Personal Data Breach Notification Procedure

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

This Personal Data Breach Notification Procedure outlines the steps to be followed in the event of a personal data breach as required by the General Data Protection Regulation (GDPR). The procedure aims to ensure prompt and appropriate notification to affected individuals and relevant authorities to mitigate the impact of the breach and uphold the rights and freedoms of individuals.

2. Scope

This procedure applies to all employees, contractors, and data processors of CNTXT who handle or have access to personal data. It covers all breaches involving accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data.

3. Personal Data Breach Notification Procedure

3.1 Definitions

- Personal Data: Personal data refers to any information relating to an identified or identifiable natural person, such as names, identification numbers, contact details, financial information, health data, etc.
- Personal Data Breach: A personal data breach refers to a breach of security that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored, or otherwise processed.

3.2 Reporting a Personal Data Breach

- Any employee, contractor, or data processor who becomes aware of a personal data breach must immediately report it to the designated Data Protection Officer (DPO) or the Privacy Officer.
- The report should include details such as the date, time, and description of the breach, the type of personal data involved, and any known or suspected causes.

3.3 Assessment and Investigation

- The Privacy Officer will promptly initiate an assessment and investigation upon receiving a personal data breach report.
- The investigation will determine the nature and scope of the breach, assess potential risks and impacts on individuals' rights and freedoms, identify affected individuals, and establish the cause and source of the breach.

3.4 Breach Notification

3.4.1 Notification to Supervisory Authority:

- In the event of a personal data breach, where it is likely to result in a risk to the rights and freedoms of individuals, CNTXT will notify the relevant Supervisory Authority within 72 hours of becoming aware of the breach unless the breach is unlikely to result in a risk to individuals' rights and freedoms.
- The notification will include details of the breach, the approximate number of affected individuals, the likely consequences, and any measures taken or proposed to address the breach.

3.4.2 Notification to Affected Individuals:

- If the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, CNTXT will notify the affected individuals without undue delay.
- The notification will include a description of the breach, the type of personal data involved, potential risks or impacts, recommended actions for individuals to mitigate harm, and contact information for further inquiries.

3.5 Mitigation and Remediation

CNTXT will take immediate and appropriate actions to mitigate the impact of the personal data breach and prevent further unauthorized access or harm.

This may include but is not limited to:

- Implementing additional security measures
- Recovering or restoring the personal data
- Coordinating with relevant authorities and stakeholders
- Offering support services to affected individuals, such as identity theft protection or credit monitoring, where necessary.

4. Document Security Classification

Company Internal (please refer to the Data Classification policy for details).

5. Non-Compliance

Compliance with this policy shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

6. Responsibilities

The Privacy Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

7. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

End of Personal Data Breach Notification Procedure. For version history, please see the next page.

Version history

Version	Log	Date
1 Current	Policy version approved by Youssef Ouyhya	26 Oct, 2024
1	New Policy version Created	26 Oct, 2024