GDPR-granskning

Mariestad Kommun

September 2020

Sofie Åberg, Projektledare

Jacob Svensson, Projektmedarbetare

Revisionsrapport

Innehållsförteckning

Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Mariestads Kommun har PwC genomfört en övergripande granskning avseende EU:s dataskyddsförordning, General Data Protection Regulation (GDPR).

Syftet med denna granskning är att bedöma om kommunstyrelsen säkerställt att ett ändamålsenligt och heltäckande arbete gällande GDPR bedrivs samt om åtgärder vidtagits för att löpande efterleva de nya reglerna.

Granskningens syfte har besvarats genom följande revisionsfrågor:

- Är metodiken och det genomförda arbetet relevant för kommunen?
- Har definierade aktiviteter genomförts på ett tillfredsställande sätt så att önskad effekt uppnåtts?
- Har kvarstående luckor och aktiviteter identifierats?
- Har utvärdering av etablerade register/processer/roller/ansvarsfördelning skett?
- Har utbildning genomförts?
- Finns det en ändamålsenlig organisation för att efterleva GDPR?

Utifrån genomförd granskning är vår **sammanfattande revisionella bedömning** att kommunstyrelsen ***i allt väsentligt*** säkerställt att ett ändamålsenligt och heltäckande arbete gällande GDPR bedrivs samt att tillräckliga åtgärder vidtagits för att löpande efterleva de nya reglerna.

Underlag för revisionell bedömning redovisas i följande avsnitt.

I syfte att utveckla verksamheten lämnas följande rekommendationer:

- Kommunstyrelsen bör säkerställa att systematisk uppföljning och utvärdering inom området genomförs.
- Kommunstyrelsen bör säkerställa att kunskapsnivån inom organisationen följs upp samt att insatser görs för att fånga upp eventuella utbildningsbehov inom området.

Inledning

Bakgrund

EU:s dataskyddsförordning, General Data Protection Regulation (GDPR), innebär en skärpning av dataskyddslagstiftningen inom EU, både avseende organisationers åligganden och de registrerade personernas rättigheter. Den gäller för alla organisationer, företag och myndigheter som hanterar uppgifter om EU-medborgare. För att den ska respekteras införs möjligheten till kraftfulla sanktioner för de organisationer som ignorerar eller brister i att uppfylla de nya kraven. Sanktionsnivåerna har valts så att de ska vara avskräckande och för att det inte ska löna sig att bryta mot reglerna för att spara pengar. Väsentliga sanktionsavgifter för bristande efterlevnad, upp till 20 miljoner kronor, kan utfärdas för myndigheter. Det har också införts en rätt för privatpersoner att kräva skadestånd av de organisationer som inte tillhandahåller deras rättigheter enligt förordningen.

Förordningen började tillämpas den 25 maj 2018. Förordningen innehåller nya krav jämfört med Personuppgiftslagen, som exempelvis att alla organisationer själva har en skyldighet att bedöma riskerna för att de registrerades integritet kränks samt vidta lämpliga åtgärder för att minska dessa risker. Organisationer måste även i vissa fall utse dataskyddsombud och rapportera allvarliga personuppgiftsincidenter till tillsynsmyndigheten (och i vissa fall de berörda registrerade) inom 72 timmar. Om man misstänker att någon personuppgiftsbehandling kan medföra höga integritetsrisker för de registrerade måste man göra en konsekvensbedömning och vidta lämpliga åtgärder för att reducera riskerna för eventuella skador.

Revisorerna har i sin riskbedömning lyft fram att det är väsentligt att granska området.

Syfte och revisionsfrågor

Revisorernas uppdrag regleras i kommunallagen kapitel 12.

Syftet med denna granskning är att bedöma om kommunstyrelsen säkerställt att ett ändamålsenligt och heltäckande arbete gällande GDPR bedrivs samt om åtgärder vidtagits för att löpande efterleva de nya reglerna.

Granskningen omfattar följande revisionsfrågor:

- Är metodiken och det genomförda arbetet relevant för kommunen?
- Har definierade aktiviteter genomförts på ett tillfredsställande sätt så att önskad effekt uppnåtts?
- Har kvarstående luckor och aktiviteter identifierats?
- Har utvärdering av etablerade register/processer/roller/ansvarsfördelning skett?
- Har utbildning genomförts?
- Finns det en ändamålsenlig organisation för att efterleva GDPR?

Revisionskriterier

Följande revisionskriterier används i granskningen:

- Dataskyddsförordningen (GDPR), Europaparlamentets och rådets förordning (EU) 2016/679

Avgränsning

Granskningen avgränsas till innehållet i lagstiftningen och best practice. Granskningen fokuserar på kommunens uppsatta mål med GDPR-arbetet och berör inte huruvida kommunen är compliant eller inte. I tid avgränsas granskningen i huvudsak till år 2020.

I övrigt se syfte och revisionsfrågor.

Metod

Granskningen har genomförts genom dokumentanalys och stickprovskontroller i för granskningen relevant dokumentation samt genom intervjuer med dataskyddssamordnare för kommunstyrelsen, administrativ chef samt dataskyddsombud.

De som intervjuats för denna granskning har givits möjlighet att faktakontrollera innehållet i rapporten. Därmed har de haft möjlighet att lämna förslag på korrigeringar i texten och i övrigt föra en dialog om rapportens faktainnehåll innan den slutligt fastställts.

Iakttagelser och bedömningar

Är metodiken och det genomförda arbetet relevant för kommunen?

Iakttagelser

Styrande dokumentation har tagits fram som är väl anpassat till kommunen. Granskningen har bl.a. identifierat följande styrande dokument inom området:

- Riktlinjer för hantering av personuppgifter (antagen av kommunstyrelsen 2018-05-14).
- Rutin för hantering av personuppgifter (antagen av kommunchef 2018-06-15).
- Rutin för informationssäkerhet (antaget av kommunchef 2020-02-24).

Av "Riktlinje för hantering av personuppgifter" framgår kommunövergripande rutiner och riktlinje med syfte att säkerställa att personuppgiftsbehandlingar i enlighet med gällande lagstiftning och praxis. Dokumentet "Rutin för hantering av personuppgifter" beskriver kommunövergripande aspekter av dataskyddsarbetet och dokumentet ska användas som stöd i dataskyddsarbetet. Rutinen inkluderar tillvägagångssätt för att hantera ny eller förändrad behandling, genomförande av konsekvensbedömning, hantering av samtycke och rutin för tecknande av personuppgiftsbiträdesavtal. Vidare finns även rutin för hantering av e-post, hantering av personuppgiftsincidenter samt rutin för tillvägagångssätt för att besvara förfrågningar från registrerade, exempelvis registerutdrag. Av intervjusvar framgår att styrande dokumentation inom området till övervägande del upplevs som heltäckande och uppdaterade.

Anpassningsarbetet till dataskyddsförordningen har till stor del utgått från SKR:s vägledningar. I ett första skede har en analys av vilka åtgärder som behövs vidtas för att efterleva dataskyddsförordningen genomförts, exempelvis framtagning av styrande dokument och registerförteckningar för att få en överblick över vilka personuppgiftsbehandlingar som utförs. Metodiken för anpassningsarbetet utgick även från en förstudie som genomförts i syfte att förstå nuläge samt identifiera åtgärder. Utifrån detta gjordes sedan prioriteringar där de viktigaste åtgärderna genomfördes. Vi noterar i sammanhanget att anpassningsarbetet även har bedrivits i samverkan med grannkommunerna Töreboda och Gullspång.

För att fördela ansvaret inom området har ett antal dataskyddssamordnare utsetts som innehar en stödjande roll samt ett dataskyddsombud som är obligatoriskt för myndigheter. Varje verksamhetsområde har minst en dataskyddssamordnare, ibland fler. Avseende dokumentation på dataskyddsområdet finns mallar för exempelvis inhämtande av samtycke och personuppgiftsbiträdesavtal, vilka finns att hämta på kommunens intranät.

Bedömning

Vi bedömer att metodiken och det genomförda arbetet är tillräckligt.

Bedömningen baseras på att övergripande anpassningsåtgärder vidtagits för att anpassa kommunens arbete till GDPR. Metodiken med förstudie för att förstå nuläge samt identifiering av åtgärder följt av ett arbete för att genomföra de viktigaste

åtgärderna är bra och väl etablerad. Metodiken utgick även från SKR:s vägledningar samt i samverkan med grannkommuner, vilket bedöms vara relevant för att fånga upp best practice avseende dataskydd inom kommuner.

Bedömningen baseras vidare på att aktualiteten och statusen på de styrande dokument som finns inom kommunen generellt är hög. Framtagen dokumentation bedöms vara ändamålsenlig och heltäckande. Bedömningen baseras slutligen på att roller och ansvar delvis är tydliga samt att tillämpade rutiner inom området upplevs fungera generellt bra.

Har definierade aktiviteter genomförts på ett tillfredsställande sätt så att önskad effekt uppnåtts?

Iakttagelser

Vår granskning visar att registerförteckningar samt förslag på riktlinjer togs fram innan GDPR trädde i kraft under ledning av utsedd projektledare samt i samverkan med andra kommuner och via SKR:s föreskrifter. De aktiviteter som identifierades i förarbetet innan GDPR trädde i kraft uppges i intervjusvar ha implementerats väl. Detta gäller framförallt kartläggningen av vilka personuppgiftsbehandlingar som sker inom kommunen, vilket redovisas i registerförteckningar, genomförande av utbildning samt framtagande av dokumentation.

Granskningen visar dock att det finns visst utrymme för förbättring avseende uppföljning och kontroll av exempelvis rutiner för radering av personuppgifter. Vid granskningstillfället uppges det inte ha skett någon kontroll på om personuppgifter har raderats i enlighet med uppsatta raderingsrutiner. Konsekvensbedömningar har även genomförts för att identifiera och hantera risker med vissa behandlingar. Mallen som har tagits fram som stöd för detta uppges fungera bra.

Av intervjuer framgår att den bild över de insatser som genomförts inom området till stor del upplevs som tillräckliga. De rutiner som tillämpas uppges också generellt fungera bra. Det framgår vidare av intervjuer att medvetenhet kring GDPR har höjts sedan anpassningsåtgärder genomförts.

Bedömning

Vi bedömer att definierade aktiviteter genomförts på ett tillfredsställande sätt.

Bedömningen baseras på att rutiner och riktlinjer tagits fram samt att de insatser som genomförts inom området till stor del upplevs som tillräckliga.

Har kvarstående luckor och aktiviteter identifierats?

Iakttagelser

Ett utvecklingsområde som identifieras i intervjuer är att stärka uppföljningsarbetet. Hitintills har fokus legat på att ta fram rutiner och strukturer och att stödja verksamheterna i dataskyddsfrågor. Det har identifierats att regelbundna granskningar och en ökad uppföljning av dataskyddsarbetet kan bli bättre. Då det i dagsläget inte genomförs regelbunden uppföljning och granskning av dataskyddsarbetet finns det heller inte någon dokumentation på kvarstående aktiviteter. Dataskyddsarbetet är dock en kontinuerlig process som ständigt behöver arbetas med.

Det framgår vidare av intervjusvar att personuppgifter lagras längre än vad som anses vara praxis och längre än vad som finns angett som tillåten lagringstid i registerförteckningarna. Uppföljning av detta identifieras som något som regelbundet behöver göras. Ansvaret för att radera personuppgifter ligger på verksamheterna och ytterst på verksamhetschef. Däremot är det i praktiken den enskilda medarbetaren som är indirekt ansvarig, då gallring sker manuellt snarare än per automation.

En ytterligare kvarstående aktivitet som identifierats avser uppföljning av personuppgiftsbiträdesavtal. Vid granskningstillfället görs en översyn av konsekvenserna av Schrems II-domen[1] och hur det kan påverka personuppgiftsbiträdesavtalen. Detta tyder på att det sker en omvärldsbevakning på dataskyddsområdet.

Vår granskning kan inte styrka att identifierade kvarvarande luckor finns dokumenterade.

Bedömning

Vi bedömer att arbetet med att identifiera kvarvarande luckor och aktiviteter för att säkerställa en tillräcklig intern kunskap inom området som delvis tillräckligt.

Bedömningen baseras på att ett antal kvarstående aktiviteter är identifierade av ansvariga. Vår granskning kan inte styrka att identifierade luckor finns dokumenterade.

Har utvärdering av etablerade register/processer/roller/ansvarsfördelning skett?

Iakttagelser

Revidering av registerförteckningar åligger varje enskild verksamhet att ajourhålla och meddela dataskyddssamordnare. Det ingår i dataskyddssamordnarnas roll att påminna om detta och ett årshjul med inslag av när detta ska göras finns som stöd. Utvärdering och uppföljning uppges generellt ske i begränsad utsträckning. Det framgår av intervjuer att det i praktiken i många fall inte finns så mycket att följa upp, ett exempel som lyfts fram är att det genomförs väldig få registerutdrag per år. Däremot framgår det att en självutvärdering genomförs efter att ett utdrag tas, dock är denna rutin något som dataskyddssamordnare själva tagit fram på eget initiativ.

Av intervjuer framgår att uppföljning av registerförteckningar sker kontinuerligt samt att de ajourhålls löpande. Det framgår även att de rutiner som finns upprättade inom området i stor utsträckning följs. Däremot kan vår granskning inte styrka att kontroller görs på att framtagna rutiner följs, d.v.s. vi kan inte styrka att rutiner följs upp eller på annat sätt kontrolleras. Vår granskning kan heller inte styrka att den interna kunskapsnivån bland medarbetare mäts eller på annat sätt följs upp i syfte att kontrollera den interna kunskapen över kommunens insamling, hantering och utlämning av personuppgifter.

Den uppsatta rutinen för hantering av personuppgiftsincidenter har testats vid ett flertal tillfällen då det inträffat skarpa incidenter. Även rutinen för att hantera förfrågan om

[1] Den 16 juli 2020 meddelade EU-domstolen dom i det så kallade Schrems II-målet. Domstolen slår fast att Privacy Shield-avtalet mellan EU och USA inte ger ett tillräckligt skydd för personuppgifter när dessa förs över till USA. Detta innebär att det inte längre är tillåtet för personuppgiftsansvariga i EU att med Privacy Shield som grund överföra personuppgifter till mottagare i USA.

registerutdrag har testats i skarpt läge, detta är dock något som uppges förekomma väldigt sällan. Vid intervjuer uppges kommunen endast mottagit två förfrågningar sedan GDPR trädde i kraft.

Vår granskning kan inte styrka att kontroll och uppföljning genomförs avseende att personuppgiftsbiträden följer de instruktioner som finns i personuppgiftsbiträdesavtal. Av intervjuer framgår även att det funnits svårigheter att få till personuppgiftsbiträdesavtal med berörda personuppgiftsbiträden.

Bedömning

Vi bedömer att utvärdering av etablerade register/processer/roller/ansvarsfördelning ej skett i tillräcklig utsträckning.

Bedömningen baseras på att utvärdering och uppföljning i begränsad utsträckning genomförs, samt på att kontroll och uppföljning saknas avseende att personuppgiftsbiträden följer instruktioner som finns i personuppgiftsbiträdesavtal. Bedömningen baseras vidare på att inga närmare kontroller genomförs för att säkerställa att framtagna rutiner följs.

Har utbildning genomförts?

Iakttagelser

Utbildning i samband med införandet av GDPR har genomförts av dataskyddsombudet. Utbildningsinsatserna har bestått av video/e-learning samt fysiska utbildningstillfällen som dataskyddsombud hållit i. E-learning har skett vid ett tillfälle (under 2018), en ny omgång av e-learnings är planerad hösten 2020. I utbildningen ingår informationssäkerhet där viss utbildning kring dataskydd och dataskyddsfrågor ingår. Fullmäktige och samtliga nämnder uppges ha genomgått utbildningen kring informationssäkerhet.

Fysiska utbildningstillfällen har även hållits med de som i stor utsträckning hanterar personuppgifter inom kommunstyrelsen, bl.a. personuppgiftsansvarig. Av intervjuer framgår dock att utbildningsinsatser endast initieras på initiativ från dataskyddsombud samt på verksamheternas egna initiativ. Vidare framgår ändock att utbildningsinsatserna överlag upplevs som tillräckliga.

Vår granskning kan inte styrka att någon flerårig utbildningsplan har tagits fram eller att insatser för att följa upp kunskapsnivån inom organisationen genomförs. Vi kan heller inte styrka att insatser görs för att fånga upp eventuella utbildningsbehov.

Bedömning

Vi bedömer att utbildning har skett i tillräcklig utsträckning.

Bedömningen baseras på att utbildningsinsatser i stor utsträckning har genomförts samt på att vidare utbildningsinsatser är inplanerade att genomföras hösten 2020. Vi noterar dock i sammanhanget att en flerårig utbildningsplan saknas samt att eventuella utbildningsbehov inte följs upp.

Finns det en ändamålsenlig organisation för att efterleva GDPR?

Iakttagelser

Vår granskning visar att ansvar och roller för att arbetet med att hantera personuppgiftsbehandlingar ska ske på ett korrekt sätt finns beskrivet i styrande dokumentation. Beskrivningen är uppdelad på linjefunktioner som finns i den ordinarie organisationen och på funktioner som är specifika för dataskyddsarbetet. Av intervjuer framgår att det generellt upplevs finnas ett fullgott stöd i dataskyddsombudets funktion samt i den styrande dokumentationen. Vidare framgår att ansvarsfördelningen mellan linjefunktioner och de särskilda dataskyddsfunktionerna till övervägande del upplevs som tydlig.

Av intervjuer framgår vidare att dialog mellan dataskyddssamordnare och dataskyddsombud även sker löpande, för att stärka upp en tydlig ansvarsfördelning. Det framgår dock att det ibland uppstår frågor där råd till verksamheterna ges av exempelvis dataskyddsombud men som kan vara frågor för dataskyddsamordnare. Av intervjuer framgår att det finns visst behov av att förtydliga dataskyddssamordnares roll.

I dagsläget sker även viss samverkan mellan Töreboda kommun och Gullspång kommun inom dataskyddsområdet. Samverkan sker främst genom att dataskyddsombudet är gemensamt för dessa kommuner vilket bidrar till synergier och samverkan. Viss samverkan sker även inom ramen för det digitaliseringsarbete som genomförs inom dessa kommuner där informationssäkerhet ingår.

För att säkerställa löpande efterlevnad av GDPR är det väsentligt att kontinuerligt bevaka nya vägledningar och framtagande av praxis på dataskyddsområdet. Detta sker främst via dataskyddsombudets omvärldsbevakning, vilket även lyfts med dataskyddssamordnare när så är relevant.

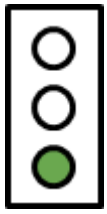
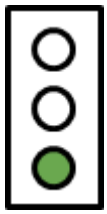
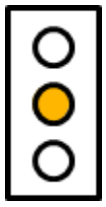
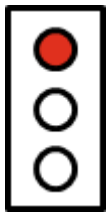
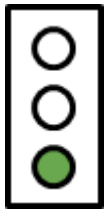
Bedömning

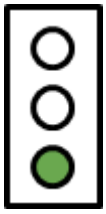
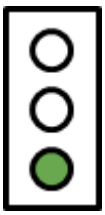
Vi bedömer att det finns en ändamålsenlig organisation för att efterleva GDPR.

Bedömningen baseras på att roller och ansvar finns beskrivna i styrande dokumentation och att ansvarsfördelningen mellan linjefunktioner och de särskilda dataskydds-funktionerna till övervägande del upplevs som tydlig. Bedömningen baseras vidare på att arbete med att ta fram nya vägledningar och praxis inom området sker löpande.

Revisionell bedömning

Bedömningar mot kontrollmål

Kontrollmål	Bedömning	
Är metodiken och de genomförda arbetet relevant för kommunen?	**Uppfyllt**	
Har definierade aktiviteter genomförts på ett tillfredsställande sätt så att önskad effekt uppnåtts?	**Uppfyllt**	
Har kvarstående luckor och aktiviteter identifierats?	**Delvis uppfyllt**	
Har utvärdering av etablerade register/processer/roller/ansvar sfördelning skett?	**Ej uppfyllt**	
Har utbildning genomförts?	**Uppfyllt**	

Finns det en ändamålsenlig organisation för att efterleva GDPR?	**Uppfyllt**	
Sammanfattande bedömning	**Granskningsområdet hanteras på ett ändamålsenligt sätt.**	

Utifrån genomförd granskning är vår **sammanfattande revisionella bedömning** att kommunstyrelsen ***i allt väsentligt*** säkerställt att ett ändamålsenligt och heltäckande arbete gällande GDPR bedrivs samt att tillräckliga åtgärder vidtagits för att löpande efterleva de nya reglerna.

Rekommendationer

I syfte att utveckla verksamheten lämnas följande rekommendationer:

- Kommunstyrelsen säkerställer att systematisk uppföljning och utvärdering inom området genomförs.
- Kommunstyrelsen säkerställer att kunskapsnivån inom organisationen följs upp samt att insatser görs för att fånga upp eventuella utbildningsbehov inom området.

2020-10-13

Lars Dahlin

Uppdragsledare

Sofie Åberg

Projektledare