Policy Number	A4IDP21
Data Protection Policy	
Date Approved	July 2018
General Objectives of the Policy	Everyone has rights with regard to how their personal data is handled. This data protection policy sets out how Advocates for International Development ("A4ID", "we", "our", "us") handle the personal data our benefactors, suppliers, employees, workers and other third parties. This data protection policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, benefactors, clients or supplier contacts, shareholders, website users or any other data subject. This data protection policy applies to all A4ID personnel ("you", "your"). You must read, understand and comply with this data protection policy when processing personal data on our behalf and attend training on its requirements. This data protection policy sets out what we expect from you in order for A4ID to comply with applicable law. Your compliance with this data protection policy is mandatory. This data protection policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Data Protection Officer. Any policy breach will be taken seriously and may result in disciplinary action.
Policy Principles	1. **ABOUT THIS POLICY** 1.1 The types of personal data that A4ID may be required to handle include details of current, past and prospective employees, benefactors, suppliers and other third parties that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation (*(EU) 2016/679*) (the "**GDPR**") and other regulations. The GDPR imposes restrictions on how we may use that personal data. 1.2 This policy provides information about how A4ID, as a data controller, processes the personal data of data subjects who are located in the European Economic Area (the **EEA**). This policy also provides data subjects with additional information relating to their rights in respect of the personal data that A4ID holds about them. 1.3 This policy does not form part of any employee's contract of employment and may be amended at any time. 1.4 The Data Protection Officer is responsible for ensuring compliance with the GDPR and with this policy. That post is held by the Chief Operating Officer. Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Officer: andrew.mackay@a4id.org 1.5 If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with your line manager or the Data Protection Officer.

	2. DEFINITION OF DATA PROTECTION TERMS
	2.1 **Automated decision-making (ADM)** is when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits ADM (unless certain conditions are met) but not automated processing.
	2.2 **Automated processing** is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.
	2.3 **Consent** is agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.
	2.4 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.
	2.5 **Data Privacy Impact Assessment (DPIA)** means tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of privacy by design and should be conducted for all major system or business change programs involving the processing of personal data.
	2.6 **Data subjects** for the purpose of this policy include all living, identified or identifiable individuals about whom we hold personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.
	2.7 **Data controllers** are the person or organisation that determines when, why and how to process personal data. They have a responsibility to establish practices and policies in line with the GDPR. We are the data controller of all personal data used in our business.
	2.8 **Data users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.
	2.9 **Data processors** include any person or organisation that processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.
	2.10 **Explicit Consent** means consent which requires a very clear and specific statement.
	2.11 **Personal data** means any information identifying a data subject or information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers that we possess or can reasonably access. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

2.12 **Personal data breach** means any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.

2.13 **Privacy by design** means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

2.14 **Privacy notices (also referred to as fair processing notices)** are separate notices setting out information that may be provided to data subjects when the business collects information about them.

2.15 **Processing** is any activity that involves use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

2.16 **Pseudonymisation or pseudonymised** means replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

2.17 **Sensitive personal data** includes information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and personal data relating to criminal offences and convictions.

3. **DATA PROTECTION PRINCIPLES**

3.1 Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

3.1.1 Processed lawfully, fairly and in a transparent manner in relation to the data subject.

3.1.2 Processed for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.

3.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

3.1.4 Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure the personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

3.1.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.

3.1.6 Processed in a matter that ensures appropriate security of the personal

data, including protection against unauthorised or unlawful processing.

3.1.7 Not transferred to another country without appropriate safeguards being in place.

3.1.8 Made available to data subjects and data subjects allowed to exercise certain rights in relation to their personal data.

3.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

4. **CONSENT**

4.1 A data controller must only process personal data on the basis of one or more of the lawful bases set out in the GDPR, which include consent.

4.2 A data subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, we will ensure that consent is kept separate from those other matters.

4.3 Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. We will refresh consent if we intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented.

4.4 Unless we can rely on another legal basis of processing (for example, processing sensitive personal data on the basis that it is within our legitimate activities with appropriate safeguards as a not-for-profit body) explicit consent is usually required for processing sensitive personal data, for ADM and for cross border data transfers. Usually we will be relying on another legal basis (and not require explicit consent) to process most types of sensitive personal data. Where explicit consent is required, we will issue a fair processing notice to the data subject to capture explicit consent.

4.5 We will evidence consent captured and keep records of all consents so that A4ID can demonstrate compliance with consent requirements.

5. **FAIR AND LAWFUL PROCESSING**

5.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

5.2 We only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the data subject.

5.3 The GDPR allows processing for specific purposes, some of which are set out below:

5.3.1 the data subject has given his or her consent;

5.3.2 the processing is necessary for the performance of a contract with the data subject;

5.3.3 to meet our legal compliance obligations;

5.3.4 to protect the data subject's vital interests; or

5.3.5 to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The purposes for which we process personal data for legitimate interests need to be set out in applicable privacy notices or fair processing notices.

You must identify and document the legal ground being relied on for each processing activity.

6. TRANSPARENCY (NOTIFYING DATA SUBJECTS)

6.1 We provide detailed, specific information to data subjects depending on whether the information was collected directly from them or from elsewhere.

6.2 Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we provide the data subject with all the information required by the GDPR including the identity of the data controller and [Data Protection Officer], how and why we will use, process, disclose, protect and retain that personal data through a fair processing notice which we present when the data subject first provides the personal data.

6.3 When personal data is collected indirectly (for example, from a third party or publically available source), we provide the data subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. We also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that personal data.

7. PROCESSING FOR LIMITED PURPOSES

7.1 Personal data will only be processed for the specific, explicit and legitimate purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the GDPR. This means that personal data will not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject will be informed of the new purpose before any processing occurs.

8. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

8.1 Personal data will be adequate, relevant and limited to what is necessary in relation to the specific purpose notified to the data subject. We will ensure that we will delete

personal data that is no longer needed for specified purposes.

9. **ACCURATE DATA**

9.1 Personal data will be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

9.2 We will ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

10. **DATA RETENTION**

10.1 Personal data will not be kept in an identifiable form for longer than is necessary for the purpose for which the data is processed. This means that all reasonable steps will be taken to destroy or erase data from our systems when it is no longer required.

11. **PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS**

11.1 Data will be processed in line with data subjects' rights. Data subjects have a right to:

11.1.1 withdraw consent to processing at any time;

11.1.2 receive certain information about A4ID's processing activities;

11.1.3 request access to their personal data that we hold;

11.1.4 prevent our use of their personal data for direct marketing purposes;

11.1.5 ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

11.1.6 restrict processing in specific circumstances;

11.1.7 challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

11.1.8 request a copy of an agreement under which personal data is transferred outside of the EEA;

11.1.9 object to ADM, including profiling;

11.1.10 prevent processing that is likely to cause damage or distress to the data subject or anyone else;

11.1.11 be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

11.1.12 make a complaint to the supervisory authority; and

11.1.13 in limited circumstances, receive or ask for their personal data to be

transferred to a third party in a structured, commonly used and machine readable format.

11.2 We will verify the identity of an individual requesting data under any of the rights listed above.

11.3 A formal request from a data subject must be made in writing. A reasonable fee is payable by the data subject for provision of this information only if the request is manifestly unfounded or excessive. A fee may also be charged for multiple requests. We respond to requests without undue delay and, at the latest, within one month (or three months in cases which are particularly complex), as such, any member of staff who receives a written request should forward it to the Data Protection Officer immediately.

11.4 You must immediately forward any data subject request you receive to Data Protection Officer.

12. TRANSFER LIMITATION

12.1 We only transfer personal data outside the EEA if one of the following conditions applies:

12.1.1 the European Commission has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms;

12.1.2 appropriate safeguards are in place such as standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the [Data Protection Officer];

12.1.3 the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

12.1.4 the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

13. DATA SECURITY

13.1 We secure personal data by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage..

13.2 The GDPR requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to

comply with those procedures and policies, or if he puts in place adequate measures himself.

13.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

13.3.1 **Confidentiality** means that only people who have a need to know and are authorised to use the data can access it.

13.3.2 **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.

13.3.3 **Availability** means that authorised users are able to access the personal data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

13.4 You must comply with, and not attempt to circumvent, the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect personal data.

13.5 Security procedures include:

13.5.1 **Entry controls**. Any stranger seen in entry-controlled areas should be reported.

13.5.2 **Secure lockable desks and cupboards**. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

13.5.3 **Methods of disposal**. Paper documents should be shredded. CD-ROMs or data drives should be physically destroyed when they are no longer required.

13.5.4 **Equipment**. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

14. TRAINING AND AUDIT

14.1 We ensure all A4ID personnel have undergone adequate training to enable them to comply with data privacy laws. We also regularly test our systems and processes to assess compliance.

14.2 Personnel must undergo all mandatory data privacy related training.

14.3 Personnel must regularly review all the systems and processes under their control to ensure they comply with this data protection policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

15. PRIVACY BY DESIGN AND DPIA

15.1 We implement privacy by design measures when processing personal data by

	implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.
	15.2 Personnel must assess what privacy by design measures can be implemented on all programs/systems/processes that process personal data by taking into account the following:
	15.2.1 the state of the art;
	15.2.2 the cost of implementation;
	15.2.3 the nature, scope, context and purposes of processing; and
	15.2.4 the risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing.
	15.3 We conduct DPIAs in respect of high risk processing.
	15.4 Staff should conduct a DPIA (and discuss any findings with the [Data Protection Officer]) when implementing major system or business change programs involving the processing of personal data including:
	15.5 A DPIA must include:
	15.5.1 a description of the processing, its purposes and the data controller's legitimate interests if appropriate;
	15.5.2 an assessment of the necessity and proportionality of the processing in relation to its purpose;
	15.5.3 an assessment of the risk to individuals; and
	15.5.4 the risk mitigation measures in place and demonstration of compliance.
	16. **AUTOMATED PROCESSING (INCLUDING PROFILING) AND ADM**
	16.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:
	16.1.1 (a) a data subject has explicitly consented;
	16.1.2 (b) the processing is authorised by law; or
	16.1.3 (c) the processing is necessary for the performance of or entering into a contract.
	16.2 If certain types of sensitive personal data are being processed, then grounds (b) or (c) will not be allowed but such sensitive personal data can be processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.
	16.3 If a decision is to be based solely on automated processing (including profiling), we

inform data subjects when we first communicate with them of their right to object.

16.4 We also inform the data subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the data subject the right to request human intervention, express their point of view or challenge the decision.

16.5 A DPIA must be carried out before any automated processing (including profiling) or ADM activities are undertaken.

17. DIRECT MARKETING

17.1 We are subject to certain rules and privacy laws when marketing to our benefactors.

17.2 For example, a data subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls).

17.3 The right to object to direct marketing is explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

17.4 A data subject's objection to direct marketing will be promptly honoured. If a benefactor opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

18. PROVIDING INFORMATION TO THIRD PARTIES

18.1 We do not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

18.2 We only share the personal data we hold with another employee, agent or representative of our business if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

18.3 We only share the personal data we hold with third parties, such as our service providers if:

18.3.1 they have a need to know the information for the purposes of providing the contracted services;

18.3.2 sharing the personal data complies with the privacy notice provided to the data subject and, if required, the data subject's consent has been obtained;

18.3.3 the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

18.3.4 the transfer complies with any applicable cross border transfer restrictions; and

18.3.5 a fully executed written contract that contains GDPR approved third party

	clauses has been obtained. 19. **DATA BREACH** 19.1 As a data controller, we report any in-scope personal data breaches to the Information Commissioner's Office within 72 hours of discovery if there is a risk to data subjects. In certain circumstances, the data subject must also be notified. 19.2 We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so. 19.3 If you know or suspect that a personal data breach has occurred, so not attempt to investigate the matter yourself. Immediately contact the Data Protection Officer. You should preserve all evidence relating to the personal data breach.
Responsibilities	Data Protection Officer
Next Review Date	Sept 2020
Person Responsible for Review	Data Protection Officer