**Procedure for Data Breach**

1. **Identification of the Data Breach**
   * Document the Incident: All details of the data breach should be documented, such as the time, how it was discovered, and which data was affected.
2. **Securing Systems**
   * Stop the Data Breach: Isolate and shut down the affected systems to prevent further data loss.
   * Investigate Security Gaps: Review the system to identify how the breach occurred and close any security gaps.
3. **Internal Evaluation**
   * Analyze the Scope of the Breach: Assess which data is affected, including whether it involves sensitive personal data as defined under GDPR.
   * Evaluate Risk for Affected Individuals: If the breach poses a risk to individuals' rights and freedoms, the severity of the situation must be assessed.
4. **Notification to the Data Protection Authority**
   * 72-Hour Deadline: Under GDPR, a data breach must be reported to the relevant supervisory authorities within 72 hours of discovery.
   * Contents of the Report: Describe the nature of the breach, the affected data, the number of individuals affected, and what nordicway has done to mitigate the situation.
   * Document the Breach: Even if it is decided not to report the incident, nordicway must document the event and provide a rationale for the decision not to report.
5. **Notification to Affected Individuals**
   * Notify Individuals: If the breach poses a high risk to individuals' rights and freedoms, affected individuals should be notified without undue delay by nordicway.
   * Contents of Notification: The notification should explain the nature of the breach, the potential consequences, and the measures taken to remedy it.
   * Contact Information: Details about whom the affected individuals can contact for further information should also be included. This will be the relevant nordicway employee's contact information at the time of the breach.
6. **Remedial Actions**
   * Repair and Restoration: nordicway must fix the vulnerabilities that led to the breach and ensure future leaks are prevented.
   * Policy Updates: nordicway should review and update internal policies, processes, and security measures to minimize the risk of future breaches.
   * Staff Training: nordicway must ensure employees are updated on data protection regulations and the handling of personal data.
7. **Monitoring and Prevention of Future Breaches**
   * Long-Term Monitoring: nordicway should develop a monitoring plan to ensure systems remain secure.
   * External Assistance: nordicway should consider whether the breach necessitates additional external consultation.
8. **Documentation and Ongoing Evaluation**
   * Detailed Log: nordicway documents the process, including decisions, actions, and results, so compliance with GDPR can be demonstrated. The log is stored internally.
   * Evaluate and Improve: After the crisis is resolved, nordicway should evaluate how the breach was handled and implement any improvements for future incidents.
9. **Interaction with Third Parties**
   * Cooperation with Data Processors: If third-party data processors are involved, they should also be informed and ensure they take necessary measures to address the breach.