Vi rekommenderar att framtida lägesrapporter i samband med årsboksluten redogör för respektive styrelse och nämnds status vad avser efterlevnaden inom olika områden som dataskydds-förordningen ställer krav på. Detta utifrån respektive nämnds ansvar som personuppgiftsansvarig.

Som tidigare nämnts har kommunstyrelsen utifrån sin **uppsiktsplikt** ett ansvar för att följa upp nämndernas och bolagens efterlevnad av dataskyddsförordningen.

Vi vill också poängtera att det är **personuppgiftsansvariga nämnder och styrelser** 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 har kommunstyrelsen ett ansvar för centrala kommunövergripande styrdokument och riktlinjer i syfte att uppnå en enhetlig hantering samt säkerställa en tillfredställande samt homogen kunskapsnivå inom verksamheterna. Enligt uppgift har dataskyddsombudet informerat kommunstyrelsen samt nämnderna om ansvaret för

efterlevnad av dataskyddsförordningen.

Vi vill också i sammanhanget betona vikten av ett kontinuerligt internkontrollarbete, där styrelse och nämnder ska årligen upprätta **verksamhetsspecifika intern-kontrollplaner** med kontrollmål som har utmynnat från en årlig risk- och väsentlighetsanalys. Vi anser att respektive styrelse och nämnd bör i sin årliga internkontrollplan uppta **ett eller flera kontrollmål** med sikte på efterlevnad av dataskyddsförordningen. Vid tid för granskningen är kommunchefen relativt nytillträdd med en tjänstgöringsperiod på ca 9 månader, där vederbörande uttrycker att ett förbättringsarbete avseende den interna kontrollen är pågående. Detta bedöms som positivt.

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

3.4 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.

3.4.1 Kommentarer och bedömning

Granskningen visar att samtliga nämnder förutom valnämnden formellt har utsett ett dataskyddsombud. Nämnderna behöver dock utse ett nytt dataskyddsombud när vederbörande tillträder sin tjänst.

3.5 Styrdokument 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 personuppgifts-biträde, (PuB), ska personuppgiftsbiträdet underrätta den personuppgiftsansvarige, (nämnd/styrelse), utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident, (artikel 33, punkt 2).

Iakttagelser

Vid tid för granskningen saknas fastställda styrdokument och rutiner för hantering och dokumentation av personuppgiftsincidenter.

Efter genomförd granskning har ett utkast men benämningen "Rutin för anmälan av personuppgiftsincident" arbetats fram. Vi har delgivits underlaget med ett önskemål att undersöka huruvida utkastet är ändamålsenligt samt se om rutinen uppfyller lagens krav och kan antas. Då vi anser att det finns ett tydligt behov av stöd och vägledning för att komma vidare har vi gått igenom aktuellt utkast. Att anta en rutin som senare skulle visa sig inte vara helt ändamålsenligt skulle innebära merarbete samt en onödig belastning för kommunledningsförvaltningen, där det inte heller främjar kommunen i ett redan eftersatt läge.

Vi har begärt in dokumentation samt statistik avseende antal upptäckta personuppgifts-incidenter sedan lagens ikraftträdande. Det underlag som erhölls från dataskydds-ombudet redovisade noll incidenter mot bakgrund av att vederbörande inte har fått in några incidentinrapporteringar. Vi begärde att kommunlednings- förvaltningen skulle genomföra ytterligare efterforskningar där vi hade misstankar om att incidenterna eventuellt inte har inrapporterats till dataskyddsombudet men har dokumenterats inom verksamheterna, då sannolikheten att inga incidenter har inträffat under en treårsperiod är ytterst låg.

Efter ytterligare efterforskningar framkom att minst tre incidenter har inträffat inom kommunstyrelseförvaltningen. Incidenterna har inte rapporterats till dataskydds-ombudet. Likaså har socialnämnden i samband med granskningen upptäckt en incident men som inte har klassats som en personuppgiftsincident.

Vid tid för granskningen finns inga dokumenterade eller anmälda personuppgifts-incidenter.

Figur 3.5.1

Nämnd	Antal incidenter 2018	Varav anmälda till DI	Antal incidenter 2019	Varav anmälda till DI	Antal incidenter 2020	Varav anmälda till DI
Kommunstyrelsen	0	0	0	0	3	0
Tekniska nämnden	0	0	0	0	0	0
Barn- och utbildningsnämnden	0	0	0	0	0	0
Socialnämnden	0	0	0	0	0	0
Miljö- och byggnämnden	0	0	0	0	0	0
Krisledningsnämnden	0	0	0	0	0	0
Kultur- och fritidsnämnd	0	0	0	0	0	0
Gemensam nämnd familjerätt*	0	0	0	0	0	0
Gemensam överförmyndarnämnd	0	0	0	0	0	0

3.5.1 Kommentarer och bedömning

Vi bedömer att det är en väsentlig brist att det sedan lagens ikraftträdande under 2018 inte har upprättats kommunövergripande rutiner för hantering av personuppgifts-incidenter, där detta berör bl.a. integritetsskyddet för kommunmedborgarna/brukarna.

Vi kan konstatera att en central styrning i frågan har saknats. Utifrån avsaknad av rutiner och en central styrning från kommunstyrelsen samt utebliven styrning från personuppgiftsansvariga nämnder i kombination med bristande kunskaper inom verksamheterna har inga personuppgiftsincidenter dokumenterats, konsekvens-bedömts eller anmälts till tillsynsmyndigheten sedan lagens ikraftträdande. Vi bedömer sannolikheten att inga incidenter eller att endast ett par incidenter har inträffat under en treårsperiod, i en organisation med ca 3000 anställda som ytterst låg. Denna bild delas av samtliga intervjuade, där det uttrycks att mörkertalet är stort.

Vi bedömer att kunskapsbrist avseende upptäckt och hantering av personuppgifts-incidenter är en grundläggande orsak. Bedömningen delas av de intervjuade.

Det bör framhållas att personuppgiftsincidenter som inte hanteras på ett korrekt sätt kan leda till **sanktionsavgifter** samt **förtroendeskador** för Ljungby kommun.

Dokumentation av personuppgiftsincidenter är obligatorisk, där den personuppgifts-ansvarige ska dokumentera samtliga personuppgiftsincidenter inbegripet:

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

Likaså ska den registrerade (i det här fallet den drabbade) informeras om personuppgiftsincidenten **utan onödigt dröjsmål**, om incidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. **Dokumentation ska ske oaktat** om nämnden bedömer att inrapportera personuppgiftsincidenten till tillsynsmyndigheten eller ej.

Den incident som har inträffat på socialnämnden är i allra högsta grad en personuppgiftsincident, där sekretessbelagd information har skickats till fel mottagare. Incidenten borde ha hanterats och dokumenterats i enlighet med dataskyddsförordningens krav (bl.a. risk- och konsekvensbedömning, korrigerande åtgärder mm).

En incident ska bedömas utifrån följande allvarlighetsgrader:

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

Sammantaget bedömer vi att det krävs en **central styrning** från kommunstyrelsen vad avser efterlevnaden av dataskyddsförordningen.

Vi anser också att kommunstyrelsens ledamöter årligen får ta del av statistik avseende samtliga inträffade personuppgiftsincidenter inom ramen för styrelsens uppsiktsplikt.

Vi bedömer att det krävs riktade utbildningsinsatser avseende upptäckt, hantering, dokumentation och konsekvensbedömning av personuppgiftsincidenter, där generellt hållna utbildningar inte är lämpliga i dagsläget. Utbildningen behöver nå samtliga medarbetare, då personuppgiftsincidenter kan inträffa inom samtliga verksamheter – det räcker alltså inte med utbildningen av tjänstepersoner på förvaltningarna.

3.6 Utkast avseende rutin för anmälan av personuppgiftsincident

Iakttagelser

Som tidigare nämnts har ett utkast avseende rutin för anmälan av personuppgifts-incidenter upprättats efter vår granskning. Utifrån önskemål har vi gått igenom utkastet.

3.6.1 Kommentarer och bedömning

Vi bedömer att rutinen behöver utvecklas enligt nedan, i syfte att säkerställa en ändamålsenlighet, där också nämnder och styrelser utifrån dagens läge är i behov av tydlig samt vägledande information.

- Vi anser att det bör tydligt framgå av rutinen att samtliga inträffade incidenter behöver genomgå en **risk- och konsekvensbedömning** i syfte att kunna avgöra huruvida incidenten ska inrapporteras till tillsynsmyndigheten samt huruvida den registrerade ska informeras.

- Vidare bör det av rutinbeskrivningen framgå att samtliga incidenter **ska dokumenteras oaktat allvarlighetsgrad** och om de ska anmälas till tillsynsmyndigheten eller ej. Detta innebär att även om en incident inte bedöms innebära en risk utifrån genomförd konsekvensbedömning och därmed inte heller behöver anmälas till Integritetsskyddsmyndigheten, ska den ändå dokumenteras och diarieföras på berörd förvaltning.

- Ytterligare information av värde är att den **registrerade ska informeras** om personuppgiftsincidenten **utan onödigt dröjsmål**, om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.

- Följande stycke behöver revideras/tas bort: *När Integritetsskyddmyndigheten blir informerad om en incident kan myndigheten fatta beslut om att den personuppgiftsansvarige måste informera de registrerade eller att det inte är nödvändigt…".*

Bedömning om huruvida den registrerade ska informeras om en incident avgörs i första hand av personuppgiftsansvarig nämnd/styrelse. Följande frågor ska ha redan 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?

Det är med andra ord inte förrän en nämnd/styrelse som gör bedömningen att inte informera den registrerade som tillsynsmyndigheten kan göra en annan bedömning och fatta beslut om att berörd nämnd/styrelse ska informera den registrerade.

- Vi rekommenderar att dagens dokumentationsmall, där vissa delar har inhämtats från IMY:s anmälningsblankett ersätts med IMY:s mall i sin helhet. På så sätt säkerställs att samtliga nödvändiga delar kommer med. Kommunstyrelsen behöver därmed inte upprätta en egen mall, utan använda sig av tillsynsmyndigheters dokumentationsmall i

sin helhet. På så sätt minimeras riskerna för bortfall av information och att viktiga delar i processen inte genomförs. Ytterligare en fördel är effektivisering och minskad administration genom att endast ett underlag behöver ifyllas, där ett och samma underlag skickas till IMY vid behov samtidigt som det diarieförs på förvaltningen. Detta underlättar för samtliga medarbetare, vilket i sin tur leder till en ökad verkställighetsgrad samt en enhetlig hantering.

- Den praktiska processen/tillvägagångssätt behöver förtydligas i utkastet, dvs. vem gör vad vid upptäckt av en personuppgiftsincident? Här behöver funktioner/titlar klargöras vad avser ansvaret för ifyllande av dokumentations-/anmälningsmallen (exempelvis att **den som har upptäck incidenten** tillsammans med dataskyddssamordnaren alt. närmaste chef eller annan utsedd funktion fyller i mallen). Det kan vara av värde att i ett startskede ta hjälp av dataskyddsombudet i samband med ifyllandet av mallen till dess att kunskapsnivån är på en tillfredställande nivå inom verksamheterna.

Vi bedömer det som positivt att kommunstyrelseförvaltningen har tagit till sig rekommendationen om att samtliga incidenter ska rapporteras till dataskyddsombudet, där denna punkt finns upptagen i utkastet.

3.7 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 personuppgiftsansvariga 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

Av granskningen framgår att arbetet är påbörjat vad avser upprättande av registerförteckningar, där vi har noterat att samtliga personuppgiftsbehandlingar inte har upptagits i befintliga förteckningar (exempelvis har miljö- och byggnämnden endast tre behandlingar). Vidare finns flertalet registerförteckningar där ställda frågor kopplad till

behandlingarna står obesvarade. Kommunstyrelseförvaltningen har på revisionens begäran efterfrågat registerförteckningar för den gemensamma familjerättsnämnden i Älmhults kommun, dock har inget svar erhållit.

Av intervju med dataskyddsombudet framgår att kunskapsnivån inom verksamheterna är låg vad gäller hantering av registerförteckningar, där det finns ett behov av en ingående och fördjupad utbildning.

Ljungby kommun har använts sig av ett digitalt systemstöd (Drafit Privacy) för upprättande av registerförteckningar över personuppgiftsbehandlingar. Verktyget innehåller ett frågebatteri utifrån dataskyddsförordningen krav med bl.a. följande frågor: *uppgifter om personuppgiftsansvarig, vilka kategorier av registrerade, ändamål med behandlingen, vilka personuppgifter som behandlas, huruvida känsliga personuppgifter behandlas, huruvida uppgifter om barn behandlas, vilken rättslig grund det finns för behandlingen, registrerades rättigheter, informationskrav, gallring och tidsfrister för lagring av uppgifter, anlitande av personuppgiftsbiträde*[2]*, huruvida det finns upprättat personuppgiftsbiträdeavtal, utlämnande av uppgifter till tredjepart, överföring till tredjeland, syftet med att uppgifterna lämnas ut, tekniska och organisatoriska säkerhetsåtgärder, vilka som har åtkomst till uppgifterna* mm.

Av granskningen framkommer att vissa nämnder har valt att inte använda sig av systemstödet då ställda frågor har upplevts som komplicerade samt för omfattande. Enligt uppgift har dataskyddsombudet tillsammans med GDPR-samordnarna fattat ett beslut under våren 2021 om att gå över till SKR:s mall. Dock har barn- och utbildningsnämnden sedan längre tid tillbaka använt sig av SKR:s mall. Enligt de intervjuade löper avtalet med Drafit ut december 2021.

Av det underlag som vi har tagit del av kan konstaterats att i dagsläget är det socialnämnden, tekniska nämnden, miljö- och byggnämnden samt kultur- och fritidsnämnden som fortfarande använder sig av systemstödet Drafit. Kommunstyrelsen, barn- och utbildningsnämnden samt överförmyndarnämnden har gått över helt till SKR:s mall. Det finns dock system/behandlingar i Drafit som inte återfinns i den nya mallen vad avser kommunstyrelsen.

Då arbetet med att upprätta registerförteckningar är långt ifrån klart har dataskydds-ombudet inte genomfört några interna kontroller av nämnders/styrelsers registerförteckningar.

Vi har noterat att det är **alltför få personuppgiftsbehandlingar som har registrerats** i förhållande till nämndernas ansvarsområden och verksamhetsomfattningar.

Som exempel kan nämnas att socialnämnden har endast registrerat 19 person-uppgiftsbehandlingar, barn- och utbildningsnämnden 23, tekniska nämnden 12, kultur- och fritid 9 och miljö- och byggnämnden 3.

Vi har genomfört en övergripande kontroll av registerförteckningarna (både de som har upprättats i Drafit samt i SKR.s mall), där bl.a. följande brister förekommer:

[2] Personuppgiftsbiträde är ett biträde som kan anlitas av personuppgiftsansvarig för hantering av personuppgifter.

- Fel angiven personuppgiftsansvarig, där det förekommer att en leverantör (personuppgiftsbiträde) anges i fältet som ansvarig. Likaså förekommer avsaknad av information om personuppgiftsansvarig i sin helhet.
- Blanka registerförteckningar som har skapats för över ett år sedan, men frågorna är fortfarande obesvarade (socialnämnden). Flertalet skolenheter inom barn- och utbildningsnämnden har inte färdigbehandlat förteckningarna över personuppgiftsbehandlingar/system, där frågorna är obesvarade i sin helhet.

"Vet ej svar/avsaknad av svar/felaktigt svar" i följande fall:

- Om informationskravet[1] uppfyllts
- Huruvida det finns gallringsrutiner
- Huruvida det finns rutiner för behörigheter
- Huruvida personuppgifterna lämnas till tredje land
- Förekomst av molntjänster
- Om uppgifter om barn behandlas
- Huruvida känsliga personuppgifter behandlas
  Vad avser "känsliga personuppgifter" är utgångspunkten att det är förbjudet att behandla dessa. Det finns dock undantag. Det ställs därmed krav på att behandling av känsliga personuppgifter ska vara väl motiverade och välgrundade med stöd i lagstiftningen.
- Huruvida samtycke har inhämtats för att registrera känsliga personuppgifter
- Vilken rättslig grund som används som stöd för behandlingen
- Vilka tidsfrister som gäller för gallring
- Om något personuppgiftsbiträde anlitas
- Huruvida det finns en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder för den aktuella personuppgiftsbehandlingen

Vidare förekommer att "**uppgift 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 lagstiftning.

Ytterligare rättslig grund som används är "myndighetsutövning", dock saknas hänvisning till aktuell författning. All myndighetsutövning ska grundas på lagar inom EU-rätten eller nationell rätt.

[1] Dataskyddsförordningen fastslår att den registrerade har rätt att få information när dennes personuppgifter behandlas. Information om personuppgiftsbehandlingen ska lämnas av den personuppgiftsansvarige både när uppgifterna samlas in och när den registrerade begär det. Informationen ska vara en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk.

3.7.1 Kommentarer och bedömning

Som tidigare nämnts fastställer dataskyddsförordningen att för påvisa att förordningen följs ska personuppgiftsansvariga föra register över behandling som sker under deras ansvar. Granskningen påvisar att det saknas en enhetlig struktur och hantering inom kommunen vad avser registerförteckningar. Kommunstyrelsen och nämnderna har till viss del upprättat registerförteckningar i olika system/mallar och med varierande kvalité.

Vi bedömer antalet registerförteckningar vara för få inom styrelsen samt nämnderna i förhållande till de verksamhetsområden som hanteras. Härigenom behöver styrelsen samt samtliga nämnder snarast genomföra en inventering och säkerställa att förteckningar upprättas för samtliga personuppgiftsbehandlingar.

Vi bedömer att det erfordras en grundlig utbildning för att komma till rätta med befintliga brister vad avser registerförteckningar.

Sammantaget bedömer vi att det krävs ett kraftigt omtag vad avser arbetet med upprättande och underhåll av registerförteckningar. Vi anser att detta arbete är än mer viktigt för de nämnder som har en myndighetsutövande funktion. Kommunen behöver i ett första skede klargöra vilket system som ska användas för upprättande av registerförteckningar, där **kommunstyrelsen** bör fatta ett kommunövergripande beslut. Detta följt av en enhetlig struktur vad avser de frågor som ska besvaras. Det bör beaktas att **obligatoriska frågor** i enlighet med dataskyddsförordningen ska finns med i registerförteckningarna. **Övriga frågor som kan vara till nytta för verksamheterna kan tilläggas**. Vidare bör **en tidsram fastställas** då samtliga personuppgifts-behandlingar bör vara registrerade. Därefter erfordras en granskning av dataskyddsombudet i syfte att åtgärda eventuella brister.

Vi vill betona att respektive nämnd och styrelse är juridiskt sett ytterst ansvariga för att uppnå en tillfredställande nivå vad avser efterlevnaden av dataskyddsförordningen. Kommunstyrelsen har dock inom ramen för sin uppsiktsplikt ett ansvar att tillse att det finns centrala styrdokument, att det finns en enhetlig hantering i kommunen samt följa upp att nämnder och bolagsstyrelser efterlever gällande lagkrav.

3.8 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

Vid tid för granskningen finns ett styrdokument med benämningen "Rutin för begäran om registerutdrag", antaget 2020-03-01.

Det finns en beskrivning av lagstiftningen avseende begäran om rättelse, radering och begränsning i styrdokumentet "Rutin för behandling av personuppgifter", antaget 2018-11-01. Vi saknar dock en rutinbeskrivning för hanteringen av en inkommen begäran avseende rättelse, radering och begränsning.

3.8.1 Kommentarer och bedömning

Vi bedömer att det finns tydliga rutiner för begäran av registerutdrag.

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

4 Slutsats och rekommendationer

Sammantaget bedömer vi att det finns väsentliga brister vad avser efterlevnaden av dataskyddsförordningen. Vi bedömer att det finns ett behov av en central styrning från kommunstyrelsens sida samt ett krafttag vad avser nämnders och styrelsens arbete med att uppfylla och efterleva dataskyddsförordningen. Likaså erfordras riktade utbildningsinsatser till samtliga nämnder, där kunskapsnivån är låg i dagsläget.

Vi bedömer det som positivt att kommunstyrelsen samt kommunstyrelseförvaltningen har varit lyhörda för genomförd granskning och har ambitioner att påbörja ett förbättringsarbete snarast.

Utifrån ett tydligt behov av stödjande insatser har rapporten utformats på ett vägledande sätt i vissa delar.

Mot bakgrund av vår granskning rekommenderar vi att följande:

- Kommunstyrelsen bör utöva en central styrning i syfte att öka graden av efterlevnad av dataskyddslagstiftningen.

- Dataskyddsombudet bör tillhandahålls erforderliga resurser och förutsättningar för att kunna genomföra ett systematiskt arbete och övervaka efterlevnaden av dataskyddsförordningen samt kunna utbilda och agera rådgivande. Likaså är kontinuitet i uppdraget av vikt.

- Vi anser att det är det är mycket viktigt att dataskyddsombudet genomför **interna granskningar** av styrelsens, nämndernas samt kommunala bolags arbete med

dataskyddsförordningen. Uteblivna granskningar och kontroller leder till att verksamheterna inte får kännedom om de brister och risker som föreligger och som behöver åtgärdas. Granskningar och kontroller genomförda av dataskyddsombudet ska dokumenteras med en återkoppling till ansvarig nämnd samt redogörelse för kommunstyrelsen inom ramen för styrelsens uppsiktsplikt.

- Granskad nämnd bör efter dataskyddsombudets granskningar inkomma med en åtgärds-/handlingsplan.

- Dataskyddsombudet bör sammanställa en **årlig lägesrapport** över styrelsers och nämndernas lägesstatus vad avser efterlevnad av dataskyddsförordningen. Denna redogörelse görs lämpligen i samband med årsbokslutet och delges kommunstyrelsen och kommunfullmäktige.

- Det bör betonas att det är **personuppgiftsansvariga nämnder och styrelser** som är juridiskt sett ytterst ansvariga för att uppnå en tillfredställande nivå vad avser efterlevnaden av dataskyddsförordningen. Dock bör kommunstyrelsen inom ramen för sin uppsiktplikt följa upp nämndernas och de kommunala bolagens arbete.

- Kommunstyrelsen bör säkerställa att det finns fastställda, ändamålsenliga samt aktuella kommunövergripande styrdokument och riktlinjer i syfte att uppnå en enhetlig hantering samt säkerställa en tillfredställande samt homogen kunskapsnivå inom verksamheterna.

- Respektive styrelse och nämnd bör i sin årliga internkontrollplan uppta **ett eller flera kontrollmål** med sikte på efterlevnad av dataskyddsförordningen.

- Kommunstyrelsen bör snarast fastställa ett styrdokument för hantering och anmälan av personuppgiftsincidenter (se avsnitt 3.6 för vägledning). Utifrån avsaknad av rutiner och styrning i kombination med bristande kunskaper inom verksamheterna har inga personuppgiftsincidenter dokumenterats, konsekvensbedömts eller anmälts till tillsynsmyndigheten sedan lagens ikraftträdande. Dokumentation av personuppgiftsincidenter är obligatorisk, där samtliga incidenter ska dokumenteras oaktat allvarlighetsgrad. Likaså ska den registrerade (i det här fallet den drabbade) informeras om incidenten **utan onödigt dröjsmål**, om incidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.

- I syfte att uppnå ett ändamålsenligt styrdokument, rekommenderar vi att utkastet avseende "Rutin för anmälan av personuppgiftsincidenter" revideras i enlighet med angiven vägledning.

- Vi rekommenderar att IMY:s mall används för dokumentation av personuppgiftsincidenter, där kommunstyrelsen inte behöver upprätta en egen mall. På så sätt säkerställs att samtliga nödvändiga delar kommer med samt att riskerna för bortfall av information och att viktiga delar i processen inte genomförs minimeras. Ytterligare en fördel är effektivisering och minskad administration för medarbetarna genom att endast ett underlag behöver ifyllas.

- Kommunstyrelsens ledamöter bör årligen får ta del av statistik avseende samtliga

inträffade personuppgiftsincidenter inom ramen för styrelsens uppsiktsplikt.

- Vi bedömer att det krävs riktade utbildningsinsatser avseende upptäckt, hantering, dokumentation och konsekvensbedömning av personuppgiftsincidenter, där generellt hållna utbildningar inte är lämpliga i dagsläget. Utbildningen behöver nå samtliga medarbetare.
- Vi bedömer att det krävs ett kraftigt omtag vad avser arbetet och underhåll av registerförteckningar (se sid 18-20).
- Vi bedömer antalet registerförteckningar vara för få inom styrelsen samt nämnderna i förhållande till de verksamhetsområden som hanteras. Härigenom behöver styrelsen samt samtliga nämnder snarast genomföra en inventering och säkerställa att förteckningar upprättas för samtliga personuppgiftsbehandlingar.
- Vi bedömer att det erfordras en grundlig utbildning för att komma till rätta med befintliga brister vad avser registerförteckningar.
- Kommunstyrelsen bör upprätta en rutinbeskrivning avseende hanteringen av inkomna begäran om rättelse, radering och begränsning.

Datum som ovan

KPMG AB

Viktoria Bernstam

Sakkunnig/Certifierad kommunal revisor