Date Effective: September 1, 2025
Distributor: COAR Information Technology

Version History

Version #	Date	Author	Key Differences
1.0	1 Sep 2025	Gerard Bou Faical	

Data Protection Policy

Policy and Guidelines

1. Purpose

The purpose of this policy and guideline document is to formally establish and communicate the principles and protocols governing the protection of personal and sensitive data within COAR Global Ltd (COAR). Furthermore, it aims to define the lawful, fair, and transparent handling of such data throughout its lifecycle. The policy encompasses the responsibilities of staff and partners, the rights of data subjects, the procedures for responding to data breaches, and the safeguards COAR applies to ensure compliance with data protection regulations such as the General Data Protection Regulation (GDPR).

2. Scope

This policy applies to all COAR Global Ltd (COAR) employees, consultants, contractors, interns, volunteers, implementing partners, and any third parties who process, access, or manage personal or sensitive data on behalf of COAR. It covers all forms of data, whether collected digitally, in writing, or verbally, that relate to individuals, including but not limited to staff, beneficiaries, research participants, and external stakeholders.

The policy applies across all locations where COAR operates and to all data processing activities, whether carried out on COAR-managed systems or third-party platforms, including cloud-based applications, mobile devices, and field data collection tools.

3. General Principles

COAR Global is committed to ensuring that personal data is processed in a manner that respects the rights and privacy of individuals. The following principles govern all data protection activities across the organization:

Lawfulness, Fairness, and Transparency	Personal data shall be processed lawfully, fairly, and in a transparent manner. Individuals must be informed about how their data is collected, used, stored, and shared.
Purpose Limitation	Data shall be collected for specific, explicit, and legitimate purposes and shall not be further processed in a manner incompatible with those purposes.
Data Minimization	Only the data that is necessary for the intended purpose shall be collected and processed.

Accuracy	Personal data shall be accurate and, where necessary, kept up to date. Inaccurate data must be corrected or deleted without delay.
Storage Limitation	Data shall be retained only for as long as necessary to fulfill the purposes for which it was collected, in line with COAR's Data Retention Policy.
Integrity and Confidentiality (Security)	Personal data shall be processed in a way that ensures appropriate security, including protection against unauthorized access, disclosure, alteration, or destruction.
Accountability	COAR shall be responsible for, and able to demonstrate, compliance with these principles. All staff and representatives have a duty to uphold them.
Data Subject Rights	Individuals whose data is processed by COAR have the right to access, correct, restrict, or request deletion of their data, and to object to certain forms of processing, in accordance with applicable law.

4. Definitions

"COAR" refers to COAR Global Ltd .

"Law" means the EU General Data Protection Regulation (as amended and replaced from time to time) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC, and as amended and replaced from time to time) as well as with the national legislation on the protection of personal data which is "The Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data" Law 125(1)/2018.

"GDPR" means the General Data Protection Regulation (Regulation (EU) 2016/679) as amended and replaced from time to time.

5. Data Collection

This section describes how data is collected by COAR Global, considering both remote operations and international field activities.

- **Methods of Collection**: Data, including scanned personal documents such as passports, national IDs, employment contracts, and other sensitive personal information, may be collected through secure online portals, encrypted email channels, secure file transfer protocols, and physical documentation in field offices.
- **Sources**: Data is primarily collected directly from data subjects (e.g., employees, beneficiaries, research participants) or authorized third parties with appropriate consent or legal basis.
- **Authority to Collect**: The collection of personal data, including sensitive documents, is always based on a lawful basis as defined by applicable data protection laws, such as explicit consent, contractual necessity, legal obligation, vital interests, public task, or legitimate interests. For scanned personal documents like passports and IDs, collection is typically for identity verification, compliance with legal and contractual obligations (e.g., employment, international travel for projects), or for specific program requirements.
- **Protections During Collection**: When collecting scanned personal documents, COAR will utilize encrypted channels and secure platforms to prevent unauthorized access during transmission. Physical documents collected in the field will be digitized securely as soon as practicable and the physical copies stored in locked, secure locations before secure destruction.
- **Data Stewards**: Specific roles within COAR, such as HR personnel for employee data, and project managers for beneficiary and research participant data, are designated as data stewards responsible for overseeing the appropriate collection of data within their respective domains.

6. Minimization and Confidentiality

COAR ensures data minimization by collecting only the personal data necessary for project objectives. Non-sensitive or anonymized data is prioritized where possible, and personally identifiable information (PII) is minimized, aggregated, or anonymized for analysis. This approach significantly reduces potential privacy risks and ensures that only essential data is processed.

Confidentiality is maintained through strict access controls, staff training, and contractual obligations with partners, ensuring that personal and sensitive data is not disclosed beyond its intended purpose.

7. Data Transfer

In the event that personal data is transferred outside the European Economic Area (EEA), COAR ensures that appropriate legal safeguards are in place. This includes the use of Standard Contractual Clauses (SCCs) or other legally recognized mechanisms under the General Data Protection Regulation (GDPR). COAR is committed to ensuring that any international data transfers are carried out securely and lawfully, maintaining the same high standards of privacy and data protection that apply within the EEA.

8. Data Retention

COAR retains personal and sensitive data in accordance with applicable data protection laws, including the General Data Protection Regulation (GDPR) and any overriding national or contractual requirements.

Retention periods for specific categories of data are defined in COAR's Data Retention Policy, which serves as the authoritative reference for how long data should be stored before being securely archived or destroyed.

The Data Retention Policy aligns with guidance from the Office of the Commissioner for Personal Data Protection and is regularly reviewed to ensure continued compliance and relevance. All staff handling data are expected to be familiar with and adhere to the retention timelines outlined in that policy.

9. Data Storage

COAR ensures that all personal and sensitive information collected, whether through digital data collection platforms, electronic communications, or scanned documents (such as passports and identification), is securely protected during transmission, storage, and access. Data is uploaded directly to encrypted and access-controlled platforms, minimizing the storage of sensitive information on local or field devices. This approach significantly reduces the risk of unauthorized access, loss, or theft of devices.

All data is stored on centralized, encrypted servers with strict access controls. COAR's cloud infrastructure uses encryption at rest and in transit in line with recognized international standards, ensuring data remains protected across all systems and environments. Current implementation includes full encryption of cloud storage volumes (e.g., AWS Elastic Block Store

with AES-256 and Key Management Service) and encrypted backups, which provide additional assurance of data integrity, availability, and continuity.

These safeguards are applied in accordance with relevant data protection regulations (including GDPR principles) and international information security standards, ensuring that personal and sensitive data is protected against unauthorized use, disclosure, alteration, or destruction.

10. File Storage Security Protocols

COAR uses trusted third-party platforms for data storage, collaboration, and communication. Each vendor applies its own security and privacy protocols, which align with international standards such as GDPR, ISO 27001, and SOC 2. Staff are expected to use only approved platforms for storing and sharing COAR data.

- **Google Workspace & Google Drive**: https://workspace.google.com/security/
- **Amazon Web Services (AWS)**: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html
- **Google Cloud Platform (GCP)**: https://cloud.google.com/docs/security
- **Slack**: https://slack.com/help/articles/202014843-Slack-data-security-and-privacy-policies

Use of any other storage or collaboration platform must be approved in advance by COAR's IT Department.

11. Data Access

Only employees with a business necessity shall be granted access to data. Data shall not be shared informally. When access to confidential information is required, employees shall request it from their manager. COAR will provide training to all employees to help them understand their responsibilities when handling data. Employees should keep all data secure, by taking sensible precautions and following the guidelines stated in the Data Security Policy.

To reinforce this, COAR invests in continuous training, offering regular updates and refreshers to staff and partners on data protection and secure handling practices.

12. Data Security Incident Process

In case of a breach or suspected incident, employees must report immediately to IT. A formal investigation and mitigation process will follow as outlined in the Incident Response Procedure.

Where a personal data breach poses a risk to individuals' rights and freedoms, COAR will notify the relevant supervisory authority within 72 hours. Where the risk is considered high, affected data subjects will also be informed without undue delay.

13. Compliance Standards

COAR complies with the General Data Protection Regulation (GDPR), applicable national data protection laws, and recognized international information security frameworks.

Zero trust principles are integrated into compliance practices by ensuring that:

- Data processing activities are continuously reviewed for adherence to GDPR principles such as lawfulness, fairness, transparency, and data minimization.
- Security measures are not static but adaptive, requiring ongoing monitoring and verification.
- Independent audits and internal reviews are carried out to validate compliance and strengthen organizational accountability (ex. Cyber Essential Plus).

Staff, contractors, and partners are expected to follow this policy and may reach out to dataprotection@coar-global.org with any questions or compliance concerns.

COAR conducts regular compliance check-ins across all data protection practices. The Data Protection Policy is formally reviewed at least once a year, and additionally whenever significant legal, organizational, or technological changes occur, to ensure continued alignment with applicable standards and regulations.

14. Data Subject Rights

COAR recognizes the rights of data subjects under GDPR, including the right to access, rectify, erase, restrict processing, object to processing, and request data portability. All requests should be directed to dataprotection@coar-global.org

COAR will acknowledge and respond within one month, in accordance with GDPR Article 12(3) requirements.

15. Responsibilities / Governance

Responsibility for implementing this policy rests with COAR's IT Department, under oversight of senior management.

Peter Luskin	2025-10-27
Policy Approved by Peter Luskin, COAR Managing Director	Date