Ashoka: Innovators for the Public
Data Protection Policy

Policy effective from May 25, 2018

1. INTRODUCTION

This Data Protection Policy (the "**Policy**") applies to Ashoka, any subsidiary or any holding company from time to time of Ashoka, and any subsidiary from time to time of a holding company of Ashoka (collectively, "**Ashoka Group**" or "**Ashoka**").

This Policy sets out the high-level statements applicable to Ashoka. This Policy is supplemented by more detailed data protection policies, guidance, and procedures, collectively known as the "Data Protection Framework", which are attached as an annex to this policy.

The protection of Personal Data (as defined below) is important to Ashoka. Maintaining the confidentiality and security of our community's data, as well as that of our Personnel (as defined below), and other people we do business with, is essential in order to meet our contractual and regulatory obligations, maintain the trust of our employees and uphold Ashoka's reputation.

2. POLICY SCOPE

This Policy applies to any Ashoka Group company which:

2.1 Processes (as defined below) information relating to an identified or identifiable natural person[1] ("**Personal Data**") in the context of the activities of an establishment in the European Union (whether or not such processing takes place in the European Union or not), which, for the purpose of this Policy, includes any such information about customers, employees and service providers;

2.2 is established outside the European Union and that offers goods or services to data subjects in the European Union or monitors their behaviour; and

2.3 provides services to any of the companies captured by Sections 2.1 or 2.2 above, to the extent that such services involve the Processing of Personal Data.

For the purpose of this Policy, "**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 Policy is applicable to all Ashoka personnel including employees, consultants, temporary employees, volunteers, and interns within or engaged by Ashoka or any of its contractors (together, the "**Personnel**").

This Policy shall apply to Personal Data relating to Ashoka Personnel, fellows, donors, customers, vendors and other people Ashoka does business with and any other individual whose Personal Data Ashoka holds and uses.

3. POLICY OBJECTIVE AND DEFINITION

The objective of this Policy is to ensure the lawful and compliant Processing of Personal Data, including the prevention of its unauthorised use, disclosure, or access.

This Policy defines the legal requirements applicable to the Processing of Personal Data, and sets out the Ashoka policies, high-level controls and individual responsibilities to ensure the Policy objectives can be met. The Data Protection Framework consists of detailed policies, processes, and controls that support this policy (e.g., Privacy by Design, Data Subject Rights, Employee Data Privacy).

[1] An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

4. GOVERNANCE AND ACCOUNTABILITY

4.1 **Compliance with the Policy**:

(a) Ashoka's President approves this Policy.

(b) Ashoka's Data Protection Compliance Team have direct responsibility for developing and maintaining this Policy and the additional Data Protection Framework, which support this Policy.

(c) Ashoka's Data Protection Compliance Team shall provide advice, guidance and training on the implementation of, and compliance with, the Data Protection Framework, along with governance, monitoring and reporting against the Data Protection Framework for all the Ashoka Group.[2]

(d) Ashoka shall form a Data Protection Governance Board comprised of diamond leaders or their representatives, Data Protection Compliance Team. The Data Protection Governance Board shall meet once per year and shall be responsible for reviewing the Data Protection Framework and advising on adjustments to the same.

(e) The Data Protection Compliance Team shall be supported by Global Program and Legal Entity Directors who shall be responsible for embedding data protection compliance within their segment.[3]

(f) Ashoka's Data Protection Compliance Team shall provide advice, guidance and training to facilitate compliance with this Policy throughout any change management process.

(g) All Personnel are directly responsible for adhering to this Policy and complying with the data protection guidance and implementing the procedures appropriate to their core business functions and operational area.

(h) All Personnel are responsible for ensuring that their team members comply with this Policy, and appropriate guidance and procedures.

(i) All Personnel have a duty to understand, support, and comply with this Data Protection Policy, guidance and procedures. Failure to comply may lead to disciplinary and/or legal action against Personnel that could lead to dismissal, breach of contract claims, and criminal prosecution.

(j) All Personnel must regularly affirm their understanding of and acceptance to abide by this Policy and appropriate guidance and procedures.

4.2 **Data Protection Officer**:

In instances where a Data Protection Officer ("**DPO**") is required to be appointed by local regulation, Ashoka will appoint a DPO as part of the Data Protection Compliance Team in order to monitor compliance, conduct audits, maintain internal records, provide advice on data protection impact assessments, raise awareness of data protection amongst staff and perform other related tasks.[4]

The Data Protection Officer must have expert knowledge of data protection law and practices and be able to perform the DPO role. The DPO may be an employee or an external contractor, and the details of the DPO must be published and communicated to the supervisory authority.

---

[2] GDPR Article 39.

[3] This shall track the final governance process.

[4] GDPR Articles 37, 38, 39.

The DPO must be consulted at the earliest stage on all issues relating to data protection and be involved in all Privacy Impact Assessments.

The DPO may not be unfairly penalised or dismissed for performing his or her tasks.

4.3 **Record of processing**:

Ashoka shall maintain a record of processing activity under its responsibility and shall make the record available to the supervisory authority on request.[5]

The Data Protection Compliance Team shall be responsible for producing and maintaining the record of processing. It shall be reviewed and updated at least annually.

(a) The **record** shall contain:

(I) the name and contact details of the legal entity that is the controller or processor for the relevant Personal Data (and the contact details of the person responsible for such Personal Data);

(II) the purposes of Processing, a description of the categories of data subjects for the Personal Data;

(III) the categories of recipients to whom Personal Data has been or may be disclosed (identifying which, if any, are established outside the European Union, or for which the data transfer involves an export of Personal Data outside the European Union);

(IV) the legal basis for Processing;

(V) where possible, the data retention rules applicable to the relevant Personal Data; and

(VI) where possible, a general description of the technical and organisational measures applicable to the relevant Personal Data.

(b) Any new IT systems, databases, or Processing activities must be communicated to the Data Protection Compliance Team so that it can be included in the record of processing.

5. POLICY STATEMENTS

5.1 **Fair and lawful processing**:

Ashoka shall Process Personal Data lawfully and fairly.[6]

(a) **Legal basis for processing**:

Ashoka shall ensure it relies on one of the following legal bases for each Processing activity:

(I) consent;

(II) Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

(III) Processing is necessary for compliance with a legal obligation to which Ashoka is subject;

[5] GDPR Article 30.

[6] GDPR Article 5(1)(a).

(IV) Processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(V) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Ashoka; or

(VI) Processing is necessary for the purposes of the legitimate interests pursued by Ashoka or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of Personal Data.

Where the Processing is based on consent from the data subject, the consent should be freely given, specific and unambiguous and be indicated by a positive action taken by the data subject. The data subject shall be informed of the method for withdrawing consent. If the consent is given in the context of a written declaration that deals with other matters, the consent should be clearly distinguishable.

Sensitive Personal Data[7] is considered extremely sensitive and therefore additional care must be taken when dealing with it. Ashoka shall ensure it relies on one of the following legal bases for each Processing activity:

(I) explicit consent;

(II) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the fields of employment, social security and social protection law under national or EU law or a collective agreement providing for appropriate safeguards for the interests of the data subject;

(III) Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent;

(IV) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the Processing relates solely to the members, former members or to persons who have regular contact with it in connection with its purposes and that the Personal Data is not disclosed outside that body without the consent of the data subjects;

(V) Processing relates to Personal Data which is manifestly made public by the data subject;

(VI) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(VII) Processing is necessary for reasons of substantial public interest, on the basis of national or EU law which shall be proportionate, to respect the right to data protection and provide for suitable measures to safeguard interests of the data subject;

(VIII) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or national law or pursuant

[7] Sensitive Personal Data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data identifying a natural person, health data or data concerning a person's sex life or sexual orientation.

to contract with a health professional and subject to appropriate conditions and safeguards;

(IX) Processing is necessary for reasons of public interest in the area of public health on the basis of national or EU law which provides for suitable measures to safeguard the rights of the data subject, in particular professional secrecy; or

(X) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with national or EU law which shall be proportionate to the aim pursued, respect the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights of the data subject.

With respect to (VIII) above, data must be processed by or under the responsibility of a professional subject to the obligation of professional secrecy under national or EU law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under national or EU law or rules established by national competent bodies.

(b) **Transparency**:

(I) Ashoka shall Process Personal Data in a transparent way ensuring notices, policies, and consents are concise, intelligible, easily accessible, provided in clear and plain language and are easy to understand and free of charge;

(II) Ashoka shall communicate the name and contact details of the data controller and the purposes of the Processing to individuals. Ashoka shall also give details of the purposes of (and the legal basis for) the Processing of Personal Data, the recipients or categories of recipients of Personal Data, the storage period applicable to such data, the source from which the Personal Data originates (where Personal Data is not obtained directly from the data subject), information on automated decision-making (where relevant) and, where applicable, the basis of any international data transfers outside of the EEA;

(III) Ashoka shall inform data subjects of their rights in relation to their Personal Data and how those rights can be exercised;

(IV) Where Ashoka Processes Personal Data based on legitimate interests, it shall describe those interests;

(V) Where Ashoka Processes Personal Data based on consent, it will inform the data subject of the method for withdrawing consent;[8]and

(VI) Ashoka shall inform data subjects of their rights and how those rights can be exercised.[9]

5.2 **Purpose limitation**:

Ashoka shall collect Personal Data for explicit and legitimate purposes and not further Process such data in a manner that is incompatible with those purposes.[10]

(a) Any further Processing of Personal Data that is incompatible with the original purpose that it was collected for must be approved by the Data Protection Compliance Team.

[8] GDPR Article 14(2)(d)

[9] GDPR Article 13

[10] GDPR Article 5(1)(b).

(b) If the Personal Data proposed to be Processed for an incompatible purpose is Sensitive Personal Data, it must be submitted for a Privacy Impact Assessment.

5.3 **Data minimisation & storage limitation**:

Ashoka shall implement measures and procedures which minimise the Processing of Personal Data to that which is adequate, relevant, and limited to what is necessary, and shall erase the data when no longer necessary for the purposes for which they were collected, except in cases of data used for statistical purposes, which may be further retained.[11]

5.4 **Accuracy**:

Ashoka shall ensure that Personal Data shall be accurate and, where necessary, kept up to date.[12]

(a) Ashoka shall provide Personnel with the ability to update their Personal Data on an ongoing basis;

(b) Ashoka shall provide Fellows with the ability to update their Personal Data through their Ashoka country representative;

(c) Ashoka shall ensure that direct marketing recipients are informed of how to update their Personal Data as part of Ashoka's direct marketing materials;

(d) Ashoka shall update service provider Personal Data when alerted to do so by the service provider or at a time of contract renewal.

5.5 **Security**:

Ashoka shall implement appropriate measures to ensure the integrity, availability and confidentiality of Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.[13]

(a) Ashoka will keep current security procedures in a Technical and Organizational Security Measures document.

5.6 **General obligations**:

Ashoka shall comply with the following obligations under the GDPR:

(a) **Personal Data breach notification**:

All Personnel are required to inform the Data Protection Compliance Team, relevant Legal Entity Director, and Ashoka Tech Support immediately upon discovering a Personal Data breach.

Ashoka shall notify the relevant supervisory authority of data breaches within 72 hours if the breach is likely to result in a risk to the rights and freedoms of natural persons. If the breach has the potential for serious harm to an individual's rights and freedoms, that individual will be notified without undue delay (with certain exceptions if there are new security standards or it would involve disproportionate effort).[14]

[11] GDPR Article 5(1)(c) and (e).

[12] GDPR Article 5(1)(e).

[13] GDPR Article 5(1)(f).

[14] GDPR Articles 33, 34.

Regardless of severity or requirement to notify, Ashoka will keep a record of Personal Data breaches including date, time, location of event, and rational for reporting or not reporting the incident.

(b) **Privacy by design and default**:

Ashoka shall consider privacy compliance at the outset of new projects (e.g., new IT systems, new research projects using Personal Data, contracting with vendors) or when looking at mergers or acquisitions, taking into consideration the risks to data subjects.[15]

(c) **Data subjects' rights**:

(I) *Subject Access:*

Ashoka shall, if applicable, provide the data subject with electronic access to (and where applicable, a copy of) Personal Data without undue delay and at the latest within one month and give reasons where Ashoka does not intend to comply with the relevant request.

(II) *Data Portability:*

Ashoka shall facilitate or provide the data subject the ability to receive, move, copy or transmit their Personal Data from Ashoka to another controller without undue delay and at the latest within one month (or within three months in complex cases), if such Personal Data was Processed on the basis of consent or necessary for a contract of which the data subject was a party and if all of the following apply:

i. the Personal Data concerns the data subject;

ii. the Personal Data is provided by the data subject and is not inferred or derived data; and

iii. the provision of the right above shall not adversely affect the rights and freedoms of other data subjects.

(III) *Rectification and Erasure*:

Ashoka shall have procedures in place allowing for the rectification of inaccurate Personal Data or erasure of Personal Data upon the request of a data subject. Ashoka shall grant the request if one of the following applies:

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 withdraws consent on which the Processing is based (and where there is no other legal ground for the Processing, to be confirmed by the Data Protection Compliance Team);

iii. the data subject objects to the Processing and there are no overriding legitimate grounds for the Processing to be confirmed by the Data Protection Compliance Team;

iv. the Personal Data has been unlawfully Processed, to be confirmed by the Data Protection Compliance Team; and

v. the Personal Data has to be erased for compliance with a legal obligation.

[15] GDPR Articles 25, 35.

(IV) *Right to Restrict Processing*:

Ashoka shall comply with a data subject's request to restrict Processing where one of the following conditions applies:

i. the accuracy of the Personal Data is contested by the data subject, for a period enabling Ashoka to verify the accuracy of the Personal Data;

ii. the Processing is unlawful and the data subject opposes the erasure of the Personal Data and requests the restriction of use of such Personal Data instead;

iii. Ashoka no longer needs the Personal Data for the purposes of the Processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or

iv. the data subject has objected to Processing, pending the verification whether the legitimate grounds of Ashoka override those of the data subject.

(V) *Objection to Processing*:

Ashoka shall have procedures in place allowing for the individual's right to object to any profiling (including online tracking and behavioural advertising).[16]

(VI) *Process for responding to Data Subject Requests*:

i. Request may be made in any written form. If any member of Personnel receives a document or other communication that may be a data subject request, this must be forwarded at the earliest to the Data Protection Compliance Team at privacy@ashoka.org.

ii. Any data subject making a request must be required to provide sufficient identification to confirm their identity before Ashoka Group shall take further steps. The types of information used to confirm a data subjects identity may vary depending on the situation and sensitivity of the information requested.

iii. Ashoka's response to Data Subject Requests will be guided by the Data Subject Request Guide.

(d) **Appointment of data processors**:

Ashoka shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures such that the Processing meets the requirements of the GDPR and ensures the protection of rights of the data subject.[17] Ashoka's process for appointing a data processor will be guided by the Privacy by Design Toolkit.

(I) When an Ashoka entity engages the services of a processor to Process Personal Data on its behalf and the processor is a third party, the Ashoka entity shall select a data processor that provides appropriate assurances as to the level of security it shall employ in respect of the Personal Data to be Processed.

[16] GDPR Articles 15, 16, 17.

[17] GDPR, Article 28.

(II) The Ashoka entity shall ensure that a contract is entered into with third-party processors which addresses relevant requirements of the GDPR and as a minimum requires that the processor shall:

i. act only on instructions from the controller;

ii. impose a duty of confidentiality on relevant staff;

iii. implement security measures;

iv. subcontract only with the controller's prior permission;

v. make arrangements to enable the controller to fulfil the rights of data subjects (see above);

vi. assist the controller in complying with its obligations regarding data security and consultation with supervisory authorities;

vii. return all relevant Personal Data to the controller after the end of the Processing and not Process the relevant Personal Data further; and

viii. make available to the controller and the supervisory authority all necessary information regarding the processor's data Processing activities.

(III) Where the Ashoka entity is established in the EEA and engages a third-party processor established outside the EEA to Process Personal Data on its behalf, the Ashoka entity shall either:

i. ensure that a contract is in place with the data processor substantially in the form of, or incorporating the terms of, the Model Clauses for data processors (subject to any amendments that may be permitted by applicable EU privacy laws); or

ii. ensure that other suitable protections are in place, in accordance with applicable EU privacy laws.

(e) **Training and awareness**:

Ashoka shall provide training to staff who are involved in any Processing of Personal Data.[18]

(I) Ashoka maintains a privacy and security awareness program focused on educating all Personnel about the Ashoka Group's privacy and security policies, as well as privacy and security best practices. A variety of communication channels shall be used to disseminate privacy and security awareness information. Best practice and privacy and security awareness tip sheets and initiatives guides are available on dedicated privacy and security intranet sites for all Personnel to access.

(II) Ashoka also ensures that Personnel who have access to, or responsibility for, handling Personal Data are provided with appropriate guidance and training.

(III) All Personnel are required to comply with our training policies and must indicate their acceptance of these policies on an annual basis.

(f) **Data transfers outside the EEA**:

[18] GDPR Article 39.

Ashoka shall ensure that all transfers of Personal Data to third parties shall be subject to the appropriate safeguards (e.g., Model Clauses, Privacy Shield, BCRs, approved codes of conduct, etc.) unless a derogation applies (such as where the data subject has given explicit consent, or where the transfer is necessary for the performance of a contract, etc.), and that enforceable rights and effective legal remedies shall be available for data subjects.[19]

(g) **Resources and audit**:

Ashoka shall ensure the necessary resources are made available to implement and monitor policies, procedures, and controls required by the Data Protection Framework, and shall regularly conduct data protection audits to ensure compliance with this Policy and the Data Protection Framework.[20]

Ashoka shall implement an audit programme, including:

(I) Internal audit - audits are carried out by Ashoka's Data Protection Compliance Team on a rolling basis, assessing information security and compliance within the Group.

(II) External audit - audits assessing the security of the firm's business systems are carried out annually by Ashoka's external auditors.

5.7 **Exceptions**:

There are no exceptions to compliance with this Policy.

[19] GDPR Chapter 5.

[20] GDPR Articles 39, 47 (BCRs).