Sammendrag – Eksternrevisjon 2021

Formålet med Relato AS sin revisjon av **Pindena AS** har vært å vurderer om selskapet har et helhetlig styringssystem for informasjonssikkerhet som er i samsvar med hovedelementene i standarden *ISO/IEC 2700:2013 – ledelsessystemer for informasjonssikkerhet (ISO 27001)*, samt ivaretar kravene i Personopplysningsloven, nærmere bestemt:

- Lov om behandling av personopplysninger (Personopplysningsloven)
- Forskrift om behandling av personopplysninger (Personopplysningsforskriften)

Revisjonen omfatter Pindenas arbeid med et ledelsessystem for informasjonssikkerhet, herunder sikkerhetsmål og sikkerhetsstrategi, samt klassifisering og risikovurdering for sikring av informasjon. Videre at det, med bakgrunn i risikovurderinger, er etablert risikoreduserende sikkerhetstiltak som er effektive, og tiltak som blir løpende oppdatert og tilpasset til endringer i risikobildet[1].

Revisjonen er gjennomført ved dokumentanalyse og møteserie med Pindena AS, hvor dokumentasjon, rutiner, teknologier, ansvarsforhold og rollefordeling har inngått som del av vurderingen. Det er også gjennomgått en DPIPA (Data Protection Impact Pre-Assessment), en forhåndsvurdering av om en fullstendig DPIA er nødvendig å gjennomføre.

Revisjonen viser at Pindena har innført et styringssystem for informasjonssikkerhet som imøtegår kravene i Personopplysningsloven, og som etterlever de relevante kravene i ISO 27001.

Hovedtrekkene er:

- Pindenas styringssystem for informasjonssikkerhet definerer prosessene for arbeidet med informasjonssikkerhet, planlegging og utførelse av sikkerhetstiltak, og hvordan arbeidet med informasjonssikkerhet skal evalueres og forbedres.
- Pindena har utarbeidet en policy, retningslinjer og rutiner for sikkerhetstiltak etter beste praksis og tilpasset størrelsen på sin bedrift, og planlagt et årshjul for revidering og oppfølging.
- Pindena har innført systemer for registrering, håndtering og oppfølging av avvik og informasjonssikkerhetshendelser.
- Pindena har gjennomført en prevurdering til DPIA for lagring av personopplysninger i sine systemer, og konkludert med at risikoen for personvernet er lav. En fullstendig DPIA er derfor ikke gjennomført. Alle relevante element for innsamling, håndtering, lagring samt sletting av personopplysninger fulgt. Pindena har også en aktiv dialog med sine kunder om personvern.
- Pindena har samlet sett innført et regime for å håndtere informasjonsikkerhet og personvern som overstiger det som er normalt å forvente, og er godt rustet for videre ivaretakelse.

[1] Oppdragets omfang omfattet ISO 27001 Ledelsessystem (ISMS) Kap 1-7 og kap 10, samt ISO 27001 Annex A, Kap A5 – A9 på et høyt nivå.