Personal Data Breach Notification Procedure

Reference: GDPR DOC 2.5
DocumentKits Issue No: 1.0
Organisation Issue No:
DocumentKits Issue Date: 15/11/2019
Organisation Issue Date:

1. Scope

This procedure applies in the event of a personal data breach under Article 33 of the GDPR – *Notification of a personal data breach to the supervisory authority* – and Article 34 – *Communication of a personal data breach to the data subject.*

The GDPR draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Each organisation should establish whether it is data controller, or a data processor for the same data processing activity; or whether it is a joint controller.

2. Responsibility

2.1 All users (whether Employees/Staff, contractors or temporary Employees/Staff and third party users) and
"owners"

of Organisation Name are required to be aware of, and to follow this procedure in the event of a personal data breach (reference Training Policy).

2.2 All Employees/Staff, contractors or temporary personnel are responsible for reporting any personal data breach to the Data Protection Officer / Head of IT (CIO).

3. Procedure – Breach notification data processor to data controller

3.1 Organisation Name reports any personal data breach or security incident to the data controller without undue delay
"if you process data for a number of controllers, where is this information specified?"

These contact details are recorded in the Internal Breach Register & Breach Notification Form. Organisation Name provides the controller with all of the details of the breach.

3.2 The breach notification is made by
"email, phone call, etc."

3.3 A confirmation of receipt of this information is made by
"email, phone call, etc."

4. Procedure – Breach notification data controller to supervisory authority

4.1 Organisation Name determines if the supervisory authority need to be notified in the event of a breach.

4.2 Organisation Name assesses whether 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, by conducting
"data protection impact assessment against the breach – Data Protection Impact Assessment (DPIA) Tool"

"and/or other means - specify."

4.3 If a risk to data subject(s) is likely, Organisation Name reports the personal data breach to the supervisory authority
"specify"

without undue delay, and not later than 72 hours.

4.4 If the data breach notification to the supervisory authority is not made within 72 hours, Organisation Name's Data Protection Officer / GDPR Owner submits it electronically with a justification for the delay.

4.5 If it is not possible to provide all of the necessary information at the same time Organisation Name will provide the information in phases without undue further delay.

4.6 The following information needs to be provided to the supervisory authority (Internal Breach Register & Breach Notification Form):

4.6.1 A description of the nature of the breach.
4.6.2 The categories of personal data affected.
4.6.3 Approximate number of data subjects affected.
4.6.4 Approximate number of personal data records affected.
4.6.5 Name and contact details of the Data Protection Officer / GDPR Owner
4.6.6 Consequences of the breach.
4.6.7 Any measures taken to address the breach.
4.6.8 Any information relating to the data breach.

<< 4.7 – 4.10 removed for sample purposes >>

5. Procedure – Breach notification data controller to data subject

5.1 If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, Organisation Name notifies those/the data subjects affected immediately
"using this form/in accordance with the Data Protection Officer / GDPR Owner recommendations."

5.2 The notification to the data subject describes the breach in clear and plain language, in addition to information specified in clause 4.6 above.

5.3 Organisation Name takes measures to render the personal data unusable to any person who is not authorised to access it using
"encryption"

5.4 The data controller takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur by
"date."

5.5 If the breach affects a high volume of data subjects and personal data records, Organisation Name makes a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder the Organisation Name's ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner.

5.6 If Organisation Name has not notified the data subject(s), and the supervisory

authority considers the likelihood of a data breach will result in high risk, Organisation Name will communicate the data breach to the data subject by
"date."

5.7 Organisation Name documents any personal data breach(es), incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

Document Owner and Control

The Data Protection Officer / GDPR Owner is the owner of this document and is responsible for keeping it up to date.

The current version of this document is available to
"Specify which members of staff this document is intended for"

and is published
"Describe the location(s) – electronic and physical – where this document is available"

Its approval status can be viewed in Master List of Document Approval.