Örebro kommun
Stadsrevisionen

Missiv 2022-10-20

Till: Kommunstyrelsen, förskolenämnden, grundskolenämnden, gymnasienämnden och socialnämnden
För kännedom: Fullmäktiges presidium

Granskning av kommunens hantering av skyddade personuppgifter
Granskningen syftar till att bedöma hur kommunen säkerställer att uppgifter som rör skyddade personuppgifter inte röjs till obehöriga samt om kommunens rutiner är ändamålsenliga och tillämpade. Vår sammanfattande bedömning är att det förekommer brister i kommunens hantering av skyddade personuppgifter.

Det finns ändamålsenliga styrande dokument och rutiner för hanteringen av skyddade personuppgifter på kommunövergripande nivå samt vissa lokala rutiner som förvaltningarna tagit fram. Utöver centrala och lokala rutiner har inga specifika åtgärder vidtagits för att minska risken för röjning av skyddade personuppgifter. Vi bedömer vidare att ansvarsfördelningen tydliggörs i de styrande dokumenten men att vissa roller inte fullt omhändertagit sitt ansvar inom informationssäkerhetsarbetet och hanteringen av skyddade personuppgifter. Vi ser det som en brist att *Instruktionen för hantering av personuppgiftsincidenter* inte är välkänd inom kommunen och att det inte finns en enhetlig hantering av personuppgiftsincidenter. Vi har under granskningen inte noterat något arbete för att sprida antagna riktlinjer och policys inom kommunen.

Säkerhetsavdelningen kan involveras för att bistå vid riskanalyser för medarbetare med skyddade personuppgifter om verksamheterna önskar det stödet. I en sådan process beaktas hotbilden och individens enskilda perspektiv. Dock sker detta endast på begäran av verksamheten och inte systematiskt, vilket vi skulle rekommendera.

Kommunstyrelsen har delvis säkerställt en tillräcklig uppföljning och kontroll av informationssäkerhetsarbetet, det sker dock ingen specifik uppföljning eller kontroll av hanteringen av skyddade personuppgifter. Det finns inget ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter. Det finns inget automatiskt sätt att samla personuppgiftsincidenter på kommunövergripande nivå utan manuell handpåläggning. Vi bedömer det även som en brist att verksamheterna inte kan koda incidenten som ett skyddat personuppgiftsärende.

Vår bedömning är att det inte genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter. Medvetandegrad och kunskapsnivån behöver stärkas genom exempelvis obligatoriska utbildningar och ökad informationsspridning.

Informationssäkerhetsfrågan lyfts vid ett flertal tillfällen, för olika nämnder, i riskanalyserna. De risker som identifierats har en indirekt koppling med hanteringen av skyddade personuppgifter, det finns ingen risk med direkt bäring på individer med skyddade personuppgifter.

Utifrån granskningens iakttagelser rekommenderar vi kommunstyrelsen att:

- Säkerställa en enhetlig hantering av personuppgiftsincidenter inom hela kommunorganisationen genom att öka medarbetares kännedom om riktlinjer och rutiner.
- Genomföra risk- och konsekvensanalyser avseende hantering av skyddade personuppgifter och vid behov låt inkludera i internkontrollplanerna.
- Prioritera att genomföra obligatoriska utbildningar för samtlig personal avseende hanteringen av skyddade personuppgifter utifrån bestämmelser i styrande dokument.
- Överväga inrättandet av ”compliancefunktion/-er”, det vill säga en funktion som ansvarar för att bestämmelser och interna verksamhetsprinciper, som exempelvis riktlinjer, rutiner och anvisningar, följs och följs upp.
- Säkerställa en ändamålsenlig nivå av uppföljning och att avvikelsehanteringen avseende skyddade personuppgifter stärks

Rapporten överlämnas härmed till kommunstyrelsen och övriga berörda nämnder. Behandlat svar till revisionen önskas senast den 31 januari 2023.

Kontaktrevisorer för granskningen var Nils Gunnarsson.

För Örebro kommuns revisorer

Lena Jansson
Ordförande

Bengt Wentzel
Vice ordförande

Revisionsfrågor:	Svar:	Bedömning:
Har kommunen analyserat risken för att skyddade personuppgifter röjs på ett ändamålsenligt sätt? Har den enskilda individens perspektiv beaktats?	Delvis.	
Har kommunen vidtagit ändamålsenliga åtgärder för att minska risken för röjning av skyddade personuppgifter och följs detta upp av berörda nämnder?	Delvis.	
Finns ändamålsenliga styrande dokument och rutiner för hantering av skyddade personuppgifter? Hur görs styrdokument och rutinbeskrivningar kända för medarbetare?	Ja.	
Har kommunen säkerställt tillräcklig uppföljning och kontroll av styrdokumentens och rutinbeskrivningarnas efterlevnad?	Delvis.	
Genomförs fortlöpande kompetensutveckling kring skyddade personuppgifter?	Nej.	
Finns ett ändamålsenligt avvikelsehanteringssystem som omfattar skyddade personuppgifter? Hur tillvaratas erfarenheter från avvikelser?	Nej.	
Har säkerhetsfrågor kopplade till skyddade personuppgifter analyserats och trygghetsskapande åtgärder vidtagits med utgångspunkt i dessa analyser?	Delvis.	

PENNEO

Signaturerna i detta dokument är juridiskt bindande. Dokumentet är signerat genom Penneo™ för säker digital signering. Tecknarnas identitet har lagrats, och visas nedan.

"Med min signatur bekräftar jag innehållet och alla datum i detta dokumentet."

LENA JANSSON
Ordförande
Serienummer: 19540413xxxx
IP: 83.187.xxx.xxx
2022-10-26 10:50:27 UTC

BENGT LILLEBROR WENTZEL
Vice ordförande
Serienummer: 19510908xxxx
IP: 212.247.xxx.xxx
2022-10-26 11:00:25 UTC