Data Protection Policy

Table of Contents

Policy Version 1.0

Agreed: May 14th 2018

1. Policy Statement

Aidlink collects and processes personal data in order to fulfil our organisational objectives. Aidlink is committed to upholding the human rights of all people including the data privacy rights of individuals. The 2018 General Data Protection Regulation (GDPR), drawing on the principles of the Universal Declaration of Human Rights (1948), the European Convention of Human Rights (1950) and the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981), exists to protect and empower all EU citizens' data privacy.

The Aidlink Data Protection Policy outlines our commitment to the principles of the GDPR and to compliance with the GDPR's legal framework. In line with the GDPR's approach to data privacy and security, Aidlink's Data Protection Policy and Procedures are *risk-designed*, ensuring threats to personal data processed by the organisation are optimally minimised, and the rights of data subjects are upheld.

2. Scope and Provisions

This policy applies to all personal data processed by Aidlink. The policy applies equally to personal data held in manual and automated form.

Responsibility for compliance and ensuring the privacy and security of data processed by Aidlink ultimately lies with the Aidlink Board of Directors.

Responsibility for operational compliance and day-to-day data processing is delegated to the Executive Director and staff. The Executive Director will name a key responsible person/privacy lead.

This policy will be reviewed at least annually.

3. Key Definitions

Personal Data

Information relating to an identified or identifiable natural person, encompassing a wide range of personal information and including online identifiers such as IP addresses and cookie identifiers.

Example: Contact information contained in Aidlink's contact databases used to communicate with our supporters, or data relating to visitors to our website captured by google analytics.

Special Categories of Data

Personal data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Example: Health information collected about immersion participants/students.

Data Subject

The individual to whom the personal data relates, an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier.

Example: Aidlink supporters, immersion participants and their family members, website visitors.

Data Controller

The legal person such as individual or an organisation, who, alone or jointly with others, determines the purpose and means of the processing of personal data.

Example: Aidlink is a Data Controller – we collect personal data and make decisions about how to use that data as part of our day-to-day operations.

Data Processor

The legal person such as an individual or a company who processes personal data on behalf of a controller but is not an employee of the controller.

Example: Aidlink is a Data Processor - Aidlink processes immersion participant data received from partner schools. Aidlink also engages third party Data Processors - we share personal data with airlines in order to book flights.

Under Irish law, both Controllers and Processors are considered to be the legal entities or organisations doing the work, not individuals.

Processing

Data processing is any[1] manual or automated use and manipulation of personal data, including collection, storage, use, disclosure and destruction.

Example: see section 4.

[1] You do not need to view the actual data, but transmitting it, backing up a file or destroying data all count as a processing activity.

4. Aidlink Data Processing and the Seven GDRP Principles

In the course of its daily organisational activities, Aidlink manipulates personal data in a number of ways. The below cases provide non-exhaustive examples of how Aidlink engages in the processing of personal data.

Fundraising

- Postal and/or email donation acknowledgment.
- Postal and/or email fundraising appeals.
- Tax back on donation claims.

Project administration

- Booking flights with personal data.
- Registering staff and immersion participants with the Dept. of Foreign Affairs citizen portal.
- Temporarily maintaining passport records for the duration of overseas travel.

Internal business functions

- Processing payroll.
- Staff and board recruitment.
- Garda vetting of relevant staff members.

It is the policy of Aidlink to uphold the seven key GDPR principles (outlined below) in all our data processing.

Lawfulness, fairness and transparency

Aidlink commits to ensuring that all personal data processed by the organisation will be processed lawfully, fairly and transparently. The legal basis for Aidlink's processing activities are outlined in section 5 of this policy. Access requests by data subjects will be granted in line with the legal framework established by the GDPR and Irish Data Protection Commissioner.

Purpose Limitation

Aidlink commits to ensuring that personal data we collect will be processed for specified, explicit and legitimate purposes and will not be processed in a manner other than those purposes. The processing purposes of all data will be identified and documented within the organisations databases.

Data minimisation

Aidlink commits to ensure that personal data collected by the organisation will be adequate, relevant and limited to only what is necessary in order to fulfil the purposes for which they are processed.

Accuracy

Aidlink commits to ensuring that, as far as is practicable, personal data collected by the organisation will be accurate and kept up to date. When made aware of inaccuracies, personal data will be corrected or deleted.

Retention

Aidlink commits to ensuring that all personal data will be stored in an accessible format for no longer than is necessary. Data that is no longer relevant will be destroyed.

Integrity and confidentiality
Aidlink commits to ensuring that, as far as is practicable, personal data will be kept securely.

Accountability
Aidlink commits to ensuring that compliance with the GDPR will be demonstrable and documented.

5. Lawful basis for data processing activities
Under Article 6 of the GDPR, organisations must demonstrate the "lawful basis for processing personal data". At least one of the following conditions must be met in order for data processing to be deemed legal:

Consent
The data subject has clearly and willingly agreed to the processing of their personal data for one or several purposes.

- Data subjects must signal agreement by "a statement or a clear affirmative action." (Silence, pre-ticked boxes or inactivity do not constitute consent).
- The consent must be freely given, specific, informed and unambiguous.
- Aidlink must be able to demonstrate that the individual has consented.
- The consent must be as easy to withdraw as it was to give in the first place.
- Data subjects must be informed of the right to withdraw consent at any time before consent is given.
- The consent language must be intelligible and in an easily accessible form, using clear and plain language.
- The request for consent must be clearly distinguished from other matters contained in the document or website.

Example: When an individual signs-up to receive the Aidlink newsletter they must consent/actively agree to receive the communication by email and are informed of their right to withdraw, or where an individual visits the Aidlink website they must consent to allow cookies to collect and store information about their browsing.

Contract
The processing activity is necessary for the performance of a contract between Aidlink and the data subject, or necessary at the request of the Data Subject prior to entering into a contract.

Example: Aidlink processes the personal data of our employees in order to make monthly salary payments as per employment contracts.

Legal Obligation
The processing is necessary for compliance with a legal obligation to which Aidlink is subject.

Example: Aidlink is legally obliged to share personal data with Tusla should we suspect a child safe-guarding issue.

Vital Interests[2]
The processing of the personal data is necessary to protect the vital interests of the Data Subject.

[2] You cannot rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.

Not relevant to Aidlink

Public Interest / Official Authority

The processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official, regulatory or statutory authority, which is vested in the Controller.

Not relevant to Aidlink

Legitimate Interest

The processing is necessary for the purposes of the legitimate interests pursued by Aidlink, except where these are overridden by the interests or fundamental rights and freedoms of the data subject, particularly where he or she is a child. Legitimate Interests is dependent on the balance between the interests of the processor and the rights and freedoms of the individual. In order to determine this, a Legitimate Interest 'Balancing Test' can be completed.

Example: Aidlink will contact the next of kin of staff members without their consent in case of an emergency.

6. Lawful basis for processing of Special Categories of Data

Special Categories of Data are personal data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Special categories of data can only be processed if one of the following criteria are met:

- The data subject has given explicit consent to the processing of those personal data for one or more specified purposes; or
- The processing is necessary for the purposes of carrying out the obligations of the Controller or of the data subject in the field of employment and social security and social protection; or
- The processing is necessary to protect the vital interests of the data subject or of another person where the Data Subject is physically or legally incapable of giving consent; or
- The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim, in connection with its ethos and purposes; or
- The processing relates to personal data which are manifestly made public by the Data Subject; or
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- The processing is necessary for reasons of substantial public interest; or
- The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services pursuant to contract with a health professional; or
- The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices; or
- The processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with the Regulation.

Example: Health information collected by Aidlink about immersion participant students falls under Special Categories of Data. Aidlink will always seek explicit consent as the legal basis of processing special categories of data.

7. Aidlink Data Security

Aidlink commits to collecting, storing, sharing and deleting personal data securely.

Technical security measures employed by Aidlink include:

- Ensuring that all computing devices such as PCs, mobile phones, and tablets are using an up-to-date operating system.
- Ensuring all computing devices are regularly updated with manufacturer's software and security patches.
- Using antivirus software on all devices.
- Implementing a strong firewall.
- Reviewing vendor supplied software and updating default system, administrator, and root passwords and other security parameters to ensure defaults are not left in place.
- Ensuring data backups are taken and are stored securely in a separate location.
- Ensuring that data backups are periodically reviewed and tested to ensure they are functioning correctly.
- Ensuring that data is stored securely.
- Ensuring that personal data is collected securely via webforms (such as for newsletter subscriptions).

Physical security measures employed by Aidlink include:

- Keeping offices locked.
- Ensuring that fire and burglar alarms are in place and that they are functioning correctly.
- Ensuring that ICT equipment such as hard drives and old laptops, computers and mobile devices are securely disposed of at end of life.

Organisational security measures employed by Aidlink include:

- Ensuring all employees are familiar with Aidlink data protection policy and procedures.
- Conducting ongoing staff training on data protection.
- Integrating Data Protection into organisational risk management processes.
- Documenting a data breach incident response plan
- Periodically reviewing contracts with 3rd party ICT providers to ensure the security measures documented are still appropriate and up to date.

Third Party Processors

Aidlink engages third party processors in order to effectively and efficiently carry out the organisation's objectives.

Under GDPR Aidlink must ensure that a contract is agreed between the data controller (Aidlink) and data processor outlining GDPR compliance.

Contracts must set out:

- Subject matter and duration of the processing.
- The nature and purpose of the processing.
- The type of personal data and categories of data subject.
- The obligations and rights of the controller.

Contracts must also include as a minimum the following terms, requiring the processor to:

- Only act on the written instructions of the controller.
- Ensure that people processing the data are subject to a duty of confidence.
- Take appropriate measures to ensure the security of processing.
- Only engage sub-processors with the prior consent of the controller and under a written contract
- Assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR.
- Assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments.
- Delete or return all personal data to the controller as requested at the end of the contract.
- Submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

In the case of non-EU based processors, it is incumbent on Aidlink to ensure that the processor is GDPR compliant before sharing any data outside of the EU.

Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. Under the GDPR, a DPIA is mandatory where data processing "is likely to result in a high risk to the rights and freedoms of natural persons." This is particularly relevant when a new data processing technology is being introduced. It is not envisaged that Aidlink will engage in data processing that would be subject to mandatory DPIA, but should such an incident arise, advice will be sought from the Data Protection Commissioner.

8. Rights and Freedoms of Data Subjects

Under the GDPR data subjects are afforded a range of rights and freedoms, some of which are outlined below. Aidlink commits to ensuring that the rights and freedoms of all Aidlink data subjects are upheld and realised.

Right to Be Forgotten

Data subjects have the right to request from the Aidlink the deletion of personal data, without undue delay.

Right to Restriction of Processing

Data subjects can request that Aidlink restrict processing their data either permanently or temporarily.

Right to Object to Certain Processing

Data subjects can object to Aidlink processing of their personal data for a particular purpose based on his or her situation, preference or state of mind. An objection to processing may be overridden in certain circumstances[3].

[3] For example, Irish law may require the Controller to continue to maintain fundraising records for the purposes of financial audit.

Right of Access to Information

Data subjects have the right to submit a written request to access any information relating to them from Aidlink. Aidlink must provide the requested information relating to the Data Subject within one month of receipt of the request. The one month period may be extended by two further months, where necessary, taking into account the complexity and number of requests, where necessary. In this case, Aidlink shall inform the Data Subject of any extension within one month of receipt of the request and the reasons for the delay.

Requests will be dealt with free of charge. However, where requests from a data subject are considered 'manifestly unfounded or excessive' (for example where an individual continues to make unnecessary repeat requests or the problems associated with identifying one individual from a collection of data are too great) Aidlink may:

Charge a reasonable fee, taking into account the administrative costs of providing the information/ taking the action requested; or

Refuse to act on the request. In such cases, Aidlink will provide proof as to why they believe the request is manifestly unfounded or excessive.

Right to Complain, Right to Judicial Remedy

If a Data Subject is not satisfied that Aidlink has adhered to its obligations under the GDPR, he or she may complain to the Irish Data Protection Commissioner or seek a judicial remedy in the Irish courts.

9. How to make a Subject Access Request from Aidlink

Should you want to stop or restrict communications from Aidlink, or request information about your data held by Aidlink, a Subject Access Request can be made by contacting

Aidlink
34 Greenmount Office Park
Harold's Cross
D6W CX81
For queries general queries contact 01 473 6488 or info@aidlink.ie

10. Data Breach

In the event of a data breach, Aidlink is obliged to notify the Data Protection Commissioner within 72 hours, (unless the data was anonymised or encrypted). Breach notifications can be made via https://www.dataprotection.ie

Breaches that are likely to bring harm to an individual – such as identity theft or breach of confidentiality – must also be reported to the individuals concerned.

Policy References and Sources

Regulation (EU) 2016/679 General Data Protection Regulation (GDPR) https://gdpr-info.eu/

Data Protection Commissioner, General Data Protection Regulation (GDPR) http://gdprandyou.ie/

Data Protection Commissioner, "*Personal Data Security Guidance For Microenterprises under the GDPR" http://gdprandyou.ie/wp-content/uploads/2018/03/Microenterprises-GDPR-Final-1.pdf*

Charities Institute Ireland *"Information and Guidance Notes General Data Protection Regulation (GDPR)"* https://www.charitiesinstituteireland.ie/information-and-guidance-notes-general-data-protection-regulation-gdpr/

The Wheel *"Good Practice Guide Preparing for the General Data Protection Regulation (GDPR) A Guide for Irish Non-profits"* (available at Aidlink)

Dóchas "*General Data Protection Legislation: What Charities Need To Know A Toolkit from Dóchas & FP Logue Solicitors"* http://dochas.ie/sites/default/files/DataProtectionToolkit.pdf

MailChimp "*The General Data Protection Regulation (GDPR): What it is, what we are doing, and what you can do."* https://kb.mailchimp.com/binaries/content/assets/mailchimpkb/us/en/pdfs/mailchimp_gdpr_sept2017.pdf

White Fuse "GDPR for small charities - data protection guide" https://whitefusemedia.com/blog/gdpr-small-charities

Information Commissioner's Office (UK) "ICO GDPR guidance: Contracts and liabilities between controllers and processors". https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf

Leman Solicitors "Dealing with Subject Access Requests under GDPR – Checklist" https://leman.ie/wp-content/uploads/2017/10/Checklist-Dealing-with-Data-Access-Requests_October-2017_2349889-002.pdf