

Comhlámh

Data Protection Policy

Contents

1	Scope	2
2	Policy Statement	2
3	Purpose and Objectives	3
3.1	Purpose.....	3
3.2	Objectives.....	3
4	Governance	3
5	Compliance with Major Principles	4
5.1	Transparency, Purpose and Lawful Basis for Processing	4
5.2	Purpose Limitation	5
5.3	Data Minimisation	5
5.4	Accuracy and Quality.....	5
5.5	Retention and Storage Limitation	5
5.6	Security and Confidentiality	5
6	Our Obligations as a Data Controller	5
6.1	Privacy Notice.....	5
6.2	Record of Processing Activities	6
6.3	Data Breaches	6
6.4	Contracts with Data processors	6
6.5	Data Subject Rights	6
6.6	Data Privacy Impact Assessment	6
6.7	Data Protection Officer	6
6.8	Overseas Transfer.....	6
7	Audits and Monitoring	7
8	Training	7

1 SCOPE

This policy applies to the processing by or on behalf of Comhlámh of personal data on natural persons (data subjects) resident in the European Economic Area regardless of whether the data is processed in the EEA or in another location. The policy is designed to ensure that Comhlámh complies with its obligations under the General Data Protection Regulation and any other relevant data protection laws and codes of conduct (herein collectively referred to as “the data protection laws”) operable within the EEA.

The policy is binding on all [trustees, senior managers, and staff of Comhlámh. **Adherence to this policy is mandatory and non-compliance could lead to disciplinary action in accordance with the Comhlámh Constitution and contracts of employment.**

2 POLICY STATEMENT

Comhlámh processes personal data in the course of its activities as the Irish Association of Development Workers and Volunteers, and a membership-based organization.

Personal data is collected from Data Subjects including members, prospective members, employees, course and event attendees, volunteers and development workers who avail of services including VDW and PSPS schemes, suppliers, contractors, donors, third party service providers and consultants.

“Personal data” is “any information relating to an identified or identifiable natural person” and includes (but is not limited to), name, address, email address, data of birth, IP address, identification numbers, bank details along with special categories of personal data as defined below.

‘Special Categories of Personal Data’ are data relating to “racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation”

Comhlámh is committed to Processing all personal data in accordance with the **General Data Protection Regulation (GDPR)**, and any other relevant data protection laws and codes of conduct (*herein collectively referred to as “the data protection laws”*) in the countries in which we operate.

Protecting the privacy of Data Subjects by ensuring and maintaining the security and confidentiality of personal and/or special category data is a compliance priority for Comhlámh. In addition to supporting our wish to be exemplary in terms of compliance, meeting our obligations also reduces the potential financial, legal, and reputational risks that may arise from non-compliance.

3 PURPOSE AND OBJECTIVES

3.1 PURPOSE

The purpose of this policy is set out Comhlámh's commitment to personal data protection and to outline the arrangements Comhlámh has made to meet its obligations under data protection laws.

This policy also serves as a reference document for employees and third parties on the responsibilities associated with processing personal data.

3.2 OBJECTIVES

Our data protection objectives are to:

- Ensure that individuals especially members who entrust us with their personal data feel confident that it will be handled in accordance with their rights under data protection laws
- Ensure that all [trustees, senior managers, and staff] involved in processing personal data are competent and knowledgeable about our data protection obligations and how they apply to their specific roles in Comhlámh
- Enhance Comhlámh's reputation as a reputable, trustworthy organisation which is committed to high standards of compliance and ethical behaviour
- Minimise as far as possible the legal, financial, or reputational risks to Comhlámh that can arise from processing personal data.

4 GOVERNANCE

In relation to the governance of our data protection policies and processes Comhlámh has:

- Assigned leadership and management responsibility for data protection across the organisation
- Allocated responsibility for data protection compliance and ensure that the designated person(s) has sufficient access, support and resources to perform the role
- Educated trustees, senior managers and staff about the requirements under the data protection laws, the benefits of applying good personal data management practices and the potential implications of non-compliance
- Provided effective data protection training for all employees consistent with their roles

Responsibility for Data Protection - Summary

Board	<p>Oversee data protection management practices.</p> <p>Allocate responsibilities and provide sufficient resources.</p> <p>Approve policies.</p> <p>Lead by example: make data protection a priority and incorporate it into management systems and processes.</p>
CEO/Senior Managers	<p>Process personal data under the control of their departments in a compliant fashion.</p> <p>Uphold data subject rights in relation to personal data under their control.</p> <p>Facilitate delivery of data protection training and awareness raising to their teams.</p> <p>Allocate data protection responsibilities and resources within their departments.</p>
Data Protection Champion	<p>Fulfil the role of DPC role in relation to the ongoing monitoring across the organisation.</p> <p>Support awareness-raising and training of staff involved in processing operations, and the related audits.</p> <p>Cooperate with the supervisory authority and act as the contact point for the supervisory authority on issues relating to processing.</p> <p>Identify and mitigate any risks to the protection of personal data,</p> <p>Stay up to date with all legislation and changes relating to data protection.</p>

5 COMPLIANCE WITH MAJOR PRINCIPLES

The principles of personal data management as described in GDPR are detailed in Appendix 2. In summary, these principles to which Comhlámh adheres are as follows:

5.1 TRANSPARENCY, PURPOSE AND LAWFUL BASIS FOR PROCESSING

Comhlámh advises all Data Subjects about what data it collects, what it is used for, who it might be shared with, where and for how long it may be retained, and how it is secured in addition to other relevant details about processing personal data. We also advise data subjects of their rights, where to get further information and how to make a complaint.

Comhlámh establishes the purpose and lawful basis for processing before processing any personal data.

5.2 PURPOSE LIMITATION

Comhlámh's processes personal data only for the stated purpose or for purposes that are compatible with the original purpose. If processing for an incompatible process is contemplated we seek the consent of Data Subject before processing the data for the new purpose.

5.3 DATA MINIMISATION

Comhlámh only ever obtains, retains, processes, and shares the minimum amount of personal data that is essential for carrying out our services and/or meeting our legal obligations.

5.4 ACCURACY AND QUALITY

Comhlámh takes steps to ensure the accuracy and quality of personal data processed and acts to rectify any inaccuracies where they occur.

5.5 RETENTION AND STORAGE LIMITATION

Comhlámh retains and stores personal data only for as long as is necessary for the purpose for which the data is Processed.

5.6 SECURITY AND CONFIDENTIALITY

Comhlámh has adequate and appropriate technical and organisational measures commensurate with the risk to the Data Subjects to ensure the security and maintain the confidentiality of personal data processed.

6 OUR OBLIGATIONS AS A DATA CONTROLLER

In addition to complying with the above principles of personal data management, Comhlámh recognises that it has specific obligations as a Data Controller. These obligations, and the measures taken or planned to address them, are:

6.1 PRIVACY NOTICE

Where personal data is obtained directly from the individual we provide the Data Subject with a Privacy Notice setting out the identity and the contact details of the controller, the contact details of our data protection lead, the purpose(s) and legal basis for the processing, the existence of the rights of data subjects and how to exercise them, the right to lodge a complaint with the Supervisory Authority and other information as required by law.

Where Comhlámh obtains and/or processes personal data that has **not** been obtained directly from the data subject, Comhlámh ensures that required information disclosures are provided to the data subject within 30 days of our obtaining the personal data.

6.2 RECORD OF PROCESSING ACTIVITIES

Comhlámh maintains a record of personal data processing activities in its Head Office.

6.3 DATA BREACHES

Comhlámh has extensive technical and organisational security measures in place to protect the security and confidentiality of personal data. However, Comhlámh recognises that breaches i.e., unauthorised release of, or access to, personal data can occur. Comhlámh understands and has procedures to assess, record and, where appropriate, notify the relevant Data Protection Commission and/or the Data Subject in the event that a breach occurs.

6.4 CONTRACTS WITH DATA PROCESSORS

Comhlámh contracts with external data processors to provide certain services that entail the processing of personal data e.g., IT Systems and Services such as Rightclick, Salesforce, Survey Monkey, Paypal, iDonate, Eventbrite, and Peninsula.

We assess all providers carefully and engage only processors who have measures in place to Process personal data appropriately on behalf of Comhlámh. All processing of personal data is subject to having a properly constituted Data Processing Agreement in place.

6.5 DATA SUBJECT RIGHTS

Comhlámh understands and upholds the rights of Data Subjects under Data Protection Law and has arrangements in place to ensure that these rights are understood by employees who process personal data and to respond to requests in a timely fashion.

6.6 DATA PRIVACY IMPACT ASSESSMENT

Where Comhlámh processes, or is considering the processing of, personal data utilising new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, we carry out a Data Protection Impact Assessment (DPIA).

6.7 DATA PROTECTION OFFICER

Comhlámh has assessed whether it meets the criteria requiring the appointment of a DPO and has concluded that a DPO is not required because Comhlámh does not meet the criteria requiring appointment of a DPO.

6.8 OVERSEAS TRANSFER

Comhlámh is aware of its obligations to safeguard personal data transferred to third countries.

7 AUDITS AND MONITORING

We carry out regular audits and compliance monitoring with a view to ensuring that our measures and controls to protect personal data are effective and compliant.

We ensure to assess, test, review and improve the processes, measures and controls in place and report improvement action plans to the Board where applicable.

8 TRAINING

Comhlámh provides training for [trustees, senior managers, and staff] in relation to data protection the content of which is tailored to the requirements of their roles and the extent to which they are involved in processing personal data.

Staff who process personal or special category information are provided with extensive data protection training and other continuing professional development and mentoring.

Appendix 1 – Glossary of Data Protection Terms

“Biometric data” means personal data relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprints.

“Consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action e.g. by applying online for a job, signifies agreement to the Processing of personal data relating to him or her.

“Cross Border Processing” means Processing of personal data which: -

- takes place in more than one Member State; or
- which substantially affects or is likely to affect data subjects in more than one Member State.

“Data controller” means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of personal data; where the purposes and means of such Processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

“Data processor” means a natural or legal person, public authority, agency or other body which Processes personal data on behalf of the controller.

“Data protection laws” means for the purposes of this document, the collective description of the GDPR and any other relevant data protection laws that the Comhlámh complies with.

“Data subject” means an individual who is the subject of personal data.

“GDPR” means the *General Data Protection Regulation (EU) (2016/679)*.

“Genetic data” means Personal Data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

“Processing” or “Process” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Profiling” means any form of automated Processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

“Recipient” means a natural or legal person, public authority, agency, or another body, to which the personal data are disclosed, whether a third party or not.

“Supervisory Authority” means an independent public authority which is established by a EU Member State.

“Third Party” means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority.

Appendix 2 - Data Protection Principles

The **General Data Protection Regulation (GDPR) (EU)2016/679** was approved by the European Commission in April 2016 and applies in all EU Member States from 25th May 2018. As a 'Regulation' rather than a 'Directive', its rules apply directly to Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As Comhlámh processes personal information regarding individuals (*data subjects*), we are obligated under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

Article 5 of the GDPR requires that personal data shall be: -

- a) Processed lawfully, fairly and in a transparent manner in relation to the data subject (**'lawfulness, fairness and transparency'**)
- b) collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes; further Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (**'purpose limitation'**)
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**)
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**'accuracy'**)
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be Processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**'storage limitation'**)
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**'integrity and confidentiality'**).

Article 5(2) requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection principles ('accountability')* and requires that firms **show how** they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of Processing.