§118

Dnr: KS 2018/185

Svar på revisionsrapport: införandet av nya Dataskyddsförordningen

Beslut

Kommunstyrelsens beslut
Kommunstyrelsen överlämnar yttrande, enligt bilaga Ks § 118/2018, till kommunrevisonen som svar på granskningsrapporten.

Ärendebeskrivning

Under våren 2018 gjordes en granskning av kommunens införandearbete av den nya Dataskyddsförordningen, GDPR. Granskningen, som gjordes drygt två månader innan GDPRs ikraftträdande den 25 maj, fokuserade främst på tydliggörande av ansvarsfördelning och identifiering av nödvändiga insatser.

Redan vid granskningstillfället stod det klart att mycket av det som revisionen ställde frågor om skulle bli svårt att svara på, då de nationella riktlinjerna för hur GDPR ska tolkas inte var färdiga vid granskningstillfället. Dessutom var mycket kommunalt arbete redan påbörjat men, av naturliga skäl, inte färdigställt vid tiden för granskningen.

Trots dessa bakgrundsfaktorer har nu ett så tydligt svar som möjligt tagits fram avseende revisionens betänkligheter. Kommunens GDPR-projektgrupp vill dock understryka att kommunen har bedrivit ett bra införandearbete, där lagstiftningen uppfylldes mer än väl den 25 maj. Självklart är arbetet ännu inte färdigt, men den grundplattform som tagits fram under våren är mycket stabil och kommer underlätta kommunens fortsatta arbete med GDPR.

Revisionen identifierade vid granskningstillfället (daterat 16 april 2018) tre punkter där de önskade att kommunen förbättrade sitt införandearbete:

1. Säkerställa att nödvändiga anpassningar identifieras och genomförs inom ramen för alla verksamheters ansvarsområden och att dessa framgår av nämndernas riktlinjer

Att identifiera och genomföra nödvändiga anpassningar inom alla verksamheters ansvarsområden innan GDPR börjar gälla är nära på omöjligt, då många lagstiftningar (särskilt inom skolans och socialtjänstens områden) fortfarande väntar på anpassning i enlighet med

dataskyddslagstiftningen. Detta innebär att nämndernas riktlinjer fortfarande är under uppbyggnad: inför ikraftträdandet av GDPR valde projektgruppen istället att ”punktmarkera” de områden där nödvändiga anpassningar krävdes akut, och att ta fram rutiner och stöddokument för dessa.
Dessa rutiner och stöddokument innefattar bland annat rutin för mejlhantering, rutin för informering till registrerad, rutin för samtycken, rutin för behörighetskontroll, rutin för check and control, rutin för hantering av dokument inom skolans värld, rutin för hantering av personalärenden, samt rutin för utlämnande av handlingar med personuppgifter inom olika verksamheter. Efter framtagande har projektgruppen arbetat för att dessa rutiner och stöddokument ska bli kända och användas inom samtliga, berörda verksamheter.
Ambitionen är att under hösten inkorporera dessa rutiner/stöddokument i de övergripande riktlinjedokumenten, och att då förhoppningsvis kunna komplettera med de första nationella ”GDPR-standardiseringarna” som bör börja dyka upp ganska snart.
Sammanfattningsvis kan alltså sägas att nödvändiga anpassningar har identifierats, men att arbetet med att genomföra dessa – av naturliga skäl – inte kommer att vara färdigt inom det närmaste året.

2. Säkerställa att det genomförs regelbundna GDPR-kontroller på såväl övergripande som verksamhetskritisk nivå

Även detta arbete är svårt att säkerställa innan GDPR börjar gälla, av samma anledning som presenterades i svaret ovan: det är fortfarande oklart hur GDPR ska appliceras – och kontrolleras – inom många områden, varför det är svårt att sätta upp rutiner för regelbundna GDPR-kontroller.
Vissa kommunövergripande kontroller har dock redan fastställts: exempelvis kommer samtliga anställda som registerfört en behandling att få en begäran om granskning en gång om året, där de ska säkerställa att deras registerföring fortfarande stämmer. Denna kontroll sker automatiskt genom kommunens registerföringssystem.
Vidare kommer det också att skickas ut en påminnelse minst en gång om året per mejl (från Säkerhetsenhetens funktionsmejl), där de anställda uppmuntras att rensa mappar och mejlkorgar.
Kontroller på verksamhetsnivå är dock inte fastställda, även om alla verksamheter starkt uppmuntras att upprätta GDPR-kontrollrutiner. Verksamheterna är, såsom det ser ut idag, ganska ojämna i sina informationssäkerhetskontroller, där exempelvis Socialtjänsten redan har ett väletablerat kontrollförfarande i enlighet med Patientdatalagen, medan Miljö- och teknik inte är lika vana vid den här typen av kontroller. Medvetenhet om behovet av att öka mängden informationssäkerhetskontroller generellt finns dock både hos de anställda och hos deras chefer, vilket främst märks genom ett ökat antal frågor och diskussioner inom kommunen. I kommunens antagna GDPR-strategi finns också ett krav på att verksamheterna ska genomföra intern kontroll avseende GDPR/informationssäkerhet minst en gång vartannat år, gärna med fokus på den praktiska hanteringen av personuppgifter (exempelvis inkomna personuppgifter).

3. Säkerställa att ledamöterna får tillräcklig kunskap inom området

Det är svårt att definiera begreppet ”tillräckligt”, men projektgruppen har varit mycket transparanta gentemot politiken och regelbundet informerat om det arbete som pågått kring GDPR. Exempelvis har samtliga nämnder haft besök minst en gång av någon från projektgruppen, och alla förtroendevalda har fått två informationsmejl plus en länk till kommunens e-utbildning. Det har dessutom lagts upp information om kommunens hantering av personuppgifter på de förtroendevaldas sidor på Kavlinge.se. Således anser projektgruppen att de förtroendevalda har fått tillräcklig kunskap inom området.

Beslutsunderlag

- Revisionsrapport - Granskning av införande av dataskyddsförordningen - Yttrande, tjänsteskrivelse
- Svar revisionsrapport GDPR
- Revisionsrapport - Granskning av införandet av dataskyddsförordningen, rapport

Yrkande

Gunni Gustafsson Nilsson (S) yrkar att utvärdering av arbetet kring dataskyddsförodningen lämnas till kommunstyrelsen om ett år, senast 2019-10-31. I övrigt yrkar hon bifall till föreliggande förslag.
Johan Ericsson (M) yrkar bifall till föreliggande förslag med Gunni Gustafsson Nilssons (S) tillägg.

Beslutsgång

Ordföranden ställer lagda förslag och yrkanden mot varandra och finner att kommunstyrelsen beslutat enligt föreliggande förslag.

Beslutet skickas till

För kännedom
Kommunfullmäktige
Kommunrevisionen
Björn Andersson, säkerhetschef
Hanna Sandberg, nämndsekreterare och säkerhetshandläggare

2018-06-05 | Dnr: KS 2018/185

Svar på Revisionsrapport: införandet av Dataskyddsförordningen

Ernst and Young identifierade vid granskningen (daterad 16 april 2018) tre punkter där de önskade att kommunen förbättrade sitt införandearbete för att säkerställa en tillräcklig beredskap den 25 maj:

1. Säkerställa att nödvändiga anpassningar identifieras och genomförs inom ramen för alla verksamheters ansvarsområden och att dessa framgår av nämndernas riktlinjer

Att identifiera och genomföra nödvändiga anpassningar inom alla verksamheters ansvarsområden *innan* GDPR börjar gälla och har gällt ett tag är nära på omöjligt, då många lagstiftningar (särskilt inom skolans och socialtjänstens områden) fortfarande väntar på anpassning i enlighet med dataskyddslagstiftningen. Detta innebär att nämndernas riktlinjer fortfarande är under uppbyggnad: inför ikraftträdandet av GDPR valde projektgruppen istället att ”punktmarkera” de områden där nödvändiga anpassningar krävdes akut, och att ta fram rutiner och stöddokument för dessa.

Dessa rutiner och stöddokument innefattar bland annat rutin för mejlhantering, rutin för informering till registrerad, rutin för samtycken, rutin för behörighetskontroll, rutin för check and control, rutin för hantering av dokument inom skolans värld, rutin för hantering av personalärenden, samt rutin för utlämnande av handlingar med personuppgifter inom olika verksamheter. Efter framtagande har projektgruppen arbetat för att dessa rutiner och stöddokument ska bli kända och använda inom samtliga, berörda verksamheter.

Ambitionen är att under hösten inkorporera dessa rutiner/stöddokument i de övergripande riktlinjedokumenten, och att då förhoppningsvis kunna komplettera med de första tydliga och nationella ”GDPR-standardiseringarna” som bör dyka upp ganska snart.

Sammanfattningsvis kan alltså sägas att nödvändiga anpassningar har identifierats, men att arbetet med att genomföra dessa – av naturliga skäl – inte kommer att vara färdigt inom det närmaste året.

2. Säkerställa att det genomförs regelbundna GDPR-kontroller på såväl övergripande som verksamhetskritisk nivå

Även detta arbete är svårt att säkerställa innan GDPR börjar gälla, av samma anledning som presenterades i svaret ovan: det är fortfarande oklart hur GDPR ska appliceras – och kontrolleras – inom många områden, varför det är svårt att sätta upp rutiner för regelbundna GDPR-kontroller.

Vissa kommunövergripande kontroller är dock redan fastställda: exempelvis kommer samtliga anställda som registerfört en behandling att få en begäran om granskning en gång om året, där de ska se till så att deras registerföring fortfarande stämmer. Detta sker automatiskt genom kommunens registerföringssystem.

Vidare kommer det också att skickas ut en påminnelse minst en gång om året per mejl (från Säkerhetsenhetens funktionsmejl), där de anställda uppmuntras att rensa mappar och mejlkorgar.

Kontroller på verksamhetsnivå är dock oklarare, även om alla verksamheter starkt uppmuntras att upprätta GDPR-kontrollrutiner. Verksamheterna är, såsom det ser ut idag, ganska ojämna i sina informationssäkerhetskontroller, där exempelvis Socialtjänsten redan har ett väletablerat kontrollförfarande i enlighet med Patientdatalagen, medan Miljö- och teknik inte är lika vana vid den här typen av kontroller. Medvetenhet finns dock både bland de anställda och hos deras chefer gällande att öka kontrollerna avseende informationssäkerhet generellt, vilket främst märks via ett ökat antal frågor och diskussioner. I kommunens antagna GDPR-strategi finns också ett krav att verksamheterna ska genomföra intern kontroll avseende GDPR/informationssäkerhet minst en gång vartannat år, vilket rimligtvis kommer efterlevas.

3. Säkerställa att ledamöterna får tillräcklig kunskap inom området

Det är svårt att definiera begreppet ”tillräckligt”, men projektgruppen har varit mycket transparanta gentemot politiken och regelbundet informerat om det arbete som pågått gällande GDPR: samtliga nämnder har haft besök minst en gång av någon från projektgruppen, alla förtroendevalda har fått två informationsmejl plus en länk till kommunens e-utbildning. Det har dessutom lagts upp information om kommunens hantering av personuppgifter på de förtroendevaldas sidor på Kävlinge.se. Således anser projektgruppen att de förtroendevalda har fått tillräcklig kunskap inom området – vad de sedan valt att ta till sig, är svårare att svara på.