Kildare Public Participation Network

Data Breach Process Policy

Reference	Approved	Ratified	For Review	Amended
Ref: DB 1	Nov 1st 2021	Nov 1st 2021	June 13th 2022	
Ref: DB 1	Sept 26th 2022	N/A	Sept 2023	

PURPOSE

The purpose of this policy is to provide the Kildare Public Participation Networks intent, objectives and procedures regarding data breaches involving personal information. As we have obligations under the General Data Protection Regulation (GDPR), we also have a requirement to ensure that the correct procedures, controls, and measures are in place and disseminated to all parties, ensuring that they are aware of what the protocols and reporting lines are for personal information breaches. This policy details our processes for reporting, communicating, and investigating incidents.

SCOPE

This policy applies to all persons within the Kildare Public Participation Network (meaning, Secretariat, Representatives, staff, volunteers, and any third-party representatives). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

DATA SECURITY , BREACH REQUIREMENTS & DEFINITION

Kildare Public Participation Network's definition of a personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. We have a legal and regulatory obligation to ensure that personal information is protected whilst being processed by us. We have implemented adequate, effective, and appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as outlined in the Data Protection Policy.

Objectives

- To adhere to the GDPR and EU Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting, and recording any data breaches
- To develop and implement adequate, effective, and appropriate technical and organisational measures to ensure a high level of security with regards to personal information
- To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes.
- To use the Data Breach Incident Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To protect all parties – including their data, information, and identity
- To ensure that where applicable, the Data Protection Officer (DPO) is involved in and notified about all data breaches and risk issues
- To ensure that the Supervisory Authority is notified of the data breach (where applicable) with immediate effect and at the latest, within 72 hours after having become aware of the breach.

DATA BREACH PROCEDURES & GUIDELINES

The Kildare Public Participation Network has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. Our procedures and guidelines for identifying, investigating and notification of breaches are detailed below.

Breach Monitoring & Reporting

Kildare Public Participation Network has appointed a Data Protection Officer who is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact, or containment. All data breaches are reported to this person with immediate effect, whereby the procedures detailed in this policy are followed. All data breaches will be investigated, even in instances where notifications and reporting are not required, and we retain a full record of all data breaches. Where a system or process failure has given rise to a data breach, that will be recorded and revised.

Breach Incident Procedures

Identification of an Incident as soon as a data breach has been identified, is reported to the Data Protection Officer immediately so that breach procedures can be initiated and followed without delay. Reporting incidents in full and with immediate effect is essential to the compliant functioning of the Network. These procedures are for the protection of all parties and are of the utmost importance for legal regulatory compliance. As soon as an incident has been reported, measures must be taken to contain the breach. The aim of any such measures should be to stop any further risk/breach prior to investigation and reporting. The measures taken are noted in all cases.

Breach Recording

A Breach Incident Form for all incidents should be used, which is completed for any data breach, regardless of severity or outcome. Completed forms are logged in the Breach Incident Folder. In cases of data breaches, the Data Protection Officer is responsible for carrying out a full investigation, containing the breach, recording the incident on the breach form, and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved. A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all involved in the breach, in addition to the Secretariat. A copy of the completed incident form is filed for audit and record purposes. If applicable, the appropriate authority and the data subject(s) are notified in accordance with the GDPR requirements. The Supervisory Authority protocols are to be followed and their 'Security Breach Notification Form' should be completed and submitted. In addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

Breach Risk Assessment

Human Error: Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the person held. A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed. Any identified gaps that are found to have caused/contributed to the breach are revised and risk assessed to mitigate any future occurrence of the same root cause. Resultant outcomes of such an investigation can include, but are not limited to:

- Re-training in specific/all compliance areas
- Re-assessment of compliance knowledge and understanding
- Suspension from compliance related tasks
- Formal warning (in-line with disciplinary procedures)

Assessment of Risk and Investigation

The DPO should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches. They should look at:

- The type of information involved
- It's sensitivity or personal content
- What protections are in place (e.g. encryption)?
- What happened to the information/Where is it now?
- Whether there are any wider consequences/implications to the incident

Breach Notifications

Kildare Public Participation recognises its obligation and a duty to report data breaches in certain instances. All staff have been made aware of the responsibilities and know to report suspected breaches straight away.

Supervisory Authority Notification (Data Protection Commissioner)

The Supervisory Authority will be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, it would lead to significant detrimental effects on the individual. Where applicable, the Supervisory Authority is notified of the breach no later than 72 hours after we become aware of it and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes. If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the DPO and deemed to be unlikely to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR. The notification to the Supervisory Authority will contain:

- A description of the nature of the personal data breach
- The categories and approximate number of data subjects affected

- The categories and approximate number of personal data records concerned
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)

Breach incident procedures and an investigation are always carried out, regardless of our notification obligations and outcomes and reports are retained to be made available to the Supervisory Authority if requested. The processor, will ensure that the controller is notified of the breach without undue delay.

Data Subject Notification

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear, and legible format. The notification to the Data Subject shall include:

- The nature of the personal data breach
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (for obtaining further information)
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects). We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational protection measures which render the data unintelligible to any person who is not authorised to access it (i.e. encryption, data masking etc) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise. If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

RECORD KEEPING

All records and notes taken during the identification, assessment and investigation of the data breach are recorded and authorised by the Data Protection Officer and are retained for a period of 6 years from the date of the incident.

RESPONSIBILITIES

Kildare Public Participation Network will ensure that all staff are provided with the time, resources, and support to learn, understand, and implement all procedures within this document, as well as understanding their responsibilities. The Data Protection Officer is

responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups.