Vård- och omsorgsnämnden
Vård- och omsorgsförvaltningen
Utredningsenheten
Silje Jangtorp Jansson

Datum
2024-03-14

Diarienummer
VON/2024:46

Handlingsnummer
2024:228

Vård- och omsorgsnämnden

Svar på kommunrevisionens granskning av rutiner för efterlevnad av GDPR/Dataskyddsförordningen

Förslag till beslut

1. Revisionsrapporten *Granskning av rutiner för efterlevnad av GDPR/Dataskyddsförordningen* läggs till handlingarna och vård- och omsorgsnämndens svar lämnas till kommunrevisionen samt kommunstyrelsen.
2. Vård- och omsorgsförvaltningen får i uppdrag att säkerställa att samtliga åtgärder som KPMG föreslår verkställs enligt nämndens åtgärdsplan.

Sammanfattning

Kommunrevisionen har med stöd av KPMG genomfört en granskning av kommunens rutiner för efterlevnad av GDPR/Dataskyddsförordningen med fokus på bland annat register över behandling av personuppgifter. Kommunrevisionens övergripande bedömning är att kommunstyrelsen samt berörda nämnder och styrelse endast har en *delvis* ändamålsenlig styrning och kontroll vad avser efterlevnad av dataskyddsförordningen. Det som rekommenderas vård- och omsorgsnämnden är att:

- genomföra en inventering för att säkerställa att samtliga personuppgiftsbehandlingar finns registrerade i behandlingsregistren.
- se över nämndens behandlingsregister för personuppgiftsbehandlingar och genomföra korrigeringar samt kompletteringar i enlighet med avsnitt 9.
- inkludera avgränsade kontrollmål avseende efterlevnad av dataskyddsförordningen i nämndens kommande internkontrollarbete, där det finns risker kopplad till hantering av personuppgifter.
- årligen följa upp och ta del av antal personuppgiftsincidenter inom respektive verksamhet som lyder under nämndens ansvarsområde.
- anordna utbildning avseende hantering av personuppgiftsincidenter för de medarbetare som hanterar personuppgifter.

En del av rekommendationerna som granskningen ger är redan åtgärdade eller är pågående. Resterande brister är vård- och omsorgsförvaltningen medveten om och planerar att åtgärda under 2024.

Ärendebeskrivning

Kommunrevisionen har skickat en granskningsrapport till vård- och omsorgsnämnden: *Granskning av rutiner för efterlevnad av GDPR/Dataskyddsförordningen* –

Register över personuppgiftsbehandlingar. Granskningsrapporten är även skickad till grundskolenämnden och Eskilstuna kommunfastigheter AB. Yttrande till granskningens iakttagelser och rekommendationer samt en tidsplan får de åtgärder som planeras utifrån granskningen ska ha inkommit till kommunrevisionen senast den 30 april 2024.

Kommunrevisionen har med stöd av KPMG genomfört en granskning av kommunens rutiner för efterlevnad av GDPR/Dataskyddsförordningen med fokus på bland annat register över behandling av personuppgifter. Genom Dataskyddsförordningen (GDPR) ska både offentliga och privata verksamheter anpassa hanteringen av personuppgifter till gällande regler inom ramen för lagstiftningen. Bristande hante,ring 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. Mot denna bakgrund har kommunrevisionen i sin riskanalys funnit det angeläget att följa upp hur nämnder och styrelser arbetar för att säkerställa efterlevnad av kraven på detta område.

Kommunrevisionens övergripande bedömning är att kommunstyrelsen samt berörda nämnder och styrelse endast har en *delvis* ändamålsenlig styrning och kontroll vad avser efterlevnad av dataskyddsförordningen. I granskningen har det framkommit utvecklingsområden och brister kring efterlevnaden av dataskyddsförordningen.

Svar på kommunrevisionens granskning

Interngranskningar
Med anledning av att dataskyddsombudet sammanställer resultatet från frågeformuläret gällande kontroll av efterlevnad av dataskyddsförordning, i en årsrapport, har personuppgiftsansvariga nämnder inte getts förutsättningar att hantera eventuella behov av åtgärder. Vård- och omsorgsnämnden anser det positivt och önskvärt att nämndspecifika rapporter tas fram med resultat, framkomna risker, brister, utvecklingsområden följt av bedömning och riktade rekommendationer. Detta för att nämnden ska kunna fullgöra sitt ansvar som personuppgiftsansvarig och åtgärda de brister som eventuellt kan finnas.

Register över personuppgiftsbehandlingar
Vård- och omsorgsnämnden är medveten om att det behöver genomföras en inventering av behandlingsregistren för att åtgärda de brister som finns.

Det framgår av granskningen att vård- och omsorgsnämnden använder ”myndighetsutövning” i kombination med ”uppgift av allmänt intresse” i register över personuppgiftsbehandlingar utan att hänvisa till aktuell författning. Enligt Dataskyddsförordningen krävs det inte att det görs hänvisning till aktuell författning i registren över personuppgiftsbehandlingar. Att hänvisa till aktuell författning är det som kan anses vara ”best practice”, alltså det nämnden bör göra. Detta gäller även där det saknas information om vilken lagstiftning och lagrum som behandlingen grundar sig på när ”rättslig förpliktelse” används som rättslig grund. Vård- och omsorgsnämnden ställer sig dock positiv till att åtgärda de brister som finns utifrån vad som är ”best practice”.

Vad gäller överföring av personuppgifter till tredje land, är USA det land som uppgifter kan överföras till från vård- och omsorgsnämndens verksamheter. EU-lagstiftningen har ändrats där USA har bedömts ha en adekvat skyddsnivå, och att det därför är tillförlitligt och tillåtet att överföra uppgifter dit.

I granskningsrapporten framkommer att det förekommer behandlingar i vård- och omsorgsnämndens register med benämning ”tilldelning av arbetsplats” i samband med rekrytering av vikarier där känsliga personuppgifter behandlas. Bristen är redan åtgärdad och är inget som görs idag.

Sammantaget är vård- och omsorgsnämnden medveten om att det förekommer brister i behandlingsregistren som behöver åtgärdas. Målet är att det ska införas ett system för kommunens alla IT-komponenter som ska kunna ersätta den Excel-fil som personuppgiftsregistret finns i idag. Detta ska underlätta hanteringen av registerförtekningen och minimera att brister kan uppstå på grund av mänskliga faktorer.

Personuppgiftsincidenter
Vård- och omsorgsnämnden är medveten om att det förekommer få rapporteringar om personuppgiftsincidenter inom förvaltningen. Det har dock skett en förbättring där det år 2020 rapporterades 4 personuppgiftsincidenter och år 2023 rapporterades 19 personuppgiftsincidenter. Förbättringen är en effekt av att själva processen för rapportering av personuppgiftsincidenter har förenklats samt att all personal inom förvaltningen genomgår utbildning för att få kunskap om vad en personuppgiftsincident är och att den ska rapporteras. Idag är det obligatoriskt för all personal att gå informationssäkerhetsutbildning, men det finns också icke-obligatorisk utbildning gällande GDPR. Utbildning av personal är något som sker regelbundet inom förvaltningen.

Vård- och omsorgsnämndens yttrande över samlad bedömning och rekommendationer
Nedan framställs vård- och omsorgsnämndens yttrande över granskningens rekommendationer och tidsplan för de åtgärder som planeras utifrån granskningen.

Utifrån den första rekommendationen för vård- och omsorgsnämnden att *genomföra en inventering för att säkerställa att samtliga personuppgiftsbehandlingar finns registrerade i behandlingsregistren* kommer en inventering av personuppgiftsbehandlingarna att genomföras under 2024.

Den andra rekommendationen att *se över hur nämndens behandlingsregister för personuppgiftsbehandlingar och genomföra korrigeringar samt kompletteringar i enlighet med avsnitt 9,* bör korrigeras till att avse avsnitt 8, eftersom avsnitt 9 avser Eskilstuna kommunfastigheter AB. En förutsättning för att kunna åtgärda alla brister i behandlingsregistren, är att granskningen hänvisar till alla de specifika brister som uppges i avsnitt 8 i rapporten. Målet är att nämnden under 2024 ska ha åtgärdat de brister som uppges i avsnitt 8 i granskningsrapporten.

Avseende tredje rekommendationen, att *Inkludera avgränsade kontrollmål avseende efterlevnad av dataskyddsförordningen i nämndens kommande internkontrollarbete, där det finns risker kopplad till hantering av personuppgifter* kommer vård- och omsorgsnämnden under 2024 att inkludera de risker som framkommit i granskningen i interkontrollplanen inför arbetet med internkontroll under 2025.

Vad avser den fjärde rekommendationen att *årligen följa upp och ta del av antal personuppgiftsincidenter inom respektive verksamhet som lyder under nämndens ansvarsområde,* är det något som redan görs. Dock har det i verksamheterna saknats en kultur och kompetens att rapportera personuppgiftsincidenter. I koppling till sista rekommendationen att *anordna utbildning avseende hantering av personuppgiftsincidenter för de medarbetare som hanterar personuppgifter,* är det också något som redan anordnats och som regelbundet fortsätter att anordnas. Utöver utbildning arbetar vård- och omsorgsnämndens verksamheter för att skapa en kultur där personalen vågar anmäla personuppgiftsincidenter.

———

VÅRD- OCH OMSORGSFÖRVALTNINGEN

Johan Lindström
Förvaltningschef

Åsa Tavemark
Utredningschef

Beslutet skickas till: Kommunstyrelsen och kommunrevisionen

Eskilstuna kommun

Kommunrevisionen

Till:
Kommunstyrelsen, Grundskolenämnden, vård- och omsorgs-nämnden samt Eskilstuna kommunfastigheter AB

För kännedom:
Kommunfullmäktige

Revisorernas granskning av rutiner för efterlevnad av GDPR/dataskyddsförordningen

Vi har med stöd av KPMG genomfört en granskning av kommunens rutiner för efterlevnad av GDPR/Dataskyddsförordningen med bland annat fokus på register över behandling av personuppgifter. Granskningen har varit en samordnad granskning mellan kommunens förtroendevalda revisorer och lekmannarevisor i Eskilstuna kommunfastigheter AB

Bakgrunden till vår granskning är att Dataskyddsförordningen (GDPR) som trädde i kraft den 25 maj 2018 och ersatta Personuppgiftslagen (PUL) bland annat syftar till ett starkare skydd för individers integritet och större makt till att kunna bestämma över sina personuppgifter. Genom lagstiftningen 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. Mot denna bakgrund har vi i vår riskanalys funnit det angeläget att följa upp hur nämnder och styrelser arbetar för att säkerställa efterlevnad av kraven på detta område.

Vår övergripande bedömning är att kommunstyrelsen och berörda nämnder och styrelse endast **delvis** har en ändamålsenlig styrning och kontroll vad avser efterlevnad av dataskyddsförordningen. Vår bedömning bygger på att det i granskningen framkommit utvecklingsområden och brister vad avser efterlevnaden av dataskyddsförordningen. Vår granskning visar bland annat att kommunstyrelsens inte genomfört uppföljningar av nämndernas arbete och efterlevnad av dataskyddsförordningen. Vår granskning av register över personuppgiftsbehandlingar visar också på centrala brister, med behov av översyn och korrigerande åtgärder.

Granskningen visar också att det i den årliga kontrollen av efterlevnad av dataskydds-förordningen, saknas nämndspecifika rapporter med resultat och rekommendation för respektive nämnds efterlevnad av dataskyddsförordningen. Nämnderna behandlar årsrapporten endast som allmän information som läggs till handlingarna, då den inte innehåller nämndspecifika redogörelser och riktade rekommendationer. I granskningen har även uppföljning av personuppgiftsincidenter genomförts och bedömningen är att det finns ett mörkertal inom detta område,
Sammanfattningsvis är vår bedömning att vår granskning visar både på ett behov av riktade utbildningsinsatser samt behov av utvecklad styrning och uppföljning i syfte att skapa en enhetlig hantering och förståelse inom nämnder och styrelser vad avser hantering av personuppgifter.

Granskningens samlade resultat presenteras i bifogad rapport. I revisionsrapporten finns också ett antal rekommendationer till berörda styrelser och nämnder.

Vi emotser kommunstyrelsens, granskade nämnders och Eskilstuna Kommunfastigheters AB:s yttrande till våra iakttagelser och rekommendationer samt en tidsplan för de åtgärder som planeras utifrån granskningen **senast 2024-04-30.**

Eskilstuna 2024-01-30

För revisorerna i Eskilstuna kommun

Tommy Kvarsell
Ordförande

Majvor Gyllhamn
Vice ordförande

Richard Karlsson
Lekmannarevisor

Granskning av rutiner för efterlevnad av GDPR/ Dataskyddsförordningen

- Register över personuppgiftsbehandlingar

Revisionsrapport
Eskilstuna kommun

KPMG AB

2024-01-29

Antal sidor: 32

Innehållsförteckning

1 Sammanfattande bedömning och rekommendationer

Vi har av Eskilstuna kommuns revisorer fått i uppdrag att granska kommunens rutiner för efterlevnad av dataskyddsförordningen med bland annat fokus på register över behandling av personuppgifter.

Vår samlade bedömning är att kommunstyrelsen delvis har en ändamålsenlig styrning vad avser efterlevnad av dataskyddsförordningen.

Vi bedömer att det finns utvecklingsområden och brister vad avser efterlevnaden av dataskyddsförordningen.

Av granskningen framkommer att det finns en dataskyddsorganisation följt av roll- och ansvarsfördelningar för berörda funktioner samt personuppgiftsansvariga nämnder.

Vi kan konstatera att styrelsen har fastställt centrala samt kommunövergripande styrdokument med sikte på hantering av personuppgifter, med undantag för rutiner för begäran om rättelse, radering och begräsning.

Kommunstyrelsen har inom ramen för sin uppsiktplikt ett ansvar att följa upp nämndernas efterlevnad av dataskyddsförordningen. Vi noterar att styrelsens uppsiktsplikt finns upptagen i styrdokumenten för behandling av personuppgifter, där det framgår att kommunstyrelsens ska regelbundet följa upp och granska att kraven i dataskyddsförordningen efterlevs.
Vid tid för granskningen har kommunstyrelsens inte genomfört uppföljningar av nämndernas arbete och efterlevnad av dataskyddsförordningen.
Vi noterar att försök till kommunövergripande insatser har genomförts som dock har avstannat på grund av organisatoriska och personella orsaker.

Det bör beaktas att kommunstyrelsens uppsiktsplikt inte ska förväxlas med rollen som personuppgiftsansvarig. Respektive nämnd och bolagsstyrelse är juridiskt sett ansvarig för hantering av de personuppgifter som sker inom nämndens ansvarsområden.

Vår granskning av register över personuppgiftsbehandlingar visar på centrala brister, där det finns behov av översyn och korrigerande åtgärder.

Vidare bör en inventering ske för att säkerställa att samtliga personuppgifts-behandlingar finns upptagna i behandlingsregistren.

Vad avser den ”årliga kontrollen av efterlevnad av dataskyddsförordningen”, framkommer avsaknad av nämndspecifika rapporter med resultat och rekommendation för respektive nämnds efterlevnad av dataskyddsförordningen. Vi noterar att en s.k. årsrapport upprättas som är på en generell nivå riktad till ”kommunen”. Nämnderna behandlar årsrapporten endast som allmän information som läggs till handlingarna, då den inte innehåller nämndspecifika redogörelser och riktade rekommendationer.

Vi bedömer att i syfte att den ”årliga kontrollen av efterlevnad av dataskydds-förordningen” ska fylla sin funktion och vara ändamålsenligt, erfordras att nämndspecifika rapporter med resultat, framkomna risker, brister, utvecklings-

områden följt av bedömning och riktade rekommendationer arbetas fram. Rapporterna ska därefter tillställas ansvarig nämnd för att möjliggöra att berörd nämnd tar ställning och beslut om erforderliga åtgärder.

Vidare är dokumenterade samt riktade nämndsrapporter nödvändiga för att möjliggöra uppföljningar inom nämnderna.

Likaså är sammanställningar av respektive nämnds resultat, risker och utvecklingsområden följt av riktade rekommendationer, av central betydelse för kommunstyrelsens utövning av uppsiktsplikten.

Vad avser personuppgiftsincidenter bedömer vi att det finns ett mörkertal.

Av granskningen framgår ett behov av riktade utbildningsinsatser samt behov av styrning i syfte att skapa en enhetlig hantering och förståelse inom nämnderna vad avser hantering av personuppgifter.

Utifrån resultatet av vår granskning, rekommenderar vi kommunstyrelsen att:

- säkerställa en enhetlig hantering samt kunskapsnivå gällande efterlevnad av dataskyddsförordningen. Detta görs bland annat genom kommun-övergripande styrdokument, områdesspecifika mallar, riktade utbildningar samt uppföljningar inom ramen för uppsiktsplikten.
- tillse att rutiner för rättelse, radering och begräsning av personuppgifter fastställts snarast.
- tillse att enkla och användarvänliga blanketter arbetas fram som underlättar för kommunmedborgarna att nyttja sina rättigheter vad avser ”begäran om rättelse, radering och begräsning”. Blanketterna bör finnas tillgängliga både i pappersform i kommunens reception samt digitalt på hemsidan.
- tillse att beslutsinstans samt fastställedatum av styrdokument i form av rutinbeskrivningar framgår.
- genomföra en inventering för att säkerställa att samtliga personuppgifts-behandlingar finns registrerade i behandlingsregistren.
- se över styrelsens behandlingsregister för personuppgiftsbehandlingar och genomföra korrigeringar samt kompletteringar i enlighet med avsnitt 8.2.
- fastställa en kommunövergripande mall som är gällande för samtliga nämnder för hantering av register över personuppgiftsbehandlingar. Detta är nödvändigt för att kunna skapa en enhetlig grundstruktur för behandlings-registren.
- säkerställa att kommunstyrelsen delges en årsrapport från dataskydds-ombudet innehållande en redogörelse för respektive nämnds resultat av genomförda kontroller följt av eventuella framkomna risker, brister och förbättringsområden avseende efterlevnad av dataskyddsförordningen. Detta i syfte att möjliggöra styrelsens utövande av uppsiktsplikten.

- genomföra uppföljningar av nämndernas arbete och efterlevnad av dataskyddsförordningen.
- tillse att nämndspecifika rapporter med resultatet av årliga interna kontroller, framkomna risker och brister, förbättringsområden följt av riktade rekommendationer arbetas fram och tillställs respektive nämnd. Detta är en grundläggande premiss för att möjliggöra att berörd nämnd tar ställning och beslut om erforderliga åtgärder.
- årligen ta del av en samlad redogörelse avseende antal inträffade personuppgiftsincidenter inom kommunstyrelsen samt nämnderna, i likhet med den tabell som vi har redogjort för på sid 20, i syfte att kunna inom ramen för uppsiktsplikten vidta åtgärder.
- inkludera avgränsade kontrollmål avseende efterlevnad av dataskydds-förordningen i styrelsens kommande internkontrollarbete, där det finns risker kopplad till hantering av personuppgifter. Avgränsningar till områdesspecifika kontroller i internkontrollplanen är av vikt för att undvika alltomfattande kontrollmål som till exempel ”*kontroll av efterlevnad av data-skyddsförordningen*”.

Grundskolenämnden

Utifrån resultatet av vår granskning, rekommenderar vi grundskolenämnden att:

- genomföra en inventering för att säkerställa att samtliga personuppgifts-behandlingar finns registrerade i behandlingsregistren.
- se över nämndens behandlingsregister för personuppgiftsbehandlingar och genomföra korrigeringar samt kompletteringar i enlighet med avsnitt 8.2.
- tillse att barn- och utbildningsförvaltningen i samband med årliga frågeformulär upprättar svar som avser grundskolenämnden. Frågorna i DSO:s formulär är riktad till respektive personuppgiftsansvarig nämnd, vilket är korrekt. Barn- och utbildningsförvaltningen lyder under tre nämnder, där respektive nämnd är personuppgiftsansvarig. För 2022 samt 2023 har ett gemensamt svar inlämnats för samtliga tre nämnder (med undantag för en enskild fråga för 2023).
  Vi har fått återkoppling om att detta kommer att åtgärdas för 2024.
- inkludera avgränsade kontrollmål avseende efterlevnad av dataskydds-förordningen i nämndens kommande internkontrollarbete, där det finns risker kopplad till hantering av personuppgifter. Avgränsningar till områdesspecifika kontroller i interkontrollplanen är av vikt för att undvika alltomfattande kontrollmål som t.ex. ”*kontroll av efterlevnad av dataskyddsförordningen*”.
- årligen följa upp och ta del av antal personuppgiftsincidenter inom respektive verksamhet som lyder under nämndens ansvarsområde.
- anordna utbildning avseende hantering av personuppgiftsincidenter för de medarbetare som hanterar personuppgifter. Grundskolenämnden hanterar en

omfattande mängd personuppgifter utifrån verksamheternas art och grunduppdrag.

Vård- och omsorgsnämnden

Utifrån resultatet av vår granskning, rekommenderar vi vård- och omsorgsnämnden att:

- genomföra en inventering för att säkerställa att samtliga personuppgifts-behandlingar finns registrerade i behandlingsregistren.
- se över nämndens behandlingsregister för personuppgiftsbehandlingar och genomföra korrigeringar samt kompletteringar i enlighet med avsnitt 9.
- inkludera avgränsade kontrollmål avseende efterlevnad av dataskydds-förordningen i nämndens kommande internkontrollarbete, där det finns risker kopplad till hantering av personuppgifter. Avgränsningar till områdesspecifika kontroller i internkontrollplanen är av vikt för att undvika alltomfattande kontrollmål som t.ex. ”*kontroll av efterlevnad av dataskyddsförordningen*”.
- årligen följa upp och ta del av antal personuppgiftsincidenter inom respektive verksamhet som lyder under nämndens ansvarsområde.
- anordna utbildning avseende hantering av personuppgiftsincidenter för de medarbetare som hanterar personuppgifter. Vård- och omsorgsnämnden hanterar en omfattande mängd personuppgifter utifrån verksamheternas art och grunduppdrag.

Eskilstuna Kommunfastigheter AB

Mot resultatet av vår granskning, rekommenderar vi styrelsen i Eskilstuna kommunfastigheter AB att:

- fastställa riktlinjer för behandling av personuppgifter.
- Fatta beslut om att utse ett dataskyddsombud.
  (*I samband med faktakontrollen har vi delgivits att styrelsen har utifrån granskningens synpunkter skyndsamt tagit beslut om ett dataskyddsombud*).
- Se över möjligheterna att centralisera hantering och underhåll av behandlingsregistren i syfte att säkerställa en korrekt hantering.
- genomföra en inventering för att säkerställa att samtliga personuppgifts-behandlingar finns registrerade i behandlingsregistren.
- se över styrelsens behandlingsregister för personuppgiftsbehandlingar och genomföra korrigeringar samt kompletteringar i enlighet med avsnitt 9.
- inkludera avgränsade kontrollmål avseende efterlevnad av dataskydds-förordningen i styrelsens kommande internkontrollarbete, där det finns risker kopplad till hantering av personuppgifter. Avgränsningar till områdesspecifika kontroller i internkontrollplanen är av vikt för att undvika alltomfattande kontrollmål som t.ex. ”*kontroll av efterlevnad av dataskyddsförordningen*”.

- årligen följa upp och ta del av antal personuppgiftsincidenter inom respektive verksamhetsområde.

2 Bakgrund

Vi har av Eskilstuna kommuns revisorer fått i uppdrag att granska kommunens rutiner för efterlevnad av dataskyddsförordningen med fokus på register över behandling av personuppgifter.

Två centrala delar inom ramen för efterlevnad av dataskyddsförordningen är upprättande av ”register över behandlingar av personuppgifter” samt ”hantering av personuppgiftsincidenter”. Denna granskning fokuserar bl.a. på den förstnämnda delen.

2.1 Syfte, revisionsfråga och avgränsning

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

- Finns en dataskyddsorganisation?
- Har samtliga nämnder beslutat om att utse ett dataskyddsombud?
- Befinner sig dataskyddsombudet i en oberoendeposition?
- Är det säkerställt att det finns registerförteckningar över personuppgiftsbehandlingar i enlighet med artikel 30.1, dataskyddsförordningen? (Avser kommunstyrelsen, vård- och omsorgsnämnden, grundskolenämnden samt Eskilstuna Kommunfastigheter AB)
- Är register över behandlingar korrekt upprättade utifrån dataskydds-förordningens grundläggande principer?
- Har inventering skett så att samtliga personuppgiftsbehandlingar finns upptagna i register i enlighet med artikel 30?
- Finns dokumenterade rutiner för begäran om registerutdrag?
- Finns dokumenterade rutiner för rättelse av uppgifter?
- Finns dokumenterade rutiner för radering och begränsning av uppgifter?

Granskningen avser kommunstyrelsen. Grundskolenämnden, vård- och omsorgsnämnden samt Eskilstuna kommunfastigheter ingår i den del som avser granskning av behandlingsregistreren.

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

Studium och genomgång av relevanta underlag, styrdokument och beslutsunderlag. Granskningen har introducerats för kommundirektören. Intervjuer har genomförts med kommunstyrelsens ordförande, kommunstrateg informationssäkerhet, central dataskyddssamordnare tillika ersättande dataskyddsombud, administrativ chef, förvaltningschef barn- och utbildningsnämnden samt förvaltningschef vård- och omsorgsnämnden. Introduktion samt samtal har ägt rum med dataskyddsombudet. Vidare har en revisionsenkät skickats till DSO, där frågor besvarats delvis.
Vad avser det kommunala bolaget Eskilstuna kommunfastigheter AB har granskningen introducerats för VD. Intervju har genomförts med utsedd nyckelperson, informationsstrateg.

Register över personuppgiftsbehandlingar för kommunstyrelsen, grundskolenämnden, vård- och omsorgsnämnden samt Eskilstuna Kommunfastigheter har begärts in för en särskild granskning.

Rapporten har faktakontrollerats av administrativ chef, kommunstrateg informationssäkerhet, förvaltningschef vård- och omsorg och förvaltningschef barn- och utbildning.
Berörda avsnitt har faktakontrollerats av central dataskyddssamordnare (kap. 4,8,10) och dataskyddsombud (kap. 7).

3. Resultat av granskningen

3.1 EU-rättslig lagstiftning

Dataskyddsförordningen (GDPR) trädde ikraft den 25 maj 2018 och är gällande ramverk för behandling av personuppgifter. I och med ikraftträdandet av dataskydds-förordningen, upphävdes personuppgiftslagstiftningen, (PuL 1998:204). Den nu gällande lagstiftningen syftar bland annat 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

4. Dataskyddsorganisation

Iakttagelser

Av granskningen framkommer att det finns utsedda dataskyddssamordnare (DSS) för respektive personuppgiftsansvarig nämnd. Dataskyddssamordnarna har till uppgift att stödja nämnden och förvaltningen vad avser dataskyddsfrågor och fungerar som en samordnade expertfunktion.

Funktionerna är organisatoriskt placerade under servicenämnden med undantag för vård- och omsorgsnämnden samt grundskolenämnden där dataskyddssamordnaren finns placerad i den egna förvaltningen.

Vi har tagit del av styrdokumenten för dataskydd, ”Riktlinje för behandling av personuppgifter”, (antagen av KF 2019-05-16), samt ”Anvisningar för behandling av personuppgifter”, (antagen av kommundirektören 2020-06-09).

Av styrdokumenten framgår att dataskyddssamordnarna ska kontaktas i första hand avseende frågor som rör dataskydd. Dataskyddssamordnaren har i nästa steg möjlighet att kontakta dataskyddsombudet för rådgivning.

Av granskningen framkommer att dataskyddssamordnarna har månatliga möten i syfte att ha en gemensam plattform samt skapa en enhetlig hantering inom förvaltningarna vad avser dataskydd.

Vad avser funktionen dataskyddsombud (DSO) ska tjänsten erbjudas av service-nämnden, vilket innebär att rollen som dataskyddsombud är organisatoriskt placerad under servicenämnden. Rollen som ersättande dataskyddsombud återfinns också under servicenämnden.

Tjänsten som dataskyddsombud samt dataskyddssamordnare (med undantag för vård- och omsorgsnämnden och grundskolenämnden avseende rollen som DSS), beställs och köps internt av servicenämnden genom en så kallad ”Årsöverens-kommelse”. Kostnaden debiteras respektive nämnd månadsvis. Kostnaden för kommunstyrelsen för perioden 2023-01-01 t.om. 2023-12-31 är 664 000 kr.

Det finns vidare en central funktion som kommunstrateg för informationssäkerhet med placering på kommunstyrelseförvaltningen med ett ansvar för det kommun-övergripande dataskyddsarbetet.

4.1 Kommentarer och bedömning

Vi bedömer att vid tid för granskningen finns en dataskyddsorganisation följt av relevanta styrdokument för dataskyddsorganisationen. Av styrdokumenten framgår roll- och ansvarsfördelningar för berörda funktioner samt personuppgiftsansvariga nämnder.

5. Utnämning av dataskyddsombud samt oberoende

Dataskyddsförordningen, (artikel 37, punkt 1), fastställer att ett dataskyddsombud 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.
Samtliga personuppgiftsansvariga nämnder ska därmed utse ett dataskyddsombud. Beslutet ska dokumenteras och vara protokollfört.

Dataskyddsombudets främsta uppdrag är att systematiskt informera och ge råd samt övervaka efterlevnaden av dataskyddsförordningen. Det är därmed av vikt att dataskyddsombudet inte innehar uppdrag och uppgifter som kan ifrågasätta oberoendet, där det till exempel inte är lämpligt att ett dataskyddsombud sitter i organisationens ledning eller är delaktig i att fatta strategiska beslut om kärnverksamheten.

Det förekommer frekvent att ett dataskyddsombud har en kombinerad tjänst där endast viss del av tjänsten ägnas uppdraget som dataskyddsombud. Det är enligt dataskyddsförordningen tillåtet att ett dataskyddsombud innehar andra uppgifter och uppdrag. Dock ska personuppgiftsansvarig nämnd och styrelse tillse att det inte uppstår intressekonflikter och jäv.

Iakttagelser

Vi har tagit del av nämndernas beslut vad avser dataskyddsombuden.

5.1 Kommentarer och bedömning

Vi bedömer att samtliga nämnder har formellt utsett och beslutat om ett dataskyddsombud.

Vid tid för granskningen är funktionen för ordinarie dataskyddombud organisatoriskt sett i en oberoende position.

6. Styrdokument och uppsiktsplikt

Kommunstyrelsen har ett ansvar för framtagande av kommunövergripande styrdokument och rutiner. Vidare har kommunstyrelsen inom ramen för sin **uppsiktplikt** ett ansvar att följa upp nämndernas efterlevnad av dataskyddsförordningen. Kommunstyrelsens uppsiktsplikt omfattar även de kommunala bolagen.

Det bör beaktas att detta inte fråntar nämndernas personuppgiftsansvar, där kommunstyrelsens uppsiktplikt inte ska förväxlas med rollen som personuppgiftsansvarig.

Iakttagelser

Av granskningen framkommer att centrala styrdokument med fokus på dataskyddsförordningen har framarbetats i form av: *Riktlinjer för behandling av personuppgifter* (antagen av KF 2019-05-16), *Anvisningar för behandling av personuppgifter* (antagen av kommundirektören 2020-06-09) samt *Rutin för hantering av personuppgiftsincident*. Det sistnämnda styrdokumentet saknar formell beslutsinstans och fastställelsedatum samt information om dokumentansvarig.

I dagsläget avser styrdokumenten endast nämnderna. Av intervjuerna framgår att det vore önskvärt om styrdokumenten kunde gälla hela kommunkoncernen.

Av granskningen framgår att riktlinjer och anvisningar för behandling av personuppgifter är under revidering. Vi har tagit del av utkasten som är under pågående justering och komplettering.

Av nuvarande styrdokumentet avseende anvisningar för behandling av person-uppgifter framgår att kommunstyrelsen är ansvarig för framtagande och uppföljning av kommunövergripande dokument.

Det fastställts vidare att kommunledningskontoret ska regelbundet granska att kommunen arbetar i enighet med gällande styrdokument för att säkerställa att kommunen efterlever kraven i dataskyddsförordningen.

I nytt utkast avseende anvisningar för behandling av personuppgifter har uppsikts-plikten förtydligats än mer, där det framgår att utifrån styrelsens uppsiktsplikt har kommunledningskontoret ett ansvar att regelbundet följa upp att kommunen och nämnderna efterlever kraven i dataskyddsförordningen samt arbetar enligt fastställda styrande dokument (Riktlinje samt anvisningar för behandling av personuppgifter).

Vidare kommer kommunstyrelsens ansvar för ajourhållning av styrdokument att läggas till med formuleringen att styrelsen är ansvarig för *framtagande, revidering* och *uppföljning* av kommunövergripande styrdokument.

Av granskningen framkommer att styrelsens inte har genomfört uppföljningar av **nämndernas** arbete och efterlevnad av dataskyddsförordningen och huruvida nämnderna uppfyller gällande krav.
Det framkommer dock att vid några tillfällen har försök till **kommunövergripande** insatser påbörjats, men som på grund av organisatoriska och personella orsaker avstannade. Ett exempel är beställning av en extern utredning under 2020 för att utreda kommunens organisation för dataskydd, som resulterade i att under 2021 tillsattes ett internt projekt med syfte att genomföra de förslag till förändringar som presenterats i utredningen, men som avstannade på grund av omorganisation. Vi har vidare delgivits en intern lista med några punktaktiviteter med benämningen ”aktiviteter dataskyddssamordnare - status”, som avser kommunövergripande rutiner samt en punkt som avser kvalitetssäkring av kommunstyrelsens egen register-förteckning, som bland annat kvarstår att åtgärda.

Av intervjuerna framgår att uppföljning av nämndernas efterlevnad är en utmaning då det inte finns dokumenterade rapporter som redogör för respektive nämnds grad av efterlevnad, risker, brister och utvecklingsområden, där den årsrapport som upprättas av dataskyddsombudet avseende ”årlig kontroll av efterlevnad av dataskyddsförordningen” är på en kommunövergripande nivå.
Dataskyddsförordningen är en omfattande och komplex lagstiftning, där kommunstyrelsen är i behov av de sakkunskaper som dataskyddsombuden ska besitta, för möjliggörande av kommunstyrelsens uppföljningar av nämndernas efterlevnad.

5.2.1 Kommentarer och bedömning

Vi bedömer att kommunstyrelsen har upprättat centrala samt kommunövergripande styrdokument med sikte på efterlevnad av dataskyddsförordningen.

Vi bedömer det som nödvändigt samt positivt att kommunstyrelsens uppsiktsplikt kommer att förtydligas i de kommande styrdokumenten för behandling av personuppgifter, där det i styrdokumentet avseende anvisningar, tydligt framgår att kommunstyrelsen ansvarar för att följa upp huruvida ”nämnderna” efterlever dataskyddsförordningen.
Vi bedömer vidare att avsnittet avseende styrelsens uppsiktsplikt bör även framgå av ”Riktlinje för behandling av personuppgifter”.

Vi bedömer att av *rutinen för hantering av personuppgiftsincident* bör beslutsinstans samt fastställelsedatum framgå, där rutinen har en betydande stödjande roll vad avser efterlevnad av dataskyddsförordningen. Denna information är av betydelse för de styrande dokumentens legitimitet.

Det finns inget hinder för att styrdokumenten (med undantag för intern-organisatoriska roller och ansvar) även omfattar de kommunala bolagen, där kommunen har ett s.k. **rättsligt bestämmande inflytande.**

Vi bedömer att kommunstyrelsen utifrån uppsiktsplikten samt gällande styr-dokument, inte har genomfört regelbundna uppföljningar av **nämndernas** arbete och efterlevnad av dataskyddsförordningen. Försök till kommunövergripande insatser har påbörjats men som har avstannat på grund av organisatoriska och personella orsaker.

7. Interngranskningar

I dataskyddsombudens (DSO) uppdrag ingår att informera och ge råd till personuppgiftsansvariga, personuppgiftsbiträden och anställda samt övervaka och kontrollera efterlevnaden av dataskyddsförordningen. Övervakning och kontroll ska ske genom granskningar. Dataskyddsombuden ska utses på grundval av bland annat sakkunskap om lagstiftning och praxis avseende dataskydd.

Resultatet samt riktade rekommendationer från interna granskningar utifrån dataskyddsombudens sakkunskap, är av vikt för att nämnderna ska kunna utveckla arbetet, hantera risker och vidta erforderliga åtgärder för att uppfylla kraven i dataskyddsförordningen.

Som tidigare nämnts har kommunstyrelsen inom ramen för uppsiktsplikten ett ansvar att följa upp nämndernas efterlevnad av dataskyddsförordningen (se avsnitt 6). Resultatet av DSO:s granskningar, utifrån fördjupade sakkunskaper som DSO ska besitta, är därmed av central betydelse för utövandet av kommunstyrelsens uppsiktsplikt. Av intervju med politik och personal inom kommunstyrelsen råder det enighet avseende vikten av styrelsens uppsiktplikt.

Det bör noteras att det är respektive nämnd som är juridiskt sett personuppgifts-ansvarig, vilket innebär att efter att DSO har avlämnat en nämndsrapport, är det nämnden som avgör vidarehanteringen i form av vilka åtgärder som ska vidtas och i

vilken omfattning. Efter avlämnade av nämndsrapporter ska DSO dock finnas tillgänglig för vägledning och stöd.

Iakttagelser

Introduktion samt samtal har genomförts med dataskyddsombudet, där DSO:s arbetssätt, former för DSO:s kontroller och leveranser, huruvida det sker dokumentation av interna granskningar för respektive nämnd, förutsättningar för DSO mm. delgivits och diskuterats.

Vad avser revisionens kärnfrågor samt efterfrågade underlag gällande interna granskningar och kontroller, har DSO hänvisat till förvaltningarna. Vi har därmed genom förvaltningarna delgivits befintligt underlag.

Vad avser dokumenterade interna granskningar och kontroller framkommer att DSO genomför årliga kontroller genom utskick av ett frågeformulär till respektive nämnd med benämningen ”kontroll av efterlevnad av dataskyddsförordningen för aktuellt år”. Frågorna rör olika områden inom dataskyddsförordningen och varierar från år till år. Vidare kan stickprov förekomma. Av granskningen framgår att DSO på begäran genomför dokumenterade kontroller av konsekvensbedömningar.

Resultatet av frågeformulären sammanställs av DSO, på en kommunövergripande nivå i en s.k. ”årsrapport”. Årsrapporten redogör inte för resultatet av den årliga kontrollen för respektive nämnd följt av status avseende huruvida nämnden uppfyller berörda krav i dataskyddsförordningen, utan är på en generell nivå riktad till ”kommunen”.

Vidare framgår, att det inte upprättas nämndspecifika rapporter som tillställs respektive personuppgiftsansvarig nämnd med resultatet av kontrollerna, bedömning och rekommendationer. Av granskningen framkommer det att det istället äger rum muntligt samtal med förvaltningarna.

Av intervju med förvaltningarna samt politik framgår att årsrapporten behandlas endast som allmän information som läggs till handlingarna, då den inte innehåller nämndspecifika redogörelser och riktade rekommendationer. Detta bekräftas av protokollsutdragen, där det framgår att rapporten inte redogör för dataskyddet hos enskilda nämnder.

Av granskningen framkommer att DSO erbjuder och genomför en muntlig presentation av årsrapporten i de fall nämnderna inte avstår. Vår genomgång av protokollen visar att redogörelse av årsrapporten har ägt rum för 6 av 13 nämnder som redovisas i tabell 10:1.

Av intervjuerna framkommer att årsrapporten inte anses vara ändamålsenlig, då den inte redogör för nämndernas arbete och lägesstatus vad avser efterlevnad av dataskyddsförordningen.

7.1 Kommentarer och bedömning

Vi bedömer att det inte är tillräckligt med en kommunövergripande årsrapport vad avser övervakning och kontroll av nämndernas efterlevnad av dataskydds-

förordningen.

Vi noterar att nämnderna hanterar årsrapporten endast som allmän information som läggs till handlingarna, då den inte redogör för dataskyddet hos enskilda nämnder.

Vi noterar avsaknad av nämndspecifika rapporter med resultat för respektive nämnds efterlevnad av dataskyddsförordningen. **Vi bedömer** att i syfte att den ”årliga kontrollen av efterlevnad av GDPR” ska fylla sin funktion samt vara ändamålsenligt, erfordras nämndspecifika rapporter med resultat, framkomna risker, brister, utvecklingsområden följt av bedömning och riktade rekommendationer. Rapporterna ska därefter tillställas personuppgiftsansvarig nämnd för att möjliggöra att berörd nämnd tar ställning och beslut om erforderliga åtgärder som rör den enskilda nämnden.

Vi bedömer vidare att dokumenterade samt riktade nämndsrapporter är nödvändiga för att möjliggöra uppföljningar inom respektive nämnd.

Vi bedömer att av den årliga rapporten med benämningen ”kontroll av efterlevnad av dataskyddsförordningen”, bör en sammanfattande redogörelse framgå för respektive nämnd med resultatet av genomförda kontroller följt av eventuella framkomna risker och brister avseende efterlevnad av dataskyddsförordningen. Detta i syfte att möjliggöra kommunstyrelsens utövande av uppsiktsplikten. Årsrapporten ska tillställas kommunstyrelsen.

Vi bedömer att de årliga frågeformulären är på en övergripande nivå.
Vi bedömer att frågor kopplade till de grundläggande principerna, bör finnas som fasta/stående frågor i det årliga frågeformuläret som skickas ut till nämnderna. De grundläggande principerna är en grundstomme och ett uppfyllande krävs för att en personsuppgiftsbehandling ska vara laglig och därmed är en central del inom ramen för efterlevnad av dataskyddsförordningen.

Vi bedömer att utöver årligt frågeformulär är det av vikt att fördjupade granskningar av avgränsade samt centrala områden genomförs och dokumenteras. Exempel på centrala områden är registerförteckningar, hantering och dokumentation av personuppgiftsincidenter, konsekvensbedömningar, registrerades rättigheter, rutiner vid upphandling avseende digitala system och tjänster, personuppgiftsbiträdesavtal mm.

8. Register över personuppgiftsbehandlingar (registerförteckningar) – Kommunstyrelsen, grundskolnämnden och vård- och omsorgsnämnden

I enlighet med dataskyddsförordningen, artikel 30, ska varje personuppgiftsansvarig föra ett register över personuppgiftsbehandling som sker under dess ansvar. Behandlingsregistren ska på begäran redovisas för tillsynsmyndigheten, dvs. Integritetsskyddsmyndigheten, där registren ska utgöra en grund för övervakning av

behandling av personuppgifter.

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

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

Iakttagelser

Vi har tagit del av kommunstyrelsens, grundskolenämndens och vård- och omsorgsnämndens upprättade registerförteckningar över personuppgifts-behandlingar. Nämnderna använder sig av SKR:s mall för registerförteckningar. Av intervju med dataskyddssamordnaren tillika ersättande dataskyddsombud uttrycks att en ny mall är under framtagning där det finns ett behov av omtag vad avser registerförteckningar. Den nya mallen kommer att arbetas fram med hjälp av systemstödet ”Arken”.

Av intervjuerna framkommer att nämnderna har genomfört en inventering av personuppgiftsbehandlingarna i varierande grad under 2019, där det är dags för en ny inventering.

Av intervju med förvaltningschefen för barn- och utbildning framhålls att de administrativa resurserna inom förvaltningen är och har varit mycket begränsande, där all administration lånats av serviceförvaltningen utifrån rådande organisations-struktur, vilket bland annat påverkar dataskyddsarbetet, HR-arbetet, ekonomi-uppföljning mm. Det framkommer vidare att under oktober 2023 gjordes på förekommen anledning omprioriteringar av handläggarresurser inom barn- och utbildningsförvaltningen som resulterade i en mer renodlad tjänst som dataskyddssamordnare med fokus på informationssäkerhet och efterlevnad av dataskyddsförordningen. Det uttrycks att innan dess har inga resurser funnits och arbetet har utförts inom befintliga tjänster i mån av tid.

8.1 Kommentarer och bedömning

Vi kan konstatera att samtliga tre granskade nämnder har upprättat register över personuppgiftsbehandlingar. Det kan dock finnas behandlingar som ännu ej upptagits i behandlingsregistren.
Vi bedömer att granskade nämnder bör genomföra en inventering i syfte att

säkerställa att samtliga behandlingar finns upptagna i behandlingsregistren.

8.2 Resultat av granskning av registren över personuppgifts-behandlingar

Vi har begärt in behandlingsregistren/registerförteckningarna för ovan nämnda tre nämnder. Det bör understrykas att vid behandling av personuppgifter måste verksamheterna stödja sig på en så kallad ”**rättslig grund**”. Utan en rättslig grund är personuppgiftsbehandling ej laglig. Vidare ska ett **särskilt, avgränsat, konkret** och **berättigat** ändamål anges för respektive behandling. Begreppet ”berättigat” innebär att ändamålet ska ha lagligt stöd.

Vi har genomfört en särskild granskning av behandlingsregistren/register-förteckningarna. Granskade behandlingsregister innehåller:

- 163 behandlingar inom kommunstyrelsen,
- 59 behandlingar inom grundskolenämnden samt
- 508 behandlingar inom vård- och omsorgsnämnden.

Vår granskning visar på nedan brister:

- Bristande rättslig/laglig grund.
  ”**Allmänt intresse/Uppgift av allmänt intresse**” återkommer frekvent som rättslig grund utan hänvisning till lagstöd inom samtliga tre nämnder. För kommunstyrelsens del är det 94 behandlingar och för grundskolenämndens del avser det 48 behandlingar (se nedan för vård- och omsorgsnämnden). För att uppgift av allmänt intresse ska kunna användas krävs stöd i lagstiftning eller beslut som har meddelats med stöd av lagstiftning eller avtal. Vi noterar att i ett fåtal fall förekommer korrekt stöd i där lagstiftning och berörd paragraf anges.

- ”**Myndighetsutövning**” i kombination med ”**Uppgift av allmänt intresse**” används i majoritet av fallen (283 behandlingar) inom vård- och omsorgsnämnden, dock saknas hänvisning till aktuell författning. All myndighetsutövning ska grundas på lagar inom nationell rätt eller EU-rätten. Se ovan stycke avseende krav för användning av ”uppgift av allmänt intresse”.

- ”**Rättslig förpliktelse**” används som rättslig grund inom samtliga nämnder. Dock saknas information om vilken lagstiftning och lagrum som behandlingen grundar sig på.

- Förekomst av behandlingar där svarsrutan för rättslig grund står tomt, inom samtliga tre nämnder.

- **Bristfälliga svar** på frågan om **tidsfrist för radering.**
  Följande svar återkommer i kommunstyrelsens behandlingar: enligt dokumenthanteringsplan, oklart, på gång, kollas upp, saknas, enligt arkivlagen, finns ej, nej, ska arkiveras mm.

  Vad avser i vård- och omsorgsnämnden hänvisas till nämndens dokumenthanteringsplan i 117 behandlingar. Det förekommer vidare svar i form av hänvisning till ”rutin”.
  Det är sammantaget inte tillräckligt med en hänvisning till dokument-hanteringsplaner eller rutiner, utan tidsfrister ska anges.

- **Avsaknad av svar avseende tidsfrist för radering** saknas i 62 behandlingar inom kommunstyrelsens behandlingsregister. Detta förekommer i ett fåtal fall inom grundskolenämnden samt vård- och omsorgsnämnden.
- **Hänvisning till PUB-avtal** (personuppgiftsbiträdesavtal) vad avser **tidsfrist för radering**, förekommer i 7 behandlingar inom grundskolenämnden, vilket inte är korrekt.
- Förekomst av **avsaknad av svar** samt **vet-ej-svar** avseende huruvida personuppgifter **överförs till tredje land** inom grundskolenämnden samt kommunstyrelsens behandlingar. Vård- och omsorgsnämnden är den nämnd som har besvarat frågan inom samtliga behandlingar.

  Av vår granskning framkommer att av grundskolenämndens 59 behandlingar finns 16 behandlingar där överföring av personuppgifter sker till tredje land.
  Av vård och omsorgsnämndens 508 behandlingar finns 4 behandlingar där det kan förekomma överföring av personuppgifter till tredje land.
  Vad avser kommunstyrelsen finns 5 behandlingar där överföring sker.

  Vi vill understryka att **överföring till tredje land är endast tillåtet under vissa förutsättningar**. Överföring till tredjeland kan ske om EU-kommissionen har tagit ett beslut om att tredjelandet har säkerställt en adekvat skyddsnivå.
  Om ett sådant beslut från kommissionen saknas kan överföring endast ske efter att ansvarig nämnd har vidtagit lämpliga skyddsåtgärder och säkerställt att rättigheter för registrerade följt av effektiva rättsmedel finna tillgängliga i berört land. Exempel på tillåtna former är:

  - Ett rättsligt bindande och verkställbart instrument mellan offentliga myndigheter
  - Bindande företagsbestämmelser (Binding Corporate Rules)
  - Standardiserade dataskyddsbestämmelser i form av EU-rättsliga standardavtalsklausuler (Standard Contractual Clauses for data transfers to third countries) mm.

  I vissa fall kan ytterliga skyddsåtgärder behövas utöver standardavtals-klausuler.

- Vi noterar vidare att i grundskolenämndens registerförteckning finns en behandling där det anges att personuppgifter överförs till USA, men att det inte finns någon risk för registrerades rättigheter då inga känsliga person-uppgifter överförs. Det framgår vidare att arbete behöver göras för att ersätta detta system med ett annat. Vi vill framhålla att lagstiftningen avseende överföring av personuppgifter till tredjeland avser samtliga personuppgifter, dvs. inte endast känsliga personuppgifter.

- Avsaknad samt bristfälliga svar av huruvida **personuppgiftsbiträden** har anlitats. Denna punkt inte är obligatoriskt i själva registren men behöver finnas dokumenterad på något sätt, där nämnder och styrelser i nästa steg i egenskap av personuppgiftsansvariga behöver säkerställa att biträden har en korrekt hantering samt adekvata säkerhetsåtgärder.

  I kommunstyrelsens register finns 34 behandlingar där det saknas information om huruvida ett personuppgiftsbiträde anlitas. Vidare återfinns 45 behandlingar där det svaret har angetts till ”behövs ej”, vilket bör korrigeras till ”nej” om det är det som åsyftas. I vård- och omsorgsnämndens register återfinns 36 behandlingar där denna information saknas.

- Avsaknad av beskrivning av **tekniska och organisatoriska säkerhets-åtgärder**. Denna punkt syftar till att säkerställa den grundläggande principen om ”**Integritet och konfidentialitet**”. Personuppgiftsansvariga nämnder och styrelser ansvarar för att samtliga personuppgifter som behandlas skyddas.

  Granskningen visar att det i kommunstyrelsens register finns 32 behandlingar där beskrivning av ovan information saknas. Inom grundskolenämnden återfinns 27 behandlingar där svar saknas.

Vi noterar att det förekommer behandling av känsliga personuppgifter s.k. särskilda kategorier av personuppgifter. Dataskyddsförordningen fastställer att det förbjudet att behandla **känsliga personuppgifter** så som exempelvis uppgifter om *hälsa, etniskt ursprung/nationalitet politiska åsikter, religiös eller filosofisk övertygelse, behandling av genetiska uppgifter* mm. Det finns dock undantag från förbudet. Vad avser behandling av känsliga personuppgifter ska samtliga personuppgiftsansvariga nämnder och styrelser säkerställa att specificerade krav enligt artikel 9 i dataskyddsförordningen, följt av krav på **konsekvensbedömningar** i enlighet med artikel 35 uppfylls. Detta ställer krav på att behandling av känsliga personuppgifter ska vara väl grundad samt stödjas av en gällande laglig grund.

- **Bristande rättslig grund** för behandling av känsliga personuppgifter.

- I kommunstyrelsens register förekommer behandlingar med benämningen ”Statistisk” där **känsliga personuppgifter** behandlas. Det anges att *födelseland, medborgarskap, uppgifter om hälsa, sexuell läggning (samkönade äktenskap)* och *inkomster* behandlas. Som rättslig grund anges ”Allmänt intresse” följt av hänvisning till offentlighets- och sekretesslagen. Vi vill uppmärksamma kommunstyrelsen att uppgifter till statistiska ändamål kan

endast behandlas om de inte är identitetsigenkännande, dvs. varken direkt eller indirekt kan kopplas till en enskild person.

- I vård- och omsorgsnämndens register förekommer behandling med benämningen ”tilldelning av arbetsplats” i samband med rekrytering av vikarier, där det anges att *etnicitet, familjeförhållande* och *andra känsliga uppgifter om personen,* behandlas. Rättslig grund anges till ”Rättslig förpliktelse”. Vi kan inte se ett berättigat ändamål med denna behandling, där behandlingen också saknar stöd i lagstiftningen. Vidare kan inte angivning av typer av uppgifter sammanslås i form av ”…*och andra känsliga person-uppgifter om personen*”.

- Bristande svar på frågorna ”**vilka typer av personuppgifter behandlas**” samt ”**vilka känsliga personuppgifter som behandlas**”, där det i vård- och omsorgsnämndens register förekommer 34 fall och i kommunstyrelsens register 38 fall där svar har angivits till ”*kan innehålla alla typer av person-uppgifter*” samt ”*allt*”.
  Grundskolenämnden är den nämnd som har hanterat frågan på ett korrekt sätt i sina behandlingar.

- Det förekommer **avsaknad av svar** på frågorna ”**vilka typer av personuppgifter behandlas**” samt ”**vilka känsliga personuppgifter som behandlas**”, inom kommunstyrelsens (31 fall) samt vård- och omsorgsnämndens behandlingar (11 fall).

- Inom vård- och omsorgsnämndens register förekommer **sammanslagna behandlingar** med flertalet ändamål så som ”*medarbetarsamtal, korrigerande samtal, underlag, omställning, minnesanteckningar, chefsöverenskommelser, sjukintyg osv*”. Detta strider mot gällande lagstiftning.

- **Inkomplett behandling.** Inom grundskolenämnden förekommer fall där endast behandlingens namn och systemägare framgår. Behandlingarna avser extern placering av ungdomar och det är av yttersta vikt att behandlingarna kompletteras snarast.

- Vi noterar att i grundskolenämndens register förekommer ett fall inom skolhälsovården med benämningen ”**Filmning av vuxen patient i utbildningssyfte**”. Behandlingens ändamål anges till ”inspelning av behandlingssituation i syfte att genomgå utbildning i KBT”.
  Som svar på vilka kategorier av registrerade som behandlingen omfattar, anges ”medarbetare, patient”.
  Vi ställer oss frågande till denna personuppgiftsbehandling inom grundskolan. Av intervju med förvaltningschefen för barn- och utbildning bekräftas att KBT-behandlingar finns inte inom grundskolan.
  Vidare ställer vi oss frågande till vilken kategori av registrerande som är ”patient”. Handlar det om barn- och ungdomar/elever som söker sig till skolhälsovården, är det förbjudet med alla former av filmning.

I samband med faktakontrollen har vi delgivits att behandlingen avser inspelning av frivillig personal inom elevhälsan inom ramen för fortbildning, Filmning av barn/ungdomar/elever har inte förekommit. Behandlingen pågår inte längre.

- Det förekommer en behandling inom grundskolan med benämningen ”**skolintyg**”, där det anges att känsliga personuppgifter så som etnicitet, religion, hälsotillstånd och sociala förhållanden behandlas. Som extern mottagare av uppgifterna anges ”statliga myndigheter”. Rättslig grund anges till ”allmänt intresse”. Vi kan inte se något stöd för behandling av känsliga personuppgifter för denna behandling, där nämnden behöver se över denna behandling.
  Av intervju med förvaltningschefen för barn- och utbildning framkommer att det med största sannolikhet avser **inkommande intyg** från externa myndigheter, dock råder det enighet att det finns frågetecken kring statliga myndigheter som **mottagare**.

  I samband med faktakontrollen har vi delgivits att behandlingen avser förfrågningar från Skatteverket och Försäkringskassan, där uppgifter kan begäras ut utifrån nämndens skolpliktbevakning i syfte att konstatera huruvida barn och vårdnadshavare är bosatta i Sverige eller ej. Vidare framgår att uppgifter som etnicitet mm. delas ej vid en sådan begäran.

  Behandlingen bör därmed korrigeras med bland annat information om att känsliga personuppgifter inte behandlas inom ramen för ”skolintyg”.

8.2.1 Kommentarer och bedömning

Vi bedömer att behandlingsregistren inte är på en tillfredställande nivå, där det erfordras översyn och korrigerande åtgärder av respektive nämnd.
Av intervjuerna med förvaltningarna framgår en medvetenhet kring behovet av ett förbättringsarbete vad avser behandlingsregistren.

Vi bedömer att nämnderna bör genomföra en inventering för att säkerställa att samtliga personuppgiftsbehandlingar finns registrerade.

9. Resultat av granskning av registren över personuppgifts-behandlingar inom Eskilstuna kommunfastigheter AB

Vi har delgivits bolagets register över personuppgiftsbehandlingar. Bolaget använder sig av systemstödet Drafit.

Vi har genomfört en granskning av bolagets behandlingsregister. Register-förteckningen för bolaget omfattar 72 personuppgiftsbehandlingar. Vår granskning visar på nedan brister som förekommer i 7–19 behandlingar.

- Förekomst av **avsaknad av rättslig/laglig grund.**

- **Bristande rättslig grund**. ”Uppgift av allmänt intresse, myndighetsutövning samt rättslig förpliktelse ” återkommer som rättslig grund utan hänvisning till lagstöd. För att dessa grunder ska kunna användas krävs stöd i lagstiftning eller beslut som har meddelats med stöd av lagstiftning eller avtal. Det bör också noteras att ”myndighetsutövning” förekommer i ytterst begränsade fall och avser de kommunala bolag där kommunen har ett rättsligt bestämmande inflytande. Exempel på detta är begäran om allmänna handlingar inom ramen för offentlighetsprincipen.

- Avsaknad av svar samt vet-ej-svar om huruvida **känsliga personuppgifter** behandlas.

- Förekomst av begreppet ”**annat**” i samband med beskrivning av vilka personuppgifter som behandlas.

- Avsaknad av **vilka typer av känsliga personuppgifter** som behandlas.

- Förekomst av avsaknad av vilka **typer av personuppgifter** som behandlas.

- Avsaknad av svar samt vet-ej-svar avseende huruvida det sker en överföring **av personuppgifter till tredje land**.

- Förekomst av vet-ej-svar gällande huruvida ett **personsuppgiftbiträde** har anlitats samt huruvida det finns det finns ett **personuppgiftsbiträdeavtal**.

- Förekomst av vet-ej-svar gällande **beskrivning av tekniska och organisatoriska säkerhetsåtgärder.**

- Förekomst av flera rättsliga grunder för en och samma behandling.

- Förekomst av behandlingar där **samtliga frågor är obesvarade.**

Övriga iakttagelser

Vi noterar att bolaget har fastställt riktlinjer för behandling av personuppgifter (antagen av ledningsgruppen 2023-03-24).

Av intervju med informationsstrateg på bolaget framkommer att respektive verksamhetsområde (för närvarande 7) har ett ansvar att upprätta och uppdatera behandlingsregistren. Det uttrycks att framkomna brister beror på avsaknad av kunskap och kompetens inom verksamheterna. Det har förts diskussioner om att centralisera hanteringen av behandlingsregistren utifrån att sakkunskap inom området inte kan tillgängliggöras inom respektive verksamhetsområde, dock finns inte resurser i dagsläget.

Det uttrycks vidare att det råder oklarheter kring nivå på behandlingarna där dessa utgår ibland från digitala system i sin helhet, ibland från enskilda processer och ibland andra grunder. Det som är av vikt är att särskilt, avgränsat, konkret och berättigat ändamål ska anges för respektive behandling oaktat om behandlingen återfinns i ett system, process mm.

Vid tid för granskningen är ett styrdokument i form av ”informationssäkerhetspolicy” under framtagning, där ett sådant styrdokument har tidigare saknats. Detta anges bero på avsaknad av tillräckliga kunskaper.

Det framgår att bolaget köper tjänsten som dataskyddsombud (DSO) från ett externt konsultföretag. Det bör noteras att det inte råder personunion vad avser dataskyddsombuden i kommunens nämnder och bolaget. Avtalet vad avser köp av tjänsten som DSO löper ut sista december 2024. Av granskningen framkommer styrelsen inte har tagit ett beslut vad avser att utse dataskyddsombud.

Av intervju med informationsstrateg uttrycks att det råder oenighet vad avser hantering av registerförteckningarna, där bolaget och DSO inte är överens om bland annat vilka rättsliga grunder som är tillämpliga. Det framgår vidare att bolaget har på grund av detta valt att ta stöd från en advokatbyrå som i tur stödjer bolagets ställningstagande.

Vi har vidare begärt in uppgifter avseende inträffade personuppgiftsincidenter för perioden 2018–2023. Granskning av bolagets hantering av personuppgiftsincidenter har inte ingått i denna revision.

Figur 9:1

Bolag	Antal PUI 2018	Varav anmälda till IMY	Antal PUI 2019	Varav anmälda till IMY	Antal PUI 2020	Varav anmälda till IMY	Antal PUI 2021	Varav anmälda till IMY	Antal PUI 2022	Varav anmälda till IMY	Antal PUI 2023	Varav anmälda till IMY
Eskilstuna kommunfastigheter AB	Data saknas	Data saknas	Data saknas	Data saknas	0	0	9	0	2	0	5	0

9.1 Kommentarer och bedömning

Vi bedömer att det finns brister i behandlingsregistren som behöver åtgärdas av styrelsen.

Vi bedömer att styrelsen behöver ta ett formellt beslut avseende att utse ett dataskyddsombud.

Vi bedömer att styrdokument i form av riktlinjer bör fastställas av styrelsen.

Vi bedömer att det med stor sannolikhet finns ett mörkertal vad avser inträffade personuppgiftsincidenter.

I samband med faktakontrollen har det framkommit att styrelsen utifrån granskningens synpunkter har skyndsamt fattat ett beslut om att utse ett dataskyddsombud. Detta bedöms som positivt.

10. Personuppgiftsincidenter

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

- att individer förlorar kontrollen över sina uppgifter eller
- att rättigheterna inskränks genom exempelvis obehörigt röjande av eller
- obehörig åtkomst till personuppgifter.

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. De personuppgiftsincidenter som inte bedöms medföra risker för individers rättigheter och friheter behöver inte anmälas.

En central punkt samt krav som samtliga nämnder och styrelser ska beakta 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 (artikel 34, punkt 1).

Vidare finns särskilda krav i lagstiftningen vad avser risk- och konsekvensbedömning samt dokumentation av respektive personuppgiftsincident.

Granskning av ovan nämnda delar har inte ingått i denna revision.

Iakttagelser

I syfte att få en överblick avseende omfattningen och därmed också kunskapssnivån inom förvaltningarna vad avser personuppgiftsincidenter, har vi begärt in antal upptäckta incidenter för samtliga nämnder *(se figur 10:1*). Vi har begärt in antal incidenter för perioden 2018 – 2023 för en jämförelse över tid.

Det bör noteras att barn- och utbildningsnämnden har genomgått en omstrukturering fr.o.m. 2019 och är sedan dess uppdelad i tre nämnder.

Figur 10:1

Nämnd	Antal PUI 2018	Varav anmälda till IMY	Antal PUI 2019	Varav anmälda till IMY	Antal PUI 2020	Varav anmälda till IMY	Antal PUI 2021	Varav anmälda till IMY	Antal PUI 2022	Varav anmälda till IMY	Antal PUI 2023	Varav anmälda till IMY
Kommunstyrelsen	1	1	1	1	1	1	1	1	0	0	3	3
Grundskolenämnden	-	-	6	3	3	3	1	1	19	11	20	16
Vård- och omsorgsnämnden	0	0	Data saknas	Data saknas	4	4	6	6	16	16	19	19
Förskolenämnden	-	-	2	2	2	2	5	5	7	6	6	5
Gymnasienämnden	-	-	3	2	2	1	2	1	1	1	4	3
Barn- och utbildningsnämnden (fr.o.m. 2019 FSN, GN, GSN)	1	1										
Socialnämnden	0	0	3	3	1	1	3	2	5	4	0	0
Arbetsmarknads- och vuxenutbildningsnämnden	0	0	2	2	0	0	3	3	2	2	10	9
Servicenämnden	0	0	1	1	6	1	0	0	2	2	0	0
Stadsbyggnadsnämnden	0	0	0	0	0	0	0	0	0	0	1	0
Kultur- och fritidsnämnden	1	1	1	0	1	1	1	1	1	1	3	3
Miljö- och räddningstjänstnämnden	0	0	0	0	0	0	0	0	1	1	0	0
Valnämnden	0	0	0	0	0	0	0	0	0	0	0	0
Överförmyndarnämnden	1	1	0	0	0	0	0	0	1	1	0	0

10.1 Kommentarer och bedömning

Vi bedömer att det finns ett mörkertal vad avser inträffade personuppgiftsincidenter. Kommunen har ca 9000 anställda, där vi bedömer sannolikheten att flera nämnder inte har haft någon personuppgiftsincident under flera år alternativt endast ett fåtal fall som låg. De intervjuade är eniga om att det med stor sannolikhet finns ett mörkertal. Vi bedömer att den främsta orsaken kan vara avsaknad av kunskap om vad en personuppgiftsincident är samt hur den ska hanteras. Vidare kan ytterligare orsak till mörkertalet vara rädsla för eventuella sanktioner.

Vi anser att det finns behov av riktade utbildningsinsatser med fokus på person-uppgiftsincidenter, för förvaltningar samt personal ute i verksamheterna som hanterar personuppgifter.
Av intervjuerna framgår att en s.k. nano-utbildning är under framtagning för både personal och politiker, vilket bedöms som positivt. Vi anser att utbildningen bör vara obligatorisk, där kännedom och korrekt hantering av personuppgiftsincidenter är central för förebyggande arbete avseende skydd av individers integritet och rättigheter.

Vid tid för granskningen saknar kommunstyrelsen inblick och uppfattning av antal inträffade incidenter inom kommunens verksamheter.

11. Registerutdrag, rättelse, radering och begränsning

Dataskyddsförordningen fastställer 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.

Den registrerade har bland annat rätt till att få information om *ändamål med behandlingen, kategorier av personuppgifter som behandlas, de mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, tidsfrist för gallring* mm.

Ytterligare rättighet avser information om *varifrån uppgifter har insamlats*, om personuppgifterna inte har samlats in från den registrerade själv.

Det bör noteras att ett registerutdrag ska på begäran utlämnas utan onödigt dröjsmål och senast **en månad** efter att begäran har mottagits.

Vidare 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 noterar att det finns en rutin för begäran av registerutdrag med benämningen ”Rutin för handläggning av begäran om registerutdrag avseende personuppgifter”, (dokumentdatum 2021-10-26).

Av granskningen framkommer avsaknaden av rutiner för rättelse, radering och begränsning. Vi har delgivits ett utkast till rutin från 2023-03-16.

11.1 Kommentarer och bedömning

Vi bedömer att kommunstyrelsen snarast bör tillse att rutinbeskrivningar för hanteringen av begäran om rättelse, radering och begränsning fastställts. Dataskyddsförordningen trädde i kraft 25 maj 2018, där det är en brist att det ännu inte finns fastställda rutiner avseende säkerställande av de registrerades rättigheter. Rutinbeskrivningen bör omfatta en praktisk hantering vid en inkommen begäran samt ansvars- och rollfördelningar. Av rutinen bör fastsällesdatum samt beslutsinstans framgå.

Vi bedömer rutinbeskrivningen avseende begäran av registerutdrag som ändamålsenlig, där det finns beskrivning av en praktisk hantering vid en inkommen begäran.

12. Samlad bedömning och rekommendationer

Vår samlade bedömning är att kommunstyrelsen delvis har en ändamålsenlig styrning vad avser efterlevnad av dataskyddsförordningen.

Vi bedömer att det finns utvecklingsområden och brister vad avser efterlevnaden av dataskyddsförordningen.

Av granskningen framkommer att det finns en dataskyddsorganisation följt av roll- och ansvarsfördelningar för berörda funktioner samt personuppgiftsansvariga nämnder.

Vi kan konstatera att styrelsen har fastställt centrala samt kommunövergripande styrdokument med sikte på hantering av personuppgifter, med undantag för rutiner för begäran om rättelse, radering och begräsning.

Kommunstyrelsen har inom ramen för sin uppsiktplikt ett ansvar att följa upp nämndernas efterlevnad av dataskyddsförordningen. Vi noterar att styrelsens uppsiktsplikt finns upptagen i styrdokumenten för behandling av personuppgifter, där det framgår att kommunstyrelsens ska regelbundet följa upp och granska att kraven i dataskyddsförordningen efterlevs.

Vid tid för granskningen har kommunstyrelsens inte genomfört uppföljningar av nämndernas arbete och efterlevnad av dataskyddsförordningen.
Vi noterar att försök till kommunövergripande insatser har genomförts som dock har avstannat på grund av organisatoriska och personella orsaker.

Det bör beaktas att kommunstyrelsens uppsiktsplikt inte ska förväxlas med rollen som personuppgiftsansvarig. Respektive nämnd och bolagsstyrelse är juridiskt sett ansvarig för hantering av de personuppgifter som sker inom nämndens ansvarsområden.

Vår granskning av register över personuppgiftsbehandlingar visar på centrala brister, där det finns behov av översyn och korrigerande åtgärder.

Vidare bör en inventering ske för att säkerställa att samtliga personuppgifts-behandlingar finns upptagna i behandlingsregistren.

Vad avser den ”årliga kontrollen av efterlevnad av dataskyddsförordningen”, framkommer avsaknad av nämndspecifika rapporter med resultat och rekommendation för respektive nämnds efterlevnad av dataskyddsförordningen. Vi noterar att en s.k. årsrapport upprättas som är på en generell nivå riktad till ”kommunen”. Nämnderna behandlar årsrapporten endast som allmän information som läggs till handlingarna, då den inte innehåller nämndspecifika redogörelser och riktade rekommendationer.

Vi bedömer att i syfte att den ”årliga kontrollen av efterlevnad av dataskydds-förordningen” ska fylla sin funktion och vara ändamålsenligt, erfordras att nämndspecifika rapporter med resultat, framkomna risker, brister, utvecklings-områden följt av bedömning och riktade rekommendationer arbetas fram. Rapporterna ska därefter tillställas ansvarig nämnd för att möjliggöra att berörd nämnd tar ställning och beslut om erforderliga åtgärder.

Vidare är dokumenterade samt riktade nämndsrapporter nödvändiga för att möjliggöra uppföljningar inom nämnderna.

Likaså är sammanställningar av respektive nämnds resultat, risker och utvecklingsområden följt av riktade rekommendationer, av central betydelse för kommunstyrelsens utövning av uppsiktsplikten.

Vad avser personuppgiftsincidenter bedömer vi att det finns ett mörkertal.

Av granskningen framgår ett behov av riktade utbildningsinsatser samt behov av styrning i syfte att skapa en enhetlig hantering och förståelse inom nämnderna vad avser hantering av personuppgifter.

Utifrån resultatet av vår granskning, rekommenderar vi kommunstyrelsen att:

- säkerställa en enhetlig hantering samt kunskapsnivå gällande efterlevnad av dataskyddsförordningen. Detta görs bland annat genom kommun-övergripande styrdokument, områdesspecifika mallar, riktade utbildningar samt uppföljningar inom ramen för uppsiktsplikten.
- tillse att rutiner för rättelse, radering och begräsning av personuppgifter fastställts snarast.

- tillse att enkla och användarvänliga blanketter arbetas fram som underlättar för kommunmedborgarna att nyttja sina rättigheter vad avser ”begäran om rättelse, radering och begräsning”. Blanketterna bör finnas tillgängliga både i pappersform i kommunens reception samt digitalt på hemsidan.
- tillse att beslutsinstans samt fastställedatum av styrdokument i form av rutinbeskrivningar framgår.
- genomföra en inventering för att säkerställa att samtliga personuppgifts-behandlingar finns registrerade i behandlingsregistren.
- se över styrelsens behandlingsregister för personuppgiftsbehandlingar och genomföra korrigeringar samt kompletteringar i enlighet med avsnitt 8.2.
- fastställa en kommunövergripande mall som är gällande för samtliga nämnder för hantering av register över personuppgiftsbehandlingar. Detta är nödvändigt för att kunna skapa en enhetlig grundstruktur för behandlings-registren.
- säkerställa att kommunstyrelsen delges en årsrapport från dataskydds-ombudet innehållande en redogörelse för respektive nämnds resultat av genomförda kontroller följt av eventuella framkomna risker, brister och förbättringsområden avseende efterlevnad av dataskyddsförordningen. Detta i syfte att möjliggöra styrelsens utövande av uppsiktsplikten.
- genomföra uppföljningar av nämndernas arbete och efterlevnad av dataskyddsförordningen.
- tillse att nämndspecifika rapporter med resultatet av årliga interna kontroller, framkomna risker och brister, förbättringsområden följt av riktade rekommendationer arbetas fram och tillställs respektive nämnd. Detta är en grundläggande premiss för att möjliggöra att berörd nämnd tar ställning och beslut om erforderliga åtgärder.
- årligen ta del av en samlad redogörelse avseende antal inträffade personuppgiftsincidenter inom kommunstyrelsen samt nämnderna, i likhet med den tabell som vi har redogjort för på sid 20, i syfte att kunna inom ramen för uppsiktsplikten vidta åtgärder.
- inkludera avgränsade kontrollmål avseende efterlevnad av dataskydds-förordningen i styrelsens kommande internkontrollarbete, där det finns risker kopplad till hantering av personuppgifter. Avgränsningar till områdesspecifika kontroller i internkontrollplanen är av vikt för att undvika alltomfattande kontrollmål som t.ex. ”*kontroll av efterlevnad av dataskyddsförordningen*”.

Grundskolenämnden

Utifrån resultatet av vår granskning, rekommenderar vi grundskolenämnden att:

- genomföra en inventering för att säkerställa att samtliga personuppgifts-behandlingar finns registrerade i behandlingsregistren.

- se över nämndens behandlingsregister för personuppgiftsbehandlingar och genomföra korrigeringar samt kompletteringar i enlighet med avsnitt 8.2.
- tillse att barn- och utbildningsförvaltningen i samband med årliga frågeformulär upprättar svar som avser grundskolenämnden. Frågorna i DSO:s formulär är riktad till respektive personuppgiftsansvarig nämnd, vilket är korrekt. Barn- och utbildningsförvaltningen lyder under tre nämnder, där respektive nämnd är personuppgiftsansvarig. För 2022 samt 2023 har ett gemensamt svar inlämnats för samtliga tre nämnder (med undantag för en enskild fråga för 2023).
  Vi har fått återkoppling om att detta kommer att åtgärdas för 2024.
- inkludera avgränsade kontrollmål avseende efterlevnad av dataskydds-förordningen i nämndens kommande internkontrollarbete, där det finns risker kopplad till hantering av personuppgifter. Avgränsningar till områdesspecifika kontroller i interkontrollplanen är av vikt för att undvika alltomfattande kontrollmål som t.ex. ”*kontroll av efterlevnad av dataskyddsförordningen*”.
- årligen följa upp och ta del av antal personuppgiftsincidenter inom respektive verksamhet som lyder under nämndens ansvarsområde.
- anordna utbildning avseende hantering av personuppgiftsincidenter för de medarbetare som hanterar personuppgifter. Grundskolenämnden hanterar en omfattande mängd personuppgifter utifrån verksamheternas art och grunduppdrag.

Vård- och omsorgsnämnden

Utifrån resultatet av vår granskning, rekommenderar vi vård- och omsorgsnämnden att:

- genomföra en inventering för att säkerställa att samtliga personuppgifts-behandlingar finns registrerade i behandlingsregistren.
- se över nämndens behandlingsregister för personuppgiftsbehandlingar och genomföra korrigeringar samt kompletteringar i enlighet med avsnitt 9.
- inkludera avgränsade kontrollmål avseende efterlevnad av dataskydds-förordningen i nämndens kommande internkontrollarbete, där det finns risker kopplad till hantering av personuppgifter. Avgränsningar till områdesspecifika kontroller i internkontrollplanen är av vikt för att undvika alltomfattande kontrollmål som t.ex. ”*kontroll av efterlevnad av dataskyddsförordningen*”.
- årligen följa upp och ta del av antal personuppgiftsincidenter inom respektive verksamhet som lyder under nämndens ansvarsområde.
- anordna utbildning avseende hantering av personuppgiftsincidenter för de medarbetare som hanterar personuppgifter. Vård- och omsorgsnämnden hanterar en omfattande mängd personuppgifter utifrån verksamheternas art och grunduppdrag.

Eskilstuna Kommunfastigheter AB

Mot resultatet av vår granskning, rekommenderar vi styrelsen i Eskilstuna kommunfastigheter AB att:

- fastställa riktlinjer för behandling av personuppgifter.
- Fatta beslut om att utse ett dataskyddsombud.
  (*I samband med faktakontrollen har vi delgivits att styrelsen har utifrån granskningens synpunkter skyndsamt tagit beslut om ett dataskyddsombud*).
- Se över möjligheterna att centralisera hantering och underhåll av behandlingsregistren i syfte att säkerställa en korrekt hantering.
- genomföra en inventering för att säkerställa att samtliga personuppgifts-behandlingar finns registrerade i behandlingsregistren.
- se över nämndens behandlingsregister för personuppgiftsbehandlingar och genomföra korrigeringar samt kompletteringar i enlighet med avsnitt 9.
- inkludera avgränsade kontrollmål avseende efterlevnad av dataskydds-förordningen i styrelsens kommande internkontrollarbete, där det finns risker kopplad till hantering av personuppgifter. Avgränsningar till områdesspecifika kontroller i internkontrollplanen är av vikt för att undvika alltomfattande kontrollmål som t.ex. ”*kontroll av efterlevnad av dataskyddsförordningen*”.
- årligen följa upp och ta del av antal personuppgiftsincidenter inom respektive verksamhetsområde.

KPMG AB

Viktoria Bernstam
Specialist
Certifierad kommunal yrkesrevisor

Viktor Tagesson
Verksamhetsrevisor

A Bilaga 1 Sammanfattande bedömning utifrån revisionsfrågor

Revisionsfråga	Bedömning
Finns en dataskyddsorganisation?	Ja
Har samtliga nämnder beslutat om att utse ett dataskyddsombud?	Ja
Befinner sig dataskyddsombudet i en oberoendeposition?	Vid tid för granskningen är funktionen för ordinarie dataskyddombud organisatoriskt sett i en oberoende position.
Är det säkerställt att det finns registerförteckningar över personuppgiftsbehandlingar i enlighet med artikel 30.1, dataskyddsförordningen? (Avser ks, GSN, VON samt Eskiltina Kommunfastigheter AB)	Vid tid för granskningen finns registerförteckningar för granskade nämnder och styrelser.
Är register över behandlingar korrekt upprättade utifrån dataskyddsförordningens grundläggande principer?	Delvis, där det finns centrala brister.
Har inventering skett så att samtliga personuppgiftsbehandlingar finns upptagna i register i enlighet med artikel 30?	Inventering har skett under 2019. Nämnderna behöver genomföra en ny inventering.
Finns dokumenterade rutiner för begäran om registerutdrag?	Ja
Finns dokumenterade rutiner för rättelse av uppgifter?	Nej
Finns dokumenterade rutiner för radering och begränsning av uppgifter?	Nej