Kristianstads kommun

KOMMUNREVISIONEN

2019-04-24

Kristianstads kommun

Kommunstyrelsen
Kommunfullmäktige

Förstudie arbetet med införandet av GDPR

På uppdrag av de förtroendevalda revisorerna i Kristianstads kommun har PwC genomfört en förstudie av arbetet med GDPR. Efter genomförd förstudie bedömer vi att komunstyrelsen och nämnder bedriver ett ändamålsenligt och heltäckande arbete gällande GDPR och att åtgärder har vidtagits för att efterleva de nya reglerna. Vi baserar vår bedömning på att:

- Kommunen har genrellt sett tagit ett helhetsgrepp på frågorna kring skyddet av personuppgifter och har ett detaljerat behandlingsregister på plats i form av ett digialt verktyg och har ett outsourcat dataskyddsombud som redan genomfört tillsyn med åtföljande rapport med åtgärdsförslag.

- Kontrollen är generellt sett god inom organisationen och åtgärder har vidtagits på central nivå för att säkerställa att processer och säkerhetskultur kring personuppgiftsbehandling kommer på plats.

Rapporten avseende förstudien överlämnas till kommunstyrelsen och till kommunfullmäktige för kännedom.

För revisorerna i Kristianstads kommun

Sven-Gunnar Linné
Ordförande

Göran Sevebrant
Vice ordförande

Arbetet med införandet av GDPR i Kristianstad kommun - en förstudie och nulägesbeskrivning

Linus Owman

Christine Axentjärn

pwc

Innehåll

1. Inledning

1.1 Bakgrund - GDPR

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 införs också 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 personuppgifts incidenter 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 genomföra en förstudie för att bilda sig en initial uppfattning om status för området. Förstudien ingår i revisionsplanen för år 2019.

1.2 Syfte och frågeställning

De förtroendevalda revisorerna i Kristianstads kommun har uppdragit åt PwC att genomföra en förstudie kring hur arbetet med införandet av bestämmelserna kopplade till den nya dataskyddsförordningen (GDPR) genomförts i kommunen, och därvid bilda sig en uppfattning om nuläget.

Frågeställningen för denna förstudie är således: *“Har ett ändamålsenligt och heltäckande arbete gällande GDPR bedrivits och har åtgärder vidtagits för att efterleva de nya reglerna?”.*

Frågeställningen ovan har besvarats genom ett frågebatteri. Intervjuer har genomförts i gruppform och de flesta av kommunens förvaltningar har därvid varit representerade. Områdena som täckts in genom intervjuerna har varit:

- Styrning
- Roller och ansvar
- Register över behandlingar av personuppgifter

- Dokumentation
- Ansvar som personuppgiftsbiträde
- De registrerades rättigheter
- Lagstiftning
- Barn
- Ostrukturerad data
- Säkerhetsåtgärder

1.3 Avgränsning och metod

Förstudien syftar inte till att kartlägga *de facto* efterlevnad av direktivet, då detta skulle ha mer av en granskande karaktär, dvs falla utanför ansatsen hos en förstudie. Förstudien har därför i sin ansats fokuserat på att ge en generell bild av hur arbetet genomförts och fortskrider, utan att detaljerade studier genomförts på förvaltningsnivå. Dokumentstudier har inte genomförts, då syftet är att genom intervjuer erhålla en ögonblicksbild av hur arbetet fortlöper. Förstudien avgränsas till de personerna inom kommunen med ett uttalat ansvar för införande och förvaltning av GDPR, exempelvis dataskyddsombud.

Intervjuer har således genomförts med följande personer som representerar de personer som haft ett särskilt ansvar i införandet av GDPR. För detta ändamål har kommunen bildat en så kallad GDPR-grupp med representanter från alla delar av förvaltningsorganisationen. Det är denna grupp som intervjuats:

- Birgitta Axelsson: Förvaltningssekreterare / Dataskyddssamordnare, Kommunledningskontoret
- Linus Johannesson: Kontaktperson GDPR Kommunledningskontoret
- Maria Permarker: Kommunjurist Kommunledningskontoret
- Emil Persson, IT Kommunledningskontoret *(ej närvarande)*
- Dennis Turesson: Kontaktperson Arbete & välfärdsförvaltningen *(ej närvarande)*
- Anna Fritzson: Kontaktperson Barn och utbildningsförvaltningen
- Annelie Bjureby: Kontaktperson Barn- och utbildningsförvaltningen
- Henrik Wester: Kontaktperson C4 Teknik (tekniska förvaltningen)
- Peter Rosengren: Kontaktperson Kultur- och fritidsförvaltningen *(ej närvarande)*
- Christian Lauritsen: Kontaktperson Medborgarcenter Kommunledningskontoret *(ej närvarande)*
- Charlotta Wedin: Kontaktperson Miljö- & samhällsbyggnadsförvaltningen
- Andréas Persson: Kontaktperson Omsorgsförvaltningen
- Linus Persson, Informationssäkerhet Räddningstjänsten *(ej närvarande)*

De personer som ej kunnat närvara har beretts möjlighet att inkomma med synpunkter och inspel på rapporten under sakgranskningen. Den generella återkopplingen är att denna grupp av personer tycker att rapporten beskriver status för arbetet med GDPR på ett adekvat sätt.

2. Kartläggning

2.1 Bakgrund - införandet av GDPR

Liksom för andra organisationer innebar 2018 bråda dagar i termer av införandet av den nya dataskyddsförordningen. Arbetet initierades av den juridiska avdelningen under 2016, för att sedan accelerera och nå toppen strax före sommaren 2018. Kommunen hade ett utsett dataskyddsombud i början av år 2018, men denna person avslutade sedan sin anställning under våren. För att inte tappa momentum har kommunen valt att outsourca funktionen dataskyddsombud till en extern leverantör (JP Infonet). Under hösten 2018 genomförde leverantören en detaljerad tillsyn över kommunens hantering av personuppgifter, med stickprover kring både dokumentation och behandlingsregister. Tillsynen utmynnade i en rapport med detaljerade åtgärdsförslag per granskad förvaltning. Tillsynen under 2018 fokuserade på:

- Ändamål och laglig grund för alla personuppgiftsbehandlingar,
- den praktiska möjligheten för registrerade att utöva sina rättigheter, samt
- att organisationen får bättre kontroll på sina informationstillgångar.

Till hjälp för att systematiskt arbeta med de behandlingar av personuppgifter som kommunen genomför har ett verktyg upphandlats (Draft-It), vilket därmed utgör kommunens behandlingsregister.

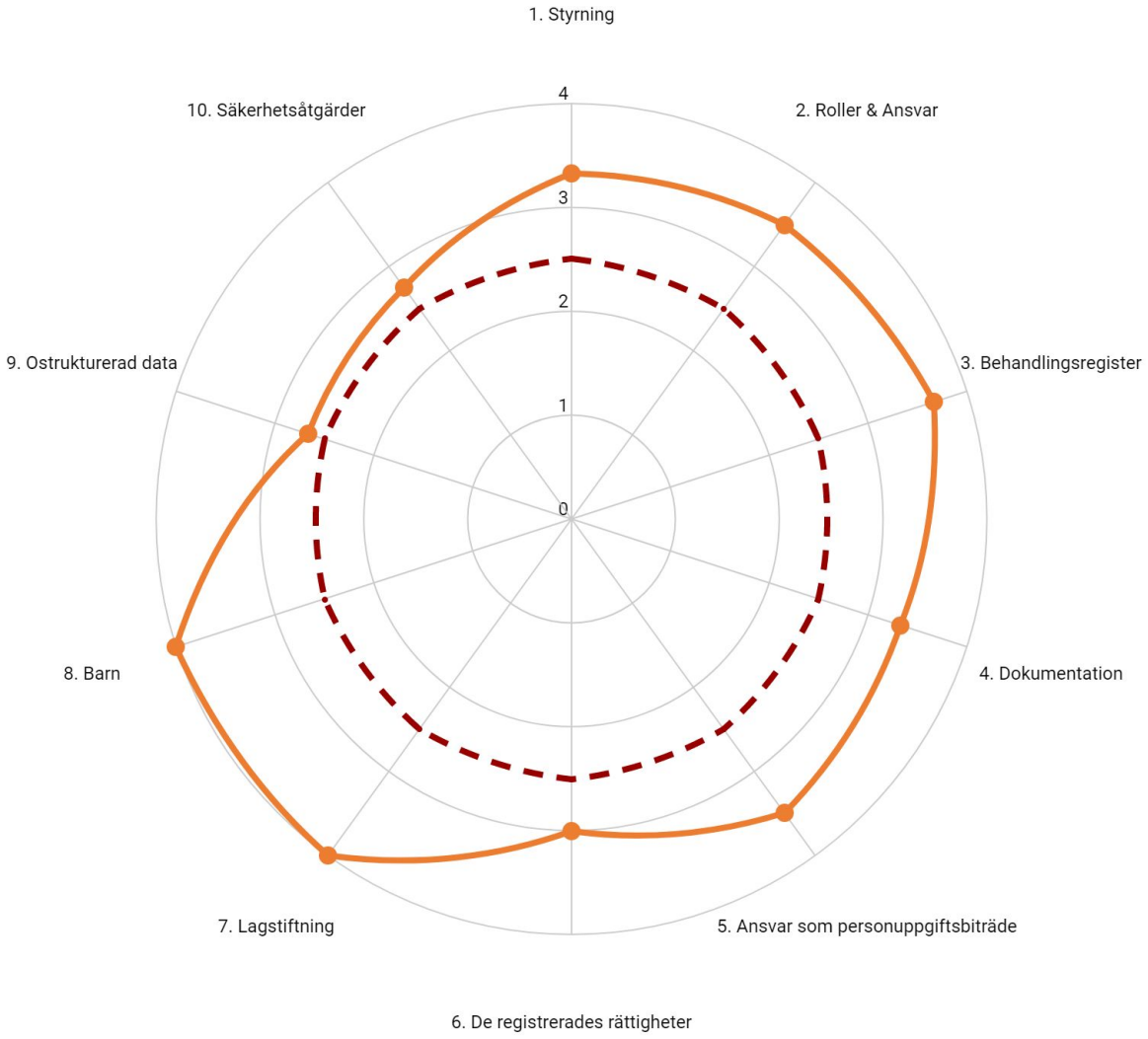
Under arbetets gång har en förvaltningsgrupp (“GDPR-gruppen”) inrättats som ett forum för att hantera gemensamma frågeställningar, dela erfarenheter och söka svar på dataskyddsförordningens praktiska tillämpningar.

2.2 Övergripande resultat

För att sammanställa denna rapport har PwC intervjuat relevanta personer med insyn i Kristianstads kommun dataskyddsarbete och det anpassningsarbete som gjorts till GDPR.

Diagrammet nedan visar resultatet av vår genomgång. Diagrammet är baserat på intervjusvar till 35 standardiserade frågor och ger en översiktsbild av alla relevanta områden för korrekt hantering av personuppgifter.

Den orangea linjen representerar Kristianstads kommuns resultat. Den röda prickade linjen utgör grundvärde för vad vi bedömer är ett godkänt dataskyddsarbete. Medelvärdet för detta är 2,5. Värdet är baserat på en generell bedömning utifrån intervjuformulärets svarsalternativ. Alternativ 1,0 innebär att kommunen inte påbörjat något arbete alls inom området och alternativ 4,0 innebär i korthet att kommunen infört en fullständig (och ofta automatiserad) process kring behandlingen. Ett värde på 2,5 innebär således att organisationen ligger över både 1,0 (inget gjort) och 2,0 (lite gjort) och tangerar 3,0 (vidtagit åtgärder).



Den sammanfattande bedömningen är att Kristianstad kommun har gjort ett gediget arbete i att ta sig an de utmaningar som den nya dataskyddsförordningen innebär. Kommunen ligger konsekvent över den nivå som vi betraktar som grundnivå. I vissa delar ligger kommunen nära den högsta möjliga nivån, baserat på den översiktliga studie som genomförts.

I den fortsatta rapporten går vi djupare in på varje område och ger specifika rekommendationer.

3. Resultat

3.1 Styrning

Kommunens resultat för området är **3,3 av 4,0**. Det har funnits ett tydligt uppdrag att införa GDPR. Den grupp som satts samman för ändamålet (GDPR-gruppen beskriver att de dels fick dessa uppgifter pålagda ovanpå existerande uppgifter, vilket inneburit en ökad arbetsbörda). Det var inledningsvis inte heller tydligt vilket mandat gruppen hade att fatta beslut. Detta har dock blivit tydligare under resans gång. Dessa två punkter utgör grunden till att den högsta poängen inte erhållits, samtidigt som åtgärder vidtagits. Kommunen har kartlagt flödet av personuppgifter i sin verksamhet.

3.2 Roller och ansvar

Inom området roller och ansvar har kommunen erhållit resultatet **3,5 av 4,0**. Kommunen har en utpekad roller för Dataskyddsombud, och ett sådant är tillsatt. Kommunen hade i början av året en dedikerad resurs på denna post, men sedan denne slutade har kommunen outsourcat funktionen till en extern leverantör (JP Infonet). Kommunen har en tydlig ansvarsstruktur för vem/vilka som ansvarar för personuppgifter inom kommunen, samt var de olika behandlingarna sker. Det saknas dock tydligt utpekade personer med ansvar för informationssäkerhet på varje förvaltning.

Rekommendation:

- Utse utpekade personer med ansvar för informationssäkerhet på förvaltningsnivå.

3.3 Behandlingsregister

För detta område har kommunen erhållit ett resultat på **3,7 av 4,0**, vilket får betraktas som mycket gott. Kommunen har implementerat digitalt verktyg (Draft-It) för att skapa en struktur kring de behandlingar som kommunen genomför. Verktyget innebär att kommunen har kontroll över syftet och de personkategorier som ingår i kommunens behandlingar. Likaså har kommunen på detta sätt kunnat kartlägga hela flödet av personuppgifter och fått fram ett automatiserat behandlingsregister som uppdateras kontinuerligt. Kommunen saknas dock full insikt i hur tredjepartsleverantörer tillgodoser skyddet av personuppgifter.

Rekommendation:

- Säkerställ att leverantörsavtal tillgodoser behovet av personuppgiftsskydd för sådana behandlingar som utförs av tredje part, exempelvis i länder utanför EU/EES.

3.4 Dokumentation

Inom fråge området för dokumentation ligger kommunen på **3,3 av 4,0**. Kommunen har förvisso ingen integritetspolicy i strikt mening, men det finns tydlig information på hemsidan kring hur behandlingen av personuppgifter går till och till vem den registrerade kan vända sig med frågor. Det finns även mallar för personuppgiftsbiträdesavtal att tillgå inom kommunorganisationen. Gruppen framhåller att det i viss mån saknas rutiner för detaljerad hantering av personuppgifter ute i organisationen, även om delegationsordningar ger visst stöd.

Rekommendation:

- Säkerställ att rutiner på mer detaljerad nivå än integritetspolicyn styr hanteringen av personuppgifter ute i förvaltningarna.

3.5 Ansvar som personuppgiftsbiträde

Kommunen hamnar här på **3,5 av 4,0**. Kommunen agerar sällan personuppgiftsbiträde till andra verksamheter, men har identifierat de tillfällen då detta sker. Eftersom det rör sig om undantag är detta inte i alla delar dokumenterat. Det finns även mallar för personuppgiftsbiträdesavtal.

3.6 De registrerades rättigheter

För fråge området kring de registrerades rättigheter hamnar kommunen på **3,0 av 4,0**. Kommunen har rutiner för att upplysa den registrerade om hur personuppgifter behandlas innan hanteringen, i de fall då det är tillämpligt, och det finns en process för hur registerutdrag lämnas ut. Det finns en osäkerhet kring huruvida registerutdraget även ska omfatta arkiverat material. Det bör dock tilläggas att rättsläget är osäkert på detta område rent generellt. Att registerutdraget skulle begränsas till att avse endast “pågående behandlingar” (den exakta ordalydelsen i direktivet) innebär dock ren praktiskt att exempelvis en före detta anställd inte skulle ha rätt att få ut den data som avser dennes avslutade anställning, eftersom behandlingen enligt denna definition inte är “pågående”. Det saknas dock rättsliga avgöranden på området, och frågan bör därför bevakas.

Det finns även dokumenterade (men ej automatiserade) processer kring rättning, radering, begränsning av behandling och invändning mot viss behandling av personuppgifter. Kommunen tillämpar inte automatiskt beslutsfattande.

Rekommendation:

- Bevaka rättsläget kring huruvida arkiverat material förväntas ingå i framtida förfrågningar om registerutdrag, och uppdatera rutinerna kring detta när det är påkallat.

3.7 Lagstiftning

Avseende bevakning av lagstiftningsområdet inom dataskyddsområdet har kommunen en utpekad funktion kring detta (dvs kommunjuristen och i förekommande fall dataskyddsombudet) som säkerställer att eventuella förändringar blir kända ute i organisationen. Organisationen i övrigt arbetar löpande med att implementera ny lagstiftning inom området i sin verksamhet. Kommunen hamnar här på maxpoäng - **4,0 av 4,0**.

3.8 Barn

Kommunen behandlar endast ett fåtal fall av personuppgifter för barn där föräldrarnas samtycke behöver inhämtas. Exempelvis inom skolan är skolplikten något som innebär att samtycke inte behöver inhämtas i alla delar eftersom dessa behandlingar har ett lagstadgat syfte. Frågebatteriet för detta område omfattar endast en fråga och kommunen hamnar här på maxpoäng - **4,0 av 4,0**.

3.9 Ostrukturerad data

Avseende området ostrukturerad data är resultatet att kommunen ligger på **2,7 av 4,0**. Personalen har informerats om hur de ska göra för att minimera användningen av

ostrukturerad data, och det finns riktlinjer för exempelvis mail och bilder. Detta sparas på godkända fildelningsytor (både Google Mail och H:), men kommunen säger sig inte ha full kontroll på efterlevnaden av detta. Personalen har delvis utbildats i förhållandet till ostrukturerad data.

Rekommendation:

- Säkerställ efterlevnaden kring lagring av data på godkända fildelningsytor. Överväg hård- och mjukvaruspärrar för att förhindra lagring på otillåtna sätt, exempelvis genom spärr för USB-minnen, installation av Dropbox etc.

- Överväg att införa utbildningsinsatser som särskilt hanterar frågan om ostrukturerad data.

3.10 Säkerhetsåtgärder

Inom området säkerhetsåtgärder får kommunen **2,8 av 4,0**. GDPR-gruppen har bland annat tillsett att upphandlingsavdelningen fått direktiv kring hur systemstöd ska upphandlas för att tillgodose kravet på “privacy by design”, även om detta inte är implementerat fullt ut i alla inköps- och upphandlingsprocesser. Kommunen har genomfört flera övergripande utbildningar, e-learnings och informationstillfällen där bestämmelserna kring personuppgifter varit i fokus. Det finns även en incidenthanteringsprocess, men den har inte testats i alla delar av verksamheten, bland annat beroende på att vissa förvaltningar ännu inte haft inträffade personuppgiftsincidenter. Det pågår ett arbete med att införa en kommungemensam incidentrapporteringsrutin för GDPR, vilken på sikt även kan tänkas inrymma andra typer av incidenter. När det gäller huruvida känsliga personuppgifter kommer att behandlas, och konsekvenserna av detta för den enskilde, finns en process på plats men processen har inte fullt ut genomförts i alla delar.

Rekommendation:

- Säkerställ att incidenthanteringsrutiner är på plats och övade inom hela organisationen. En incident är aldrig fråga om *om* utan om *när*. Rutiner kring incidenthantering bör vara kända i alla delar av organisationen. Denna medvetandehöjande insats kan med fördel kombineras med utbildning kring ostrukturerad data (se 3.9 ovan).

- Säkerställ att processen för konsekvensbedömningar tillämpas, exempelvis genom övningar på mindre känsliga case för att bygga en vana kring detta inom organisationen.

4. Slutsatser

Inledningsvis ställdes frågan *"Har ett ändamålsenligt och heltäckande arbete gällande GDPR bedrivits och har åtgärder vidtagits för att efterleva de nya reglerna?"*

Frågeställningen ovan har besvarats genom ett frågebatteri som besvarats genom intervjumetodik. Intervjuer har genomförts i gruppform och de flesta av kommunens förvaltningar har därvid varit representerade. Områdena som täckts in genom intervjuerna har varit:

- Styrning
- Roller och ansvar
- Register över behandlingar av personuppgifter
- Dokumentation
- Ansvar som personuppgiftsbiträde
- De registrerades rättigheter
- Lagstiftning
- Barn
- Ostrukturerad data
- Säkerhetsåtgärder

Svaret på frågeställningen om huruvida "*ett ändamålsenligt och heltäckande arbete gällande GDPR bedrivits och har åtgärder vidtagits för att efterleva de nya reglerna"* får besvaras med ett ja.

Kommunen har generellt sett tagit ett helhetsgrepp på frågorna kring skyddet av personuppgifter och har ett detaljerat behandlingsregister på plats i form av ett digitalt verktyg och har ett outsourcat dataskyddsombud som redan genomfört tillsyn med åtföljande rapport med åtgärdsförslag. Kontrollen är generellt sett god inom organisationen (baserat på den översiktliga studie som här genomförts) och åtgärder har vidtagits på central nivå för att säkerställa att processer och säkerhetskultur kring personuppgiftsbehandling kommer på plats, exempelvis utbildningar, projektet kring gemensam e-tjänst för incidenthantering och direktiv kring "privacy by design" till upphandlingsenheten.

Nivån enligt applicerad frågemetodik ger ett resultat som ligger över, och ibland mycket över, den grundläggande nivån. Liksom inom andra områden finns det alltid utrymme för förbättringar och ett fåtal rekommendationer har föreslagits i föregående avsnitt.

Mellan raderna skulle eventuellt kommunen vara betjänt av att koppla arbetet med skyddet av personuppgifter till ett bredare informationssäkerhetsarbete, med åtföljande IT-styrning kring exempelvis hård- och mjukvara, för att säkerställa att policyer och rutiner även får genomslag i konfiguration av system, applikationer och hårdvara. På så sätt minskas risken för mänskliga oavsiktliga fel och antagonistiska handhavanden med avsikt att skada.

“Dataskyddsförordningen (The General Data Protection Regulation) är till att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.”

Datainspektionens hemsida