ActionAid Ireland Data Protection Policy

2018

Purpose
The purpose of this policy is to outline Employees and Employers rights and responsibilities under the Data Protection Act 1988, the Data Protection (Amendment) Act 2003 and the General Data Protection Regulation 2018 (GDPR). ActionAid Ireland is committed to complying with its legal obligations with regards to the data protection legislation.

The Data Protection legislation imposes obligations on Data Processors and Data Controllers regarding how they process personal data and sensitive personal data. The purpose of this policy is to assist ActionAid Ireland to meet its statutory obligations as a Data Processor and/or a Data Controller, to explain those obligations to Employees, Volunteers and Interns and to inform data subjects how their data will be processed. The GDPR applies to Organisations that:

- are established in one or more Member State(s);
- process personal data (either as controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

Scope
This policy applies to all Employees, Volunteers and Interns of ActionAid Ireland.

Policy
Under the Data Protection legislation, Employees, Volunteers and Interns have a right to receive information on data collection, access their personal data, have inaccuracies corrected, have information erased and have a right to data portability.

Personnel records held by Employers come within the terms of the Data Protection legislation. Employees, Volunteers and Interns can make access requests for information held about them. All Employees, Volunteers and Interns are required to process personal data in line with this policy.

Data Protection Principles
The Organisation will comply with the data protection principles set out in the General Data Protection Regulation, 2018.

ActionAid Ireland ensures that all data is:

1. **Obtained and processed lawfully, fairly and in a transparent manner.**

The Organisation will meet this obligation by informing Employees, Volunteers and Interns of the purpose(s) for which their data is being processed as well as the legal basis for the processing; to whom their data may be disclosed and if the Organisation intends to transfer data to a third country or international Organisation outside of the EEA.

Where processing is necessary for the purposes of the legitimate interests of the Organisation, ActionAid Ireland will inform Employees, Volunteers and Interns of the legitimate interests being pursued. Where the Organisation intends to record activity on CCTV, signage will be posted in full view.

2. **Collected for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes.**

ActionAid Ireland will obtain data for purposes which are specific, lawful and clearly stated. The Organisation will inform Employees, Volunteers and Interns of the reasons they collect their data and will inform them of the uses to which their data will be put. Should the Organisation subsequently intend to use the data for another purpose, the consent of the Employee concerned will be sought prior to doing so unless a relevant exemption applies.

Data relating to Employees, Volunteers and Interns will only be processed in a manner consistent with the purposes for which it was collected. Information will only be disclosed on a need to know basis, and access to it will be strictly controlled.

ActionAid Ireland will not share Employee personal information for direct marketing purposes outside of the Organisation.

3. **Adequate, relevant and limited to what is necessary in relation to the purposes for which data are processed.**

ActionAid Ireland will ensure that the data it processes are relevant to the purposes for which those data are collected. Any personal data which is not required will not be collected in the first instance. Prior to obtaining personal data, the Organisation will ensure that the information sought is essential for the purpose for which data is being obtained and that data will not be kept for longer than is necessary for the purpose for which it was collected.

4. **Accurate and up to date.**

ActionAid Ireland is required to keep Employee's data accurate and up to date. The Organisation will meet this obligation by:

- Obtaining and processing only the necessary amount of information required to provide an adequate service;
- Conducting periodic reviews to ensure that relevant data is kept accurate and up-to-date;
- Conducting regular assessments in order to establish the need to keep certain Personal Data.

If an Employee informs the Organisation of a change in their personal information the Organisation will ensure this information is updated on all the Organisations internal systems and all third-party providers are notified of this change where necessary.

5. **Limited retention in a format that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.**

ActionAid Ireland will ensure that the data is kept in a form that permits identification of Employees, Volunteers and Interns for no longer than is necessary for the purposes for which the personal data was processed.

Personal data is retained for a period of time to meet certain legal obligations.

For employment statutes generally, a 3-year retention period is applicable, other retention periods apply regarding:

- Employment Permit records - 5 years (or period equal to duration of employment – whichever is longer);
- Parental Leave records - 8 years;
- Accident records - 10 years.

Once the respective retention period has elapsed, the Organisation undertakes to destroy or erase personal data.

6. Secure and confidential processing of data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The Organisation will undertake appropriate technical and organisational measures to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, unlawful processing, accidental loss, destruction or damage of any personal data held by the Organisation in its capacity as Data Controller.

Only Employees, Volunteers and Interns with a genuine reason for doing so may gain access to the information. Sensitive Personal Data is securely stored under lock and key- in the case of manual records / protected with firewall software and password protection- in the case of electronically stored data.

Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the Organisation's premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.

- Employees, Volunteers and Interns are also expected to keep Personal Data secure by adopting the following measures:
- Using secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold personal data.
- Paper documents should be shredded.
- Data users should ensure that individual monitors do not show Personal Data to passers-by and that they log off from their PC when it is left unattended.

If the Organisation discovers that there has been a data security breach that poses a risk to the rights and freedoms of individuals, it will report it to the Data Protection Commissioner within 72 hours of discovery. If the breach is likely to result in a high risk to the data protection rights and freedoms of an Employee, it will inform affected individuals that there

has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

7. **The Organisation is committed to be accountable, liable and comply with the Data Protection Principles.**

Purposes for which staff records are held
Staff records are provided to the Organisation by Employees, Volunteers and Interns by way of a contractual and statutory requirement for the following purposes:

- the management and administration of the Organisation;
- to facilitate the payment of salary, and calculate other benefits/entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant);
- human resources management generally;
- to enable the Organisation to comply with its legal obligations as an employer including the preservation of a safe, efficient working environment (including complying with its responsibilities under the Safety, Health and Welfare At Work Act 2005 and the 2007 Health and Safety Regulations).

Collection and Storage of data
This Policy applies to all Personal and Sensitive Personal Data collected, processed and stored by the Organisation. In the course of its activities and in order to carry out its function, the Organisation processes personal data from a variety of sources. These sources include data in relation to its Employees, Volunteers and Interns, Volunteers, service providers, suppliers, customers and any other Data Subjects in the course of its activities.

The main categories of Personal Data held by the Organisation may include:

- Name, address and contact details, PPS number
- Details of approved absences (career breaks, maternity, parental leave, study leave etc.)
- Details of work record
- Details of any accidents/injuries sustained on Organisation property or in connection with the staff member carrying out their duties
- Details of salary and other benefits
- Personnel records including contract and offer letters, performance management information and, if applicable, records of any interactions under the headings of grievance and discipline
- Training courses completed and qualifications awarded
- Occupational health reports and sick certificates
- Door access control system data/ biometrics
- Email system data
- Financial data
- Human resources data
- Phone records
- Records of application and appointment to promotion posts

ActionAid Ireland will ensure that personal data will be processed in accordance with the principles of data protection, as described in the Data Protection legislation.

Personal data is normally obtained directly from the Employee concerned. In certain circumstances, it will, however, be necessary to obtain data from third parties e.g. references from previous Employers.

Data Processing in line with Employees, Volunteers and Interns' Rights
The Organisation will process data in line with Employees, Volunteers and Interns' right to:

- receive certain information regarding the collection and further processing of their personal data;
- request access to any data held about them by a data controller;
- have inaccurate data corrected;
- have information erased;
- object to the processing of their data for direct-marketing purposes;
- prevent processing that is likely to cause damage or distress to themselves or anyone else;
- restrict the processing of their information;
- where processing is based on consent, to withdraw that consent at any time;
- data portability;
- object to automated decision-making and profiling.

Right to opt-out
The Organisation will inform individuals that information is being collected and used for these purposes prior to doing so. Individuals have the right to object to any specific type of data processing. Where such objection is justified, the Organisation will cease processing the information unless it has a legitimate business interest that prevents this.

Right to be forgotten
Employees, Volunteers and Interns may request that any information held on them is deleted or removed if there are no legitimate reason for the Organisation to keep it. Any third parties who process or use that data will comply with the request.

Storage of personal data
Personal data kept by ActionAid Ireland shall normally be stored on the Employee's personnel file or HR electronic database. Highly sensitive data such as medical certificates, reports and other documents related to an Employee's illness or injury will be securely stored to ensure the highest levels of confidentiality.

ActionAid Ireland will ensure that only authorised personnel have access to an Employee's personnel file. The Employee's Manager or Supervisor may have access to certain personal data where necessary.

ActionAid Ireland has appropriate security measures in place to protect against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

Changes in Personal Details
Employees, Volunteers and Interns are responsible for ensuring that they inform their Manager of any changes in their personal details e.g. change of address.

ActionAid Ireland will endeavour to ensure personal data held by is up-to-date and accurate.

ActionAid Ireland is under a legal obligation to keep certain data for a specified period of time.

In addition, the Organisation will need to keep personnel data for a period of time in order to protect its legitimate interests e.g. Intra-group transfer of Employee/ client data for administrative purposes (within the EEA).

Disclosure of Personal Data to Data Processors
In the course of its role as Data Controller, the Organisation engages a number of Data Processors to process personal data on its behalf. This may include, but is not limited to payroll providers, benefit providers etc. In each case, it is the Organisation's policy to have a contract in place with the Data Processor, outlining their obligations in relation to the personal data, the specific purpose or purposes for which they are engaged, and the requirement that they will process the data in compliance with the Data Protection legislation.

As a Data Controller, the Organisation ensures that any entity which processes personal data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation. This is achieved through a data processor contract.

Security and Disclosure of Data
ActionAid Ireland shall take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of both electronic and manual data.
Security measures will be reviewed from time-to-time having regard to the technology available, the cost and the risk of unauthorised access. Employees, Volunteers and Interns must implement all Company security policies and procedures e.g. use of computer passwords, locking filing cabinets etc.

HR data will only be processed for Employment-related purposes and in general will not be disclosed to third parties, except where required or authorised by law or with the agreement of the Employee. HR files are normally stored in a locked file in the CEO's office and on a secure Drive with limited access, and Employees, Volunteers and Interns who have access to these files must ensure that they treat them confidentially and in accordance with the data protection principles set out above.

If Employees, Volunteers and Interns are in any doubt regarding their obligations they should contact the CEO.

Any breach of the data protection principles is a serious matter and may lead to disciplinary action up to and including dismissal.

Medical Data
Occasionally, it may be necessary to refer Employees, Volunteers and Interns to the company doctor for a medical opinion and all Employees, Volunteers and Interns are required by their contract of Employment to attend in this case. The Organisation will receive a copy of the medical report, which will be stored in a secure manner with the utmost regard for the confidentiality of the document.

Employees, Volunteers and Interns are entitled to request access to their medical reports. Should an Employee wish to do so, please contact the HR lead who will consult with the doctor who examined you and request the data. The final decision lies with the doctor to decide whether the data should be disclosed to you or not in accordance with Statutory Instrument No. 82 of 1989.

Employees, Volunteers and Interns are required to submit sick certificates in accordance with the sick pay policy. These will be stored by the Organisation having the utmost regard for their confidentiality.

Interview Records
The Organisation will retain records of interview notes, application forms etc in order to ensure compliance with the Employment Equality Acts, 1998 and 2015 and with the company's Equal Opportunities Policy for at least 1 year from the date that the position was filled.

Email Monitoring
The Organisation provides email facilities and access to the internet. In order to protect against the dangers associated with email and internet use, screening software is in place to monitor email and web usage.

Mailboxes are only opened upon specific authorisation by a Manager in cases where the screening software or a complaint indicates that a particular mailbox may contain material which is dangerous or offensive; where there is a legitimate work reason or in legitimate interest of the Organisation.

Data Protection champion
Louise Cribbin is the data protection champion for ActionAid Ireland. Louise has responsibility for promoting compliance with data protection legislation. All Employees, Volunteers and Interns must co-operate with Louise when carrying out his/her duties.

Access Requests
Employees, Volunteers and Interns are entitled to request data held about them on computer or in relevant filing sets. This includes personnel records held by ActionAid Ireland. The Organisation will ensure that such requests are forwarded to the CEO in a timely manner, to enable them to process the request within the required timeframe. To make a subject access request, an Employee should send the request to the CEO. In some cases, the Organisation may need to ask for proof of identification before the request can be processed. The Organisation will inform the Employee if it needs to verify his/her identity and the documents it requires.

A data access request will be responded to within 1 month of receipt of the request though this period may be extended for up to 2 further months where necessary, taking into account the complexity and number of requests. The Organisation will write to the individual within 1 month of receiving the original request to tell him/her if this is the case.

Information will be provided in electronic form if the individual has made a request electronically, unless he/she agrees otherwise. Documents are provided free of charge, unless the request is "manifestly unfounded or excessive", in which case a fee of €6.35 may be applied. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Organisation has already responded. If an Employee makes a data access request, the Organisation will inform him/her of:

- The purposes of the processing;
- The categories of personal data concerned;
- To whom the personal data has been or will be disclosed;
- Whether the data will be or has been transferred outside of the EU;
- The period for which the data will be stored, or the criteria to be used to determine retention periods;
- The right to make a complaint to the DPC;
- The right to request rectification or deletion of the personal data;
- Whether the data has been subject to automated decision making.

Formal requests, invoking the right to access to personal data must be made in writing. Employees, Volunteers and Interns are only entitled to data about themselves and will not be provided with data relating to other Employees, Volunteers and Interns or third parties. It may be possible to block out the data relating to a third party or conceal his/her identity, and if this is possible the company may do so.

Data that is classified as the opinion of another person, will be provided unless it was given on the understanding that it will be treated confidentially. Employees, Volunteers and Interns who express opinions about other Employees, Volunteers and Interns in the course of their Employment should bear in mind that their opinion may be disclosed in an access request, e.g. performance appraisals.

An Employee who is dissatisfied with the outcome of an access request has the option of using the Organisation's grievance procedure.

Retention of personal data

Personal data is retained for a period of time to meet certain legal obligations. Once the respective retention period has elapsed, the Organisation undertakes to destroy or erase personal data.

Specifically, the following rules apply for personal details relating to Employees, Volunteers and Interns:

Legal basis	Data & Record Keeping Requirement
Organisation of Working Time Act 1997	Hours worked (Time sheets), Medical certificates, Annual leave & special leave requests to be retained for 3 years
Protection of Young Persons Act 1996	1 year as claims must be brought within 12 months of the date of the offence.

National Minimum Wage Act 2000	Salary information – pay slips to be retained for 3 years.
Protection of Employment Acts, 1977-2007	To be retained for 3 years. Records in relation to collective redundancies to be retained for 3 years.
Minimum Notice and Terms of Employment Acts 1973-2005	To be retained for 1 year
Terms of Employment (Information) Acts 1994 – 2014	A copy of the written statement to be held for the duration of the employee's employment and for 1 year thereafter.
Payment of Wages Act 1991	To be retained for 1 year
Carer's Leave Acts 2001-2006	To be retained for 8 years.
Parental Leave Acts 1998-2013	Parental Leave and Force Majeure leave records to be kept for 8 years.
Paternity Leave and Benefit Act 2016	Must be kept for 8 years
Employment Permits Acts 2003 to 2014	The records to be retained for 5 years or for the duration of employment.
Safety Health and Welfare at Work Act 2005	Records containing full details of all accidents or dangerous occurrences to be kept for 10 years from the date of the accident and notified to the Health & Safety Authority at the time of the incident.
Best Practice	**Data & Record Keeping Recommendation**
Employment Equality Acts 1998-2015	Records relating to the recruitment process should be retained for a 1-year period. 1 year as complaints can be made within 6 months from the date of an alleged discrimination which can be extended to 12 months in exceptional circumstances. Adjudication Officer authorised under the Act to inspect an employer's records during an investigation. Discrimination claims may result in awards in respect of arrears of up to 6 years pay so records should be kept for at least 6 years.
Equal Status Act 2000-2011	To be retained for 1 year
Maternity Protection Act 1994-2004	To be retained for a minimum of 1 year
Adoptive Leave Act 1995-2005	To be retained for a minimum of 1 year
Unfair Dismissals Acts 1977-2015	To be retained for a minimum of 1 year
Redundancy Payments Acts 1967-2014	To be retained for a minimum of 1 year
Protected Disclosures Act 2014	To be retained for at least 1 year

Transfer of Undertakings Records - EC (Safeguarding of Employees' Rights on Transfer of Undertakings) Regulations 2003	To be retained for at least 1 year

Responsibilities

Management will endeavour to ensure that this policy is communicated to all Employees, Volunteers and Interns and will ensure that the policy is maintained and updated in line with legislative changes.

Employees, Volunteers and Interns are expected comply with this policy and to raise issues of concern to their Manager.

Failure by Employees, Volunteers and Interns to process personal data in compliance with this policy may result in disciplinary proceedings up to and including dismissal.

Complaints

Employees, Volunteers and Interns have the rights to lodge a complaint to the Data Protection Commissioner if they believe their rights under the Data Protection legislation are not being complied with by the Organisation.