Langslide

Data Breach Management Procedure

Version 1.0

PURPOSE

Rudramsa Systems Pvt. Ltd. (herein referred to as Organization) to process personal data during its business operations. This Procedure provides general principles and an approach model to respond to and mitigate breaches of personal data (a "personal data breach") in one or both of the following circumstances:

- The personal data identifies data subjects who are residents of the Member States of the European Union (EU) and countries in the European Economic Area (EEA), regardless of where that data is subject to processing globally and
- The personal data is subject to processing in the EU and/or EEA, regardless of the country of residency of the data subject.
- The Procedure outlines the general principles and actions for successfully managing the response to a data breach and fulfilling the obligations surrounding the notification to Supervisory Authorities and individuals as required by the EU GDPR.

SCOPE

The Procedure applies to all security incidents affecting our processes that involve personal data. It is to be followed at all locations where personal data is processed by the organization or by a third party on behalf of the organization. The Procedure shall be applied to all our personnel, suppliers, contractors, and subcontractors. It must be considered in conjunction with other applicable organization standards and policies regarding the protection of protecting.

DEFINITIONS

- **Personal Data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person Regulation.
- **The controller** is responsible for determining the purposes and means of processing the personal data.
- A **Data Protection Officer or DPO** means, where applicable, a data protection officer appointed per the General Data Protection Regulation (GDPR)/CCPA or an individual responsible for protecting personal data.
- A **Data Subject** is a natural person whose personal data is processed by a controller or processor.
- **Personal Data Breach** means a security breach that leads to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
- **Personal Data** shall have the meaning given to it under the GDPR/CCPA and shall include any information relating to an identified or identifiable natural person.
- The term **"processor"** shall mean the party who processes personal data on behalf of the Controller; "responder" means a person/team designated to handle a Personal Data Breach.
- **Supervisory Authority** shall have the meaning assigned to it under the GDPR/CCPA; Personal Data Breaches shall be categorized as:
    - **Confidentiality Breach** – where there is accidental or unauthorized access to, or disclosure of, personal data.
    - **Availability Breach** – where there is accidental or unauthorized loss of access to, or destruction of, personal data.
    - **Integrity Breach** – where there is an accidental or unauthorized alteration of personal data.

ROLES AND RESPONSIBILITIES

- The DPO should also review ongoing compliance.
- The DPO is responsible for ensuring appropriate security measures to protect Personal Data.

PROCEDURE

Data Breach Response Team

- A data breach response team must be a multi-disciplinary team of knowledgeable and skilled individuals in the IT department, IT security, and legal, legal, and public affairs. The team may be a physical (local) or virtual (multiple locations) team that responds to any suspected/alleged personal data breach.
- Chief Information Security Officer (CISO) appoints the Data Breach Response Team Leader and members of the Data Team. The team must be appointed by members regardless of whether or not a breach has occurred.
- The team must ensure the readiness for a personal data breach response, along with the needed resources and preparation (such as call lists, substitution of key roles, desktop exercises, and required review of Organization policies, procedures, and practices).
- The team's mission is to provide an immediate, effective, and skillful response to any suspected/alleged or actual personal data breaches affecting the Organization.
- If required, the team members may also involve external parties (e.g., an information security vendor to carry out digital forensics tasks or an external communications agency to assist the organization in meeting crisis communications needs).
- The Data Breach Response Team Leader can choose to add additional personnel to the team to handle data breaches.
- The Data Breach Response Team may deal with more than one suspected/alleged or actual personal data breach at a time. Although the core team may be the same for each, this is not a requirement.
- The Data Breach Response Team must be prepared to respond to a suspected/alleged or actual personal data breach 24/7, year-round. Therefore, the contact details for each Team member, including personal contact details, shall be stored in a central location and used whenever notification of a suspected/alleged or actual personal data breach is received.

Data Breach Response Team Duties

Once a personal data breach is reported to the Data Breach Response team leader, the team must implement the following:

- Validate/triage the personal data breach
- Ensure proper and impartial investigation (including digital forensics if necessary) is initiated, conducted, documented, and concluded
- Identify remediation requirements and track resolution
- Report findings to the top management
- Coordinate with appropriate authorities as needed
- Coordinate internal and external communications
- Ensure that impacted data subjects are adequately notified, if necessary

The Data Breach Response Team will convene for each reported (and alleged) personal data breach and will be headed by the Data Breach Response Team Leader.

Data Breach Response Process

The Data Breach Response Process is initiated when anyone notices a notice or actual personal data breach occurs and notifies any Data Breach Response team member. The team is responsible for determining whether the breach should be considered affecting personal data.

The Data Breach Team leader is responsible for documenting all decisions of the core team. Since the supervisory authorities might review these documents, they must be written precisely and thoroughly to ensure traceability and accountability.

Personal data breach notification: Data processor to data controller

When a personal data breach or suspected data breach affects personal data being processed on behalf of a third party, the Data Protection Officer of the Organization acting as a data processor must report any personal data breach to the respective data controller/controllers without undue delay.

The Data Protection Officer will send a Notification to the controller that will include the following:

- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the Data Breach Response Team Leader/ Data Protection Officer
- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any information relating to the data breach

Chief Information Security Officer (CISO) will record the data breach in the Data Breach Register.

Personal data breach notification: Data controller to a supervisory authority

When the personal data breach or suspected data breach affects personal data that the Organization is processing as a data controller, the following actions are performed by the Data Protection Officer:

- The Organization must establish whether the personal data breach should be reported to the Supervisory Authority. If the Organization is established outside the European Union, the Organization's EU representative should be informed about the data breach.
- To establish the risk to the rights and freedoms of the data subject affected, the Data Protection Officer must perform the Data Protection Impact Assessment on the processing activity affected by the data breach.
- No notification is required if the personal data breach is not likely to risk the rights and freedoms of the affected data subjects. However, the breach should be recorded in the Data Breach Register.
- Suppose the personal data breach is likely to risk the rights and freedoms of the individual. In that case, the Supervisory Authority must be notified of affected data subjects without undue delay but no later than 72 hours. Any possible reasons for delay beyond 72 hours must be communicated to the Supervisory Authority.

Chief Information Security Officer (CISO) will send Notifications to the Supervisory Authority that will include the following:

- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the Data Breach Response Team Leader/ Data Protection Officer
- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any information relating to the data breach

Personal data breach notification: Data controller to the data subject

[Top management of the Organization] must assess if the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject. If yes, the Data Protection Officer of the Organization must notify the affected data subjects with undue delay.

The Notification to the data subjects must be written in clear and plain language and contain the same information listed in Section 7.

If notifying each affected data subject is disproportionately tricky due to the number of affected data subjects, the Chief Information Security Officer (CISO) must take the necessary measures to ensure that the affected subjects are notified using appropriate, publicly available channels.

Annexure I

PERSONAL DATA BREACH IMPACT MATRIX

IMPACT	LOW-RISK	MEDIUM-RISK	HIGH-RISK
Risk to individual due to accidental or unauthorized:			
1. Access to/loss or access to; 2. Destruction of or alteration of Personal Data	No/minimal risk to affected. Individual's rights or freedoms.	Small to medium risk to affected individual's rights or freedoms.	There is a high risk of long-term impact on the affected individual's rights and freedoms, requiring urgent action (e.g., identity theft).
The distress caused or damage to the individual's standing or reputation.	There is no negligible distress; there is no public disclosure concern.	Small to medium amount of /short-term distress – damage limited to localized public disclosure/restricted internal knowledge	Substantial/long-term distress to many people – damage not controlled.
Threat to Organization's ability to protect personal data due to information security breach	No/negligible threat to or disruption of business, IT systems, and protection mechanisms.	Minimal/short-term controllable threat to or disruption of localized business, IT systems, and protection mechanisms.	Cessation of multiple essential systems for an extended period/significant disruption to various business operations
Impact on organization Finances and commercial interests	No/negligible impact – consequences resolved immediately.	Negligible to medium impact.	Substantial damage/longer-term impact.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Mar 14 2026	Initial Release	Pronoy	Kartikeya	Kartikeya