## 1. Purpose

Being an organization that processes personal data, **[XYZ]** is fully committed to ensure that appropriate privacy measures are in place if an incident occurs and results in loss, alteration, unauthorized disclosure of, or access to, personal data.

According to GDPR, data breaches that are likely to result in high risk to the rights and freedoms of data subjects must be reported to the supervisory authority by the controller without undue delay and, where feasible, within 72 hours of becoming aware about the breach. On the other hand, in cases where the **[XYZ]** has the role of the processor in data-related projects or activities, it must inform the controller(s) about the personal data breaches “without undue delay.”

Whether as a controller or a processor, the procedure presented in this document ensures that **[XYZ]** has an effective approach for managing personal data breaches. As such, the personal data breach notification procedure ensures that:

- Data breaches are detected, reported, and monitored
- Appropriate actions are taken to reduce the impact of the breach
- Improvements are made to prevent recurrence of the incident

It should be noted that actions provided in this document should be used only as guidance when responding to personal data breaches. It is important to have a common sense in case of an incident as the exact nature and impact of the incidents cannot be predicted. In addition, using this personal data breach notification procedure will ensure that **[XYZ]** fulfills the GDPR requirements.

All employees of the **[XYZ],** and third parties working for, or acting on behalf of the **[XYZ]** must be aware of, and follow this personal data breach notification procedure.

### 1.1 Main Definitions

| Term | GDPR definition |
|---|---|
| Personal data | *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who 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;* |
| Processing | *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;* |
| Controller | *the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;* |
| Processor | *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;* |
| Personal data breach | *a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;* |
| Supervisory authority | *an independent public authority which is established by a Member State pursuant to Article 51;** |

**1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').*

## 2. Personal Data Breach Notification Procedure

Once a data breach is identified, the personal data breach notification procedure is initiated. GDPR requires that the following three parties to be informed in case a personal data breach occurs:

1. The controller(s) of the personal data
2. The supervisory authority
3. The data subjects affected

## 3. The Controller(s) of the Personal Data

When the personal data breach affects the personal being processed by **[XYZ]** on behalf of one or more controllers, **[XYZ]** is obliged to report the breach to the respective controller(s) without undue delay. They must provide the following information to the controller(s):

- The nature of the breach
- The date and time that the breach was discovered, and is believed to have occurred
- The approximate number of data subjects affected
- The volume of data involved
- Measures taken to address the breach
- Contact details of the person's responsible for handling the breach within **[XYZ]**
- Any other information that is deemed necessary to the breach

After that, it is up to the controller(s) to report the breach and to take further actions.

## 4. The supervisory authority

When **[XYZ]** is the controller of the affected personal data, they must inform the supervisory authority about the breach, *unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons* (GDPR, article 33). As such, **[XYZ]** is required to assess the level of risk resulting from the breach and decide whether or not to notify the supervisory authority. As part of this risk assessment, the following factors must be considered:

- The encryption of the personal data
- Turning personal data into pseudonyms (Can the individuals be identified from the data?)
- The nature of the personal data involved
- The number of the data subjects affected

- The nature of the breach
- Any other factor deemed necessary

Based on the results of risk assessment, **[XYZ]** should determine on one of the following conclusions:

- The personal data breach does not need to be reported
- The personal data breach must be reported to the supervisory authority only
- The personal data breach must be reported to both the supervisory authority and the data subjects affected

If the personal data breach requires notification to the supervisory authority, **[XYZ]** must report the breach *without undue delay and, where feasible, not later than 72 hours after having become aware of it* (Article 33). If the notification is not carried out in due time, the reasons for its delay must be included within the notification itself.

**[XYZ]** should use secure means for reporting to the relevant supervisory authority by using the form *Personal Data Breach Notification Report*.

As part of this notification, the following information must be given:

- The nature of the personal data breach, including the approximate number of affected data subjects
- The contact details of the data protection officer (if applicable) or of the other individual(s) responsible for the data breach notification procedure
- The consequences of the personal data breach
- The actions taken to address the personal data breach
- Any other information that is deemed necessary to the personal data breach

## 5. The data subjects affected

According to the GDPR, **[XYZ]**, as the controller of the involved personal data, shall notify the affected data subjects without undue delay *if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons* (Article 34). **[XYZ]** should determine the impact of the breach through the risk assessment process described earlier (section 2, the supervisory authority).

However, if appropriate technical and organizational measures to mitigate the high risk have been applied, the notification to the affected data subjects is no longer required by the GDPR. Additionally, if there is a large number of affected data subjects, that would result in disproportionate efforts in notifying each of them about the breach. Thus, **[XYZ]** should ensure that the affected data subjects are notified by using publicly available channels.

If the personal data breach requires notification to the affected data subjects, the communication *shall describe in clear and plain language the nature of the personal data breach* (GDPR, Article 34), and must also contain:

- The contact details of the data protection officer or other contact point
- The likely consequences of the personal data breach
- The measures taken or proposed to address the personal data breach

It would be appropriate to offer advice to data subjects regarding the actions that they can take to reduce the risk corresponding with the breach of personal data. Some of the means that the controllers can notify the affected data subjects include letters, emails, a combination of both, etc.

## 6. Conclusion

**[XYZ]** should retain documented information as evidence of each personal data breach. The documentation should, then, be used by the supervisory authority to verify compliance with the GDPR.