Nacka kommun

Revisionsskrivelse 2023-05-24

Lekmannarevisorerna i Nacka vatten och avfall AB

Till: Nacka vatten och avfall AB
För kännedom: Kommunfullmäktige

**Granskning av Nacka vatten och avfall ABs hantering av skyddade personuppgifter**
Vi lekmannarevisorerna i Nacka vatten och avfall AB har låtit EY genomföra en granskning med syftet att bedöma hur styrelse och VD för Nacka vatten och avfall AB (NVOA) 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 inte har säkerställt att skyddade personuppgifter röjs till obehöriga.

Det finns en tydlig organisation med ansvarsfördelning för hantering av kunder, medarbetare och anställningshandlingar med skyddade personuppgifter. Det finns en arbetsrutin, som endast till viss del säkerställer en tillräcklig vägledning på såväl övergripande som detaljerad nivå för bolagets medarbetare. Dokumenten är dessutom inte antagna av bolagets styrelse eller VD. Vi bedömer att bolaget bör upprätta en övergripande riktlinje och att styrelsen eller VD bör fastställa denna givet områdets komplexitet och medföljande risker som kräver insyn i hanteringen samt regelbunden uppföljning.

Nya medarbetare ska introduceras till bolagets arbetsrutiner 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.

Vi noterar därutöver att bolaget inte har genomfört risk- och konsekvensanalyser kring hanteringen av skyddade personuppgifter inom ramen för bolagets systematiska internkontrollarbete. Det ser vi som en brist. Arbetet med skyddade personuppgifter bör prioriteras, tas in i bolagets systematiska utvecklingsarbete, följas upp och revideras, t ex en gång per år.

Avdelning kundrelationer har vidtagit åtgärder för hanteringen av skyddade personuppgifter. Vi bedömer dock att det finns vissa brister i dem, 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 saknas ett avvikelsehanteringssystem som omfattar skyddade personuppgifter i och med att det inte går att identifiera skyddade personuppgifter från övriga avvikelser. Vår bedömning är att det behöver tydliggöras att incidenter med skyddade personuppgifter måste hanteras särskilt varsamt och skyndsamt, givet de möjliga konsekvenserna av en röjning.

Vi rekommenderar styrelsen och VD i Nacka vatten och avfall AB att:

- Upprätta risk- och konsekvensanalyser avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanen.
- Upprätta och anta en riktlinje av övergripande karaktär för hanteringen av skyddade personuppgifter.
- Genomföra obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument samt hanteringen av skyddade personuppgifter regelbundet.
- Begränsa åtkomsten till personuppgifterna genom strikt behörighetstilldelning.

- Genomföra kontroller av användarloggar som en organisatorisk säkerhetsåtgärd för att minska riskerna för röjning av skyddade personuppgifter.
- Säkerställa möjligheten att systematiskt följa upp avvikelser avseende skyddade personuppgifter.

Vi önskar svar på rekommendationerna från Nacka vatten och avfall AB senast 2023-11-15

För lekmannarevisorerna i Nacka vatten och avfall AB

Yvonne Wessman
Ordförande

Lars Berglund
Vice ordförande

Bilaga: Revisionsrapport 6/2023 Granskning av Nacka vatten och avfall AB hantering av skyddade personuppgifter