Kildare Public Participation Network

Data Protection Policy

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

The following document describes some of the practical actions in place within Kildare Public Participation Network to ensure compliance with the General Data Protection Regulation (GDPR). This policy is to assist Kildare Public Participation Network to manage personal data; in the day-to-day running of Kildare Public Participation Network, in line with changes brought about by GDPR.

Designated Responsibility

The General Data Protection Regulation sees no distinction between the status of data management activities, the Secretariat, Employees or third parties such as Controllers, Controller Agents, and processors. Therefore, all parties are collecting and processing data, on behalf of Kildare Public Participation Network. Therefore, all parties must comply with the data protection policy and other relevant policies to protect the personal data in our care to minimise data breaches. As a result, Kildare Public Participation Network have appointed a Data Protection Officer to ensure they are meeting their Data Protection obligations. The Data Protection Officer's tasks include identifying and recording the specific locations where data is held, ensuring that consent is obtained in the appropriate manner and maintained accordingly.

Roles

The Controller: Is the PPN as an Entity

Controller Agents: The Kildare Public Participation Network Secretariat

The Processor: Salesforce

The Data Protection Officer: whose role is accountable for, but not responsible for the Data. (May act on behalf of the Controller and the Agents of the Controller).

The Data Subject: All member organisations, its nominated contacts, representatives, secretariat members, employees, and any other party to which the Kildare Public Participation Network retains personal data.

Data Processed

Salesforce on behalf of Kildare Public Participation Network process information for the purpose of PPN business only and do not distribute it for any other reason.

We retain, Name, E-mail address (s), Phone numbers and Postal Addresses

Other likely categories of Personal Information held by us include:

- Information required for a membership application
- Text or messaging systems
- Email lists or contact groups

Purpose

Kildare Public Participation Network hold this information to enable us to contact member groups and circulate information deemed relevant or beneficial to Kildare PPN member groups.

How

Kildare Public Participation Network collect data and process data when you:

- Register with Kildare Public Participation Network through our website.
- Register for Linkage Groups/ Training / Events
- Submit nomination forms for Kildare PPN Representative positions.

Who

This information is only disclosed to internal parties working with or volunteering on behalf of the PPN

No information is circulated to other countries or international organisations

Kildare Public Participation Network will not share your information to any third party that is not engaged in the Public Participation Network or activities.

Duration

Your data will be held for the duration of your involvement with Kildare PPN.

Subject Data Rights

You (the subject) retain the right to request rectification or erasure of personal data or restriction of processing of personal data concerning you at any time.

You have the right to lodge a complaint with the Information Commissioners Office ("ICO"); if your data has not been collected from you.

Data Breach Process

If unauthorised access to Personal Data occurs or Personal Data is lost or stolen, this must be notified to the Data Protection Commissioner within 72 Hours of being identified. This is a requirement for all paper information and all electronic information (unless the data is encrypted or anonymised). If the breach is likely to cause harm to the individual (Identity Theft or breach of confidentiality) then the individual must also be informed. A procedure to detect, report and investigate data breaches is in place.

Please see the Data Breach Process Policy

Note: The 72-hour deadline for notification to the Data Protection Commissioner applies irrespective of any steps being taken to understand the causes of the breach.

Subject Access Request

Process Subject Access Requests or SARS allow for any member to request a copy of information held about them. This must be provided in paper format or in a standard electronic format within thirty days. It is no longer allowable to charge for responding to SARs. It is of utmost importance that Subject Access Requests are responded to and dealt with within the allocated time frame.

Subject Access Request Procedure

- Recognise/Acknowledge the access request
- Identify the individual making the request
- Act quickly and clarify the access request if required
- Identify personal data to be disclosed
- Identify personal data exemptions
- Securely disclose the data in the appropriate format
- Keep a record

Communications

It is critically important that the wishes of individuals regarding communications sent to them are respected. Consent to contact must be recorded and maintained and if an individual has not given consent to receive communications, they must not be contacted unless we have a lawful reason.

Group Messaging/Emailing/WhatsApp and any Group or section sending communications on behalf of Kildare Public Participation Network or using Kildare Public Participation Network members or volunteers contact details must be aware that the communication must be compliant with GDPR, specifically the seven principles set out in legislation. Communications sent via email containing several recipients the 'BCC' ("blind carbon copy") field must be used to prevent the unnecessary disclosure of recipients' email addresses (Unless otherwise agreed). Kildare Public Participation Network, Sections, etc. using group messaging services such as WhatsApp and Messenger should ensure the administrator has received prior consent from everyone in writing. This is necessary, due to the fact that once an individual is added to a group their phone number (data) is automatically shared with all those within the group. Emails containing personal/confidential data sent through smartphones, mobile devices, tablets, etc. should be kept to a minimum. Data sent this way should only be sent using secure devices and secure email. If necessary, the security settings on email providers such as Gmail/Hotmail etc should be reviewed.

Secure Storage

All Personal Data held by the Kildare Public Participation Network is stored safely and securely. Paper copies of Personal Data are locked in cabinets and securely shredded once they have fulfilled their purpose. Electronic copies of Personal Data are password protected and encrypted.

Secure Electronic

All computers, laptops and mobile devices, 'lock' after a few minutes of inaction or when left unattended, and only re-activated by keying in a password. Encryption/Password – Membership Management System, computers/mobile devices are password protected, and access/login codes will not be shared with anyone else.

Training

All Kildare Public Participation Network staff members have attended GDPR/Data Protection Training with IBEC and members of the Secretariat are encouraged to review the content of the Data Protection Policy regularly.

If you would like to exercise any of these rights, please contact the Kildare PPN by email at kildareppn@gmail.com , or write to Kildare Public Participation Network, Level 7, Áras Chill Dara, Naas, Co Kildare.