

Databeskyttelseslovgivning

recallTM
Your Information. Securely Managed.

Databeskyttelseslovgivning

Muligheten til å følge, spore og finne kritiske data er viktig for å overholde forskriftsmessige krav, for eksempel:

Gramm-Leach-Bliley Act (GLBA), 1999

GLBA krever at finansinstitusjoner har administrative, tekniske og fysiske verktøy for å beskytte integriteten og konfidensialiteten til kunderegistre. Selskaper må også sikre tilgang til finansiell informasjon og forretningskontinuitet. Dersom denne informasjonen ikke er tilgjengelig, kan dette føre til bøter på opptil 1 million dollar i tillegg til andre straffer.

Sarbanes-Oxley Act (SOX), 2002

SOX ble vedtatt som en direkte respons på skandaler i selskaper som Enron og WorldCom. Forskriftene skal sikre integriteten i selskapenes finansielle informasjon og håndtere bedriftsansvar. SOX påvirker amerikanske børsnoterte selskaper, men kan også påvirke ledere, styremedlemmer og revisorer globalt, ved å holde dem personlig ansvarlig for nøyaktigheten og opprettholdelsen av økonomisk informasjon. Betydelige straffer og bøter - inkludert fengselsstraff - kan forekomme.

Health Insurance Portability and Accountability Act (HIPAA), 1996

HIPAA ble vedtatt for å beskytte helseforsikringsdekning for arbeidere og deres familier når de bytter eller mister jobb. En del, Title II, krever opprettelse av standarder for elektroniske pasientregistre, administrative og økonomiske data, og beskyttelse og sikkerhet for helserelaterte data. HIPAA kan påvirke organisasjoner som er involvert i eller relatert til helsevern. Den kan også utvides til selskaper som tilbyr tjenester til helsesektoren, for eksempel leverandører av informasjonssystemer. Selv om HIPAA ikke spesifiserer tiltak for overholdelse, kan manglende beskyttelse av informasjon som dekkes av HIPAA på rimelig vis føre til bøter på opptil 250 000 dollar og opptil 10 års fengselsstraff.

Løpende eller planlagte revisjoner er nødvendig for å bekrefte nøyaktigheten og tilgjengeligheten til informasjonen som er spesifikk for de nevnte lovene. Systemene blir ofte testet for å sikre at de leverer den relevante informasjonen på en tidriktig måte. Mens bevaringstiden kan være opptil syv år for økonomiske data og for helsesektoren, kan det hende at data som blir håndtert av helsesektoren, må bevares i over 20 år. Hovedpoenget er at denne informasjonen må være lett tilgjengelig når som helst, og at innholdet kan gå over en betydelig tidsperiode.

I Australia krever Privacy Act, 2001, under Principle 4, Storage and Security of Personal Information, at den som er i besittelse av registrene, sikrer at informasjonen i dem blir beskyttet mot tap, uautorisert tilgang og bruk, modifikasjon, avsløring og annen form for misbruk ved å gjennomføre sikkerhetstiltak som er rimelige og innen registerbeholderens myndighet å bruke. Manglende overholdelse gjør den som besitter registrene, personlig ansvarlig og gjenstand for rettsforfølgelse.

Nesten alle land som Recall har virksomhet i har nå innført en form for lovgivning for å sikre at sensitiv informasjon blir beskyttet. Vanligvis tar det utgangspunkt i økonomi og er iverksatt av landets økonomiske eller finansielle myndigheter. For EU gjelder direktivet Markets in Financial Instruments Directive (MiFID) og for Storbritannia gjelder loven Data Protection databeskyttelse and Freedom of Information Acts.

* Kilde: B&L Associates, "Compliance through Proper Tape Management"