Data Principles

References: Digital Accountability and Transparency Act of 2014 (DATA Act)

ADS 579 USAID's Policy on Development Data

The European Union Guide to the General Data Protection Regulation (GDPR)

Effective date: May 25, 2018

Last update: July 31, 2018

Introduction

International Republican Institute ("IRI", "Institute", or "we") respects the privacy of data collected from employees, beneficiaries, volunteers, contractors, and subawardees together referred to as "Data Subjects". The following IRI Data Principles ("Principles") outline:

- How we process data.
- How we classify that data.
- Right of IRI Data Subjects.

These principles do not apply to, and IRI is not responsible for: (i) the practices of any other organizations or individuals, or (ii) any third-party websites, platforms, devices, applications, or services that you access via links from IRI's website or services ("Third Party Services").

IRI Data Principles and Data Management Guidelines outline measures that we take to ensure that we are treating Data Subjects ethically and responsibly along the entire data lifecycle.

Data Classification

We classify data into three groups: personal, non-personal internal, and public. We determine the data classification based on the level of data sensitivity and approaches to management of such data.

These principles do not apply to personal data related to legal persons including sole-proprietary entities.

Personal Data

In the course of its daily activities, IRI processes personal data from various types of Data Subjects and in many forms. The examples provided below represent the most frequently processed types of personal data at IRI, but should not be understood to include all such types. IRI staff are required to consider any personal data that does not match one of the examples below but nonetheless meets the following definition of personal data as personal data, and to comply with the Principles listed here and the Data Management Guidelines.

INTERNATIONAL REPUBLICAN INSTITUTE

"Personal data" means any information relating to an identified or identifiable natural person ("Data Subject"). 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. Personal data may be pseudonymized or anonymized without losing its designation as such. The following is an illustrative list of the personal data IRI processes:

- Name(s)
- Age
- Birthdate
- Addresses (physical and email) and other contact information
- IP addresses
- Website cookies
- Rational identification numbers (Social Security, driver's license, passport numbers, known traveler number, Global Entry number, etc.);
- Biometric identifiers
- Phone numbers
- Employment history
- Tax information
- Photos and videos
- Social media handles + posts

- Religious affiliation
- Political affiliation
- Tribal affiliation
- Sexual orientation
- Gender identity
- Family status
- Education history
- Bank information including credit cards
- Opinion/perception research
- Personnel and human resource data including employment contracts, medical information, payroll, etc.
- Individual's GPS coordinates and other information that can be used to identify individual's location.

Most frequently, IRI processes personal data from the following groups:

- Program participants and/or beneficiaries
- Employees
- Contractors, consultants, vendors, trainers, experts, etc.
- Subawardees
- Volunteers (trainers, election observers, etc.)
- Individual and corporate donors making financial and in-kind contributions
- Research targets or informants

Personal data also includes any dataset or file that contains data attributes or combinations of attributes that meet the definitions outlined above. Examples of such files and datasets include, but not limited to:

- Event participant/attendee list;
- Polling data that captures information about interviewee's location;
- Focus group transcripts
- Audio/Video recordings of research fieldwork
- List of travelers;
- An agenda for an event not open to the public.

Non-personal Internal Data

"Non-personal internal data" is IRI's organizational information. Loss of or unauthorized use of such data could cause limited harm to IRI. IRI staff will not share non-personal internal data with any external parties without a written approval obtained by email to DataPrivacy@iri.org.

Examples of non-personal internal data include, but not limited:

- IRI internal policies and procedures not open to the public;
- Program methodology;
- IRI financial information such as non-labor general ledger;
- Intellectual property developed for IRI activities not open to public. Examples of such intellectual property include but not limited to: training agenda, training presentation, activity assessments. This limitation does not apply to materials developed for business development purposes such as concept notes, sharing success stories with potential donors, etc.;
- Compensation plan and employment benefit information;
- Unpublished research data.

Public Data

"Public data" is openly available information, the sharing of which cannot result in any harm to the Institute and IRI Data Subjects. Examples of public data are:

- Website, blog, and publicly available marketing information;
- Research publications including polling research and any research data;
- Job descriptions and other advertisement;
- Information made available by IRI funders and clients:
 - Program reports published on Development Experience Clearinghouse and other public databases that do not contain any personal data
 - Financial information available on the Federal Audit Clearinghouse.

Overview

IRI collects and processes data in a manner that ensures appropriate security including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage. IRI staff with access to personal data cannot share such data with any non-IRI staff without a written approval obtained by emailing DataPrivacy@iri.org or a written agreement designating

access to personal data. Examples of cases when IRI may grant non-IRI staff access to personal data collected by IRI include, but not limited to, auditors, evaluators, researchers, and polling consultants.

IRI processes personal data in accordance with the following principles:

Lawfulness, Fairness, and Transparency

IRI processes personal data when permitted by one or more of the following set of lawful bases:

- Consent of the data subject
- Necessity for the performance of IRI work and in order to fulfill obligations to IRI donors, funders, and clients
- Necessity for compliance with a legal obligation, such as the requirements of IRI's
 agreements with its funders and clients, Federal laws, labor laws, and other legal
 mandates. IRI also designed data polices for offices outside of the United States to comply
 with local laws and regulations.

When a Data Subject shares unsolicited personal data with IRI, the data subject gives IRI implicit consent to process the personal data agreeing to IRI General Data Consent and IRI Data Principles.

IRI establishes all lawful bases for data processing in a fair and transparent manner, communicating honestly and in good faith with all data subjects about potential data processing and its underlying purpose. This approach enables potential data subjects to make informed, free choices based on the purposes and modalities of proposed data processing.

Purpose Limitation

IRI processes personal data only for specific, limited purposes. IRI informs Data Subjects of these purposes at the point of data collection, and whenever the purposes change.

Data Minimization

IRI eschews the processing of personal data in excess of such data required to fulfill the limited purpose identified at the point of data collection, or a modified purpose identified thereafter.

Accuracy

IRI strives to maintain the accuracy of personal data under its control, and takes reasonable steps to eliminate or rectify inaccurate personal data. IRI established specific data collection processes based on the purpose of data collection (employment, research, etc.).

Storage Limitation

IRI retains all data for a period of seven (7) years from the time of receipt or creation, unless longer retention is required for historical reference, legal compliance, or for other purposes as

set forth herein. All data related to a grant or program, including partner records, must be retained for a period of seven (7) years following the closing date of the award.

Integrity and Confidentiality

IRI processes personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organizational measures. IRI established specific data security processes based on the purpose of data collection (employment, research, etc.).

IRI Data Processing Roles

Depending on the specific scope of work, IRI assumes a role of a data controller or a data processor.

Controller

When IRI acts as a controller, IRI determines the purpose and means of processing of data. IRI may determine this as part of the program and/or activity design under a legal arrangement that grants IRI control over the scope of work and ownership of the data. In most circumstances, IRI acts as a data controller.

Processor

IRI assumes a data processor role when administering data on behalf of a data controller. In such circumstances, IRI (i) does not design the scope of work, (ii) has limited influence on the scope of work, (iii) does not own the data, and (iv)can use the data only with the controller's approval. Further, as a data processor, IRI acts as a service provider under a contract, service agreement, and other legal arrangement. Examples when IRI acts as a data processor include but not limited to:

- Code and analyze quantitative and qualitative data on behalf of a client who owns the data
- Manage logistics including venue, participant sign-in, translation, etc. for an event organized on behalf of a client, who will retain all data collected during the event including sign-in sheets, photos, etc.

Third Party

As a data controller or a data processor, IRI uses third parties to collect and process data on IRI's behalf. "Third party" is a natural or legal person, public authority, agency, or body other than the Data Subject and IRI who under the direct authority of IRI, are authorized to process personal data. Example of third parties include but not limited to:

- UltiPro, human resource management software

- Key Travel, corporate travel agency
- Deltek CostPoint and/or Jamis Prime, financial management software.
- DocuSign
- Devex and Indeed website

Data Subject Rights

All Data Subjects have the following rights:

The right to opt-out

Data Subjects have a right to opt-out from collection of personal data when presented IRI data consent. However, if IRI is legally obligated to process such data, IRI may choose not to provide assistance to or engage in business with individuals and parties that opt-out from the collection of personal data. Examples of such legal obligations include, but not limited to collections of data for performance and financial reporting purposes.

The right to be informed

IRI informs potential Data Subject about the collection and use of their personal data before collecting such data. IRI memorializes individual's explicit consent (verbal or in writing) before collecting personal data.

When engaging data subjects who:

- Require an interpreter and translated consent materials, or
- Understand the consent language but cannot read due to medical condition or illiteracy,
 or
- Understand the consent language but cannot talk or write due to incapacitation.

In such cases, IRI will provide interpretive services and other necessary support to ensure the Data Subject's comprehension of the consent. Once informed, the Data Subject signs the consent form.

When the Data Subject is unable to sign the consent, IRI staff or IRI authorized third party will document the oral consent by capturing the Data Subject's name, date when the Data Subject was informed of the consent, and checking off a designed field in the consent form.

IRI makes sure to:

- Clearly outline the purpose for processing personal data, for example, reporting data to IRI client;
- Indicate how long IRI will retain the data;
- Indicate the format in which IRI will store the data;
- And third parties IRI will share the data with and/or who will process the data for IRI.

The right of access

Each Data Subject has the right to access their personal data free of charge when requesting a reasonable amount of data. A reasonable request is a request that remains within the scope of the data collection outlined in the consent agreed to by the Data Subject and does not jeopardize the rights of other Data Subject.

The right to rectification

IRI will fulfill the request of the Data Subject to rectify personal data. IRI will also take reasonable steps to rectify the data retained by third parties including, but not limited to IRI vendors, funders, clients, etc. However, IRI does not bear the responsibility for rectification of personal data by third parties.

The Right to Erasure

Data Subjects have the right to request IRI to erase personal data. IRI will respect such request as long as it does not put IRI at risk of not fulfilling other legal obligations including obligations to IRI auditors, funders, and clients.

The Right to Restrict Access

Data Subjects have the right to request IRI to restrict access to personal data. IRI will respect such request as long as it does not put IRI at risk of not fulfilling other legal obligations including obligations to IRI auditors, funders, and clients.

The Right to Data Portability

Data Subjects that provide personal data in a structured, commonly used and machine readable form have the right to request their personal data from IRI for personal or third party use. In general, "machine readable data" includes documents and structured datasets that contain data that can be searched, shared, and modified.

Machine readable data is available in but not limited to the following formats:

- API: Application Programming Interface
- Atom
- CSV: Comma separated values
- Five-star (linked open) Data
- HTML: HyperText Markup Language
- JSON: JavaScript Object Notation
- Microsoft Office Suite formats (.doc, .xmls, xlsb, ppt, etc.)

- PDF: Portable Document Format
- RSS: Really Simple Syndication
- Schema.org
- Syndication formats use to publish continuous feeds of information
- TXT
- XML: extensible Markup Language

The Right to Object

Data Subjects have the right to object processing of personal data based on legitimate interests, public interest, direct marketing (including profiling), scientific/historical research and statistics. IRI will respect such request as long as the Data Subject does not make such request after benefiting from IRI's work that requires collection of data and such request does not put IRI at risk of not fulfilling other legal obligations including obligations to IRI auditors, funders, and clients

Right to Not Be Evaluated on the Basis of Automated Processing

Data Subjects have the right not to be evaluated or in other way profiled in any material sense based on automated processing of their personal data. IRI reserves the right to deny a Data Subject from participation in IRI programs, activities, and business if such request puts IRI at risk of not fulfilling other legal obligations including obligations to IRI auditors, funders, and clients.

Oversight and Enforceability

IRI's Data Protection Officer is responsible for overall Institute-wide oversight of our Data Principles. The Data Officer and the COO share the overall responsibility for management and enforcement of these Principles including all personnel related matters. Data Officer and COO IRI Data Principles are also manage any breaches of IRI Data Principles by IRI staff, processors, and third parties.

When working with data processers and third parties handling IRI data, staff managing relationships with these parties are responsible for holding them accountable to these Principles.

Reference

IRI believes that we must be responsible stewards of information that we collect and process. Our Data Principles promulgated with reference to the following:

- Digital Accountability and Transparency Act of 2014 (DATA Act), May 9,2014
- ADS 579 USAID's Policy on Development Data, October 2, 2014
- The European Union Guide to the General Data Protection Regulation (GDPR), April 14, 2016 for EU citizens