Data Breach Response and Notification Procedure

Table of Contents

1. Scope and Purpose

This Procedure provides general principles and 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 lays out the general principles and actions for successfully managing the response to a data breach as well as fulfilling the obligations surrounding the notification to Supervisory Authorities and individuals as required by the European Union's General Data Protection Regulation (GDPR).

All employees, contractors or temporary employees and third parties working for or acting on behalf of Tovie AI UK Limited and affiliated companies, hereinafter referred to as the "Company", must be aware of, and follow this Procedure in the event of a personal data breach.

2. Definitions

The following definitions of terms used in this document are drawn from Article 4 of the GDPR:

"Personal Data" means 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 Regulation.

"Controller" is the natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

"Processor" is a natural or legal person, public authority, agency or any other body that processes personal data on behalf of a Controller.

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether 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.

"Personal Data Breach" means 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" means an independent public authority that is established by a Member State pursuant to Article 51.

3. Data Breach Response Team

A Data Breach Response Team must be a multi-disciplinary team comprised of knowledgeable and skilled individuals in Information technology, Security, Legal and Public Affairs. The team may be a physical (local) or virtual (multiple locations) team which responds to any suspected and/or alleged personal data breach. The Team must be appointed regardless of whether or not a breach has occurred. Team members and contact information are listed in Appendix 1. The Team headed by the Data Breach Response Team Leader.

The team must ensure that necessary readiness for a personal data breach response exists, along with the needed resources and preparation. The team's mission is to provide an immediate, effective, and skilful response to any suspected, alleged or actual personal data breaches affecting the Company.

If required, the team members may also involve external parties, e.g. an information security vendor for carrying out digital forensics tasks or an external communications agency for assisting the Company in crisis communications needs. The Data Breach Response Team Leader can choose to add additional personnel to the team for the purposes of dealing with a specific personal data breach.

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 suspected, alleged or actual personal data breach, there is no requirement for this.

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 member of the Data Breach Response Team, including personal contact details, shall be stored in a central location, and shall be used to assemble the team whenever notification of a suspected, alleged or actual personal data breach is received.

4. 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 and triage the personal data breach
- Ensure proper and impartial investigation 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 properly notified, if necessary

The Data Breach Response Team will convene for each reported and alleged personal data breach.

5. Data Breach Response Process

The Data Breach Response Process is initiated when anyone who notices that a suspected, alleged or actual personal data breach occurs, and any member of the Data Breach Response team is notified. The team is responsible to determine if the breach should be considered a breach affecting personal data.

When the (suspected) personal data breach affects personal data that is being processed by the Company, the following actions are performed:

1. Information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk.
2. If the Company act as a controller:
   2.1. The risk to data subjects from a breach should then be assessed, as the likelihood of no risk, risk or high risk.
   2.2. Notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if the Company act as a controller and notification required.
      2.2.1. If the personal data breach is not likely to result in a risk to the rights and freedoms of the affected data subjects, no notification is required.
      2.2.2. The Supervisory Authority must be notified with undue delay but no later than in 72 hours, if the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach.
      2.2.3. If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, the Company must notify with undue delay the affected data subjects.
3. When the personal data breach or suspected data breach affects personal data that is being processed on behalf of a third party, the Data Protection Officer must report any personal data breach to the respective controller.
4. At the same time, the Company should act to contain and recover the breach.
5. Documentation of the breach should take place as it develops.

The Data Breach Response Team leader is responsible for documenting all decisions of the core team. These documents need to be written very precisely and thoroughly to ensure traceability and accountability.

6. Personal Data Breach Notifications

6.1. Processor to Controller

When the personal data breach or suspected data breach affects personal data that is being processed on behalf of a third party, the Data Protection Officer must report any personal data breach to the respective controller **without undue delay** or in accordance with the timeline specified in the relevant contract with the controller.

The Data Protection Officer will send 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 Protection Officer
- Measures taken to address the personal data breach
- Any information relating to the data breach

Data Protection Officer will record the data breach into the Data Breach Register.

6.2. Controller to Supervisory Authority

When the personal data breach or suspected data breach affects personal data that is being processed by the Company as a controller, Data Protection Officer 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 Protection Officer
- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any information relating to the data breach

6.3. Controller to Data Subject

If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, the Data Protection Officer of the Company must notify with undue delay the affected data subjects.

The notification to the data subjects must be written in clear and plain language and must contain:

- A description of the nature of the breach
- Categories of personal data affected
- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Name and contact details of the Data Protection Officer
- Any information relating to the data breach

If, due to the number of affected data subjects, it is disproportionately difficult to notify each affected data subject, the Data Protection Officer must take the necessary measures to ensure that the affected data subjects are notified by using appropriate, publicly available channels.

7. Records

Based on this Procedure, the following documents are maintained.

Record name	**Storage location**	**Person responsible for storage**	**Controls for record protection**	**Retention time**
Documented decisions of the Data Breach Response Team		Data Protection Officer	only Data Breach Response Team can edit the files	5 years
Data breach notifications		Data Protection Officer	only Data Breach Response Team can edit the files	5 years
Data Breach Register		Data Protection Officer	only Data Protection Officer can edit the files	Permanentl y

Appendix 1. Data Breach Response Team

Person	Role	e-mail	Phone number	

Appendix 2. Processor to Controller Data Breach Notification Form

From: *[Company]*

To: *[name and address of the Controller]*

Please be informed that on [date] we suffered a data breach that consisted of:

[description of the nature of the breach]

Following the data breach, the following personal data were affected:

[categories of personal data affected].

We estimate that around [__] data subjects and [__] records were affected by the data breach.

The following measures have been taken/will be taken to address the data breach:

[list all the measures taken]

If you have any questions or concerns regarding the data breach, we encourage you to contact *[contact name]*, who is our Data Protection Officer, by email at *[email address]*, or by post at *[physical address]*.

Data Protection Officer

_____

[name]

_____

[date and time]

Appendix 3. Controller to Supervisory Authority Data Breach Notification Form

From: *[Company]*

To: *[name and address of the Supervisory authority]*

Please be informed that on [date] we suffered a data breach that consisted of:

[description of the nature of the breach]

Following the data breach, the following personal data were affected:

[categories of personal data affected].

We estimate that around [__] data subjects and [__] records were affected by the data breach.

We believe that the personal data breach might have the following consequences:

[list all possible consequences]

The following measures have been taken/will be taken to address the data breach:

[list all the measures taken]

If you have any questions or concerns regarding the data breach, we encourage you to contact *[contact name]*, who is our Data Protection Officer, by email at *[email address]*, or by post at *[physical address]*.

Data Protection Officer

_____

[name]

_____

[date and time]

Appendix 4. Controller to Data Subject Data Breach Notification Form

From: *[Company]*

To: *[Affected data subject name]*

Dear customer, we regret to inform you that on [date] we have discovered that we have been the subject of a personal data breach that consisted of:

[description of the nature of the breach]

The following personal data were affected:

[categories of personal data affected].

As a result of the above mentioned personal data breach, the personal data concerning you might have been:

- ☐ Disclosed
- ☐ Destroyed
- ☐ Lost
- ☐ Modified
- ☐ Accessed
- ☐ Other [please specify other possible results]

  _____

by

- ☐ unauthorized persons
- ☐ internal accident

Please be aware that the personal data breach might have the following consequences:

[list all possible consequences]

The following measures have been taken/will be taken to address the data breach:

[list all the measures taken]

If you have any questions or concerns regarding the data breach, we encourage you to contact *[contact name]*, who is our Data Protection Officer, by email at *[email address]*, or by post at *[physical address]*.

Data Protection Officer

_____

[name]

_____

[date and time]

Appendix 4. Data Breach Register Template

Date of breach	Date of internal notification to the response team	Date of notification by data processor (if applicable)	Type/Nature of the beach	Description of the breach	Personal data affected	Number of data subjects affected	Number of data records affected	Consequences of the breach	Are data subjects informed?	Date of notification to data subject	Whether a data breach/security incident was notified to authorities	Date of notification to authorities	Actions to contain the data breach and minimize impact for data subjects	Date of remediation completed	Other information