Data Breach Response and Notification Procedure

Tovie AI UK Limited

Version 2.0

Last updated: February 2026

Table of Contents

1. Scope and Purpose
2. Definitions
3. Data Breach Response Team
4. Data Breach Response Team Duties
5. Data Breach Response Process
6. Personal Data Breach Notifications
   6.1. Processor to Controller
   6.2. Controller to Supervisory Authority
   6.3. Controller to Data Subject
7. Records

Appendix 1. Data Breach Response Team

Appendix 2. Processor to Controller Data Breach Notification Form

Appendix 3. Controller to Supervisory Authority Data Breach Notification Form

Appendix 4. Controller to Data Subject Data Breach Notification Form

Appendix 5. Data Breach Register Template

1 Scope and Purpose

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.

This Procedure applies to personal data breaches affecting the Company's websites and internal systems, as well as the Tovie AI Agent Platform and its integrations with third-party systems and sub-processors. It covers situations where the Company acts as a **Controller** (for example for its own websites, accounts, billing and marketing) and where the Company acts as a **Processor** on behalf of its Clients for personal data processed through the Platform.

The Procedure lays out the general principles and actions for successfully managing the response to a personal data breach as well as fulfilling the obligations surrounding notification to supervisory authorities and individuals as required by the EU GDPR, the UK GDPR and other applicable data protection laws, in particular Articles 33 and 34 GDPR.

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

Internal reports of suspected or actual personal data breaches should be sent to privacy@tovie.ai or reported directly to any member of the Data Breach Response Team listed in Appendix 1.

This Procedure should be read in conjunction with the Company's Privacy Policy and any applicable Data Processing Agreements with Clients.

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.

"Controller" means 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" means a natural or legal person, public authority, agency or any other body which 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, organisation, 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, unauthorised 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 GDPR, or the competent data protection authority under applicable law (for example the ICO in the UK).

"Designated data protection contact" means the person appointed by the Company as the primary contact point for data protection matters (which may be a privacy, legal or security lead, or a Data Protection Officer where one is appointed).

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 is 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 skillful response to any suspected, alleged or actual personal data breaches affecting the Company.

If required, the Team members may also involve external parties, for example 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 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 a suspected, alleged or actual personal data breach occurs and any member of the Data Breach Response Team is notified. The Team is responsible for determining if the incident 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 acts 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 to the rights and freedoms of natural persons, taking into account Articles 33 and 34 GDPR.

   2.2. Notification to the supervisory authority, and potentially communication of the breach to the affected individuals, should be made where required by law.

   2.2.1. If the personal data breach is unlikely to result in a risk to the rights and freedoms of the affected data subjects, no notification to the supervisory authority is required.

2.2.2. The supervisory authority must be notified without undue delay and, where feasible, not later than 72 hours after the Company has become aware of the personal data breach, if the breach is likely to result in a risk to the rights and freedoms of the data subjects affected. If the notification is not made within 72 hours, it shall be accompanied by reasons for the delay.

2.2.3. If the personal data breach is likely to result in a **high risk** to the rights and freedoms of the data subjects, the Company must communicate the breach to the affected data subjects without undue delay.

3. When the personal data breach or suspected data breach affects personal data that is being processed on behalf of a third party (Client acting as Controller under a Data Processing Agreement), a designated privacy or security lead must report any personal data breach to the respective Controller without undue delay and in accordance with the timeline specified in the relevant contract with the Controller. The Controller is then responsible for assessing risk and determining whether notification to a supervisory authority and/or data subjects is required.

4. At the same time, the Company should act to contain and recover from the breach, including:

   - Stopping unauthorised access or disclosure.
   - Securing affected systems and data.
   - Applying temporary and then permanent fixes where appropriate.

5. Documentation of the breach should take place as it develops, including facts relating to the breach, its effects and the remedial action taken, in line with Article 33(5) GDPR.

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 (Client acting as Controller), the Company's designated data protection contact must report any personal data breach to the respective Controller without undue delay after becoming aware of it, and in any event within the timeline specified in the relevant Data Processing Agreement (which shall not exceed the period required to comply with Article 33(2) GDPR).

The notification to the Controller should include, where possible:

- A description of the nature of the personal data breach.
- The categories of personal data affected.

- The approximate number of data subjects affected.
- The approximate number of personal data records affected.
- The name and contact details of the Company's data protection contact.
- Measures taken or proposed to be taken to address the personal data breach.
- Any other relevant information relating to the personal data breach, including whether further details will follow as the investigation progresses.

The designated data protection contact will record the personal data breach in the Data Breach Register.

6.2. Controller to Supervisory Authority

When a personal data breach or suspected data breach affects personal data that is being processed by the Company as a Controller, the Company's designated data protection contact will send notification to the competent supervisory authority where required by law.

Notification must be made without undue delay and, where feasible, not later than 72 hours after the Company has become aware of the personal data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. If notification is not made within 72 hours, it must be accompanied by reasons for the delay.

The notification to the supervisory authority shall at least include:

- A description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
- The name and contact details of the Company's data protection contact.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken or proposed to be taken by the Company to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- Any other information relating to the personal data breach that the supervisory authority reasonably requires.

Where it is not possible to provide all the information at the same time, the information may be provided in phases without undue further delay.

6.3. Controller to Data Subject

If the personal data breach is likely to result in a **high risk** to the rights and freedoms of data subjects, the Company, acting as Controller, must communicate the personal data breach to the affected data subjects without undue delay, in accordance with Article 34 GDPR.

However, communication to the data subject shall not be required if any of the following conditions is met (Article 34(3) GDPR):

(a) the Company has applied appropriate technical and organisational protection measures to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;

(b) the Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; or

(c) it would involve disproportionate effort, in which case the Company shall instead make a public communication or take a similar measure whereby the data subjects are informed in an equally effective manner.

Where any of the above exceptions is relied upon, the rationale must be documented in the Data Breach Register.

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

- A description of the nature of the personal data breach.
- The categories of personal data affected.
- The likely consequences of the personal data breach.
- The measures taken or proposed to be taken by the Company to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- The name and contact details of the Company's data protection contact.
- Any other relevant information relating to the personal data breach and recommended steps that data subjects can take to protect themselves.

If, due to the number of affected data subjects, it is disproportionately difficult to notify each affected data subject individually, the Company's designated data protection contact must take the necessary measures to ensure that the affected data subjects are informed by using appropriate, publicly available channels (for example public notices, website banners, press releases), in a manner that is equally effective.

7. Records

In accordance with Article 33(5) GDPR, the Company shall document all personal data breaches, including those that do not require notification to a supervisory authority or to data subjects. The documentation shall comprise the facts relating to the personal data breach, its effects and the remedial action taken. This documentation shall enable the supervisory authority to verify compliance with this Procedure.

Based on this Procedure, the following documents and records are maintained.

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Documented decisions of the Data Breach Response Team	Internal secure repository	Designated data protection contact	Only authorised members of the Data Breach Response Team can edit the files	5 years
Data breach notifications	Internal secure repository	Designated data protection contact	Only authorised members of the Data Breach Response Team can edit the files	5 years
Data Breach Register	Internal secure repository	Designated data protection contact	Only the designated data protection contact can edit the files	Permanently

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 Contact, by email at *[email address]*, or by post at *[physical address]*.

Data protection contact

_____

[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 Contact, by email at *[email address]*, or by post at *[physical address]*.

Data protection contact

_____

[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

- € unauthorised 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 Contact, by email at *[email address]*, or by post at *[physical address]*.

Data protection contact

_____

[name]

_____

[date and time]

Appendix 5. 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 breach	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 minimise impact for data subjects	Date of remediation completed	Other information