§166

Dnr: KS 2019/371

Revisionsrapport – Granskning av behörighet till känsliga personuppgifter samt interna kontroller - yttrande

Beslut

Kommunstyrelsens beslut
Svar på revisionsrapport, enligt nedan, godkänns och översänds till revisionen.

Ärendebeskrivning

Under våren 2019 har revisionsfirman Ernst & Young, EY, på uppdrag av kommunrevisionen genomfört en granskning av omsorgsnämndens respektive kommunstyrelsens arbete med behörigheter, åtkomst, loggkontroller och intern kontroll kopplat till detta. Kommunstyrelsen har granskats utifrån sitt lednings- och samordningsansvar, och omsorgsnämnden har granskats utifrån sitt systemansvar för IT-systemen ProCapita och Nationell patientöversikt.

Granskningen som helhet resulterade i fyra rekommendationer. Tre av rekommendationerna riktar sig till omsorgsnämnden och behandlades på deras sammanträde den 20 augusti (se ON § 48/2019), och en av rekommendationerna riktar sig till kommunstyrelsen:

Kommunrevisionen rekommenderar omsorgsnämnden att
- Stärka styrningen vid behörighetstilldelning
- Säkerställa att åtkomstkontroller sker i den utsträckning som krävs i fråga om frekvens och omfattning
- Upprätta systemförvaltarplaner i enlighet med systemförvaltarmodellen

Kommunrevisionen rekommenderar kommunstyrelsen att
- Stärka styrningen av arbetet med informationssäkerhet i kommunens verksamhetssystem.

Svar på de tre rekommendationer som riktar sig till omsorgsnämnden (se omsorgsnämndens fullständiga yttrande i beslut ON § 48/2019):
EY:s bedömning är att omsorgsnämndens styrning, kontroll och uppföljning i vissa delar sker ändamålsenligt. Granskningen visade att det finns dokumenterade rutiner, men att dessa inte följs i full utsträckning, därtill bedömer EY att dokumentationen inom vissa områden bör utökas och förtydligas. Gällande styrning av behörigheter bedömer EY utifrån gällande lagstiftning och

Datainspektionens rekommendationer att behörighetstilldelningen bör ses över.

Utifrån EY:s identifiering till förbättringsområden/rekommendationer kommer omsorgsnämnden att:
- Ta fram en modell för att stärka styrningen vid behörighetstilldelning
- Säkerställa att åtkomstkontroller sker i den utsträckning som krävs i fråga om frekvens och omfattning genom att utarbeta ett års hjul för åtkomstkontroller och förtydliga ansvarsfördelningen
- Upprätta systemförvaltarplaner i enlighet med systemförvaltarmetod

Svar på den rekommendation som riktar sig till kommunstyrelsen:
I rapporten lyfts behovet av en översyn med tillhörande standardisering av hela kedjan som rör IT- och informationssäkerhet. Detta innebär, enligt Revisionen, att den systemförvaltarmodell som finns behöver stämmas av med hur verksamheternas systemförvaltning ser ut i praktiken, samt att mallen för systemförvaltningsplanering kan behöva ses över. Revisionen lyfter också att det fortfarande saknas diverse rutiner och riktlinjer avseende informationssäkerhet. Sammantaget gör dessa faktorer att kommunstyrelsen anses otydliga i sitt lednings- och samordningsansvar avseende behörighetsstyrning, gallring och loggkontroller.

Kävlinge kommuns informationssäkerhetsarbete har intensifierats som en följd av att flera lagstiftningar och direktiv tillkommit under kort tid (några exempel är GDPR, beslut om totalförsvarsupprustning, NIS-direktivet, säkerhetsskyddslagen och förtydliganden avseende informationssäkerhet i flera befintliga lagstiftningar). De många nya lagstiftningarna innebär en kontinuerligt ökande press på kommunernas informationssäkerhetsarbete, både avseende ny och befintlig hantering. Den ökade pressen har förstås goda intentioner och lyfter ett viktigt område, men det är inte helt lätt att som en liten kommun hinna integrera alla lagstiftningar i samma takt som de beslutas nationellt. Detta kan resultera i att exempelvis lednings- och samordningsansvar bitvis kan bli otydligt innan det fallit på plats.

För att nu ”komma ifatt” integreringen av de nya lagstiftningarna har kommunens säkerhetsenhet anlitat en informationssäkerhetskonsult som ska se över informationssäkerhetsarbetet i flera 5Yes-kommuner. I detta arbete ingår att titta på hela IT- och informationssäkerhetskedjan; från ledning och samordning, till enskilda rutiner, till uppföljning. Dessutom är kommunens informationssäkerhetsstrategi ute på remiss hos nämnderna, i vilken alla nya lagstiftningar och deras krav beskrivs och tydliggörs. Förhoppningen är att strategin ska antas i november 2019, för att sedan kunna utgöra en bärande pusselbit i det fortsatta IT- och informationssäkerhetsarbetet som planeras för år 2020-2021.

Kommunstyrelsens informationssäkerhetssamordnare håller med andra ord med Revisionen om de brister som lyfts i granskningen, men anser också att ett åtgärdsarbete redan pågår. Arbetet är dock mycket stort, och kommer inte vara ”färdigt” förrän tidigast slutet av år 2021.

Beslutsunderlag

- Svar på revisionsrapport, hantering av känsliga personuppgifter, tjänsteskrivelse
- Revisionsrapport - Granskning av behörighet till känsliga uppgifter samt interna kontroller, följebrev
- Revisionsrapport - Granskning av behörighet till känsliga uppgifter samt interna kontroller, rapport
- Omsorgsnämndens beslut § 48/2019 Remiss - Granskning av behörighet till känsliga uppgifter samt interna kontroller

Beslutet skickas till

För kännedom
Kommunrevisionen
Björn Andersson, säkerhetschef
Kommunfullmäktige