

Kommunrevisionen informerar

Uppföljande granskning: Hantering av skyddade personuppgifter (Umeå Energi och Vakin)

Granskningens inriktning

Vi har granskat om Umeå Energi AB och Umeå Vatten och Avfallskompetens i Norr AB (Vakin) har vidtagit ändamålsenliga åtgärder utifrån tidigare revision av hanteringen av skyddade personuppgifter. Granskningen omfattar uppföljning av rekommendationer från 2023 års revision.

Resultat

Vår sammanfattande bedömning är att Umeå Energi AB samt Umeå vatten och avfallskompetens AB **har** vidtagit ändamålsenliga åtgärder med utgångspunkt från revisionens tidigare granskning och rekommendationer.

Resultatet av granskningen visar att både Umeå Energi AB och Vakin har förbättrat sin hantering av skyddade personuppgifter, men det finns fortfarande några utvecklingsområden. Bolagen har tagit fram eller reviderat styrdokument som nu tydligt omfattar hantering av skyddade personuppgifter. Vakin har infört ett särskilt kapitel i sina riktlinjer för informationssäkerhet och en uppdaterad rutinbeskrivning för praktisk hantering, medan Umeå Energi har tagit fram ett utkast till riktlinje som väntas beslutas om under 2025.

Båda bolagen har tagit fram mallar och processer för konsekvensbedömningar enligt GDPR artikel 35, och Umeå Energi har genomfört sådana bedömningar. Trots detta har ingen av bolagen inkluderat hanteringen av skyddade personuppgifter i sina internkontrollplaner, vilket innebär att systematisk uppföljning och riskanalys på styrelsenivå kan förbättras.

När det gäller utbildning och kompetens har Umeå Energi säkerställt att hantering av skyddade personuppgifter ingår i den årliga utbildningen om dataskydd och informationssäkerhet för samtliga medarbetare. Vakin erbjuder årliga digitala utbildningar i GDPR och informerar särskilt berörda medarbetare om rutiner för skyddade

personuppgifter, men det saknas dokumentation som styrker att all relevant personal fått kompetensutveckling.

Umeå Energi har analyserat sina system och konstaterat att skyddade personuppgifter inte hanteras i IT-system, utan hanteringen sker manuellt. Vakin hanterar skyddade personuppgifter manuellt på papper, förvarade i säkerhetsskåp, och endast tre personer har tillgång.

Båda bolagen har processer för att anmäla och följa upp personuppgiftsincidenter. Umeå Energi har särskilt kategoriserat skyddade personuppgifter i sin incidenthantering, medan Vakin följer upp avvikelser vid behov. Slutligen har båda bolagen behandlat revisionsrapporten i styrelsen och gett VD i uppdrag att åtgärda brister, men återrapporering av vidtagna åtgärder till styrelsen har inte alltid skett, vilket är ett tydligt förbättringsområde.

Rekommendationer

Vi rekommenderar bolagsstyrelserna att:

- Besluta om riktlinjerna för hantering av skyddade personuppgifter.
- Säkerställa att vidtagna åtgärder, särskilt de som vidtagits utifrån granskningar, återrapporeras till styrelsen.
- Överväga att genomföra riskanalyser avseende hantering av skyddade personuppgifter och inkludera området i internkontrollplanerna.

EY:s rapport "Uppföljande granskning av hantering av skyddade personuppgifter Umeå Energi och Vakin, november 2025". För ytterligare information, kontakta revisionens ordförande Ewa Miller, ewa.miller@umea.se