IMPACT Shaping practices Influencing policies Impacting lives

DATA PROTECTION POLICY

Version 1 | 2016

Content

Article 1 – Aim of the Data Protection Policy

IMPACT Initiatives (hereafter referred to as 'IMPACT') acknowledges that information technology should be at the service of every citizen. Information technology development shall take place in the context of international co-operation. Information technology shall not violate human identity, human rights, privacy, or individual or public liberties.

IMPACT is committed to international compliance with data protection laws. This Data Protection Policy applies worldwide to IMPACT and is based on globally accepted, basic principles on data protection. Ensuring data protection is the foundation of trustworthy relationships and the reputation of IMPACT as a credible organisation.

The Data Protection Policy ensures the adequate level of data protection as prescribed by relevant legal frameworks, including in countries that do not yet have adequate data protection laws.

IMPACT data protection policy is meant to be a practical and easy to understand document to which all IMPACT departments, stakeholders and partners can refer to.

Article 2 – Scope of the Data Protection Policy

This Data Protection Policy applies to all entities of IMPACT, including network and branch offices in all countries of operation.

1. The policy applies to all IMPACT staff and governance members.
2. The provision of this policy may also be applied to any person employed by an entity that carries out missions for IMPACT.
3. In particular, this policy applies to implementing partners, suppliers, sub-grantees, stakeholders and other associated entities.

IMPACT's Data Protection Policy applies to all personal data that IMPACT holds relating to identifiable individuals, meaning any information relating to an identified or identifiable individual.

Article 3 – IMPACT's sets of data and definitions

IMPACT's Data Protection Policy applies to all sets of personal data, currently stored, maintained and handled by IMPACT, and more specifically to the following identified sets of personal data:

- IMPACT's personnel, including national and international staff, interns and volunteers,
- IMPACT's direct and indirect beneficiaries, including interviewees,
- IMPACT's individual donors and sympathisers,
- IMPACT's contractors, suppliers, consultants, implementing partners currently under contract with IMPACT.

Personal data herein referred to, means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. This can include in particular:

- Names of individuals
- Postal or living addresses
- Email addresses
- Telephone numbers
- Identity card and passport
- Date and place of birth

- Identification of relatives
- Fingerprints
- Business reference
- Geo-referencing

Processing of personal data means any operation or set of operations in relation to such data, whatever the mechanism used, especially the obtaining, recording, organisation, retention, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction.

Article 4 - Application of National Laws and sources of authority

IMPACT is headquartered in Switzerland and observes the laws of Switzerland and of the Geneva Canton, including the Federal Act on Data Protection of 19 June 1992 (the Data Protection Act, the "DPA") and the Ordinance to the Federal Act on Data Protection of 14 June 1993 ("ODPA"). It also operates in more than 15 countries. IMPACT Country Operations observe the laws of their country.

This Data Protection Policy comprises the internationally accepted data privacy principles without replacing the existing national laws. It supplements the national data privacy laws. The relevant national law will take precedence in the event that it conflicts with this Data Protection Policy, or it has stricter requirements than this Policy. The content of this Data Protection Policy must also be observed in the absence of corresponding national legislation. The reporting requirements for data processing under national laws must be observed. Each entity of IMPACT, including network and branch offices is responsible for compliance with this Data Protection Policy and the legal obligations.

At the same time, IMPACT has rules and standards that seek to create a consistent approach and which, in some cases, may be stricter than national or local laws. This Policy must, therefore, be followed in addition to the relevant national and local laws on data protection.

In the event of conflicts between national legislation and the Data Protection Policy, IMPACT will work with the relevant country offices to find a practical solution that meets the purpose of the Data Protection Policy.

The purpose of the policy is aimed at guiding IMPACT staff and must be considered together with:

- ACTED's Child Protection Policy; IMPACT's Code of Conduct and policies that are annexed to it;
- IMPACT's global manuals and guidelines.

Article 5 - Principles for Processing Personal Data

1. Fairness and Lawfulness
    - When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.
    - Collected data shall be adequate, relevant and not excessive in relation to the purposes for which they are obtained and their further processing.
    - Individual data can be processed upon voluntary consent of the person concerned.

2. Restriction to a specific purpose
    - Personal data can be processed only for the purpose that was defined before the data was collected. Personal data shall be obtained for specified, explicit and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible

with those purposes. Subsequent changes to the purpose are only possible to a limited extent and require justification.

- However, further data processing for statistical, scientific and historical purposes shall be considered compatible with the initial purposes of the data collection, if it is not used to take decisions with respect to the data subjects.

3. Transparency
   - The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be made aware of, or informed of:
     - The purpose of data processing;
     - Categories of third parties to whom the data might be transmitted
   - Processing of personal data must have received the consent of the data subject or must meet one of the following conditions: compliance with any legal obligation to which IMPACT is subject; the protection of the data subject's life; the performance of a public service mission entrusted to IMPACT.

4. Confidentiality and Data Security
   - Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organisational and technical measures to prevent unauthorised access, illegal processing or distribution, as well as accidental loss, modification or destruction.

5. Deletion
   - Personal data shall be retained in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.

6. Factual Accuracy and Up-to-datedness of Data
   - Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

Article 6 – Data Processing

1. Consent to Data Processing
   - Individual data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. In certain exceptional circumstances, consent may be given verbally.

2. Data processing Pursuant to Legitimate Interest
   - Personal data can also be processed if it is necessary to enforce a legitimate interest of IMPACT. Legitimate interests are generally of a legal (such as filing, enforcing or defending against legal claims), audit or financial nature. Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the individual merit protection. Before data is processed, it must be determined whether there are interests that merit protection. Control measures that require processing of personal data can be taken only if there is a legal obligation to do

so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the organisation in performing the control measure (e.g. compliance with legal provisions and internal rules of the organisation) must be weighed against any interests meriting protection that the individual affected by the measure may have in its exclusion, and cannot be performed unless appropriate.

3. Telecommunications and Internet
    - Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by IMPACT primarily for work-related assignments. They are a tool and an organisational resource. They can be used within the applicable legal regulations and internal IMPACT communication policies. In the event of authorised use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.
    - There will be no general monitoring of telephone and e-mail communications or intranet/ internet use. To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to the network used by IMPACT that block technically harmful content or that analyse the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be blocked for a temporary period. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of policies and/or procedures of IMPACT. The evaluations can be conducted only by investigating departments while ensuring that the principle of proportionality is met. The relevant national laws must be observed in the same manner as the IMPACT regulations.

4. Rights of the Data Subject

All individuals who are the subject of personal data held by IMPACT are entitled:

- To request information on which personal data relating to him/her has been stored, how the data was collected, and for what intended purpose. If there are further rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws, these will remain unaffected. If personal data is transmitted to third parties, individuals should be informed of such a possibility. If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.
- To request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.
- To object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

Article 7 - Transmission of Personal Data

Transmission of personal data to recipients outside or inside IMPACT is subject to the authorisation requirements for processing personal data under Section 6 and requires the consent of the data subject. The data recipient must be required to use the data only for the defined purposes.

In the event that data is transmitted to a recipient outside IMPACT, this recipient must agree to maintain a data protection level equivalent to this Data Protection Policy. This does not apply if transmission is based on a legal obligation.

The processing of personal data is also permitted if national legislation requests, requires or authorises this. The type and extent of data processing must be necessary for the legally authorised data processing activity, and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the individual that merit protection must be taken into consideration.

In certain circumstances, the IMPACT Data Protection Policy allows personal data to be disclosed, based on a legal obligation, to law enforcement agencies, without the consent of the data subject.

Only IMPACT's Executive Director can validate any such disclosure in writing, ahead of the disclosure, after ensuring the request is legitimate, motivated by the requester, appropriate, necessary and does not pose a threat or direct risk to IMPACT.

Before approving such disclosure, IMPACT's Executive Director will check that the recipient of the data uses the data for the defined purposes only, and that it demonstrates the capacity and will to abide by such an obligation.

Where necessary, IMPACT's Executive Director will refer to legal advisers for advice, and to IMPACT's Committee for validation, notably but not only in cases involving direct security threats and implications or global organisational risks including reputation.

Article 8 - Subject access and modification requests to personal data

All IMPACT staff and external individuals to the NGO can contact IMPACT to request rights as listed in Article 6 section 4 - Rights of the Data Subject to be applied.

Individual subject access requests from individuals should be addressed by email or in writing. If not in writing, the request should be taken and handled by a duly authorised IMPACT staff and registered in a log for reference and follow up.

Any individual subject access request received by IMPACT will be duly verified before being handled, with the verification of the identity of anyone making a subject access request, before handing over any information.

IMPACT will ensure to respond to individual requests in a timely manner.

IMPACT will ensure that any data subject, including but not only personnel, individual donors and sympathisers, and beneficiaries, have the means to contact IMPACT to verify the data IMPACT holds about them, and can have authorised IMPACT personnel update and correct personal information. Such an obligation entails the following:

- IMPACT staff should have access to their personal files and to any information held by IMPACT on them, by simple request to Human Resources department, to be presented and corrected by a duly authorised staff only. The consultation of any information on any other staff is strictly prohibited.
- Individual donors and sympathisers listed by IMPACT can reach out to IMPACT to check the data held by IMPACT and have it corrected as well as deleted. Information on this right and on how to reach out to IMPACT for such a purpose should be clearly indicated on IMPACT website, as well as on the main media of communication to Individual donors and sympathisers, including

donation receipts and donor documentation, and upon request when calling IMPACT HQ. Such a responsibility lies at the global level with the IMPACT Head of Human Resources.

- IMPACT current direct and indirect beneficiaries (including survey interviewees) shall have access to IMPACT to check any data IMPACT holds on them, to ensure its correctness, fairness, and to have it modified and updated upon request by duly authorised IMPACT personnel. For such a purpose, IMPACT teams at country level should set up and maintain complaints response mechanism that is both open and accessible to individuals, with limited constraints, while ensuring that any request by individuals is duly followed by appropriate corrective measures and communications. Contact information to uphold this right and reach out to IMPACT for such a purpose should be clearly indicated on IMPACT website as well as on other means of public information at country level. Such a responsibility lies with the IMPACT Country Focal Point at country level and with IMPACT's Heads of Programmes and Research at the global level.
- IMPACT contractors and suppliers can reach out to IMPACT Hub to check data held by IMPACT and have it corrected. Such a responsibility lies with the HQ officer in charge of Hub
- IMPACT implementing partners shall have access to IMPACT to check any data IMPACT holds on them, to ensure its correctness, fairness, and to have it modified and updated upon request by duly authorized IMPACT personnel. Such a responsibility lies with the IMPACT Country Focal Point at country level and with the IMPACT head of Programmes at the global level.

Article 9 - Providing information

IMPACT aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used;
- How to exercise their rights;

To these ends, the current policy is shared with all IMPACT staff and available on request by individuals. A version of this Policy is also available upon request to IMPACT HQ.

Any subscriber or user of an electronic communication service shall be informed in a clear and comprehensive manner by IMPACT, except if already previously informed, regarding: the purpose of any action intended to provide access, by means of electronic transmission, to information previously stored in their electronic connection terminal device, or to record data in this device; the means available to them to object to such action.

Article 10 - Confidentiality of Processing

Personal data is subject to data secrecy. Any unauthorised collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorised to carry out as part of his/her legitimate duties is unauthorised. The "need to know" principle applies. Duly-authorised employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities.

Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorised persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

Article 11 - Processing Security

Personal data must be safeguarded from unauthorised access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organisational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing, and the need to protect the data (determined by the process for information classification). The technical and organisational measures for protecting personal data are part of IMPACT's ITC management and must be adjusted continuously to the technical developments and organisational changes.

Article 12 - Data Protection Control

Compliance with the Data Protection Policy and the applicable data protection laws is checked regularly with data protection audits and other controls. The performance of these controls is the responsibility of IMPACT's Executive Director or appointed representative. The results of the data protection controls performed by appointed representative must be reported to the Executive Director. IMPACT's Committee must be informed of the primary results as part of the related reporting duties. On request, the results of data protection controls will be made available to the responsible data protection authority. The responsible data protection authority can perform its own controls of compliance with the regulations of this Policy, as permitted under national law.

Article 13 - Violation, sanction and reporting

Any failure to comply with the current policy or to deliberately violate the rules set in the policy will result in the launch of an appropriate investigation by IMPACT.

Depending on the gravity of the suspicion or accusations, IMPACT may suspend staff or relations with other stakeholder during the investigation. This will not be subject to challenge.

Depending on the outcome of the independent investigation, if it comes to light that anyone associated with IMPACT has deliberately violated the rules set in the policy for its personal profit or any other usage of personal data, or has systematically and deliberately contravened with the principles and standards contained in this document, IMPACT will take immediate disciplinary action and any other action which may be appropriate to the circumstances. This may mean, for example, for:

- Employees - disciplinary action/dismissal;
- Trustees, officers and interns - ending the relationship with the organisation;
- Partners - withdrawal of funding/support;
- Contractors and consultants - termination of contract.

Depending on the nature, circumstances and location of the case and violation, IMPACT will also consider involving authorities such as the police to ensure the protection of personal data and victims.

The reporting of suspected or actual violations to this policy is a professional and legal obligation of all staff and partners. Failure to report information can lead to disciplinary action.

IMPACT encourages its staff and stakeholders to report suspected cases which involve any IMPACT staff, consultants, board members, guests or staff of IMPACT's partner organisations, their board members, staff and or suppliers.

IMPACT encourages its staff and stakeholders to report suspected cases through the following means:

- Staff and interns can report contacting
  - standard lines of hierarchy (contained in staff Terms of Reference);
  - the Head of Human Resources.
- Beneficiaries and their representatives can report using the Complaints and Response Mechanism (CRM) [1].
- Suppliers and contractors can use the confidential email address transparency.geneva@impact-initiatives.org.
- Individual donors and sympathisers can refer to the confidential email address transparency.geneva@impact-initiatives.org.

All reports will be treated as confidential in line with IMPACT's Code of Conduct and IMPACT's Human Resources guidelines.

IMPACT will not tolerate false accusations which are designed to damage a member of staff's reputation. Anyone found making false accusations will be subject to investigation and disciplinary action.

Article 14 - Responsibilities

IMPACT's Committee is responsible to ensure that the legal requirements, and those contained in this Data Protection Policy, for data protection are met (e.g. national reporting duties).

Management staff are responsible for ensuring that organisational, Human Resources, and technical measures are in place so that any data processing is carried out in accordance with data protection. The managers must ensure that their employees are sufficiently trained in data protection

Compliance with these requirements is the responsibility of the relevant employees.

Article 15 – Implementation of the policy

This policy has been approved by IMPACT's Executive Director on November 2016 and comes into effect immediately. It could be reviewed regularly.

*****

[1] In the framework of the global partnership between ACTED and IMPACT, all beneficiaries (understood as interviewees, respondents to IMPACT/REACH field surveys, assessed populations and stakeholders) will be directed towards ACTED's CRM mechanisms in countries where ACTED hosts IMPACT's operations. In other contexts, the deployment of CRM mechanisms will be implemented by IMPACT or its partners, as relevant.

DATA PROTECTION POLICY