**Procedur för dataläcka**

1. **Identifiering av dataläckan**
   * Dokumentera händelsen: Alla detaljer om dataläckan dokumenteras, såsom tidpunkt, hur den upptäcktes och vilka data som påverkades.
2. **Säkring av system**
   * Stoppa dataläckan: Isolera och avbryt de påverkade systemen för att förhindra ytterligare dataförlust.
   * Undersök säkerhetshål: Granska systemet för att identifiera hur läckan skedde och åtgärda eventuella säkerhetsbrister.
3. **Intern utvärdering**
   * Analysera omfattningen av läckan: Bedöm vilka data som påverkas, inklusive om det handlar om känsliga personuppgifter som definierats i GDPR.
   * Utvärdera risken för berörda personer: Om läckan innebär risk för individernas rättigheter och friheter måste allvaret av situationen bedömas.
4. **Anmälan till IMY**
   * 72-timmars tidsfrist: Under GDPR ska ett dataintrång rapporteras till de relevanta tillsynsmyndigheterna inom 72 timmar efter upptäckt.
   * Innehåll i anmälan: Beskriv intrångets art, de berörda data, antalet registrerade personer och vad nordicway har gjort för att åtgärda situationen.
   * Dokumentera intrånget: Även om det beslutas att händelsen inte ska rapporteras, måste nordicway dokumentera händelsen och ge en motivering för den uteblivna rapporteringen.
5. **Meddelande till de berörda personerna**
   * Meddelande till personerna: Om intrånget utgör en hög risk för individernas rättigheter och friheter, ska de berörda personerna informeras utan onödig försening av nordicway.
   * Innehåll i meddelandet: Meddelandet ska förklara intrångets art, potentiella konsekvenser och åtgärder som vidtagits för att åtgärda det.
   * Kontaktinformation: Information om vem de berörda kan kontakta för mer information ska också inkluderas. Detta kommer att vara kontaktuppgifter till relevant nordicway-medarbetare vid tidpunkten för läckan.
6. **Åtgärder**
   * Reparation och återställning: nordicway måste åtgärda de sårbarheter som ledde till intrånget och säkerställa att framtida läckor förhindras.
   * Uppdatering av policyer: nordicway måste granska och uppdatera företagets interna policyer, processer och säkerhetsåtgärder för att minimera risken för framtida dataintrång.
   * Vidareutbildning: nordicway måste se till att medarbetarna är uppdaterade angående dataskyddsregler och hantering av personuppgifter.
7. **Övervakning och förebyggande av framtida intrång**
   * Långsiktig övervakning: nordicway måste utveckla en övervakningsplan för att säkerställa att systemen förblir säkra.
   * Extern hjälp: nordicway bör överväga om intrånget kräver ytterligare extern konsultation.
8. **Dokumentation och kontinuerlig utvärdering**
   * Detaljerad logg: nordicway dokumenterar förloppet, inklusive beslut, åtgärder och resultat, så att det är möjligt att visa att GDPR-kraven har uppfyllts. Loggen sparas internt.
   * Utvärdera och förbättra: Efter att krisen är löst, ska nordicway utvärdera hur läckan hanterades och implementera eventuella förbättringar för framtida incidenter.
9. **Samarbete med tredje parter**
   * Samarbete med databehandlare: Om tredje parts databehandlare är inblandade, ska de också informeras och säkerställa att de vidtar nödvändiga åtgärder för att åtgärda läckan.