Appendix 1: DATA PROTECTION POLICY

ACTIONAID INTERNATIONAL
DATA PROTECTION POLICY

Policy Information

POLICY NAME:	DATA PROTECTION POLICY
VERSION:	1.0
APPLICABLE DATA PROTECTION LEGISLATION:	EU GDPR 2016/679 (REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016 ON THE PROTECTION OF NATURAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, AND REPEALING DIRECTIVE 95/46/EC) ("GDPR") AND ASSOCIATED NATIONAL LEGISLATION

Governance Information

Policy Owner	Head of Digital and Technology
Policy Sponsor	Resource Mobilisation and Innovation Director
Date Ratified by SLT	17th November, 2020
Date ratified by Board:	4th December, 2020
Date last updated	December 2020
Date of next review	December, 2021

Table of Contents

1 Overview of this policy
2 Our Obligations.
3 Definitions
4 The Principles of data protection
4.1 Principle 1 - Lawfulness, Fairness & Transparency
4.2 Principle 2 - Process it only for one or more specified, explicit and lawful purposes
4.3 Principle 3 - Process the data to the minimum extent necessary to satisfy these purposes
4.4 Principle 4 - Keep it accurate, complete and up to date
4.5 Principle 5 - Retain data for no longer than is necessary for the specified purpose or purposes
4.6 Principle 6 - Protect the security and integrity of the data

PAPER 11.

4.7 Principle 7 - The controller shall be responsible for, and be able to demonstrate compliance with the Data Protection Legislation.

5 How AAI meets our other obligations under the GDPR

6 How AAI meets our responsibilities under the E-Privacy Directive

7 Roles & Responsibilities

8 Training

9 Implementation and monitoring

10 Updates and revisions to the policy

1 Overview of this policy

ActionAid International (AAI/ActionAid) collects personal information as this is fundamental to enabling us to effectively carry out our everyday functions and activities. The data is in particular collected from Employees, Beneficiaries, Donors, Partners and Suppliers and includes (but is not limited to), name, address, email address, date of birth, IP address, identification numbers, private and confidential information, sensitive data and bank/credit card details.
Data is a valuable asset and this policy lays out how AAI manages data and draws together the content of other policies covering data protection matters to provide assurance that we meet all Applicable Legislation. It outlines the responsibility each individual has around data protection and what we need to do to ensure the rights of Data Subjects (those we have collected data on).

The purpose of this Data Protection Policy is to provide for the protection of the rights and privacy of individuals about whom AAI processes personal data and is to be read along with the various other policies relating to data. It cannot be overstated that as an organisation, there is a strong duty of care owed to data subjects given the nature of the data collected.

This policy is internal to the organisation but can be shared upon request by a supplier or partner.

2 Our Obligations

ActionAid International has a legal requirement to ensure compliance with the Applicable Data Protection Legislation[2], the Directive on Privacy and Electronic Communications[3] and local legislation in-country pertaining to Data Protection. However, AAI also believes in a strong duty of care to data subjects above that required by law. Our processes are designed to ensure legal compliance, but our subject centered approach means that there will be instances where we go beyond the minimum requirements in the legislation.

In the course of daily activities AAI acquires, processes and stores Personal Data in relation to individuals. To that extent, AAI is a Data Controller and has obligations under the Data Protection Legislation reflected in this document. AAI may directly (through its employees) process the data which it controls. All such data must be acquired and managed fairly, in accordance with the relevant Data Protection Legislation as described above.

---

[2] General Data Protection Regulations governs how information pertaining to natural persons is handled. See more here.

[3] The Directive on Privacy and Electronic Communications sits alongside the GDPR. They give people specific privacy rights in relation to electronic communications. See more here.

In order to address this, AAI will take the following general steps:

- Ensure that all staff members are trained and equipped with the ability to anticipate and identify data protection issues
- Appoint a Data Protection Officer (DPO) to monitor compliance and to advise staff when data protection issues arise and adhere to the reporting requirements to the Supervisory Authority as per the Applicable Data Protection Legislation
- Design AAIs processing activities so that they are in full compliance with the law
- Provide secure storage for all Personal Data
- Ensure that AAI develops protocols for the secure (internal or external) transfer of personal data.
- Ensure AA data protection standards and responsibilities are cascaded to all partner organisations

3 Definitions

Data Processing	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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. This includes both automated and manual data and data in other forms, if in scope of Applicable Data Protection Legislation. • Automated data means data held on computer or stored with the intention that it is processed on computer. • Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Data Subject	An individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.
Data Controller	The legal entity (or natural person) responsible for the processing of the Personal Data. The Data Controller determines the purposes and means of the processing (In the context of this policy, AAI is the Data Controller).
Data Processor	A person or entity who processes Personal Data on behalf of AAI, but who is not an employee of AAI (an example of a Processor currently engaged by AAI would be an entity like Bamboo HR).
Data Protection Legislation	The GDPR and associated national legislation.
Data Protection Officer (DPO)	A person appointed by AAI, in particular to inform and advise on data protection related matters and to monitor compliance with the applicable Data Protection Legislation.
Data Protection Impact Assessment	A formal assessment for high-risk Data Processing activities described in Art. 35 GDPR (DPIA).
General Data Protection Regulation (GDPR)	The General Data Protection Regulation (GDPR) became enforceable on the 25th May 2018, replacing the data protection framework under the EU Data Protection Directive. It emphasizes transparency, security and accountability by Data Controllers and Data Processors, while at the same time standardizing and strengthening the right of individuals to data privacy[4].
Legitimate Interest	One of the legal basis for Data Processing under Data Protection Legislation; this legal basis requires a balancing of interests which is carried out via a Legitimate Interest Assessment (LIA).

[4] https://gdpr-info.eu/

Personal Data	Information that relates to an individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of AAI.
Special Categories of Data	Special categories of Personal Data include Personal Data which relates to specific aspects of one's identity or personality, and in particular includes information relating to ethnic or racial identity, political or ideological beliefs, religious beliefs, trade union membership, mental or physical well-being, sexual orientation, or criminal record. In this Data Protection Policy, such categories of data are also referred to as sensitive information.

4 The Principles of data protection

The following key principles are enshrined in Data Protection Legislation and are fundamental to AAI's Data Protection Policy. In its capacity as Data Controller, AAI seeks to ensure adherence to the following principles:

4.1 Principle 1 - Lawfulness, Fairness & Transparency

AAI will obtain and process Personal Data fairly, in an open and transparent manner, in accordance with the fulfilment of its functions and its legal obligations.

For data to be obtained fairly and processed transparently, the data subject will, at the time the data is being collected, or at the latest within one month of acquiring the data, will be made aware of:

- The identity of the Data Controller (AAI)
- The purpose(s) for which the data is being collected
- The person(s) to whom the data may be disclosed by the Data Controller
- Any other information that is necessary so that the processing may be fair.

unless there is exemption provided for under applicable Data Protection Legislation.

AAI will meet this obligation particularly in the following ways:

- Identifying and documenting lawful bases for the collection and processing of data
- Where required, the informed consent of the Data Subject will be sought before their data is processed
- Where it is not possible or appropriate to seek consent, AAI will ensure that any collection of Personal Data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.
- Processing of the Personal Data will be carried out only as part of AAI's lawful activities, and it will safeguard the rights and freedoms of the data subject
- The Data Subject's data will not be disclosed to a recipient other than to a party contracted to AAI and operating on its behalf, or where AAI is required to do so by law
- Where AAI intends to record activity on CCTV or video, a notice will be posted in full view, prior to the recording.

4.2 Principle 2 - Process it only for one or more specified, explicit and lawful purposes

- AAI will process Personal Data for purposes that are specific, lawful and clearly stated and the data will only be processed in a manner compatible with these purposes
- We will review our processing periodically taking a risk-based approach as part of our operational planning and ensure our processing records and privacy information is updated as necessary
- If we identify a new purpose, we ensure that we only use data legally for this purpose.

4.3 Principle 3 - Process the data to the minimum extent necessary to satisfy these purposes

AAI will ensure that the data it processes in relation to Data Subjects is relevant to the purposes for which the data is collected. Data that is not relevant to such processing will not be acquired or maintained.

4.4 Principle 4 - Keep it accurate, complete and up to date

- AAI will ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy
- We will conduct periodic reviews and audits to ensure that relevant data is kept accurate and up to date
- We will further conduct regular assessments in order to validate the need to keep certain Personal Data.

4.5 Principle 5 - Retain data for no longer than is necessary for the specified purpose or purposes

- AAI will prepare and maintain a set of data standards for each business unit, which will detail the data held and the appropriate data retention period for each category. The standards will cover data in both a manual and automated format as well as data in other forms subject to Data Protection Legislation.
- AAI will only keep data in a form that permits the identification of the Data Subject for the duration necessary to fulfil its legal obligations and operational objectives. Once the respective retention period has elapsed, AAI undertakes to anonymize, destroy or erase this data.

4.6 Principle 6 - Protect the security and integrity of the data

- AAI will take appropriate organisational and technological measures to prevent unauthorised or unlawful processing and against accidental loss, destruction or damage. AAI acknowledges that high standards of security are essential for processing all personal information.
- It will ensure that access to, and management of, Personal Data is limited to those staff members with appropriate authorisation and password access
- The Information Security Policy outlines the approach to be adopted from an internal perspective
- The Data Breach Policy outlines the approach to data breaches, the key theme being mitigating the impact of any breach
- The Data Protection Officer completes reporting on any breaches, reports, and communications to Data Subjects.

4.7 Principle 7 - The controller shall be responsible for, and be able to demonstrate compliance with the Data Protection Legislation.

AAI will adopt the appropriate protocols and methodologies in order to ensure that the organisation achieves and maintains compliant standards of data management across the organisation.
AAI will meet this obligation in the following way:

4.7.1 Data Protection Officer (DPO)

- AAI has appointed a DPO to manage our commitment to compliant and responsible Data Processing
- Our DPO can be contacted on dpo.hellas@actionaid.org. This address is continually monitored, with other staff able to deputise on urgent issues if necessary.

4.7.2 Contracts

- AAI will put an appropriate contract in place with any third party before work commences, as per the Procurement process and documents on the Commercial pages of the intranet.
- When working with third parties who act as a Data Processor on our behalf, we will ensure that either they have signed our Data Processing Agreement, or that the clauses mandated by Data Protection Legislation (e.g. Article 28 GDPR) are reflected in any formal, contractual arrangements between the parties.
- Whenever we work with a third party we will ensure that both parties' responsibilities around data breaches are documented for clarity.

4.7.3 Documentation

- We keep a record of our Data Processing Activities and the records are updated regularly and are reviewed on an annual basis.
- As a matter of course, our DPO also documents Decisions, Risks, Issues and where we have engaged with the legislative consultation process. These can be accessed through our evidence base list.

4.7.4 Legitimate Interest Assessments and Data Protection Impact Assessments

- Where AAI cites its own (or a third party's) Legitimate Interest as a lawful basis for processing Personal Data, the organisation will document a Legitimate Interest Assessment (LIA) in order to support decisions made and DPO advice given.
- We use a screening checklist to determine when a Data Protection Impact Assessment (DPIA) may also be needed, and log these regardless of whether a DPIA is ultimately completed.
- LIAs and DPIAs are signed off at Director level and then saved on the AA Intranet.

5 How AAI meets our other obligations under the GDPR

5.1 Ensuring an individual's rights

The rights of Data Subjects apply to the organisation as a whole and are not restricted to each / any individual function. The specific rights established under the Data Protection Legislation are detailed below, along with AAI's approach to ensuring that these rights are fully protected and upheld.

5.1.1 Right to be informed

Our privacy information outlined in paragraph 4.1 above ensures that Data Subjects are made aware of how we operate. Our AAI Privacy Policy is date stamped for transparency of last review and in the event of material update, we will also communicate changes to supporters.

5.1.2 Right of access

We have a Subject Access Request (SAR) Policy and Process, owned by our DPO. The DPO will work with the business function to whom the SAR applies to collate the information, for data subjects exercising this right. Reporting on Subject Access Requests is provided to the International Board on an annual basis at minimum.

5.1.3 Right to rectification

As per Principle 4 (Accuracy), we take a strong stance on the accuracy of the data on our systems and use our AAI Privacy Policy to openly encourage individuals to advise us of any detail that they view as inaccurate or incomplete.

5.1.4 Right to erasure / to be forgotten

Our AAI process is to always clarify an individual's request to determine whether their intention is erasure, or restricted processing; particularly processing for direct marketing purposes.
Whilst the right to erasure is not an absolute right, AAI will always endeavour to honour the request of the individual. Where there are implications for AAI of us enacting this request (i.e. the risk to a Gift Aid audit if we delete information before the end of the audit period) we will explain these to the individual before going ahead.

5.1.5 Right to restrict processing

We encourage individuals to discuss their right to restrict processing, so that we can understand their request and answer any concerns that they may have. Other requests are passed to the DPO to coordinate with appropriate teams on a case by case basis.

5.1.6 Right to data portability

Under certain circumstances, individuals can obtain a copy and reuse their Personal Data for their own purposes. If a data portability request is received, then the DPO will coordinate this with the relevant department.

5.1.7 Right to object

We offer the right to object wherever possible when we use Legitimate Interest as our legal basis for any processing. In addition to that, Data Subjects have the right to object to the processing of their Personal Data for direct marketing purposes at any time.

5.1.8 Rights related to automated decision-making including profiling

Automated decision-making is classified as a decision made by automated means without any human involvement. Additional rights apply where automated decision-making has legal or similarly significant effects on individuals. Currently, AAI does not conduct any automated decision-making.

5.2 International Data Transfers

Our remit as an international organisation means that we sometimes have a requirement to transfer data outside of the European Economic Area (EEA). Where this is unavoidable, we work to analyse the potential risks in doing so and ensure that only the minimum data is transferred and safeguard that the data is either transferred to a country for which an adequacy decision of the European Commission exists or is otherwise sufficiently protected. We also work with the colleagues across the ActionAid Federation to raise overall standards of data protection even outside of those countries subject to the GDPR and do have an Inter-Group Data Transfer Agreement governing the transfer of data across the federation.

6 How AAI meets our responsibilities under the E-Privacy Directive

The E-Privacy Directive, regulates electronic communications; so in particular those by email, telephone, SMS (text message), instant messages and fax. As a directive, the specific requirements are laid down in local Member State legislation and may differ.

PAPER 11.

Among other aspects, the local Member State legislation implementing the E-Privacy Directive determines when we must gather consent for communications, and the Data Protection Legislation defines how that consent must be structured to be valid. Our consent processes are therefore designed to meet our responsibilities under both pieces of legislation. We treat marketing consent as valid whilst that supporter has an active relationship with us.

We communicate with supporters by post under the legal basis of Legitimate Interest, with our Impact Assessments documented and reviewed on at least an annual basis (see also section 4.7.4). We currently only make marketing calls to an individual where we have their consent, and so have no requirement to screen numbers against the Telephone Preference Service (TPS).

Staff who communicate externally with supporters and the general public (primarily staff in our Fundraising & Campaigns teams) will undergo additional training on the E-Privacy Directive and Applicable Local Legislation to understand the requirements of this legislation.

7 Roles & Responsibilities

All staff have a responsibility to ensure data protection compliance in their own area or work. The DPO leads on data protection matters across the organisation escalating to the Head of Digital and Technology as necessary who then advises on further escalation.

8 Training

AAI will make available a range of training resources for staff to use in data protection matters. All staff will undergo mandatory cyber security training upon induction, which outlines basic data protection requirements across AAI. Staff who communicate with the general public (primarily those in Fundraising & Campaigns teams) also have training on induction to outline specific Data Protection Legislation requirements given the day to day communication with people outside AAI.

This Data Protection Policy and our Compliance Manual are also provided to all staff at induction, with the external AAI Privacy Policy additional required reading for Fundraising & Campaigns staff.

The DPO leads on all training content and classroom sessions and provides additional face to face training for teams as required. The DPO may delegate training duties to another trained member of staff as necessary.

9 Implementation and monitoring

This policy will take effect from 31 December, 2020. AAI will aim to have put all necessary procedures in place prior to that date and will further provide on-going training to its staff to ensure effective implementation.
Implementing the policy will be the responsibility of all staff. Any failure of staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.
As a Data Controller, AAI is also required to ensure that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection Legislation. Failure of a Data Processor to manage AAI data in a compliant manner will be addressed directly with the supplier and may result in commercial or legal sanctions.
The Data Protection Officer will be required to monitor compliance with this policy on an ongoing basis. Some of this monitoring will be relatively informal, however it is expected that compliance with this policy will be formally reviewed

on a cyclical basis for all Personal Data holdings. For those holdings that are large, complex or where problems arise, they may be scheduled for more frequent review. The results of all formal compliance reviews will be documented. They will be reported as follows:

- In each individual case to the responsible Director and the International Leadership Team
- An annual summary to SMT and the Board (or the governing body that it delegates to review this area).

The Data Protection Officer will be provided with reasonable budgetary resources to secure such external support/expertise as may be necessary to adequately discharge responsibilities. AAI ensures Data Protection Officer does not receive any instructions regarding the exercise of his/her tasks and may directly report to the SMT and the Board where he/she deems this necessary at any time.

10 Updates and revisions to the policy

The Data Protection Officer's annual report on compliance to SMT and the Board will also consider whether policy revisions/adjustments are required. Any suggested amendments will be considered at the same time as the compliance review.

In the interim, revisions to the policy may be approved by SMT where they involve minor changes/clarifications or where they are required to give effect to changes in legal requirements.

All other revisions must be approved by the Board.

PAPER 11.

Appendix 2: Privacy Notice

ACTIONAID INTERNATIONAL

PRIVACY NOTICE

Policy Information

POLICY NAME:	DATA PRIVACY NOTICE
VERSION:	
APPLICABLE LEGISLATION:	EU GDPR 2016/679 (REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016 ON THE PROTECTION OF NATURAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, AND REPEALING DIRECTIVE 95/46/EC)) ("GDPR") and associated national legislation

Governance Information

Policy Owner	Head of Digital and Technology
Policy Sponsor	Resource Mobilisation and Innovation Director
Date Ratified by SLT	17th November, 2020
Date ratified by Board:	4th December, 2020
Date last updated	December, 2020
Date of next review	December, 2021

PAPER 11.

1. ActionAid International: who we are and what we do

ActionAid International is an international development organization working in 44 countries around the world to achieve social justice, gender equality and eradicate poverty. Our dedicated local staff work to help end violence against women and girls and changing lives, for good. At ActionAid International, everything we do is geared towards ensuring the rights and improving the lives of women and girls and the implementation of our international strategy which is action for global justice. We seek to develop a greater understanding of our supporters through their personal data in order to help us give them the best possible experience, fundraise more efficiently and help us change lives for good.

This policy applies to all the pages hosted on this site and other services ActionAid International runs. It does not apply to pages hosted by other ActionAid sites around the world, or to other organisations to which we may link and whose privacy policies may differ.

Please read the following policy to understand how your personal data will be treated. It may change from time to time, so please check back periodically.

2. Information on this Privacy Notice

This Privacy Notice, refers to your relationship with ActionAid International only and details why we collect your data, what data we collect, how we protect it and your rights.

Your personal data (such as your name and contact details, known as 'personal data') is protected by specific legislation:

- If you are in the European Union / European Economic Area:
  - General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and associated local laws
  - Directive on Privacy and Electronic Communications ("ePrivacy-Directive") and implementing local laws
- If you are in the United Kingdom:
  - The GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR");
  - The UK Data Protection Act 2018;
  - The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and other data protection or privacy legislation in force from time to time in the United Kingdom ("UK Data Protection Laws")

– In the following also referred to as "Applicable Data Protection Laws" –

The laws in this area continue to develop quickly. We take our responsibilities around data very seriously, and it's important to us that you understand how and why we ask for and work with your details. Your privacy is important to us and we have policies to ensure that we collect only the data that we need to carry out the work that we do, and that we don't keep it any longer than we need to. This policy explains how we collect, manage, use and protect your personal data, including how we work with third parties. We never sell or swap your details with any other organisation for their marketing purposes.

PAPER 11.

3. Contact details of our data protection officer

If you have any questions about this privacy notice or the processing of personal data by ActionAid in general you can contact our data protection officer. The contact details of our data protection officer are:

By Email at DPO.hellas@actionaid.org

By Post at Data Protection Team
ActionAid Hellas
204 Mesogeion Avenue
Zip code:15561
Athens
Greece

4. The information that we collect, how it is collected and used.

To comply with Applicable Data Protection Laws, we will always ensure we have legal justification for processing (e.g. collecting and using) your personal data. We will collect personal data about you in a number of ways:

Where you have provided your consent to allow us to use your data in a certain way;

When you support us by;

- Signing one of our petitions
- Signing up to make a donation to ActionAid International
- Engaging with our social media and digital advertising
- Joining our volunteer and activist communities

As well as

- When you apply for a job at ActionAid International
- When you visit our website
- When you contact our Supporter Care team

To comply with data protection rules, we will always ensure we have legal justification for collecting and using your personal information.

The legal justification (also called "legal basis") that we rely on will depend upon the circumstances in which we process your personal data. Our processing of your personal data will fall into one of the following categories:

- Where you have provided your consent to allow us to use your data in a certain way.
- Where it is necessary for us to process your data in order to comply with a legal obligation.
- Where it is in our legitimate interests, for example to contact you in order to raise funds and achieve our campaign objectives. Where we rely on a legitimate interest to use your information, we will always ensure that this is done in a way so as not to be intrusive or cause distress, and that respects your rights by conducting a Legitimate Interest Assessment beforehand.
- Where it is necessary for us to process your data in order to carry out the performance of a contract with you.

Where a legal basis is relevant which is not listed here, we will expressly refer to it at the appropriate section in this Privacy Notice.

4.1 People who support us

There are a number of ways that we collect information; most often this will be directly from you, for example, if we are collecting data on our field visits, if you fill out a form on our website, or directly with one of our fundraisers. Whenever

we ask for information from you, we will explain why we are asking for it (including by reference to this policy), and you will always be given a choice about how we communicate with you.

In some very specific circumstances, we will gather data from publicly available sources. We use data from third parties to keep our records up to date, (from within the Federation) or to enhance the information that we hold.

We do not buy lists of data to use for our marketing purposes or share data with other charities for them to use in their marketing purposes.

4.1.1 How we collect your data

ActionAid International obtains personal data from you when you support a campaign, engage with our social media and digital advertising or make a donation.

In most circumstances, we will only ask for your name and contact details (plus payment details if you are joining or donating). Sometimes we may ask for additional information where it may either help us in our campaigns or help us keep our communications relevant to you. We may occasionally supplement your data with other publicly and commercially available information where it meets Applicable Data Protection standards. We may store relevant information about you that you voluntarily share with us.

We will only collect sensitive personal data where absolutely necessary and with your explicit consent.

4.1.2 Call recording data

ActionAid International has a telephone call recording system in operation and may record both outgoing and incoming telephone calls from and to our Supporter Services team. An 'incoming call' is a call received by us, and an 'outgoing call' is a call made by us. We record calls for quality and training purposes so that we can make sure we are dealing with your questions in the best way that we can.

When we make outgoing calls, we will ask for your consent before making a recording and will only make such a recording with your consent. For incoming calls, due to the volume of calls we receive, we will make an announcement around the recording of calls before the call begins.

Incoming calls are recorded under the legal basis of legitimate interest; we have a legitimate in improving the quality of calls with our Support Services team. If you would prefer for your call not to be recorded, you may state this at any time during the call and we will stop the recording immediately.

Call recordings will be retained in line with our Retention Policy and deleted once they fall outside time limits determined in this policy. Call recording data will be stored securely and in an encrypted manner within the UK.

4.1.3 How we use your data

ActionAid uses the supporters' personal data in a variety of ways which include the following:

- Providing you with information or products that you have requested from us.
- Providing you with information that is relevant to your interests.
- Processing donations and joining fees received from you.
- Making enquiries or informing you about your interactions with us (e.g. resolving issues with Direct Debits or informing you of changes to events).
- Responding to any complaints from you.
- Offering you ways to fund our work.
- Inviting you to campaign with us.

- Keeping you updated on our campaigning work.
- Informing you of volunteering opportunities.
- Inviting you to participate in surveys or research.
- Reviewing records such as for financial audits.
- Compliance with applicable statutory retention periods (e.g. resulting from tax laws).
- Analysing and refining our advertising, campaigning and other operations to increase our effectiveness.
- Monitoring your information to prevent fraud.
- Working with authorities in cases of fraud or criminal investigations.
- Establish or exercise our legal rights or defend against legal claims.

Where a purpose for processing is relevant which is not listed here, we will expressly refer to it at the appropriate section in this Privacy Notice.

4.2 Job Applicants

If you apply for a job on our careers site your personal data will be collected and processed by ActionAid International and our Recruitment Software Provider.

We will collect a range of information about you, including:

- Your name, address and contact details, including email address and telephone number.
- Details of your qualifications, skills, experience and employment history
- Whether or not you have a disability for which we need to make reasonable adjustments during the recruitment process.
- Information about your entitlement to work in any of our offices.
- Equal opportunities monitoring information, including information about your ethnicity, sexual orientation, health, and religion or belief. We will only collect this sensitive information with your explicit consent, which can be withdrawn at any time. We keep this information separate from your application.

We initially rely on your consent to process your information as a job candidate. Your information will not be used for any purpose other than processing and managing your job application, and for internal reporting on our recruitment processes. Only people involved in the recruitment process for the role you apply for will have access to your personal data.

Personal information about unsuccessful candidates will be held for one year after the recruitment exercise has been completed and will then be destroyed. We retain de-personalised statistical information about applicants to help inform our recruitment activities, but no individuals are identifiable from that data.

If you are successful in your application, our use of your data will be set out in our policies for ActionAid International Staff.

4.3 Cookies

Like most websites, the ActionAid International site uses cookies; small data files that are downloaded when you use a website, to make the site easier to use. The information that is gathered helps us to see how people use our site, so that we can provide a better user experience.

Cookies are small text files that are placed on your computer or other mobile or handheld device (such as smartphones or tablets) when you visit certain pages on the internet. They are used to ‘remember’ when your computer or device accesses our website. Cookies are stored in your browser. The cookie will help us, or another website, to recognise

your device the next time you visit. Most cookies won't collect information that identifies you as a person (personal data),and will instead collect more general information such as how visitors arrive at and use our website.

4.3.1 Types of cookies

- Session cookies: Session cookies are stored only temporarily during a browsing session and are deleted from the visitor's device when the browser is closed.

- Persistent cookies: This type of cookie is saved on your computer for a fixed pre-defined period of time (usually a couple of months) and is not deleted when the browser is closed. Persistent cookies are used where we need to be able to recognise your device for more than one browsing session. Persistent cookies used on this website have a maximum storage period of twelve months, please see below for further details.

- First party cookies: First party cookies are set by the website you are visiting and they can only be read by that site.

- Third party cookies: Third party cookies are set by a different organisation than the owner of the website you are visiting. For example, advertisers and other third parties may use their own cookies when you click on an advertisement or link on our website or we might engage a third party analytics company who will set their own cookie to perform this service. The website you are visiting may also contain content embedded from, for example, YouTube or Twitter, and these sites may set their own cookies.

4.3.2 Categories of cookies

The different types of cookies set out above (section 4.3.1) can be further categorized as follows:

- Strictly necessary cookies:

  These cookies are necessary for the website to function and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as setting your privacy preferences. You can set your browser to block or alert you about these cookies, but some parts of the site might not work then. These cookies do generally not store any personally identifiable information.

- Performance or analytics cookies:

  These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us to know which pages are the most and least popular and see how visitors move around the site and gather information on error messages. All information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies we will not know when you have visited our site, and will not be able to monitor its performance.

- Functional cookies:

  These cookies enable the website to provide enhanced functionality and personalisation. They may be set by us or by third party providers whose services we have added to our pages. If you do not allow these cookies then some or all of these services may not function properly.

- Targeting cookies:

  These cookies record your visit to our website, the pages you have visited and the links you have followed. We will use this information to make our website and the advertising displayed on it more relevant to your interests. We may also share this information with third parties for this purpose. These cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites. They do not store personal data, but are based on

uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

4.3.3 How we use cookies on our website

We will use cookies which are not strictly necessary cookies only based on your consent. You may choose to withdraw given consent at any time without affecting the lawfulness of the use of cookies based on consent before its withdrawal. You can withdraw consent here.

ActionAid International uses cookies to ensure your privacy and security when you visit secure areas of our website, such as donation pages and registration forms.

ActionAid will also collect information such as your Internet Protocol (IP) address for monitoring and improving the effectiveness of our website services (legal basis: legitimate interests in improving our services) as well its security (legal basis: legitimate interests in ensuring security of our website services).

A complete list of the cookies we use can be found below in section 4.3.7.

4.3.4 Third party cookies on our website

ActionAid International uses Google Analytics to compile statistics on how our website is being used, which can help us to improve our website and online services.

Our website also uses Google Analytics advertising features to enable us to better understand the interests of our audience and to tailor our communications to be more relevant to you.

If you do not wish to see these adverts, you can:

- opt out of Google's use of cookies through Google's Ads Settings
- refuse the use of cookies by downloading and installing Google Analytics Opt-out Browser Add-on.

4.3.5 Controlling your cookie preferences

All Internet browsers allow you to control which cookies you accept and which you delete. For more information about cookies, please see www.allaboutcookies.org.

4.3.6 Third party cookies and our social media and web advertising

You may also see our advertising online and on some social media sites if you have supported us before, or if your use of these channels suggests that you would find our campaigns relevant.

We use cookies to ensure that any investments we make in online advertising are as cost-effective as possible, by tracking how well individual adverts perform. These cookies are issued by third party service providers that we have assessed as secure.

If you do not wish to see these adverts, you can do so by managing the privacy settings on your social media accounts including Facebook, Instagram and Twitter

Depending on your settings or the privacy policies for social media and messaging services, you may have given these services permission to share your details with us. For example, if choosing to register for an activity using a 'Sign up with Facebook' link, Facebook may share information such as your name and email address with us.

Our Social Media Pages such as Facebook, Instagram and Twitter may also use 'live chat' services to allow ActionAid International representatives to offer you assistance or the opportunity to engage with us in a manner relevant to you.

PAPER 11.

These services may involve the use of cookies and the transfer of information about your site navigation, such as your IP address, to secure networks for the purposes of storage and analysis. This information will only be used for the purposes of administering these live chats.

ActionAid International does not perform direct marketing with any data that they collect from you.

4.3.7 List of the cookies in use

Name	Category	Purpose	Third party provider	Retention term
ga	Performance or Analytics cookie	used to analyse how visitors interact with our website so we can improve functionality and the visitor experience	Google LLC; 1600 Amphitheatre Parkway in Mountain View, California, United States	30 days

5. How your Data is kept secure.

5.1 What ActionAid International does to keep your data secure

ActionAid International (also "AAI") uses industry-standard tools to safeguard the confidentiality of your personal data. We make every effort to protect against the loss, misuse and alteration of the information under our control. ActionAid International takes the care of your data very seriously and we use a combination of organisational and technological security measures to protect your personal data to the highest possible standards. This includes the use of secure servers, firewalls, virus & malware protection, secure socket layer (SSL) encryption and secure file transfer protocol for our work with third parties. We follow payment card industry (PCI) security compliance guidelines when processing credit card payments.

Access to all ActionAid International data is protected by complex passwords, including letters, numbers and characters: in some cases, more than one method of authentication is used. We make sure that only staff that need to access your personal data can do so. Any member of our staff who has access to your personal data is given training to make sure that they understand the importance of keeping your information safe and secure at all times.

We always use a secure connection when collecting personal financial information from you and conform to PCI standards. All forms which request credit card or bank details use Secure Sockets Layers (a security protocol that provides communications privacy over the Internet in a way that is designed to prevent eavesdropping, tampering, or message forgery) for encryption. Most web browsers support Secure Socket Layers.

The link between your web browser and the server is secure if your web browser displays a small padlock or key symbol somewhere in the frame, or the address bar shows a web address beginning https:// (rather than http://)

We endeavour to keep all supporter data inside the European Economic Area (EEA), and ensure that any time data is transferred outside the EEA appropriate safeguards on data security and processing are applied.

5.2 Who has access to your data?

- Within ActionAid International

Within ActionAid International, only those authorised to process your data can access your data. We work hard to ensure our staff and volunteers can only see the data they need to perform their tasks. Our staff are trained to understand Applicable Data Protection Law requirements and what they need to do to keep your data secure. We review our data awareness training regularly to ensure it is up to date. We ensure volunteers are given appropriate data awareness and protection training where they are responsible for handling data, for example, if they are collecting petition signatures at an event.

- Working with Third Parties

We will never sell or swap your details with other organisations

We do use trusted companies like fundraising agencies, fulfilment houses and software platform providers to administer some activities, in which case they will use your details only for that purpose – for example, applying your name and address to a mailing of Connect magazine. In this case, we will ensure appropriate contracts are in place with the third party service provider.

Where possible, we transfer your personal data to service providers which have been engaged by us as so-called data processors that process your personal data only on our behalf and in accordance with our instructions. Furthermore, we may transfer your data to the following categories of third parties:

- Fundraising agencies
- Consultants (auditors, lawyers)
- Governmental authorities
- Courts

5.3 Data Retention

Data collected by ActionAid International will be retained only for an appropriate length of time; we have a data retention policy which sets out how long we will keep information according to the type of record. In some cases, the retention periods are governed by law, while in others we are guided by best practice and our operational needs.
When we no longer need to retain your personal data, we will ensure it is securely disposed of.
You have the right to ask us to delete personal data we hold about you in some circumstances, for example, if we are processing the data on the basis of consent and you wish to withdraw that consent.

6. Understanding your rights

PAPER 11.

It is important that you understand your legal rights around your personal data and how we may use it. If you would like to discuss or exercise any of these rights, please do get in touch with our Data Protection Team using the contact details at the end of this notice.

- Right of access: You have a right to ask for a copy of the information we hold about you, which we will supply to you within one month. We will ask for proof of identity and may charge a fee should any request be unusually complex or time-consuming. If you would like to request a copy of the personal information ActionAid holds on you, please contact our DPO.
- Right to withdraw consent: Where the processing is based on consent, you have the right to withdraw your consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
- Right to rectification: You have the right to request correction of personal data related to you that is inaccurate and/or completion of such data which is incomplete.
- Right to erasure: You have the right to request the deletion of your personal data in certain circumstances, including where (i) it is no longer necessary in relation to the purposes for which it was collected or otherwise processed, (ii) you objected to the processing and there are no overriding legitimate interests for processing, (iii) your personal data has been unlawfully processed or (iv) your personal data has to be erased for compliance with a legal obligation to which ActionAid is subject. You should know that there are some circumstances where we may need to keep your details nonetheless, for example, if it is necessary to comply with a legal obligation to which we are subject or for the establishment, exercise or defense of legal claims. If this situation occurs, then we will explain and discuss these circumstances with you.
- Restriction of processing: You have the right to restrict our processing of your data if there is disagreement about its accuracy or legitimate usage.
- Right to not be subject to a decision based solely on automated processing: You have rights to avoid being subject to decisions based solely on automated processing (including profiling) which has a significant effect on you. At ActionAid International we do not carry out any such processing.
- Right to data portability: You have the right to receive personal data concerning you in a structured, commonly used machine-readable format and transmit those data to another controller without hindrance from ActionAid, where the processing is based on consent or a contract and the processing is carried out by automated means; you may also request to have your personal data transmitted directly to another controller where this is technically feasible.
- You also have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, place of work or place of an alleged infringement if you consider that the processing of personal data relating to you infringes the GDPR

- Right to object:

Right to object
You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you which is based on legitimate interests of the ActionAid or third parties. We then will no longer process your personal data unless we are able to demonstrate compelling legitimate grounds for the processing which override your interests, rights, and freedoms or for the establishment, exercise or defense of legal claims.

You should know that there are some circumstances where these rights may not apply, but where this is the case, we will always explain this to you. Please do contact us if you have any questions or concerns on how we collect and use your personal data, or on your rights, as we are always happy to speak to you.

PAPER 11.

7. Where we keep your information and when it might be transferred outside of Europe

ActionAid International is aware that countries outside of the European Economic Area have differing standards of data privacy. You also need to be aware that we work with members in the federation that are located outside the EEA and your data may be shared with them under certain circumstances.

There is an inter-group data transfer agreement that has been signed by the members of the federation that governs data sharing across the federation.

Some countries (but not every country in which we work) have been determined by the European Commission to have "adequate" standards of data protection compliance. Organisations we work with who process data in the USA have verified that their data processing standards meet the standards in the EU-US Privacy Shield, which sets out clear safeguards and transparency responsibilities for US-based organisations processing data from EU citizens, or that they otherwise have proper safeguards in place.

Your data may leave the European Economic Area if you travel with us, for example by signing up to one of our first-hand experiences, or volunteering trips. This will only be information specifically related to your trip, for example to book your travel, or to arrange your visit to one of our sites with our overseas colleagues.

8. How AAI protects children's privacy

The safety of children is very important to us. If you are aged under 16 and would like to support or get involved with ActionAid International, please make sure you have your parent/guardian's permission before sharing any personal data with us.

All applicable laws are followed with respect to data collection from children. Where we have date of birth information, we will not share data collected from children with any third parties at any time under any circumstances.

9. People in vulnerable circumstances

ActionAid International recognises the importance of protecting people in vulnerable circumstances. We do have in place strict SHEA and Safeguarding policies which supports our staff and volunteers to safeguard the privacy of people in vulnerable circumstances.

10. How to find out more or make a complaint

ActionAid International operates in accordance with all relevant GDPR legislation. If you would like to find out more about these laws and how you could be affected beyond this policy, more information can be found here
If you have any specific questions about how ActionAid International processes your data which are not answered here or you would like to make a complaint about how we have managed your data then please either write, call or email us via the details below.

By Email at DPO.hellas@actionaid.org
By Phone on +30 21 2000 6416
By Post at Data Protection Team
ActionAid Hellas
204 Mesogeion
Avenue
Zip code:15561
Athens
Greece

PAPER 11.

11. Changes to this Notice

From time to time, we may make changes to this Notice and you will always be able to see here when it was last updated. If we make significant changes, such as in how or why we process your personal data, we will also publicise these changes on our website or may contact you directly with more information.

Please do revisit this notice each time you consider giving your personal data to ActionAid International.

The last significant updates to this policy were in December 2020.

Appendix 3: Data Breach Policy

ACTIONAID INTERNATIONAL

DATA BREACH POLICY

Policy Information

POLICY NAME:	DATA BREACH POLICY
VERSION:	
APPLICABLE DATA PROTECTION LEGISLATION:	EU GDPR 2016/679 (REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016 ON THE PROTECTION OF NATURAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, AND REPEALING DIRECTIVE 95/46/EC) ("GDPR") AND ASSOCIATED NATIONAL LEGISLATION

Governance Information

Policy Owner	Head of Digital and Technology
Policy Sponsor	Resource Mobilisation and Innovation Director
Date Ratified by SLT	17th November, 2020
Date ratified by Board:	4th December, 2020
Date last updated	December,2020
Date of next review	December, 2021

INTRODUCTION

ActionAid International (hereinafter referred to as AAI) are committed to our obligations under the regulatory system and in accordance with the Applicable Data Protection Legislation. While we do have policies in place that ensure

security of the personal data we hold, we recognise that breaches can occur, hence this policy outlining the way such incidents are to be dealt with.
Under the Applicable Data Protection Legislation, certain personal data breaches must be notified to the Supervisory Authority and sometimes affected data subjects need to be told too. The purpose of this policy is to outline the internal breach reporting procedure of AAI and our internal and external response plan and it should be read in conjunction with our data protection policy.

The protection and security of the personal data that we process is of paramount importance to us and we have developed data specific protocols for any breaches relating to Applicable Data Protection Legislation.

Scope

This policy applies to all staff within AAI (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Organisation). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

The ActionAid International Data Protection Officer has overall responsibility for the day-to-day implementation of this policy.

What constitutes a personal data breach?

A personal data breach is a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".
A breach is therefore a type of security incident and there are three different types of breach that may occur:

- Confidentiality breach – an accidental or unauthorised disclosure of, or access to, personal data.
- Availability breach – an accidental or unauthorised loss of access to, or destruction of, personal data.
- Integrity breach – an accidental or unauthorised alteration of personal data.

A breach can concern confidentiality, availability and integrity of personal data at the same time, as well as any combination of these.
A personal data breach would, for example, include:

- personal data being disclosed to an unauthorised person, e.g. an email containing personal data being sent to the wrong person.
- an unauthorised person accessing personal data, e.g. an employee's personnel file being inappropriately accessed by another member of staff due to a lack of appropriate internal controls.
- a temporary or permanent loss of access to personal data, e.g. where a client's or customer's personal data is unavailable for a certain period of time due to a power, hardware or software failure, infection by ransomware or viruses or denial of service attack, where personal data has been deleted either accidentally due to human error or by an unauthorised person or where the decryption key for securely encrypted data has been lost.

This list is not exhaustive.

The local offices across the various jurisdictions in which AAI operates will be required to make reasonable security arrangements to protect the personal data that we possess or control, to prevent unauthorized access, collection, use, disclosure, or similar risks.

PAPER 11.

Data Security & Breach Requirements

As above, AAI'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.

Alongside our 'Privacy by Design' approach to protecting data, we also have a legal, regulatory and a surpassing moral obligation to ensure that personal information is protected whilst being processed by AAI. Our technical and organisational measures are detailed in our [Data Protection Policy and Information Security Policies].

We will periodically carry out information audits to ensure that all personal data processed by us is adequately and accurately identified, assessed, classified and recorded. We carry out risk assessments that assess the scope and impact of any potential data breach; both on the processing activity and the data subject. We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate to the risks which can be found in the [Data Protection Policy]

Data Breach Procedures & Guidelines

AAI has 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. The documented breach incident policy aims to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

Breach Monitoring & Reporting

The organisation has 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 to ensure that gap and pattern analysis are available and used. Where a system or process failure has given rise to a data breach, revision to any such process is recorded in the Change Management and Document Control records.

Breach Incident Procedures

Identification of an Incident

As soon as a data breach has been identified, it should be reported to the direct line manager and 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 AAI to enable the organisation to fulfil its reporting requirements under Applicable Data Protection Legislation. These procedures are thus for the protection of the organisation, its employees' and various stakeholders 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. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measures should be to stop any further risk/breach to the organisation, customer, client, third-party, system or data prior to investigation and reporting. The measures taken are noted on the incident form in all cases.

Breach Recording

The Organisation utilises a [Breach Incident Form] for all incidents, which is completed for any data breach, regardless of severity or outcome. Brief details of the breach should be recorded by the staff member who identified the breach.

Thereafter, completed forms are logged by the Data Protection Officer and will be reviewed periodically against existing records to ascertain patterns or reoccurrences.
In cases of data breaches, the Data Protection Officer is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, 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 staff involved in the breach, in addition to senior management. A copy of the completed incident form is filed for audit and documentation purposes.
If applicable, the Supervisory Authority and the data subject(s) are notified in accordance with the Applicable Data Protection Legislation requirements (refer to section 6 of this policy). 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 a system error/failure, the IT team are to work in conjunction with the Data Protection Officer to assess the risk and investigate the root cause of the breach. A gap analysis is to be completed on the system/s involved and a full review and report to be added to the Breach Incident Form.
A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed in accordance with the organisation's Risk Assessment Procedures. 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 employee 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 the Organisation's disciplinary procedures)

System Error

Where the data breach is the result of a system error/failure, the IT team are to work in conjunction with the Data Protection Officer to assess the risk and investigate the root cause of the breach. A gap analysis is to be completed on the system/s involved and a full review and report to be added to the Breach Incident Form.
Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause. Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident: -

- Attempting to recover any lost equipment or personal information
- Shutting down an IT system
- Removing an employee from their tasks
- The use of back-ups to restore lost, damaged or stolen information

- Making the building secure
- If the incident involves any entry codes or passwords, then these codes must be changed immediately and members of staff informed

Assessment of Risk and Investigation

The Data Protection Officer 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.

In the process of conducting an assessment, the following should be considered;

- 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

An ongoing log and clearly reporting and detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions will be maintained.

Breach Notifications

AAI recognises our obligation and duty to report data breaches in certain instances. All staff will be made aware of the Organisation's responsibilities and the strict internal reporting lines that are in place to ensure that data breaches falling within the notification criteria are identified and reported without delay.
Not all personal data breaches have to be notified to the Supervisory Authority. The breach will not need to be notified if it is unlikely to result in a risk to the rights and freedoms of data subjects, and this needs to be assessed by the Organisation on a case-by-case basis. A breach is not unlikely to result in a risk to the rights and freedoms of data subjects if, for example, it could result in:

i. loss of control over their data
ii. limitation of their rights
iii. physical harm to employees, beneficiaries and donors.
iv. discrimination
v. identity theft
vi. fraud
vii. damage to reputation
viii. financial loss
ix. unauthorised reversal of pseudonymisation
x. loss of confidentiality
xi. any other significant economic or social disadvantage

Supervisory Authority Notification

Where applicable, the Supervisory Authority is notified of the breach without undue delay, no later than 72 hours after the organisation becoming 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 Data Protection Officer 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 Applicable Data Protection Legislation.
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 (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)

Breach incident procedures are always followed and an investigation carried out, regardless of our notification obligations and outcomes, with reports being retained and made available to the Supervisory Authority if requested.
Where the organisation acts in the capacity of a data processor, we will ensure that controller is notified of the breach without undue delay. In instances where we act in the capacity of a data controller using an external processor, we have an agreement in place to state that the processor is obligated to notify us without delay after becoming aware of a personal data breach.

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 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, in compliance with Applicable Data Protection Legislation.

PAPER 11.

Record Keeping

AAI will maintain a register of all personal data breaches, regardless of whether or not they are notifiable to the Supervisory Authority. The register will include a record of:

- the facts relating to the breach, including the cause of the breach, what happened and what personal data were affected;
- the effects of the breach
- the remedial action we have taken
- documentation of the risk assessment carried out in order to ascertain whether breach notifications are necessary.

Responsibilities

The Organisation 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 and the breach incident reporting lines.

The Data Protection Officer is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups. There is a continuous audit trail of all compliance reviews and procedural amendments and feedback to ensure continuity through each process and task.

PAPER 11.

APPENDIX 4: Data Retention and Erasure Policy

ACTIONAID INTERNATIONAL

DATA RETENTION AND ERASURE POLICY

Policy Information

POLICY NAME:	DATA RETENTION AND ERASURE POLICY
VERSION:	1.0
APPLICABLE DATA PROTECTION LEGISLATION:	EU GDPR 2016/679 (REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016 ON THE PROTECTION OF NATURAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, AND REPEALING DIRECTIVE 95/46/EC) ("GDPR") AND ASSOCIATED NATIONAL LEGISLATION – ALL TOGETHER "APPLICABLE DATA PROTECTION LEGISLATION"

Governance Information

Policy Owner	Head of Digital and Technology
Policy Sponsor	Resource Mobilisation and Innovation Director
Date Ratified by SLT	17th November, 2020
Date ratified by Board:	4th December, 2020
Date last updated	December 2020
Date of next review	December, 2021

Table of Contents

1 Policy Statement

2 Policy Scope

3 Policy References

4 Principles of Data Retention

4.1 Retention Schedule

4.2 Retention Safeguarding

4.3 Data Destruction

4.4 Breach and Enforcement of Policy

5 Document Management

6 Policy Review

7 Data Retention and Erasure Schedule

7.1 Financial Records

7.2 Business Records

PAPER 11.

7.3 HR: Employee Records

7.4 Contracts

7.5 Beneficiary Data

7.6 Supporter Data

7.7 IT

7.8 Programmes and Projects

7.9 Miscellaneous

1 Policy Statement

ActionAid International ("AAI") needs to collect personal information to effectively carry out its everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from Beneficiaries, Donors, Partners, Suppliers and Employees and includes (but is not limited to), name, address, email address, data of birth, IP address, identification numbers, private and confidential information, sensitive data and bank/credit card details.

This policy also serves as a reference document for employees and third parties that create, collect, use, store or dispose of Personal data on behalf of ActionAid International and it is their responsibility to familiarise themselves with this Policy and ensure adequate compliance with it.

The purpose of this policy is to provide AAI's statement of intent on how it provides a structured and compliant data and records management system. It further serves to ensure that all AAI staff and partners understand and are aware of their responsibilities to meet our legal, statutory and regulatory requirements under the data protection laws in relation to the retention and erasure of personal data.

This Data Retention Policy and the Schedule sets the guidelines and retention periods for the specified categories of personal data that we process and sets out the minimum standards to be applied when destroying certain information within ActionAid International. Information held for longer than necessary carries additional risk and cost and can infringe data protection rules and principles. AAI strives to only ever retain records and information for legal business reasons and to always comply fully with the data protection laws, guidance and best practices.

2 Policy Scope

This policy covers the work of ActionAid International and the Country Programme Offices it is accountable for and their staff (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents) that may collect, process, or have access to data (including both personal and sensitive data). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

This policy applies to all personal information.

Examples of documents/media include:

- Emails
- Hard copy documents both originals and copies
- Soft copy documents both originals and copies
- Photographs, Video and audio

- Database Records
- Web Pages
- Social Media
- Business Applications

This policy also covers, but not restricted to personal data held on:

- Work Laptops
- Work Desktops
- Back-up Devices
- Mobile Phones
- Memory Cards/Sticks
- Shared Drives
- Cloud Services
- Data Servers/File Servers and
- data stored in archive, both on-premises and with off-site service providers

3 Policy References

- ActionAid International Data Protection Policy
- ActionAid International Privacy Notice

4 Principles of Data Retention

AAI's principles of data retention comply fully with the fifth principle in Article 5 of the General Data Protection Regulation[5]. This principle speaks to the fact that data should not be stored for no longer than is necessary for the purposes for which the personal data is processed.

Accordingly, in order to satisfy legal obligations in relation to storage limitation, there is a need to ensure that certain data records are retained for a specific length of time. Furthermore, that where such data is no longer in use or required to be kept for a specific purpose then the organisation should either delete it altogether or anonymize all parts of the information that would give away the identity of the individual. By dealing with data in this way Action Aid is are adhering to the organisational and technical safeguards stipulated by the GDPR.

5 Retention guidelines

- Records must be periodically reviewed to ensure that the information contained is accurate and up to date.

- In the event that data is no longer in use or required to be kept for a specific purpose then it should either be deleted altogether or all parts of the information that would give away the identity of the individual should be anonymised. By dealing with data in this way you are adhering to the organisational and technical safeguards stipulated by the GDPR.

6 Retention Schedule

The Data Protection Officer controls the time period for which the documents and electronic records should be retained through the Data Retention Schedule, in line with appropriate legal obligations and operational objectives.

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=DE. /.

PAPER 11.

By exception under GDPR guidelines, retention periods stated within the Schedule can only be extended in the following circumstances:

- Ongoing investigations from Member State authorities, if there is a chance records of personal data are needed by the Organisation to demonstrate compliance with any legal requirements; or
- When exercising legal rights or protecting the organisation in cases of lawsuits or similar court proceeding recognized under local law.

For any category of documents not specifically defined within this Policy or the Data Retention Schedule and unless otherwise mandated by applicable data protection law or other local laws, the retention period set by ActionAid International is 3 years from the date the document was created.

Overall responsibility for the auditing of the destruction of data falls to the Data Protection Officer.

7 Retention Safeguarding

If electronic storage media are chosen for the archiving of personal data, any information in relation to procedures and systems ensuring that the data can be accessed to the extent necessary and with sufficient logging procedures in place during the retention period shall also be stored in order to safeguard the data against loss as a result of future technological changes.

If any data is stored by a 3rd party processor, for example a cloud service provider, any SLAs or Data Processor agreements should reference the archived data and should detail both the procedures for recovering such archived data as well as the strict access controls to be implemented.

The responsibility for the storage falls to the Data Protection Officer.

8 Data Destruction

All data should be regularly reviewed to decide whether the purpose for which the documents were created is no longer relevant, in which event the said data should be disposed of.

Once the decision is made to dispose according to the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their level of confidentiality as detailed in the Retention Schedule.

It is the responsibility of employees to perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the Data Protection Officer subcontracts for this purpose.

The Data Protection Officer shall fully document and approve the destruction process in line with the applicable statutory requirements.

Important Notice - All permitted document destruction should cease immediately if ActionAid International (or any other Member Organisation within the Federation) is being investigated by a governmental law enforcement agency including any of the Data Protection Supervisory Authorities and should not resume without authorisation from the ActionAid International Data Protection Officer.

PAPER 11.

9 Breach and Enforcement of Policy

The Data Protection Officer has the responsibility to ensure that each of the ActionAid International offices and those of the Country Programmes complies with this Policy. It is also the responsibility of the Data Protection Officer to assist any local office with enquiries from any local data protection or governmental authority.

Any suspicion of a breach of this Policy must be reported immediately to Data Protection Officer. All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate.

Failure to comply with this Policy could have a major impact on the work of ActionAid International through damage to the Organisation's reputation and financial penalties.

Non-compliance with this Policy by permanent, temporary or contract employees, or any third parties, who have been granted access to Company premises or information, may result in disciplinary proceedings and could lead to legal action against the parties involved.

10 ERASURE

In specific circumstances, data subjects' have the right to request that their personal data is erased. However, AAI recognises that this is not an absolute 'right to be forgotten'. Data subjects only have a right to have personal data erased and to prevent processing if one of the below conditions applies:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent on which the processing is based, and where there is no other legal ground for the processing
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data must be erased in order to comply with a legal obligation to which AAI is subject
- The personal data have been collected in relation to the offer of information society services to a child

Where one of the above conditions applies and a request to erase data has been received, we first ensure that no other legal obligation or legitimate interest applies, in particular that processing is not necessary for compliance with a legal obligation or for the establishment, exercise or defense of legal claims. If we are confident that the data subject has the right to have their data erased, this is carried out under instruction by the Data Protection Officer in conjunction with any department manager and the IT team to ensure that all data relating to that individual has been erased.

These measures enable us to comply with a data subject's right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing. Whilst our standard procedures already remove data that is no longer necessary, we still follow a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

Where we receive a request to erase and/or remove personal information from a data subject, the below process is followed:

1. The request is allocated to the Data Protection Officer and recorded on the Erasure Request Register

2. The Data Protection Officer locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
3. The request is reviewed to ensure it complies with one or more of the grounds for erasure: -
    i. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
    ii. the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing
    iii. the data subject objects to the processing and there are no overriding legitimate grounds for the processing
    iv. the personal data has been unlawfully processed
    v. the personal data must be erased for compliance with a legal obligation
    vi. the personal data has been collected in relation to the offer of information society services to a child
4. If the erasure request complies with one of the above grounds and processing is not necessary for compliance with a legal obligation or for the establishment, exercise or defense of legal claims, it is erased without undue delay and in any case within 30 days of the request being received
5. The Data Protection Officer writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure
6. Where AAI has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

If for any reason, we are unable to act in response to a request for erasure, we always provide a written (including in electronic form) explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy. Such refusals to erase data include:

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defense of legal claims

11 Document Management

Each team within the scope of this policy is required to have in place a set of adequate procedures to ensure that their activities are fully documented and that information within the team is easily and readily accessible. It is recommended that teams set an individual with the responsibility to ensure that data is managed according to the guidelines within this policy.

The following should be considered:

- Any non-electronic data/manual documents are secured safely but in a manner that means they can be retrieved quickly and efficiently.
- Documents should be filed and indexed following guidelines for titling and version control and in accordance with the AAI IT Policies, and where appropriate security marking and access controls. See the AAI IT Policy.
- Documents should be kept up to date and accurate

- Any paper documents are adequately cross referenced to electronic records
- Adequate secure storage is available for non-electronic records
- Any movement and locations of records are tracked and monitored to provide an audit trail
- Ensure there is adequate recovery planning
- Documents are disposed of according to this schedule

12 Policy Review

This data retention policy and the schedule will be reviewed bi-annually. However, it is the responsibility of all staff to ensure that this document is always as accurate as possible, and if any discrepancies or inaccuracies are noted, staff should please inform the Data Protection Officer.

PAPER 11.

13 Data Retention and Erasure Schedule

14 Financial Records

Personal data record category	Location	Retention period	Disposal Method	Owner
Payroll records		Seven years after audit		Finance
Supplier contracts		Seven years after terminated		Finance
Chart of Accounts		Permanent		Finance
Financial Policies and Procedures		Permanent		Finance
Audits Results and Recommendations		Permanent		Finance
Financial statements		Permanent		Finance
General Ledger including A/P and A/R		10 years		Finance
Investment records (deposits, earnings, withdrawals)		10 years		Finance
Invoices A/R and A/P		10 years		Finance
Cash Books		10 Years		Finance
Cancelled cheques for important payments like taxes, property. Checks should be filed with transaction paperwork		Permanent		Finance
Cancelled cheques other		10 years		Finance
Bank deposit slips and Statements		10 years		Finance
Leases		10 years after expiration		Finance
Business expenses documents		10 years		Finance
Cheque registers/books		10 years		Finance
Property/asset inventories		10 years		Finance
Credit card receipts		3 years		Finance
Petty cash receipts/documents		3 years		Finance
General Correspondence		3 years		Finance
Legal Correspondence		Permanent		Finance
Expense Claims including per diems and supporting evidence		10 Years (non-relevant personal data should be redacted from supporting evidence at time of claim)		Finance
Insurance Policies and associated records like claims		Permanent		Finance
Journals		10 years		Finance
Purchase Orders		3 years		Finance
Scrap and disposal records		10 years		Finance
Tax Returns and supporting documents		Permanent		Finance
Asset registers		10 years after disposal of asset		Finance
Miscellaneous Internal Reports		3 years		Finance

PAPER 11.

15 Business Records

Personal data record category	Location	Retention period	Disposal Method	Record owner
Article of Incorporation registration		Permanent		Finance
Board policies		Permanent		Finance
Charity Registration		Permanent		Finance
Board meeting minutes (International and Assembly)		Permanent		Finance
Fundraising Certification and other memberships		Permanent		Finance
Office and team meeting minutes		Permanent		Finance
Annual filings		Permanent		Finance
Vat Exemption certificates		Permanent		Finance
Tax Exemption certificates		Permanent		Finance

16 HR: Employee Records

Personal data record category	Location	Retention period	Disposal Method	Record owner
Disciplinary, grievance proceedings records, oral/verbal, written, final warnings, appeals		As per legal requirement		HR
Applications for jobs, CV, interview notes Recruitment/promotion panel Internal. • Where the candidate is unsuccessful • Where the candidate is successful		Deleted immediately Duration of employment		HR
Payroll input forms, wages/salary records, overtime/bonus payments Payroll sheets, copies		10 years		HR
Bank details – current		Duration of employment		HR
Payrolls/wages		Duration of employment		HR
Job history including staff personal records: contract(s), Ts & Cs; previous service dates; pay and pension history, pension estimates, resignation/termination letters, performance appraisals		As per legal requirement		HR
Employee address details		Duration of employment		HR
Annual leave records		Duration of employment		HR
Accident reports and		As per legal requirement		HR

correspondence				
Certificates and self-certificates unrelated to workplace injury; statutory sick pay forms		As per legal requirement		HR
Pregnancy/childbirth certification		As per legal requirement		HR
Parental leave		Duration of employment		HR
Maternity pay records and calculations		As per legal requirement		HR
Redundancy details, payment calculations, refunds, notifications		As per legal requirement		HR
Training and development records		Duration of employment		HR
List of Volunteers	CP's Files			Country Programme (CP)
Holiday Requests		Duration of employment		HR

17 Contracts

Personal data record category	Location	Retention period	Disposal Method	Record owner
Signed Contracts		Permanent		Finance
Contract amendments		Permanent		Finance
Successful tender documents		Permanent		Finance
Unsuccessful tenders' documents		Permanent		Finance
Tender – user requirements, specification, evaluation criteria, invitation		Permanent		Finance
Contractors' reports		Permanent		Finance
Operation and monitoring, e.g. complaints		Permanent		Finance

18 Beneficiary Data

Personal data record category	Location	Retention period	Disposal Method	Record owner
Child Profiles including photos and videos	NK	Until Child reaches 25	Anonymisation of personal data.	Fundraising
Child Messages	NK	Until Child reaches 25	Electronic file and record deletion from primary and backup systems. Secure shred and disposal of stored hard copies or redaction of personal/sensitive data.	Fundraising
Child photo's, video and stories	StoriesHub	Until Child reaches 25	Electronic file and record deletion from primary and backup systems. Secure shred and disposal of stored	Fundraising

			hard copies or redaction of personal/sensitive data	
Child Photo's, video and stories archived	Server in UK data room	Until Child reaches 25	Electronic file and record deletion from primary and backup systems. Secure shred and disposal of stored hard copies or redaction of personal/sensitive data.	Fundraising
Child Profiles shared Drives	CP shared drives, individual hard drives, memory sticks and cards.	Until Child reaches 25	Electronic File and Data Record deletion or anonymisation, redaction of personal data.	CP
Child Sponsorship Data files	CP shared drives, individual hard drives, memory sticks and cards.	No time limit if not personal data. Otherwise same as personal data retention limits.	Electronic file and record deletion from primary and backup systems. Secure shred and disposal of stored hard copies or redaction of personal/sensitive data.	CP
Child Stories	CP shared drives, individual hard drives, memory sticks and cards.	If contains personal information of child, then until 25 years. If anonymous no time limit.	Electronic file and record deletion from primary and backup systems. Secure shred and disposal of stored hard copies or redaction of personal/sensitive data.	CP
Photo/Child Message Collection Lists	CP shared drives, individual hard drives, memory sticks and cards. Hard copies at LRP	Until the youngest child on the list reaches 25.	Electronic file and record deletion from primary and backup systems. Secure shred and disposal of stored hard copies or redaction of personal/sensitive data.	CP
Templates	CP shared drives, individual hard drives, memory sticks and cards.	No time limit. Does not have personal data.		CP/FA
Reports	CP shared drives, individual hard drives, memory sticks and cards.	No time limit if not personal data. Otherwise same as personal data retention limits.	Electronic file and record deletion from primary and backup systems. Secure shred and disposal of stored hard copies or redaction of personal/sensitive data.	CP
Queries and Complaints	CP paper files at LRP and Regional soft copies are stored at the LRP and CP levels	No time limit if not personal data. Otherwise same as personal data retention limits		CP

*See Partnership and CS data management schedule for detailed listing of documents and storage at Country Programmes

19 Supporter Data

Personal data record category	Location	Retention period	Disposal Method	Record owner

PAPER 11.

Supporter full names	Current NK database which is accessible to Fas/Funders, CPs, GS. In the new database no personal data is held.	As Funder Retention		
Supporter addresses	Current NK database which is accessible to the Funders/FAs, CPs, GS. Not help in the new CS system	In NK as Funder Retention, in new CS not applicable.		
Supporter emails & telephone nos.	This information is held in FA CRMs only accessible to them. In NK or the new database no emails or telephone numbers will be stored.	In NK as Funder Retention, in new CS not applicable.		
Queries & complaints	On the Funders CRM & NK database, accessible to the Fas/Funders, respective CP and GS. Does not include personal data. Will also be held on the new CS system.	In NK as Funder Retention. In new CS until the associated child record is 25 Years.		
Supporter letters, cards and photos	On the funder CRMs, and new CS system, respective CP, LRPs and the sponsored child/community. The CPs/respective LRPs handle the hard copies of this data. Sometimes the soft copies are maintained on emails and computer hard drives in the CPs/LRPs. The child is given the hard copies of the cards/letters/photos.	In NK as Funder Retention. In new CS until the associated child record is 25 Years.		

PAPER 11.

20 IT

Personal data record category	Location	Retention period	Disposal Method	Record owner
Recycle Bins	Desktop	30days	Delete	Employee
Downloads	Desktop	3 months	Move to recycle bins	Employee
Inbox	Office 365	2 years	Move to Archive	Employee
Deleted Emails	Office 365	30 days	Delete	Employee
Personal Network Drive	File Server	7 years	Move to Archive	Employee
Local Drives & files	File Server	7 years	Move to Archive	Employee
One Drive	Office 365	7 years	Move to Archive	Employee

21 Programmes and Projects

Personal data record category	Location	Retention period	Disposal Method	Record owner
Log Frames				
Tender Requests				
Proposals				
Project Plans				
Risk Registers				
M&E reporting				

22 Miscellaneous

Personal data record category	Location	Retention period	Disposal Method	Record owner
Travel Requests	Share Point and Emails			Finance

PAPER 11.

APPENDIX 5: Subject Access Request Policy and Procedure

ACTIONAID INTERNATIONAL

SUBJECT ACCESS REQUEST (SAR) POLICY AND PROCEDURE

Policy Name:	Subject Access Request Policy and Procedure ("Policy")
Version:	1.0
Applicable Data Protection Legislation:	EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)) ("GDPR") and associated national legislation

Governance Information

Policy Owner	Head of Digital and Technology
Policy Sponsor	Resource Mobilisation and Innovation Director
Date Ratified by SLT	17th November 2020
Date ratified by Board:	4th December 2020
Date last updated	December 2020
Date of next review	December, 2021

PAPER 11.

Table of Contents

1 Policy Statement

2 Policy Purpose

3 Policy Scope

4 Policy References

5 Rights of Access – What is a SAR?

6 How a Subject access request is made

6.1 Categories of data subject

6.2 Third Party requests

6.3 Requests from children

7 What we do when we receive a request

7.1 Identity Verification

7.2 Information Gathering

7.3 Information Provision

7.4 Logging and Recording Requests

8 Timeframes and Fees

9 Other Rights of a Data Subject

10 Exemptions and Refusals

11 Submission and Lodging a Complaint

12 Supervisory Authority

13 Staff Training & Awareness

14 Policy Review

15 Subject Access Request Form

Policy Statement

ActionAid International (AAI) needs to collect personal information to effectively carry out its everyday business functions and activities and to provide the products and services in the various communities we work with. Such data is in particular collected from beneficiaries, donors, partners, suppliers and employees and includes (but is not limited to), name, address, email address, date of birth, IP address, identification numbers, private and confidential information, sensitive data and bank/credit card details.

The data protection laws include provisions that promote accountability and governance and as such AAI has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimize the risk of breaches and uphold the protection of personal data.

PAPER 11.

This Policy serves as a reference document for employees and third parties that create, collect, use, store or dispose of personal data on behalf of AAI and it is their responsibility to familiarize themselves with this Policy and ensure adequate compliance with it.

Policy Purpose

The purpose of this Policy is to ensure that all AAI staff and partners understand and are aware of their responsibilities to meet our legal, statutory and regulatory requirements under the data protection laws in relation to Subject Access Requests (SAR's) as defined and legislated under the GDPR and Associated National Data Protection Legislation.
This Policy supplements the right of access provisions set out in AAI's Data Protection Policy & Procedures and provides the process for individuals to use when making an access request, along with the protocols followed by AAI when such a request is received.

Policy Scope

This Policy is related to personal data collected by AAI for the purpose of effectively carrying out its everyday business functions and activities. The protection it affords should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data by AAI.

This Policy covers the work of ActionAid International and the Country Programme Offices it is accountable for (hereinafter collectively referred to as the "AAI"), and their staff (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents) that may collect, process, or have access to data (including both personal and sensitive data). Adherence to this Policy is mandatory and non-compliance may lead to disciplinary action.

Policy References

- ActionAid International Data Protection Policy
- ActionAid International Privacy Notice
- ActionAid International Data Retention and Erasure Policy

Rights of Access – What is a SAR?

The General Data Protection Regulation (GDPR) as read with Associated National Data Protection Legislation gives individuals the right to know what information is held about them, to access this information and to exercise other rights, including the rectification of inaccurate data. The GDPR is a standardized regulatory framework which ensures that personal information is obtained, handled, and disposed of properly.
Under Article 15 of the GDPR, an individual has the right to obtain from the controller, confirmation as to whether personal data concerning them is being processed. We are committed to upholding the rights of individuals and have dedicated processes in place for providing access to personal information. Where requested, we will provide the following information: -

- the purposes of the processing of the data
- the categories of personal data concerned
- the recipient(s) or categories of recipient(s) to whom the personal data have been or will be disclosed
- If the data has been transferred to a third country or international organisation(s) (and if applicable, the appropriate safeguards used)
- the envisaged period for which the personal data will be stored (or the criteria used to determine that period)

- where the personal data was not collected directly from the individual, any available information as to its source
- the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to processing
- the right to lodge a complaint with a Supervisory Authority
- the existence of automated decision-making (if applicable; currently, AAI does not conduct any automated decision-making)

Furthermore, we will provide a copy of the personal data undergoing processing to the extent required under applicable laws.

Overall responsibility for the management of the response to the Subject Access Requests falls to the Data Protection Officer, but all staff have a joint responsibility to support this process to fully meet our obligations under the specified timeframes.

How a Subject access request is made

A Subject Access Request (SAR) is a request for access to the personal information that AAI holds about the individual which we are required to provide under the GDPR (unless an exemption applies see section 10). The information that we provide is covered in section 7 of this document.

In order to be able to respond to the Data Subject Access Requests in a timely manner, please request that the data subject should where possible:

- Submit their request using the Subject Access Request Form found at the end of this policy.
- Provide the Company with sufficient information to validate their identity (to ensure that the person requesting the information is the data subject or his/her authorized person).

Subject to the exemptions referred to in this Policy, AAI will provide information to data subjects whose requests are in writing (or by some other method explicitly permitted by the local law) and are received from an individual whose identity can be fully validated.

Factors that can assist in narrowing the scope of a search include identifying the processing of the request and ensuring it is appropriately allocated include, the likely time period in which the information was generated or processed (requests will be processed regardless but the narrower the time frame, the quicker a request will be turned around) and being specific about the nature of the data sought is helpful (e.g. a copy of a particular form or email records from within a particular department). The processing of the SAR should not be denied simply because the data subject has not been able to provide further particulars requested.

As outlined within GDPR, AA should ordinarily only accept Subject Access Requests in writing but will do so via any reasonable method.

Requests made by telephone

- if a data subject requests a SAR by telephone, we will direct them to how they hand in a request in a manner which allows for their identity to be fully validated subject – see Section 7: Identity Verification.
- In the event we are unable to verify the individuals identity by telephone, we will direct the Data Subject

to how they can formalise their request in writing.

Requests made by social media

Whilst a request made via social media is in writing, AAI will always move the conversation away from public view i.e. to direct messages or email for the security of the data subject.

Requests not using the term 'Subject Access Request'

Any formal request for personal information will be treated as potentially indicating a Subject Access Request, even if this term is not explicitly used. For example, use of the following wording:

- I would like you to supply me with all the information you hold on me
- Please send me details of everything you hold about me
- Please send me a copy of my data

All front-facing staff will receive specific training on how to identify an SAR, regardless of the nature of the request.

Categories of data subject

Most SARs will be made by the data subject themselves: any person on whom AAI processes (collects, stores and uses) data. This may include, but is not limited to:

- Supporters, including donors, volunteers and campaigners
- Past, present and prospective employees
- Named contacts at suppliers and funding bodies
- Parents or guardians of children under the age of consent as set by the country of residence of the subject

Third Party requests

AAI will also accept and fulfil requests made by an authorised third party acting on behalf of the data subject, for example a solicitor, or anyone acting under Power of Attorney. The third party will need to provide proof of their eligibility to act on behalf of the data subject – see Section 7: Identity Verification.

Requests from children

Children have a right to request their own data, and ActionAid respects the guidance from the competent Supervisory Authority and EU that children between the ages of 13 and 16 may well be able to make an informed SAR. We will judge these on a case by case basis, and if we are satisfied that a child understands the implications of their request and would understand the information that we intend to give them, we will fulfil this request, with information provided directly to the child (not their parent).

What we do when we receive a request

If AAI acts as a data controller towards the data subject making the request then the SAR will be addressed based on the provisions of this Policy.

If the Company acts as a data processor the Data Protection Officer will forward the request to the appropriate data controller on whose behalf AAI processes personal data of the data subject making the request.

PAPER 11.

Identity Verification

Subject Access Requests (SAR's) are passed to the Data Protection Officer as soon as received and a record of the request is made. The Data Protection Officer will use all reasonable measures to verify the identity of the individual making the access request, especially where the request is made using online services.

Please note that a request is only considered valid where the identity of the individual can be verified to our satisfaction using the criteria below.

We will utilize the request information to ensure that we can verify the data subject's identity and where we are unable to do so, we may contact the data subject for further information, or ask to provide evidence of its identity prior to actioning any request. This is to protect the data subject's information and rights.

Acceptable forms of identification for a data subject:

- Proof of address, for example, on a utility bill provided in either hard or soft copy (before provision any information which is not necessary for identification, i.e. information other than name, address and indication that the document is usable for proof of address, shall be made unreadable, e.g. by blackening, and the data subject shall be informed accordingly)
- Proof of email address used for recent correspondence, by using that account to send us an email
- Confirmation of identity from a qualified person

If a third party, relative (including parent/guardian) or, representative is requesting the information on the data subject's behalf, we will be required to verify their authority to act for the data subject. The data subject may at this point be contacted for identity confirmation and to obtain authorization prior to actioning any request.

Acceptable forms of identification for a third party:

- Legal power of attorney documentation
- A written authority from the data subject for the requester to submit the SAR
- Birth certificate in case of a child or Certificate of guardianship

We are aware that the nature of our work means that some of our data subjects may have difficulty in providing the necessary resources to confirm identification, so in some extreme cases where due to the nature of our relationship with the data subject or the context in which the data was gathered i.e. through our field work in remote locations, AAI may rely on a face to face visit to verify the identification of the data subject. AAI fully commits to upholding the rights of every data subject, no matter what the circumstances of our relationship may be or location.

Information Gathering

When enough information is provided in the SAR to collate the personal information held about the data subject, AAI will gather all documents relating to the Data Subject and ensure that the information required is provided in an acceptable format. If there is not enough information to locate the records, the data subject may be contacted for further details. This will be done as soon as possible and within the timeframes set out in Clause 8.

AAI will check the following to fully satisfy a Subject Access Request: -

- Child Sponsorship System
- Financial System
- HRMIS system
- Contract management System
- Email Servers
- Network Drives
- Non-Digital records i.e. paper records

- Any 3rd Party where data may have been shared as per our privacy notice
- Other Members Organisations within the ActionAid Federation where we may have shared your data as part of our everyday business activities. Requests directed to a specific ActionAid entity will be the responsible of that entity.

Information Provision

Once we have collated all the personal information held, a copy of this information will be sent to the data subject (or in a commonly used electronic form if requested) together with the information as specified in section 5. The information will be in a concise, transparent, intelligible and easily accessible format, using clear and plain language. Originals of any data held will continue to be held by AAI as the Data controller.

Information sent to the requester will be transferred either by registered post, or through use of a password protected PDF file sent via email. Large volumes of data will be sent by post on an encrypted USB stick.

We will also supply a cover sheet to list the sources of data, to assist the requester in understanding how information was compiled.

Logging and Recording Requests

All SARs submitted are entered onto the SAR log to track progress: this includes SARs where identity verification could not be completed. SAR reporting from this log is then included in the quarterly compliance report for our Board.

Timeframes and Fees

We will in general confirm receipt of the SAR to the requester within 2 working days, using the medium by which they made their request. E.g. a letter for a postal request or email for an electronic request. This confirmation may also include a request for due proof of identity (see section 7).

We aim to complete all SAR within one month from the date of receipt of a valid request and provide the information free of charge, as obliged by law. Where the request is made by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.
Whilst we provide the information requested without a fee, further copies requested by the individual may incur a charge to cover our administrative costs.
AAI always aim to provide the requested information at the earliest convenience, but at a maximum, one month from the date the valid request is received. However, where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by up to two further months. If this is the case, we will write to the data subject within 30 days of receipt of the request and keep you informed of the delay and provide the reasons.

Under no circumstances will AAI provide information to a requester whose identity we cannot verify. If we do not receive a response to a request for identification within 10 working days, we will send a further prompt for identification. If we have still not received a response after a further 10 working days, we will endeavour to contact the requester via another channel. If we are unable to do so, then we will close the Subject Access Request. The exception to this is where it is clear to AAI that a longer period is required by the Data Subject to respond to the proof of identification request due to the extreme circumstances set out in section 7.1.

PAPER 11.

Other Rights of a Data Subject

Under the GDPR and the national legislation where applicable, the data subject inter-alia has the right to request rectification of any inaccurate or incomplete data held by AAI. Where a notification is received relating to inaccurate or incomplete data, the details should be amended immediately as directed by data subject and a note should be made on the system (or record) of the change and reason(s). Any errors will be rectified within 30-days and the data subject will be informed in writing of the correction and where applicable, provided with details of any third-party to whom the data has been disclosed in the previous 12 months, with instructions to make amendments.
If for any reason, we are unable to act in response to a request for rectification and/or data completion, we will always provide a written explanation to the data subject and inform the data subject of its right to complain to the Supervisory Authority and to seek a judicial remedy.
In certain circumstances, data subjects may also have the right to request from AAI, the erasure of personal data or to restrict the processing of its personal data, to receive personal data in a structured, commonly used and machine-readable form or have the personal data transmitted directly to another controller; as well as the right to object to such processing. Data subjects may withdraw their consent or object to direct marketing at any time. Data subjects can use the contact details in section 11 to make such requests. Details on those rights can be found in our Privacy Notice.

Exemptions and Refusals

The GDPR and in some instances the Applicable local legislation contains certain exemptions from the obligation to provide personal information following a Subject Access Request. If one or more of these exemptions applies to a Subject Access Request or where AAI does not act upon the request, we shall inform the data subject at the earliest convenience, or at the latest, within one month of receipt of the request.

An individual does not have the right to access information recorded about someone else, unless they are an authorized representative, or have parental responsibility.

AAI is not required to respond to requests for information unless it is provided with sufficient details to satisfy itself as to the identity of the data subject making the request (see section 7.1 above).

In principle, AAI will not normally disclose the following types of information in response to a Subject Access Request:

- Information about other people – A Data Subject Access Request may cover information which relates to an individual or individuals other than the data subject. . Access to such data will not be granted if this adversely affects the rights and freedoms of such other individuals or in case there is another exemption under applicable national legislation; in such cases, any reference to these other individuals will be redacted or removed prior to fulfilling the request.
- Repeat requests – Where a similar or identical request in relation to the same data subject has previously been complied with within a reasonable time period, and where there is no significant change in personal data held in relation to that data subject, any further request made within a six month period of the original request will be considered a repeat request, and AAI will not normally provide a further copy of the same data. In exceptional circumstances where AAI responds to such a repeat request, a reasonable administration fee will be charged, namely if a request is manifestly unfounded or excessive.
- Publicly available information – AAI is not required to provide copies of documents which are already in the public domain.

- Opinions given in confidence or protected by copyright law – AAI does not have to disclose personal data held in relation to a data subject that is in the form of an opinion given in confidence or protected by copyright law.
- Privileged documents – Any privileged information held by AAI usually need not be disclosed in response to a SAR in accordance with applicable national legislation. In general, privileged information includes any document which is confidential (e.g. a direct communication between AAI and a Solicitor) and is created for the purpose of obtaining or giving legal advice.

Where possible, we will provide you with the reasons for not acting and any possibility of lodging a complaint with the Supervisory Authority and your right to seek a judicial remedy. Details of how to contact the Supervisory Authority are laid out in section 11 of this document.

ActionAid will always provide all reasonable information asked for, and explain if we withhold any information, which is anticipated to be rare. If a requester questions the information provided, we will work with them to understand the scope of their concern, for example, if there were particular documents they were expecting to receive.

As stated above the data subject has the right to refer the matter to the ICO, but We will always seek to resolve the dispute with them directly where possible.

Submission and Lodging a Complaint

To submit a SAR, data subjects can contact us at DPO.hellas@actionaid.org. They can also submit your request in writing using the form at the end of this Policy, sending the request to:
The Data Protection Officer
ActionAid Hellas
204 Mesogeion Avenue
Zip code:15561
Athens
Greece

If a data subject is unsatisfied with our actions or wishes to make an internal complaint, he or she can contact us in writing at: -

By Email at DPO.hellas@actionaid.org
By Phone on +30 21 2000 6416

By Post at Data Protection Team
ActionAid Hellas
204 Mesogeion
Avenue
Zip code:15561
Athens
Greece

PAPER 11.

Supervisory Authority

If a data subject remains dissatisfied with our actions, he or she has the right to lodge a complaint with a Supervisory Authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement.

Staff Training & Awareness

Information on SARs will be included in the Compliance Manual to be issued to all staff, who will self-certify that they have read this.

More in-depth training, including detail on the process, will be given to those teams most likely to receive a request: at present HR and Supporter Contact. This will also be logged.

Policy Review

This Subject Access Request Policy will be reviewed bi-annually, however it is everyone's responsibility to ensure this document is as accurate as possible at all times, and if you see sometimes that has changed please inform the Data Protection Officer.

Subject Access Request Form

See next page

PAPER 11.

ActionAid International Subject Access Request Form

Under the General Data Protection Regulation, you are entitled as a data subject to obtain from the ActionAid International, confirmation as to whether we are processing personal data concerning you, as well as to request details about the purposes, categories and disclosure of such data.

You can use this form to request information about, and access to any personal data we hold about you. Details on where to return the completed form can be found at the end of the document. You are, however, not required to use this form.

1. Personal Details:			
Data Subject's Name:		DOB:	___ / ___ / _____
Home Telephone No:		Email:	
Data Subject's Address:			
Any other information that may help us to locate your personal data:			

2. Specific Details of the Information Requested:

3. Representatives (only complete if you are acting as the representative for a data subject) [Please Note: We may still need to contact the data subject where proof of authorisation or identity are required]			
Representative's Name:		Relationship to Data Subject:	
Telephone No:		Email:	
Representative's Address:			

I confirm that I am the authorised representative of the named data subject:

Representative's Name: _____ Signature: _____

4. Confirmation
Data Subject's Name: _____ [print name] Signature: _____ Date: ____ /____ /_____

5. Details of any accompanying documents including proof of Identity or representation

PAPER 11.

6. Completed Forms
For postal requests, please return this form to: The Data Protection Officer ActionAid Hellas, 204 Mesogeion Avenue Zip code:15561, Athen, Greece For Email requests, please return this form to: DPO.hellas@actionaid.org