Granskning av dataskyddsarbetet

Rapport

Fagersta kommun

KPMG AB

2024-05-22

Antal sidor 23 exkl. bilagor

Antal bilagor 1

Fagersta kommun
Granskning av dataskyddsarbetet

2024-05-22

Innehållsförteckning

1 Sammanfattning

KPMG har av Fagersta kommuns revisorer fått i uppdrag att översiktligt granska kommunens arbete med dataskydd utifrån krav i Dataskyddförordningen (GDPR). Uppdraget ingår i revisionsplanen för år 2024.

Syftet med granskningen har varit att bedöma om kommunstyrelsen, socialnämnden, välfärd- och servicenämnden, utbildningsnämnden samt Norra Västmanlands ekonominämnd bedriver ett ändamålsenligt arbete utifrån dataskyddsförordningens krav.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen och nämnderna delvis bedriver ett ändamålsenligt arbete utifrån dataskyddsförordningens krav.

Vi baserar vår bedömning på att det finns etablerade rutiner samt en ändamålsenlig organisation för incidenthantering utifrån dataskyddsförordningens krav. Vi kan dock konstatera att det saknas ändamålsenliga policys, riktlinjer, instruktioner, arbetsbeskrivning för dataskyddsombudet samt ändamålsenlig uppföljning av arbetet. Vidare kan vi konstatera att det finns ett utvecklingsarbete avseende registerförteckning, konsekvensbedömningar och kunskap om GDPR i kommunen.

I det följande redovisas våra bedömningar kopplat till revisionsfrågorna. För närmare beskrivning av bakgrund till våra bedömningar hänvisar vi till respektive avsnitt i revisionsrapporten.

Revisionsfråga	**Bedömning:**
Finns det ändamålsenliga policys, riktlinjer och instruktioner upprättade för att uppnå regelefterlevnad av dataskyddsförordningen?	**Nej**
Revisionsfråga	**Bedömning:**
Finns registerförteckning upprättad för de personuppgiftsbehandlingar där styrelsen respektive nämnderna är personuppgiftsansvariga?	**Delvis**
Revisionsfråga	**Bedömning:**
Har konsekvensbedömningar gjorts på personuppgiftsbehandlingar som kan bedöms ha en påverkan på den registrerades rättigheter och friheter?	**Delvis**
Revisionsfråga	**Bedömning:**
Har kommunstyrelsen genom beslut fastställt en arbetsbeskrivning för dataskyddsombudet utifrån dataskyddsförordningens krav?	**Nej**

Revisionsfråga	Bedömning:
Har åtgärder vidtagits för att säkerställa en tillräcklig kunskap hos medarbetarna om de krav som ställd på personuppgiftshanteringen?	**Delvis**
Revisionsfråga	**Bedömning:**
Finns etablerade rutiner och en ändamålsenlig organisation för incidenthantering utifrån dataskyddsförordningens krav?	**Ja**
Revisionsfråga	**Bedömning:**
Finns en ändamålsenlig kontroll och uppföljning av arbetet utifrån dataskyddsförordningen?	**Nej**

2 Bakgrund

KPMG har av Fagersta kommuns revisorer fått i uppdrag att översiktligt granska kommunens arbete med dataskydd utifrån krav i Dataskyddsförordningen (GDPR). Uppdraget ingår i revisionsplanen för år 2024.

Kommuner hanterar en stor mängd personuppgifter där flertalet är att klassa som känsliga. Det ställer höga krav på att hanteringen av dessa så att den sker utifrån de krav som dataskyddsförordningen stipulerar. Dataskyddsförordningen (GDPR, The General Data Protection Regulation) trädde i kraft den 25 maj 2018. Europaparlamentets och rådets dataskyddsförordning (EU) 2016/679 gäller i hela EU och ersatte i Sverige den äldre personuppgiftslagen (PUL) från 1998.

Det främsta syftet med dataskyddsförordningen är skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Andra syften med dataskyddsförordningen är att modernisera dataskyddsdirektivets regler från 1995 och att anpassa dessa till det nya digitala samhället. I jämförelse med PUL ställer Dataskyddsförordningen högre krav på företag och organisationers interna kontroll kopplat till hanteringen av personuppgifter. Vid överträdelse av förordningens artiklar föreligger skärpta sanktioner.

I samband med uppföljning av internkontroll 2023 identifierades inom vissa nämnder brister i kunskap och kännedom om rutiner vid personuppgiftsincidenter.

Med utgångspunkt från ovan har kommunens revisorer i sin riskanalys bedömt att efterlevnad av dataskyddsförordningen behöver granskas.

2.1 Syfte, revisionsfrågor och avgränsning

Syftet med granskningen är att bedöma om kommunstyrelsen och nämnderna bedriver ett ändamålsenligt arbete utifrån dataskyddsförordningens krav.

Granskningen har omfattat följande revisionsfrågor:

- Finns det ändamålsenliga policys, riktlinjer och instruktioner upprättade för att uppnå regelefterlevnad av dataskyddsförordningen?
- Finns registerförteckning upprättad för de personuppgiftsbehandlingar där styrelsen respektive nämnderna är personuppgiftsansvariga?
- Har konsekvensbedömningar gjorts på personuppgiftsbehandlingar som kan bedömas ha en påverkan på den registrerades rättigheter och friheter?
- Har styrelsen genom beslut fastställt en arbetsbeskrivning för dataskyddsombudet utifrån dataskyddsförordningens krav?
- Har åtgärder vidtagits för att säkerställa en tillräcklig kunskap hos medarbetarna om de krav som ställs på personuppgiftshanteringen?

- Finns etablerade rutiner och en ändamålsenlig organisation för incidenthantering utifrån dataskyddsförordningens krav?

- Finns en ändamålsenlig kontroll och uppföljning av arbetet utifrån dataskyddsförordningen?

2.2 Avgränsning

Granskningen avgränsas till kommunstyrelsen, socialnämnden, välfärd- och servicenämnden, utbildningsnämnden samt Norra Västmanlands ekonominämnd.

2.3 Revisionskriterier

I granskningen utgörs revisionskriterierna av:

- Kommunallagen 6 kap.6 § (2017:725)
- Dataskyddsförordningen
- Tillämpbara interna regelverk, policys och beslut

2.4 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer/avstämningar med berörda tjänstepersoner och politiker. Se bilaga A för dokumentförteckning.

Intervjuer har genomförts med:

- Kommundirektör
- Kommunstyrelsens ordförande
- Ordförande i utbildningsnämnden samt socialnämnden
- Dataskyddsombud
- Avdelningschef, kommunledningsförvaltningen
- Dataskyddssamordnare för kommunledningsförvaltningen, Norra Västmanlands ekonominämnd, socialförvaltningen, välfärd- och serviceförvaltningen samt utbildningsförvaltningen
- Förvaltningschefer för Norra Västmanlands ekonominämnd, socialförvaltningen, välfärd- och serviceförvaltningen, utbildningsförvaltningen,

Samtliga intervjuade har fått möjlighet att faktakontrollera rapporten i syfte att verifiera dess uppgifter.

3 Dataskyddsförordningen

Dataskyddsförordningen trädde i kraft den 25 maj 2018. Lagstiftningen syftar bland annat till ett starkare skydd för individens integritet och större makt till att kunna bestämma över sina egna personuppgifter. Genom detta ska både offentliga och privata verksamheter anpassa hantering av personuppgifter till gällande regler inom ramen för dataskyddsförordningen.

Tillsynsmyndigheten ska säkerställa påförande av administrativa sanktionsavgifter för överträdelse av förordningen. Sanktioner ska vara i nivåer för att fungera effektivt, proportionellt och avskräckande.

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

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

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

4 Resultat av granskningen

4.1 Styrning av dataskyddsarbetet

Vi har inom ramen för granskningen erhållit dokumentation i form *av Rutin för hantering av registerutdrag* samt *Rutin för hantering av personuppgiftsincidenter*. Därtill finns ett dokument *Roller, ansvar och organisation för dataskyddsarbetet* i vilket ansvarsfördelning för arbetet beskrivs.

De dokument som vi erhållit är inte politiskt beslutade och inte daterade. Intervjuade beskriver att det är ett vägval som gjorts, att inte politiskt anta styrande dokument, då lagen i sig är styrande. Det behov som funnits uppges ha varit att upprätta stödmaterial för själva utförandet av arbetet.

- Rutin gällande hantering av begäran om registerutdrag beskriver vad ett registerutdrag ska innehålla samt hur processen för en begäran går till.
- Rutin för hantering av personuppgiftsincident innehåller en definition av personuppgiftsincident, exempel på en personuppgiftsincident, när en incident ska rapporteras samt beskriver process för incidenthantering.

Inom ramen för granskningen har vi även tagit del av en sammanställning av den information som framgår på kommunens intranät. Där finns övergripande information om dataskyddsförordningen samt mer specifik information om behörighet, efterlevnad, e-post, informationsplikt, personuppgiftsbiträdesavtal, personuppgiftsincident, registerförteckning samt systemsäkerhet. Fagersta kommun har även information om GDPR på kommunens externa hemsida. Det finns möjlighet att rapportera personuppgiftsincidenter både på kommunens interna och externa hemsida.

Vi kan utifrån styrelsens och nämndernas uppföljning av intern kontroll 2023 konstatera avvikelser identifierats avseende bristande kännedom om kommunens rutiner för dataskyddsarbetet. Vi kan genom protokollsgranskning konstatera att avvikelser inte mötts med åtgärder eller uppdrag från personuppgiftsansvariga. Detta beskrivs mer utförligt i avsnitt 4.6.2.

4.1.1 Bedömning

Vår bedömning är att det inte finns ändamålsenliga policys och riktlinjer upprättade för att uppnå regelefterlevnad av dataskyddsförordningen. Vissa instruktioner finns upprättade i syfte att nå regelefterlevnad.

Det saknas styrande dokument för kommunens dataskyddsarbete. Vi noterar att samtliga dokument som vi mottagit ej är politiskt antagna samt saknar datering och uppgift om dokumentansvarig. Det saknas därigenom en fastställd ansvarsfördelning samt tydliggörande av interna krav på hur dataskyddsarbetet ska genomföras. Vi konstaterar att det finns stöd genom vissa rutiner för dataskyddsarbetet. Vi bedömer att dessa är kända av nyckelfunktioner i arbetet men inom samtliga nämnders verksamheter finns en bristande kännedom om rutiner för att uppnå lagkrav. Detta har identifierats i uppföljning av intern kontroll 2023 utan att erforderliga åtgärder vidtagits.

4.2 Dataskyddsorganisation

4.2.1 Roller, ansvar och organisation för dataskyddsarbetet

Varje styrelse och nämnd i Fagersta kommun är personuppgiftsansvariga för den behandling av personuppgifter som sker inom respektive nämnd och styrelse. Enligt dokumentet för ansvarsfördelning ansvarar personuppgiftsansvariga för:

- Upprätta förteckning över de behandlingarna som personuppgiftsansvarig genomför
- Säkerställa och kunna visa att behandlingar utförs i enlighet med EU:s dataskyddsförordning och den nationella dataskyddslagen
- Ta fram lämpliga strategier för dataskydd
- Ta fram riktlinjer för hantering av behandlingsrelaterade händelser, såsom registerutdrag, rätta felaktiga uppgifter och personuppgiftsincidenter
- Tydligt kommunicera hur hantering av dataskyddet samt den personliga integriteten hanteras i kommunen
- Skadeståndsansvar gentemot registrerad vid incident
- Utse dataskyddsombud

Vidare framgår vilket ansvar nämndsekreterare, dataskyddsombud, dataskyddsgruppen, verksamhetschefer och samtliga medarbete har.

4.2.2 Dataskyddsombud

Dataskyddsförordningen, artikel 37.1, fastställer krav på när ett dataskyddsombud, (DSO) ska utses. Enligt artikeln ska ett dataskyddsombud utses om personuppgiftsbehandlingen genomförs av en myndighet eller ett offentligt organ. Beslutet ska dokumenteras och vara protokollfört. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten.

Enligt kommunstyrelsens delegationsordning[1] har kommundirektören rätt att utse dataskyddsombud. I Fagersta kommun innehar kommunjurist rollen dataskyddsombud för styrelsen och samtliga nämnder[2].

[1] Senaste ändringen antagen av KS 2024-02-06, §7
[2] Utnämnd av utbildningsnämnden 2021-06-09 §69, utbildnings- och fritidsnämnden 2018-12-12 §159, Norra Västmanlands ekonomiförvaltning 2018-11-23 §23, kommunstyrelsen 2018-12-05 §241, socialnämnden 2018-12-17 §194, Välfärd- och servicenämnden 2024-03-13 §27

4.2.2.1 Dataskyddsombudets uppgifter

Dataskyddsombudet ska enligt dataskyddsförordningens, artikel 37, utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i artikel 39.

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

- Att övervaka och kontrollera efterlevnad 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 genomförande av den.
- Att samarbeta med tillsynsmyndigheten.
- Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, och vid behov samråda i alla frågor.

Europeiska dataskyddsstyrelsens riktlinjer fastställer att dataskyddsombudets främsta prioritering bör vara att möjliggöra efterlevnaden av dataskyddsförordningen.

I rollbeskrivningen för dataskyddsarbetet i Fagersta kommun framgår att dataskyddsombudet har följande ansvar:

- Vara kontaktperson internt och externt genom att t.ex. svara på enklare frågor, ge allmänna vägledning, förmedla kontakter och dirigera frågor till rätt funktion inom organisationen
- Vara ett kunskapsstöd inom Fagersta kommun gällande dataskyddsförordningen och annan tillämplig dataskyddslagstiftning
- Övervaka den interna efterlevnaden av dataskyddsförordningen och annan tillämplig dataskyddslagstiftning
- Rapportera till organisationens ledning om dataskyddsfrågor och organisationens brister och utvecklingsbehov, samt ge förslag på åtgärder och utveckling
- Om den personuppgiftsansvarige inte inom rimlig tid rättar till påpekade brister har ombudet skyldighet att anmäla förhållandet till Integritetsmyndigheten
- Tillsammans med sakkunniga inom Fagersta kommun kravställa och arbeta för att införa säkerhetsskyddsåtgärder enligt lagstiftning inom dataskydd
- Bevaka och kravställa dataskydd vid upphandling av verksamhetssystem och dylikt
- Identifiera kompetensutvecklingsbehov, planera och genomföra utbildning avseende dataskyddsförordningen och angränsade lagstiftning

- Övervaka efterlevande av lagstiftningens krav
- Ta fram konsekvensbedömning avseende dataskydd vid behandling av personuppgifter som innebär integritetsrisker
- Bistå utredning av personuppgiftsincidenter
- Informera Integritetsmyndigheten vid personuppgiftsincident inom 72 timmar
- Omvärldsbevakning och nätverkande/kunskapsinhämtning rörande dataskyddslagen, dataskyddsförordningen och patientdatalagen
- Fungera som kontaktpunkt för tillsynsmyndigheten och vid behov genomföra förhandssamråd
- Hjälpa till att granska de avtal som biträden skickar till den personuppgiftsansvarige
- Erbjuda utbildning inom området dataskyddslagstiftning
- Delta vid Dataskyddsgruppens planerade sammanträden
- Bistå i framtagande/revidering av rutiner och riktlinjer kring dataskydd
- Hjälpa registrerade att erhålla rättelse eller radering
- Förteckna respektive förvaltnings/verksamhets personuppgiftsbehandling i kommunens registerförteckning
- Säkerställa att övergripande instruktioner och riktlinjer finns och hålls uppdaterade

I faktakontrollen har dataskyddsombud återkopplat att det finns en medvetenhet om att rutinerna i vissa delar har en felaktig beskrivning av ansvarsfördelning. Bland annat avseende att dataskyddsombud ska förteckna personuppgiftsbehandlingar och att ta fram konsekvensbedömningar. Ansvaret för detta är i praktiken fördelat till utsedda dataskyddssamordnare, se avsnitt 4.2.3. Dataskyddsombudets ansvar i dessa uppgifter är en granskade roll och inte en genomföranderoll med upprättande av underlag.

Vi har inom ramen för granskningen inte tagit del av eller fått information om specifika arbetsuppgifter eller hur mycket resurser som arbetet för dataskyddsombudet ska omfatta. Det uppges att omfattningen i arbetet varierar över tid men att dataskyddsfrågorna prioriteras utifrån de behov som finns. Intervjuade från nämndernas verksamheter beskriver att dataskyddsombudet har hög kunskap och utgör ett bra stöd i arbetet men att dataskyddsombudet även har andra viktiga frågor inom sitt ansvar som kommunjurist där de också efterfrågar stöd i mer komplexa frågor.

I intervjuer lyfts även risk i dataskyddsombudets oberoende. Detta som en följs av att ombudet i hög grad behöver delta i det operativa arbetet med dataskyddsfrågor hos respektive personuppgiftsansvariga. Som framgår av både lagen och intern rollbeskrivning är en av dataskyddsombudets uppgifter att granska och kontrollera efterlevnaden, vilket kan försvåras vid för stort deltagande i det operativa arbetet.

4.2.3 Övriga resurser i dataskyddsarbetet

I dataskyddsförordningens artikel 38, som reglerar dataskyddsombudets ställning framgår krav på att den personuppgiftsansvariga ska stödja dataskyddsombudet i utförande av de uppgifter som åligger dataskyddsombudet, se avsnitt 4.2.2, genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter. Därtill framgår att den personuppgiftsansvarige ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

Intervjuade beskriver att nyckelfunktioner i arbetet utöver dataskyddsombud är av respektive nämnd och styrelse utsedda dataskyddssamordnare. Vid intervjuer beskrivs att dataskyddssamordnarna arbetar med dataskydd vid sidan av sina ordinarie arbetsuppgifter. Inom ramen för granskningen har vi inte tagit del av eller fått information om att det finns några riktlinjer för hur mycket resurser som ska läggas på dataskyddsarbetet.

Vi noterar att det i den dokumenterade roll- och ansvarsfördelningen inte framgår vilket ansvar eller vilka arbetsuppgifter som dataskyddssamordnare ansvarar för. Som vi nämnt ovan så finns i nuläget en felaktig beskrivning av uppgifterna. Enligt dataskyddsförordningens artikel 30 ska den personuppgiftsansvariga ansvara för registerförteckningen. Detta ansvar tillhör därmed inte dataskyddsombudet. Genom intervjuer uppfattar vi att dataskyddssamordnarna är de som för personuppgiftsansvarigas räkning utför det operativa dataskyddsarbetet inom förvaltningarna. Bland annat har de följande uppdrag:

- Förteckna respektive förvaltnings/verksamhets personuppgiftsbehandling i kommunens registerförteckning
- Vara kontaktperson för nätverk inom dataskydd som leds av dataskyddsombud
- Hjälpa registrerade att erhålla rättelse eller radering
- Hantera anmälda personuppgiftsincidenter och vid behov involvera dataskyddsombud för bedömning
- Vid behov göra konsekvensbedömningar för personuppgiftsbehandlingar

4.2.4 Bedömning

Vår bedömning är att kommunstyrelsen och nämnderna inte genom beslut fastställt en arbetsbeskrivning för dataskyddsombudet utifrån dataskyddsförordningens krav.

Vi kan konstatera att det finns ett dokument som beskriver roller, ansvar och organisation, vilket är positivt. Samtidigt är inte dokumentet formellt beslutat utan upprättat av dataskyddsombudet som stöd till organisationen.

Vi ser även att nuvarande dokument behöver revideras i enlighet med kommunens fördelning av ansvar och uppgifter. Bland annat avseende rollen dataskyddssamordnare, vilken är en nyckelfunktion i personuppgiftsansvarigas fullgörande av ansvar.

I kommande avsnitt gör vi bedömningar av hur arbetet genomförs och i förhållande till dessa så ser vi en risk med nuvarande roll- och ansvarsfördelning. Dels avseende att dataskyddsombud inte har en tillräckligt oberoende roll i organisationen, dels att utsedda dataskyddssamordnare inte har tillräckliga förutsättningar att genomföra arbetet så att det når upp till dataskyddsförordningens krav.

4.3 Hantering av personuppgifter

4.3.1 Registerförteckning

I enlighet med dataskyddsförordningen, artikel 30, ska varje personuppgiftsansvarig föra register över personuppgiftsbehandling som utförts under dess ansvar. Registerförteckningarna ska på begäran redovisas för Integritetsmyndigheten, där registren ska utgöra en grund för övervakning av behandling av personuppgifter.

I dataskyddsförordningen regleras vilka uppgifter en behandling minst ska innehålla. Bland annat måste personuppgiftsansvarig beskriva ändamål med behandlingen, beskrivning av kategori av registrerade samt om behandlingen innehåller känsliga personuppgifter. Varje behandling måste ha en laglig grund för behandlingen.

Av dataskyddsförordningens principer för behandling av personuppgifter, kap 2, femte artikeln framgår att behandling av personuppgifter ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas utan dröjsmål ska raderas eller rättas.

Vi har inom ramen för granskningen tagit del av registerförteckning för kommunstyrelsen och samtliga nämnder. Registerförteckningen finns sammanställd i *Draftit*[3]*.*

Vid genomgång av förteckningen noterar vi att den inte är helt uppdaterad. Vid intervjuer får vi detta bekräftat och information om att det pågår ett arbete att uppdatera och inventera registerförteckningen för samtliga personuppgiftsansvariga. En anledning till att arbetet har varit eftersatt beskrivs bland annat bero på omorganisationer där nämndernas strukturer har förändrats. En annan orsak som nämns är att det är ett omfattande arbete att gå igenom samtliga registerförteckningar samt att det händer att nya behandlingar inte tas med. Detta beror främst på att dataskyddssamordnarna inte alltid får kännedom om nya behandlingar så att de registreras i förteckningen eller på grund av tidsbrist att genomföra processen att registrera behandlingen. Av samma anledning har inte tidigare registrerade behandlingar tagits bort eller aktualiserats i den utsträckning som skulle behövas. Samtliga dataskyddssamordnare har i uppdrag att hålla registerförteckningen uppdaterad och aktuell. Samtliga har dock rollen vid sidan av andra uppdrag, vilket bidrar till att det inte alltid finns utrymme att prioritera dataskyddsarbetet i den omfattning som hade önskats.

[3] Webbaserat verktyg som utgör stöd i arbetet med personuppgiftshantering och där arbetet kan dokumenteras på ett samlat sätt.

Av intervjuade beskrivs de processer som ska genomföras i systemstödet som omfattande och tidskrävande. Samtidigt beskrivs det ge stöd i att det ska bli korrekt. Dock lyfts att det finns utvecklingspotential då vissa funktioner uppges saknas i systemet. Bland annat uppfattar vissa verksamheter att systemstödet inte är anpassat efter deras verksamhet och behov, vilket försvårar arbetet att registrera alla personuppgiftsbehandlingar.

Vid intervjuer framkommer även att kommunen har påbörjat ett gemensamt arbete avseende dataskydd och informationssäkerhet. Syftet är att etablera ett ledningssystem för informationssäkerhet, ett så kallat LIS. Inom ramen för arbetet planeras ett införande av nytt system där registerförteckning senare ska ingå tillsammans med övriga underlag inom informationssäkerhet. Vid tiden för granskningen är detta arbete i ett inledande skede och vi har därigenom inte inkluderat hur detta kommer att bidra eller påverka dataskyddsarbetet framgent.

4.3.2 Konsekvensbedömningar

Dataskyddsförordningen, artikel 35, reglerar att den personuppgiftsansvarige, för vissa typer av behandlingar, före behandlingen ska utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. Kravet gäller behandling som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Detta kallas konsekvensbedömning. Den personuppgiftsansvariga ska rådfråga dataskyddsombudet vid genomförande av konsekvensbedömningar.

Konsekvensbedömningar är särskilt viktigt när personuppgifter hanteras i nya informationssystem. Detta för att säkerställa att integriteten hos enskilda inte riskeras som följd av att systemleverantören inte efterlever dataskyddsförordningen eller pga bristande säkerhet så att uppgifter kan röjas. Det kan även handla om digitala hjälpmedel som registrerar hälsotillstånd hos enskilda, där insamlade och kommunicerade uppgifter behöver göras med hög säkerhet och försiktighet.

Av mottaget underlag framgår att dataskyddsombudet ansvarar för att ta fram konsekvensbedömning avseende dataskydd vid behandling av personuppgifter som innebär integritetsrisker. Konsekvensbedömningar genomförs utifrån upprättad mall och checklista.

Intervjuade beskriver att det finns en medvetenhet om när konsekvensbedömningar ska genomföras. Samtliga intervjuade bekräftar att dataskyddsombudet involveras i genomförandet. Det framgår dock en osäkerhet om konsekvensbedömningar har gjorts i samtliga fall där detta behövts eller varit önskvärt. Bland annat lyfts detta mot bakgrund av att registerförteckningen inte är helt uppdaterad och att vissa behandlingar inte är registrerade.

4.3.3 Bedömning

Vår bedömning är att det delvis finns registerförteckning upprättad för de personuppgiftsbehandlingar där styrelsen respektive nämnderna är personuppgiftsansvariga.

Av den registerförteckning vi tagit del av konstaterar vi att förteckningen inte är uppdaterad. Vi ser det som positivt att det finns ett tydliggjort ansvar för respektive personuppgiftsansvarigas arbete med registerförteckning men ser samtidigt att samordnarnas utrymme för att prioritera arbetet inte är tillräckligt.

I och med att förteckningen ännu inte har inventerats och uppdaterats i sin helhet bedömer vi att det finns risk för att förteckningen inte är komplett. Är inte förteckningen komplett kan det finnas en risk att personuppgiftsbehandlingar sker utan att behandlingen finns förtecknad. Dataskyddsförordningen ställer krav på att förteckningen vara aktuell och korrekt. Därigenom är det av vikt att kommunstyrelsen och samtliga nämnder säkerställer att arbetet prioriteras så att det finns förutsättningar att hålla förteckningen uppdaterad och aktuell så att dataskyddsförordningen efterlevs.

Vår bedömning är att kommunstyrelsen och nämnderna delvis har gjort konsekvensbedömningar på personuppgiftsbehandlingar som bedöms ha en påverkan på den registrerades rättigheter och friheter.

Det finns en medvetenhet om att konsekvensbedömningar ska göras för vissa behandlingar. Samtidigt kan vi konstatera att detta inte alltid görs så att kraven i dataskyddsförordningen efterlevs fullt ut.

4.4 Medvetenhet och kunskap om dataskydd

Dataskyddsförordningen innehåller särskilda skyldigheter för de som behandlar personuppgifter. Behandling av personuppgifter får exempelvis endast ske efter instruktion från den personuppgiftsansvarige och behandlingen måste ske i enlighet med dataskyddsförordningens krav. Dataskyddsförordningens bestämmelser om de registrerade rättigheterna innebär skyldigheter för de som behandlar personuppgifter. Detta medför att det behöver finnas en grundläggande kunskap och förståelse för de krav som ställs för att kunna skydda personuppgifter och hantera de i enlighet med förordningen.

4.4.1 Utbildning och medvetenhet hos medarbetare

Intervjuade uppger att medarbetare i kommunen har genomfört så kallade nanoutbildning[4] inom området dataskydd. Dock beskrivs utbildningarna genomförts för några år sedan. Det finns därav ingen sammanställning i vilken utsträckning utbildningen har genomförts av medarbetare i kommunen.

[4] Kortare digitala utbildningspass som skickas via e-post till målgrupper med ett visst intervall.

Vidare framgår vid intervjuer att dataskydd är en stående punkt på verksamheternas APT. Främst riktas fokus på om det har skett någon incident samt hur verksamheten ska arbeta för att undvika att incidenten sker igen.

Dataskyddsombud har även genomfört utbildningsinsatser i styrelse och nämnder för att tydliggöra ansvaret som åligger styrelse och nämnder som personuppgiftsansvariga. Vi tolkar genom våra intervjuer att det finns en otydlighet eller okunskap över personuppgiftsansvarigas ansvar för att tillse att lagen efterlevs. Vi uppfattar att vissa nämnder, efter att denna granskning introducerats, bjudit in dataskyddsombud och dataskyddssamordnare till kommande sammanträde för att beskriva ansvar och det arbete som genomförs. Detta som ett sätt att uppdatera sig på dataskyddsarbetet.

Intervjuade upplever att det har varit en högre medvetenhet om dataskydd och dess arbete tidigare, men att det möjligen har sjunkit under de senaste åren. Detta beskrivs bero på att det var ett mer intensifierat arbetet när lagen infördes. Samtidigt beskrivs att det finnas en medvetenhet i kommunen att exempelvis använda sig av *secure mail* vid hantering av personuppgifter i mail, men att kunskapen om vad som är en incident inte är lika självklar.

4.4.2 Utbildning och medvetenhet hos dataskyddssamordnare

Intervjuade beskriver att dataskyddssamornarna i respektive styrelse och nämnd inte har tagit del av särskild utbildning om dataskydd, utifrån sin roll som dataskyddssamordnare.

Vidare beskrivs att det finns en dataskyddsgrupp där dataskyddssamordnarna ingår. Dataskyddsombudet är sammankallande och koordinerar gruppen. Enligt uppgift så får samordnarna viss utbildning vid gruppens möten samt även information om nyheter inom området samt om väsentliga händelser med incidenter mm.

Av kommunens dokument för roller, ansvar och organisationen för dataskyddsarbetet framgår att gruppen har till uppgift att:

- Vara kontaktyta/stöd för dataskyddsombudet
- Koordinera respektive förvaltnings/verksamhets dataskyddsarbete
- Ta fram övergripande såväl som verksamhetsanpassade mallar, rutiner, och processer för registrerade rättigheter
- Utföra och understödja informationsspridning och utbildning inom den egen verksamheten

Vid intervjuer framkommer gruppen under de senaste åren inte varit så aktiv. Planen är dock att gruppen ska börja ses mer regelbundet igen.

4.4.3 Bedömning

Vår bedömning är att det delvis har vidtagits åtgärder för att säkerställa en tillräcklig kunskap hos medarbetarna om de krav som ställs på personuppgiftshanteringen.

Vi bedömer att det finns ett behov av att styrelse och nämnderna får ytterligare information och utbildning över deras ansvar. Detta då brister i arbetet kan leda till viten och sanktioner för kommunen.

Vi baserar vår bedömning på att det finns utbildningar tillgängliga för samtliga medarbetare i kommunen, samt att området är en stående punkt på verksamheternas APT. Vi noterar dock att utbildningen inte genomförts på en återkommande basis. Vi bedömer att samtliga medarbetare och förtroendevalda återkommande bör utbildas och informeras om dataskyddsarbetet. Detta med anledning av den mängd integritetskänsliga uppgifter som hanteras i en kommun samt att det finns risk att viten drabbar personuppgiftsansvariga om lagen inte efterlevs.

4.5 Personuppgiftsincidenter

En personuppgiftsincident kan innebära risker för registrerade personers fri- och rättigheter och kan få allvarliga konsekvenser, bland annat:

- Ekonomisk skada
- Diskriminering
- Identitetsstöld
- Bedrägeri
- Skadlig ryktesspridning

En personuppgiftsincident som inte hanteras på ett lämpligt sätt kan påverka tilltron till den organisation som behandlar personuppgifter. Det kan också leda till att Integritetsmyndigheten genom tillsyn kan döma ut sanktionsavgifter.

I dataskyddsförordningen, artikel 33, om anmälan av personuppgiftsincident framgår att personuppgiftsincident ska anmälas av personuppgiftsansvarig utan dröjsmål, senast inom 72 timmar till tillsynsmyndigheten. Om anmälan till myndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till försening. Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera en registrerade om personuppgiftsincidenten.

I samband med incidentrapportering till Integritetsskyddsmyndigheten ska en beskrivning av incidenten göras tillsamman med de kategorier av och ungefärligt antal registrerade som berörts. Därtill ska konsekvenser beskrivas och de åtgärder som personuppgiftsansvarig vidtagit eller föreslår för att mildra potentiella negativa effekter.

4.5.1 Hantering av personuppgiftsincidenter i kommunen

Som framgår av *avsnitt 4.1,* har kommunen upprättat en rutin för personuppgiftshantering. Av rutinen framgår att anställda och förtroendevalda inom kommunen ska rapportera vid en inträffad incident, om misstanke finns att det har inträffat en incident eller om det finns risk för att en incident kan inträffa. Rapporteringen ska ske till ansvarig chef eller via kommunens e-tjänst. Incidenterna ska rapporteras så snart som möjligt vid upptäckt, även om incidenten har hunnit åtgärdas.

Vid en rapportering är det dataskyddssamordnaren tillsammans med ansvarig verksamhetschef som gör en bedömning av allvarlighetsgrad samt eventuella åtgärder som behöver vidtas omgående. För hjälp och vid behov ska även dataskyddsombudet kontaktas.

Inom ramen för granskningen har vi tagit del av en sammanställning av personuppgiftsincidenter som diarieförts under 2023. Vi noterar vid genomgång att incidenterna är få, samt att incidenter oftast rapporterats under ett kortare tidsintervall.

Intervjuade beskriver att ett fåtal incidenter har rapporterats till Integritetsskyddsmyndigheten, men att det inte har gått vidare med någon ytterligare utredning av ärendena.

4.5.2 Bedömning

Vår bedömning är att det finns etablerade rutiner och en ändamålsenlig organisation för incidenthantering från dataskyddsförordningens krav.

Kommunen har en dokumenterad rutin som beskriver vad som är en incident och hur dessa ska hanteras. Det finns därtill en etablerad digital tjänst som förenklar anmälan med tillhörande eskaleringsvägar. Trots rutinen och systemstödet konstaterar vi dock att antal incidenter är få i förhållande till den mängd personuppgifter som hanteras inom styrelsen och nämnderna. Vi ser därför en risk för bristande medvetenhet om vad som är incidenter och hur dessa ska anmälas. Det är väsentligt att uppmuntra anmälan av incidenter då detta är en viktig källa för kunskap om behov av förbättringsåtgärder för att hantera personuppgifter korrekt.

4.6 Uppföljning och kontroll

I 6 kap. 6 § Kommunallagen (2017:725) framgår att nämnder inom sitt område ska se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt, samt de bestämmelser i lag eller annan författning som gäller för verksamheten. De ska även se till att den interna kontrollen är tillräcklig och att verksamheten bedrivits på ett i övrigt tillfredställande sätt.

4.6.1 Kontroll av dataskyddsarbetet

Som framgår av avsnitt 4.2.2.1 ansvarar dataskyddsombudet för att;

- Övervaka den interna efterlevnaden av dataskyddsförordningen
- Rapportera till organisationens ledning om dataskyddsfrågor och organisationens brister och utvecklingsbehov, samt ge förslag på åtgärder och utveckling
- Övervaka efterlevnad av lagstiftningens krav

Inom ramen för granskningen har vi i enlighet med krav i dataskyddsförordningen tagit del av tillsynsrapporter för kommunstyrelsen, norra Västmanlands ekonominämnd, socialnämnden samt utbildnings- och fritidsnämnden. Av tillsynsrapporterna framgår att kommunstyrelsen och samtliga nämnder påvisade brister i sitt arbete.

Vi noterar vid granskningen att samtliga tillsynsrapporter avser verksamhetsåret 2019. Vi har efterfrågat tillsynsrapporter genomförda efter detta men enligt uppgift har ingen tillsyn genomförts. I intervjuer uppges detta bland annat bero på en intern bedömning av tjänstepersoner att det inte funnits behov att genomföra någon ny granskning av efterlevnaden av dataskyddsförordningen hos styrelsen och nämnderna.

4.6.2 Internkontroll

Inom ramen för granskningen har vi tagit del av kommunstyrelsens, Norra Västmanlands ekonominämnd, socialnämndens och utbildningsnämndens internkontrollplaner för 2023. Då välfärd- och servicenämnden är en ny nämnd för år 2024, har vi inte tagit del av internkontrollplan avseende 2023.

Under 2023 ingick området GDPR som en kommungemensam kontrollpunkt i internkontrollplanerna. Av planerna framgår att det skulle genomföras ett stickprov av hantering av personuppgifter, kontrollen skulle genomföras vid ett tillfälle under året.

Utifrån den uppföljning vi har tagit del av har kontrollen genomförts med hjälp av stickprov med frågeställningar till ett antal anställda i verksamheterna inom respektive nämnder och styrelsen. Syftet var att ta reda på vad medarbetarna kände till gällande begäran om registerutdrag. Det skulle även göras en kontroll om det fanns delegationsbeslut för hantering av begäran om registerutdrag i nämndernas delegationsordning. Av uppföljningen framgår att kommunstyrelsen bedömde resultatet av kontrollen som *nära målvärde.* Samtliga nämnder bedömde resultatet av kontrollen som *ej accepterat värde.*

Styrelsen och samtliga nämnder har tagit del av resultatet och uppföljning av internkontrollen. Kommunstyrelsen uppdrog vid sammanträdet, 2024-02-06, nämnderna att vidta åtgärder med anledning av de framkomma avvikelserna. Utifrån dokumentgranskning av protokollförd uppföljning saknas beslut om specifika åtgärder i förhållande till avvikelsen. Intervjuade har inte tagit del av något beslut eller uppdrag i syfte att stärka arbetet genom åtgärder i förhållande till resultatet i internkontrollen. Däremot uppges av intervjuade att kontrollområden med avvikelser ska tas med i kommande års internkontrollplaner. Vid tiden för granskningen hade inte internkontrollplaner för 2024 antagits i styrelse och nämnder. Vi har däremot tagit del

av arbetsmaterial av vilket vi kan konstatera att GDPR avses vara ett kommungemensamt kontrollområde under 2024.

4.6.3 Rapportering av dataskyddsarbetet

Vid intervjuer beskrivs att styrelse och samtliga nämnder har tagit del av återrapportering avseende utfallen av kontrollmomentet som genomfördes inom ramen för internkontrollplanen under 2023. Utöver uppföljningen av kontrollmomentet beskrivs att styrelse och nämnder får rapportering om det har skett någon personuppgiftsincident. Det råder dock en osäkerhet om när detta ska göras och för vilka incidenter. Vissa intervjuade uppger att samtliga personuppgiftsincidenter ska rapporters till styrelsen och nämnderna medan andra uppger att endast allvarliga incidenter ska rapporteras. Med hänvisning till det låga antal incidenter som skett så har rapportering endast gjorts vid ett fåtal sammanträden.

4.6.4 Bedömning

Vår bedömning är att det inte finns en ändamålsenlig kontroll och uppföljning av arbetet utifrån dataskyddsförordningen.

Vi kan konstatera att det inte sker någon etablerad och regelbunden rapportering avseende dataskyddsarbetet till de personuppgiftsansvariga. Tillsyner inom området har inte genomförts sedan 2019. Det är av vikt att kontroller genomförs för att säkerställa efterlevnaden av dataskyddsförordningen, samt att beslut fattas om åtgärder vid identifierade brister.

Utifrån resultatet av den internkontroll som genomfördes under 2023 bedömer vi att kommunstyrelsen och nämnderna inte vidtagit åtgärder i tillräcklig grad för att säkerställa att dataskyddsförordningen efterlevs. Trots identifierade avvikelser har inget förbättringsarbete initierats.

Det är av vikt att dialog om dataskyddsfrågorna är levande i kommunen för att säkerställa att det finns en tillräcklig kunskap hos medarbetare. Vid bristande kunskap hos enskilda medarbetare kan detta vara förknippat med risker i den vardagliga hanteringen. Det medför även en risk att personuppgiftsincidenter inte upptäcks, som i sin tur kan medföra att de inte hanteras i enlighet med dataskyddsförordningens krav. Risken kan i sin tur leda till personlig skada för de registrerade, men även för ekonomisk skada eller förtroendeskada för kommunen.

5 Samlad bedömning och rekommendationer

Syftet med granskningen har varit att bedöma om kommunstyrelsen och nämnderna bedriver ett ändamålsenligt arbete utifrån dataskyddsförordningens krav.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen och nämnderna delvis bedriver ett ändamålsenligt arbete utifrån dataskyddsförordningens krav.

Vi bedömer att det finns en dokumenterad rutin i kommunen för hur en personuppgiftsincident ska hanteras. Vi noterar dock att det inkommer få rapporteringar, vilket kan tyda på en risk för att medvetenhet och kunskapen hur och vad som ska anmälas är låg i kommunen.

Granskningen visar att det saknas styrande dokument för kommunens dataskyddsarbete samt att samtliga dokument vi mottagit inom ramen för granskningen saknar datering och uppgift om dokumentansvarig. Vi ser att den arbetsbeskrivningen som idag finns för dataskyddsombudets arbetsbeskrivning är i behov av att revideras i enlighet med kommunens fördelning av ansvar och uppgifter.

Vi noterat i granskningen att det finns en upprättad registerförteckning, men att den är i behov av att uppdateras.

Avseende uppföljning och rapportering av dataskyddsarbetet noterar vi att detta inte skett på ett ändamålsenligt och regelbundet sätt.

Utifrån resultatet av vår granskning rekommenderar vi **kommunstyrelsen** att:

- Säkerställa att styrdokument beslutas politiskt.
- Tillse att styrande dokument uppdaterade i enlighet med nuvarande organisation och ansvarsfördelning, särskilt för rollerna dataskyddsombud och dataskyddssamordnare.
- Beakta hur dataskyddsombudets oberoende kan säkerställas i högre grad.

Utifrån resultatet av vår granskning rekommenderar vi **kommunstyrelsen** samt **samtliga nämnder** att:

- Säkerställa att personuppgiftsansvariga har kännedom och förståelse för det arbete och ansvar som åligger de i förhållande till dataskyddsförordningens krav.
- Tillse att det finns tillräckliga förutsättningar för utsedda roller att genomföra arbetet så att det når förordningens krav.
- Uppdatera registerförteckning för samtliga personuppgiftsbehandlingar för respektive personuppgiftsansvarige.
- Tillse att det finns rutiner för ett systematiskt arbete för att löpande uppdatera personuppgiftsbehandlingar i registerförteckningen samt att konsekvensbedömningar görs i enlighet med förordningen och interna beslut.

— Tillse att samtliga medarbetare som hanterar personuppgifter återkommande genomför utbildning inom området.
— Överväga att erbjuda ytterligare utbildning till nyckelfunktioner och ansvariga för dataskyddsarbetet.
— Säkerställa att efterlevnaden av dataskyddsoförordningen kontrolleras genom tillsyn, samt att återrapportering sker till personuppgiftsansvariga. Vid identifierade brister ska åtgärder beslutas för att säkerställa att arbetet når upp till dataskyddsförordningens krav.

Datum som ovan

KPMG AB

Jenny Thörn
Verksamhetsrevisor

Sofia Gunnarsson
Verksamhetsrevisor

Linnéa Grönvold
Certifierad kommunal yrkesrevisor

6 Bilagor

6.1 Bilaga A: Dokumentförteckning

Dokument
Roller, ansvar och organisation, daterad 2024-04-19
Rutin gällande hantering av personuppgiftsincidenter
Rutin gällande hantering om begäran av registerutdrag
Registerförteckning för kommunstyrelsen och samtliga nämnder
Internkontrollplaner för 2023 samt arbetsmaterial för 2024
Uppföljning av internkontrollplaner 2023
Incidentrapportering under 2023
Delegationsordning för kommunstyrelsen och samtliga nämnder
Tillsynsrapport för kommunstyrelsen och samtliga nämnder, 2019