

# Personal Data Breach Notification Procedure

## 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 Data Protection Act 2018 codifies GDPR into UK Law. For this policy, GDPR 2016 and Data Protection Policy 2018 are used interchangeably to mean the enforceable legislation.

## 2 Responsibility

- 2.1 All employees (permanent, temporary, and sessional), volunteers, contractors, and third party users of PKAVS are required to be aware of, and to follow, this procedure in the event of a personal data breach.
- 2.2 All listed above are responsible for reporting any personal data breach to PKAVS' Privacy Officer/PKAVS HR Function.
- 2.3 Any personal data breach or security incident must be notified without undue delay.
- 3.2 The breach notification is made in-person, by phone, or by email.
- 3.3 A confirmation of receipt of this information is made by email.

## 3 Procedure – Breach Notification to Supervisory Authority

- 3.1 PKAVS' Privacy Officer/HR Function determines if the Information Commissioner's Office needs to be notified in the event of a breach.
- 3.2 PKAVS' Privacy Officer/HR Function 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 a Data Protection Impact Assessment against the breach.
- 3.3 If a risk to data subject(s) is likely, PKAVS' Privacy Officer/HR Function reports the personal data breach to the Information Commissioner's Office without undue delay, and not later than 72 hours.
- 3.4 If the data breach notification to the Information Commissioner's Office is not made within 72 hours, PKAVS' Privacy Officer/HR Function submits it electronically with a justification for the delay.
- 3.5 If it is not possible to provide all of the necessary information at the same time, PKAVS will provide the information in phases without undue further delay.
- 3.6 The following information needs to be provided to the Information Commissioner's Office:

- 3.6.1 A description of the nature of the breach.
- 3.6.2 The categories of personal data affected.
- 3.6.3 Approximate number of data subjects affected.
- 3.6.4 Approximate number of personal data records affected.
- 3.6.5 Name and contact details of PKAVS' Privacy Officer/HR Function
- 3.6.6 Consequences of the breach.
- 3.6.7 Any measures taken to address the breach.
- 3.6.8 Any information relating to the data breach.
- 3.7 PKAVS' Privacy Officer/HR Function notifies the Information Commissioner's Office.
- 3.8 In the event the Information Commissioner's Office assigns a specific contact in relation to a breach, these details are recorded in a breach record file.
- 3.9 The breach notification is made by phone or email in the first instance.
- 3.10 A confirmation of receipt of this information is lodged with PKAVS' Privacy Officer/HR Function.

## **5 Procedure – Breach Notification to Data Subject(s)**

- 5.1 If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject(s), PKAVS will notify those affected immediately.
- 5.2 The notification to the data subject describes the breach in clear and plain language, in addition to information specified in clause 3.6 above.
- 5.3 PKAVS will take measures to render the personal data unusable to any person who is not authorised to access it.
- 5.4 PKAVS will take subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur.
- 5.5 If the breach affects a high volume of data subjects and personal data records, PKAVS will make a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder PKAVS 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 PKAVS has not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, PKAVS will communicate the data breach to the data subject by as soon as feasible.
- 5.7 PKAVS will document any personal data breach(es), incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

## Document Control

PKAVS' Privacy Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the GDPR.

A current version of this document is available to all members of staff on the corporate network or on request.

This procedure was approved by the Chief Executive Officer on 22/05/18 and is issued on a version controlled basis under his/her signature.

Signature:



Date: 22/05/18

## Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Chief Executive Officer	22/05/18
2	Updated for Data Protection Act 2018	Privacy Officer	31/01/20