**Procedure for datalæk**

**1. Identifikation af datalækket**

* **Dokumentér hændelsen**: Alle detaljer omkring datalækket dokumenteres, såsom tidspunkt, hvordan det blev opdaget, og hvilke data der blev påvirket.

**2. Sikring af systemer**

* **Stop datalækket**: Isoler og afbryd de berørte systemer for at forhindre yderligere tab af data.
* **Undersøg sikkerhedshuller**: Gennemgå systemet for at identificere, hvordan lækket skete, og luk eventuelle sikkerhedshuller.

**3. Intern evaluering**

* **Analyser omfanget af lækket**: Vurder, hvilke data er berørt, herunder om det drejer sig om følsomme persondata, som defineret i GDPR.
* **Vurder risikoen for berørte personer**: Hvis lækket indebærer risiko for de registrerede personers rettigheder og friheder, skal situationens alvor vurderes.

**4. Anmeldelse til Datatilsynet**

* **72-timers frist**: Under GDPR skal et databrud anmeldes til de relevante tilsynsmyndigheder inden for 72 timer efter opdagelsen.
* **Indhold af anmeldelsen**: Beskriv bruddets art, de berørte data, antallet af registrerede personer, og hvad nordicway har gjort for at afhjælpe situationen.
* **Dokumentér bruddet**: Selv hvis det besluttes, at hændelsen ikke skal rapporteres, skal nordicway dokumentere hændelsen og angive en begrundelse for den undladte rapportering.

**5. Meddelelse til de berørte personer**

* **Meddelelse til personer**: Hvis bruddet udgør en høj risiko for individernes rettigheder og friheder, skal de berørte personer underrettes uden unødig forsinkelse af nordicway.
* **Indhold af meddelelse**: Meddelelsen skal forklare bruddets natur, de potentielle konsekvenser og de foranstaltninger, der er iværksat for at afhjælpe det.
* **Kontaktinformation**: Oplysninger om, hvem de berørte kan kontakte for yderligere information, skal også medtages. Det vil være kontaktoplysninger til den relevante nordicway medarbejder på tidspunktet for lækket.

**6. Afhjælpende handlinger**

* **Reparation og genoprettelse**: nordicway skal rette op på de sårbarheder, der førte til bruddet, og sørg for at forhindre fremtidige lækager.
* **Opdatering af politikker**: nordicway skal gennemgå og opdate virksomhedens interne politikker, processer og sikkerhedsforanstaltninger for at minimere risikoen for fremtidige databrud.
* **Efteruddannelse**: nordicway skal sørge for, at medarbejderne er opdateret med hensyn til databeskyttelsesregler og håndtering af persondata.

**7. Overvågning og forebyggelse af fremtidige brud**

* **Langsigtet overvågning**: nordicway skal udarbejde en overvågningsplan for at sikre, at systemer fortsat er sikre.
* **Ekstern bistand**: nordicway skal overveje, om bruddet bør føre til yderligere ekstern konsulentbistand.

**8. Dokumentation og løbende evaluering**

* **Detaljeret log**: nordicway dokumenterer forløbet, herunder beslutninger, tiltag og resultater, så det er muligt at eftervise overholdelse af GDPR-kravene. Loggen gemmes internt.
* **Evaluér og forbedr**: Efter at krisen er løst, evaluer nordicway, hvordan lækket blev håndteret, og implementer eventuelle forbedringer for fremtidige hændelser.

**9. Samspil med tredjeparter**

* **Samarbejde med databehandlere**: Hvis tredjepartsdatabehandlere er involveret, skal de også underrettes, og sikre sig at de følger de nødvendige foranstaltninger for at afhjælpe lækket.