

Kommunrevisionen informerar

Umeå Energi AB:s hantering av skyddade personuppgifter

Granskningens inriktning

Den som är utsatt för hot kan i vissa fall få skyddade personuppgifter. Antalet personer i Sverige med skyddade personuppgifter har de senaste åren ökat. Mellan åren 2011 och 2023 har antalet personer med skyddade personuppgifter ökat från drygt 12 000 personer till drygt 28 000 personer. Personer med skyddade personuppgifter kan drabbas av mycket allvarliga risker och problem om kommuners verksamheter inte har en ändamålsenlig kontroll över uppgifterna.

Resultat

Av granskningen framgår att Umeå Energi har övergripande styrande dokument för arbetet med informationssäkerhet och dataskyddsförordningen som innehåller få skrivelser om hanteringen av skyddade personuppgifter. Att det inte finns ett övergripande styrande dokument specifikt för hanteringen av skyddade personuppgifter, bedömer vi vara en brist. Vi ser positivt på att det pågår en översyn av bolagets styrdokument kopplat till informationssäkerhet och dataskyddsförordningen. Vi noterar att det har upprättats vissa verksamhetsnära rutinbeskrivningar för hanteringen av skyddade personuppgifter och tillhörande processer. Rutinbeskrivningarna utgör ett värdefullt stöd i sammanhanget, även om vi bedömer att de kan utvecklas för att spegla det totala arbetet som bedrivs för hanteringen av skyddade personuppgifter.

Bolagets styrelse har inte gjort någon uppföljning inom området avseende exempelvis arbetsrutiner, kompetensutveckling eller avvikelshantering. Det har heller inte genomförts risk- och konsekvensanalyser avseende röjning av skyddade personuppgifter inom ramen för det systematiska internkontrollarbetet. Vi ser dock positivt på att det har påbörjats en översyn och genomlysning av bolagets informationssäkerhetsarbete i allmänhet och hantering av skyddade personuppgifter i synnerhet. I processen har bolagsspecifika risker och brister identifierats som antingen har åtgärdats eller ska åtgärdas i närtid.

Arbetsrutinerna introduceras vid nyanställning, och innan årsskiftet 2024 kommer hanteringen av skyddade personuppgifter ingå i bolagets utbildning om GDPR. Det är positivt och en förutsättning för att samtliga medarbetare ska vara införstådda i hanteringen av skyddade personuppgifter specifikt. Det bör ske regelbundet i syfte att hålla kunskapen vid liv över tid.

Rekommendationer

Utifrån granskningens resultat rekommenderar vi styrelsen och VD i Umeå Energi AB att:

- Upprätta risk- och konsekvensanalyser specifikt avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanerna.
- Upprätta och anta ett styrdokument av övergripande karaktär för hanteringen av skyddade personuppgifter. Riktlinjen bör tydliggöras genom verksamhetsnära rutiner/instruktioner.
- Genomföra regelbundna utbildningar för samtliga medarbetare som hanterar skyddade personuppgifter, exempelvis som en del av ett årshjul. Överväg också att på en övergripande nivå informera samtliga medarbetare om skyddade personuppgifter.
- Säkerställa ändamålsenliga systemstöd för hanteringen av skyddade personuppgifter.

EY:s rapport "Granskning av Umeå Energi ABs hantering av skyddade personuppgifter, 2023-12-14".

För ytterligare information, kontakta:
Revisionens ordförande Ewa Miller,
ewa.miller@umea.se