



Privacy Policy

v202412

December 2024

Responsibility for This Policy

IRMA holds responsibility for this document and its contents.

Version No.	Date	Description of Action or Amendment
v202412	December 2024	Approved by the IRMA Board of Directors

Purpose

The Initiative for Responsible Mining Assurance ("IRMA," "we," "our") protects people, communities and the environment affected by mining by overseeing the only independent and transparent process for assessing individual mines' performance against an equally governed, best-practice standard of responsibility, and measuring companies' progress in reducing social and environmental harm.

To support its mission, IRMA may collect and, with proper consent, publish certain personal information from stakeholders, community members, participating mines, NGOs, and customers. IRMA is dedicated to safeguarding this information in compliance with all applicable privacy laws.

IRMA recognizes the importance of privacy and is committed to safeguarding personal data. This Privacy Policy explains how we collect, use, and protect personal information to ensure our practices align with the privacy and data protection laws in the jurisdictions in which we operate.

Scope

- This Policy applies to the following: all IRMA employees, officers, directors and independent contractors in all locations and roles, all third-party management companies with access to personal information.
- This Policy applies globally to IRMA's operations and should be read in full.

Governing Laws and Regulatory Guidelines

IRMA is a 501(c)(3) non-profit organization based in the United States of America that operates globally and as such is bound by the European Union's General Data Protection Regulation ("GDPR"). Regionally or locally supplementary privacy laws may apply, such as California's Consumer Privacy Act ("CCPA"), the Brazilian Personal Data Protection Law 13.709 of 2018 ("LGPD"), as well as other applicable privacy laws and regulations.

IRMA recognizes that local laws and regulations in relation to privacy and data protection may either differ between jurisdictions or be comparable but differ in execution. This Policy is guided by GDPR.

This Policy focuses on our obligations as a Controller (where we alone, or jointly with others, determine the purposes and means of the processing of personal data). Whenever we process personal data in a capacity as a Processor on behalf of another Controller, i.e. a third party contractor, IRMA and the third party will enter a Joint Data Processing Agreement which ensures appropriate personal data protections.

Examples of Personal Data

- Name
- Home address
- Financial accounts
- Details about family
- Photographs
- HR records and performance reviews
- Business contact details
- Telephone number
- E-Mail address
- IP address
- Device name or ID

Examples of Sensitive Personal Data

- Government-issued identification
- Personal legal history
- The commission or alleged commission of any offense
- Biometric information
- Children's data
- The racial or ethnic origin of the Individual
- Political opinions
- Religious beliefs
- Physical or mental health

Policy Requirements

IRMA will keep Confidential Information secure and protected against unauthorized or unlawful access, disclosure, use, or processing, and against accidental loss, destruction or damage.

1.1 Accountability

IRMA is accountable for proper handling of personal data and how we comply with the Principles for processing personal data set forth below (1.2).

IRMA must have appropriate measures and records in place to be able to demonstrate its compliance.

1.2 Principles for processing personal data

We will observe the following principles when processing personal data. Personal data will be:

- processed fairly and lawfully
- processed with consent and only for those purposes originally collected
- accurate, and where applicable, kept up to date
- kept no longer than necessary
- processed in accordance with the rights and freedoms of individuals

- kept secure against unauthorized or unlawful processing, accidental loss, damage, or destruction
- transferred to third countries only if adequate data protection measures have been put in place.

1.2.1 Processed fairly and lawfully:

We are always transparent in what we do with personal data, and only use it for the purposes for which it was collected, and for which we have lawful grounds to do so. We aim to be fully transparent about the types of personal data we collect, and the purposes for which we collect and use it.

Personal data may only be processed if one of the following lawful grounds exists:

- processing of personal data is necessary for the performance of a contract between IRMA and the individual or to enter into a contract with the individual
- processing of personal data is necessary for IRMA's legitimate interests (or the legitimate interests of another) which are not overridden by the rights of the individual
- processing of personal data is necessary for compliance with IRMA's legal obligations
- processing of personal data is based on the consent of an individual
- processing of personal data is necessary for the performance of a task in the public interest or the exercise of an official authority.

1.2.2 Processed only for the purposes it was collected for:

Personal data must be processed only for specified and lawful purposes, and not further processed in a manner that is incompatible with those purposes. We may only use personal data for the purpose for which we said we would, unless we have a legal ground for the secondary use of personal data. We do not use personal data in other ways or pass it on to any others, unless, of course, we provide information about the new purpose and, if required, obtain prior consent.

We collect personal data via our business activities. When planning a new IT solution, service or project (or when changing an existing IT solution, service, or project), we review the solution's privacy policies to ensure we use the personal data only as specified and not for unrelated, secondary purposes.

1.2.3 Adequate, relevant and not excessive in relation to the specified purpose:

We will act responsibly when collecting personal data, using and accessing only the personal data needed to achieve the purpose we have specified.

1.2.4 Accurate, up to date, and not kept longer than necessary:

Data integrity is important, particularly where it may be used in making decisions or when making assumptions. This means:

- Having systems that allow errors to be corrected and inaccuracies to be amended.
- Acting promptly on requests from individuals to correct or update their personal data.
- Once we have collected personal data, we will only keep it for as long as necessary to carry out the original purpose, unless we are under a legal or regulatory obligation to keep it longer. In certain circumstances, and only with informed consent, we keep the data for purposes of transparency.

1.2.5 Processed in accordance with individuals' rights:

Individuals have the following rights in regard to the processing of their personal data:

Individuals' Rights		Explanation
	Right to Information and Access	Obtaining access to the personal data or information relating to it
	Right to Rectification	Correction of erroneous personal data
	Right to Erasure	'Right to be forgotten' - deletion of personal data
	Right of Restriction	Right to limit processing of personal data
	Right of Data Portability	Right to obtain a copy of the personal data



Right to Object

Right to revoke consent to processing of the information not collected under legal obligation

Individuals should contact the Information Systems Director in the event there is a question about failure to comply with this Policy. To the extent further action is necessary, the Individual together with the Information Systems Director, and General Counsel can decide the need to report the matter to the Data Protection Authority, see Section 1.3.

1.2.6 Personal data must be kept secure against unauthorized or unlawful access and processing, and against accidental loss, damage, or destruction:

Personal data is stored in different ways depending on how it is collected. Information about Users who sign up for the newsletter is stored in IRMA's third party platform. IRMA will remove individuals who unsubscribe from our email newsletter on an annual basis. Complaints and Comments are posted on our website with consent, if consent is not authorized, then the posting will be anonymized.

IRMA's responsibility for information security also applies to personal data being processed on our behalf by Third Parties and we must ensure that they have in place appropriate data protection measures that meet our information security standards. This should be achieved as part of our procurement through Joint Data Processing Agreements with Third Parties.

1.2.7 Personal data must not be transferred to third countries without adequate data protection measures:

The movement of personal data is a particular area of risk which may be compounded if the personal data is transferred to another country.

1.3 Personal Data Breaches

A Personal Data Breach refers to a breach of security leading to – amongst others – the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access to personal data, processed by us or by a

Third Party. This can, if not addressed in an appropriate and timely manner, lead to significant impact to the privacy and data protection rights and freedoms of individuals.

In case of a Personal Data Breach and depending on the risk to the individual, **local laws might require us, as the Controller, to notify the Data Protection Authority and/or the individuals concerned. Any personnel aware of or concerned that there has been a data breach should immediately notify the Information Systems Director.** The Information Systems Director will alert the Executive Director and Operations Director.

The need for any notification to a Data Protection Authority, government, or regulatory body will be determined in consultation with the Information Systems Director and General Counsel. No other individuals may notify a Personal Data Breach to a Data Protection Authority, government, regulatory body without the express involvement and agreement from the Information Systems Director or General Counsel.

Roles and Responsibilities

Board of Directors

The Board of Directors promotes compliance with this Policy and ensures that adequate resources are available to manage privacy risk.

Management

All Managers should ensure that the requirements set out in this Policy are implemented in operating procedures and complied with by personnel.

Managers, in conjunction with the Information Systems Director, provide the necessary leadership to personnel throughout the process of implementing the requirements of this Policy as well as during the day-to-day activities.

Specifically:

- Managers should hold team members/individuals accountable for compliance with this Policy;
- Managers should ensure their team members/employees are made aware of and understand this policy.

Information Systems Director

The Information Systems Director is accountable for the implementation of effective data protection management, the integration of effective data protection into business practices, and that adequate resources and budget are available.

The Information Systems Director is responsible for review of the effectiveness of the implementation of this policy, and where new risks and/or regulatory developments emerge.

The Information Systems Director will alert the General Counsel and the Executive and Operations Director to provide notification of a breach, or consult where there exists a conflict between the applicable law and this Privacy Policy.

Additionally, the Information Systems Director manages and coordinates the investigation of reports on potential situations of personal data breaches and ensures the appropriate training of privacy and data protection is developed and provided to relevant employees.

Employees, Independent Contractors, and Third Parties

Employees and independent contractors are responsible for understanding and complying with the requirements of this Policy. Employees have the responsibility to raise any privacy-related suspicions or breach of this Policy to their Manager or the Information Systems Director.

Disciplinary Action

To ensure the protection of personal data and compliance with this Privacy Policy, IRMA enforces strict disciplinary measures for violations. Potential disciplinary actions for breaches of this policy include, but are not limited to, written warning, retraining, suspension, or termination. All disciplinary actions will be taken in accordance with applicable laws and organizational policies, ensuring fair and consistent treatment of all personnel.