Nacka kommun

Revisionsskrivelse 2023-05-24

Lekmannarevisorerna i Nacka Energi AB

Till: Nacka Energi AB
För kännedom: Kommunfullmäktige

Granskning av Nacka Energi ABs hantering av skyddade personuppgifter

Vi lekmannarevisorerna i Nacka Energi AB har låtit EY genomföra en granskning med syftet att bedöma hur styrelse och VD för Nacka Energi AB (NEAB) säkerställer att skyddade personuppgifter inte röjs till obehöriga samt om bolagets rutiner är ändamålsenliga och tillämpade. Detta har avsett skyddade personuppgifter för både kunder och anställda i bolaget. Vår övergripande bedömning är att styrelsen och VD har säkerställt att skyddade personuppgifter inte röjs till obehöriga, men att det finns ytterligare åtgärder att vidta.

Det finns en tydlig organisation med ansvarsfördelning för hantering av kunder, medarbetare och anställningshandlingar med skyddade personuppgifter. Det finns en riktlinje och två rutinerna upprättade, vilka säkerställer en tillräcklig vägledning på såväl övergripande som detaljerad nivå för bolagets medarbetare. Dokumenten är inte antagna av bolagets styrelse eller VD med hänvisning till att riktlinjer (motsv) som rör daglig operativ verksamhet inte ska antas av styrelsen eller VD. Vi bedömer dock att riktlinjen bör antas av styrelsen eller VD givet områdets komplexitet och medföljande risker som kräver insyn i hanteringen samt regelbunden uppföljning. Vi noterar även att riktlinjen och rutinerna nyligen är upprättade och således behöver implementeras i hela organisationen, även bland de medarbetare som sällan kommer i kontakt med skyddade personuppgifter.

Nya medarbetare ska introduceras till bolagets riktlinje och rutiner gällande hantering av skyddade personuppgifter och ingår således i den obligatoriska utbildningsplanen vilket vi ser positivt på. Däremot bedömer vi att det finns ett behov av att utbilda samtliga medarbetare i hanteringen av skyddade personuppgifter specifikt och att det bör ske regelbundet i syfte att hålla kunskapen vid liv över tid. Det skulle stärka grundkunskaperna bland de medarbetare som sällan kommer i kontakt med skyddade personuppgifter i syfte att undvika fel orsakade av den mänskliga faktorn. Den anser vi vara den största risken i hanteringen av skyddade personuppgifter.

Risk- och väsentlighetsanalyser kring hanteringen av skyddade personuppgifter har upprättats inom ramen för bolagets systematiska internkontrollarbete. Skyddade personuppgifter utgör sedan årsskiftet en del av bolagets systematiska dataskyddsarbete genom att följa ett årshjul, vilket bland annat innefattar uppföljning av efterlevnad av rutiner och att dessa vid behov revideras en gång per år. Vi ser positivt på att det har påbörjats en förändringsprocess och genomlysning av bolagets dataskyddsarbete i allmänhet och hantering av skyddade personuppgifter i synnerhet.

Bolaget har vidtagit åtgärder för hanteringen av skyddade personuppgifter. Vi bedömer dock att det finns vissa brister och svagheter i nuvarande hantering, däribland avsaknad av automatiska behörighets- och åtkomstbegränsningar inbyggda i verksamhetssystemen, att vissa nuvarande arbetsprocesser delvis kräver manuell hantering samt att det inte genomförs loggkontroller. Bolaget är medvetet om bristerna och har eller ska utifrån genomförd risk- och väsentlighetsanalys vidta ytterligare åtgärder.

Det finns ett avvikelsehanteringssystem som omfattar skyddade personuppgifter i och med att det går att identifiera skyddade personuppgifter från övriga avvikelser. Vi ser positivt på att det finns en framtagen mall med en särskild kategori som omfattar skyddade personuppgifter som används för att riskbedöma en eventuell personuppgiftsincident. Nuvarande rutiner för avvikelsehantering möjliggör att erfarenheter från avvikelser tillvaratas och kan skapa systematik för att åtgärda eventuella brister kopplat till hanteringen av skyddade personuppgifter.

Vi rekommenderar styrelsen och VD i Nacka Energi AB att:

- Fastställa riktlinjen för hanteringen av skyddade personuppgifter.
- Genomföra obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument samt hanteringen av skyddade personuppgifter regelbundet.
- Säkerställa att pågående upphandling av ett nytt kundinformationssystem, som säkerställer en mer ändamålsenlig hantering av skyddade personuppgifter och minskar manuell hantering, implementeras skyndsamt.
- Säkerställa att det inköpta systemet för säkra meddelanden skyndsamt implementeras.
- Genomföra kontroller av användarloggar som en organisatorisk säkerhetsåtgärd för att kompensera påtalade brister i systemstödens avsaknad av behörighet.

Vi önskar svar på rekommendationerna från Nacka Energi AB senast 2023-11-15

För lekmannarevisorerna i Nacka Energi AB

Yvonne Wessman
Ordförande

Lars Berglund
Vice ordförande

Bilaga: Revisionsrapport 5/2023 Granskning av Nacka Energi ABs hantering av skyddade personuppgifter