SLOW

Regenerative Cocoa & Coffee

Data Protection and Privacy Policy

Slow's commitment to protecting the personal data of employees, workers, farmers, and communities

Document Code	GOV-POL-04
Document Title	Data Protection and Privacy Policy
Document Type	Topic Policy (Tier 3)
Tier	Tier 3 — Topic Policies
Version	1.0
Status	Approved
Effective Date	2026
Next Review Date	2029
Owner	Senior IT Technical Specialist
Approver	Chief Executive Officer (CEO)
Geographic Scope	All Slow entities, employees, contractors, and data processing activities globally, with particular attention to GDPR applicability
Standards Alignment	EU General Data Protection Regulation (GDPR) 2016/679, applicable national data protection laws, IFC Performance Standard 1 (worker data), EcoVadis, B Corp

1. Policy Statement

Slow collects and processes personal data in the course of its operations -- from employees and contractors, from workers and farmers in its supply chain, and from communities and individuals who engage with its grievance and impact management processes. Slow is committed to handling all personal data lawfully, transparently, and with respect for the privacy rights of individuals.

This Policy sets out how Slow collects, uses, stores, shares, and protects personal data, and the rights of individuals in relation to their own data. It applies across all Slow operations. Where Slow operates in the European Union or processes the data of EU-based individuals, the EU General Data Protection Regulation (GDPR) applies and sets the minimum standard.

2. Scope

This Policy applies to:

- All personal data processed by Slow in the course of its business activities, in any format (digital, paper, oral).
- All Slow employees, contractors, and interns who process personal data in the course of their role.
- All systems, platforms, and third-party processors used by Slow to store or process personal data.

Personal data processed by Slow includes: employee and contractor HR records; farmer and worker contact details, household data, and survey results; grievance records; community engagement records; FPIC records; age verification forms; worker interview records; and contact details for suppliers and business partners.

3. Data Protection Principles

Slow processes personal data in accordance with the following principles, consistent with GDPR Article 5:

- Lawfulness, fairness, and transparency: data is collected and processed on a clear legal basis; individuals are informed about how their data is used.
- Purpose limitation: data is collected for a specified, explicit, and legitimate purpose and not further processed in a manner incompatible with that purpose.
- Data minimisation: only data that is adequate, relevant, and necessary for the stated purpose is collected.
- Accuracy: reasonable steps are taken to ensure data is accurate and kept up to date where necessary.
- Storage limitation: data is retained only for as long as is necessary for its purpose, per the retention schedule in MGT-07 Document Control SOP.
- Integrity and confidentiality: appropriate technical and organisational measures protect data against unauthorised access, loss, destruction, or damage.
- Accountability: Slow is responsible for compliance with these principles and can demonstrate compliance.

4. Legal Bases for Processing

Slow processes personal data on one or more of the following legal bases:

- Contract: processing necessary to perform an employment contract, supplier agreement, or farmer-partnership agreement.
- Legal obligation: processing required to comply with applicable law, including labour law, tax law, EUDR, and health and safety regulation.
- Legitimate interests: processing necessary for Slow's legitimate business interests (supply chain due diligence, human rights monitoring, security) where those interests are not overridden by the individual's rights.
- Consent: where none of the above bases apply, Slow seeks freely given, specific, informed, and unambiguous consent. Consent may be withdrawn at any time without detriment.

Special categories of personal data (health data, ethnicity, trade union membership) are processed only where strictly necessary and on a specific legal basis. Worker interview data and grievance records that may contain sensitive data are treated as special category data.

5. Data Subject Rights

Individuals whose data Slow processes have the following rights (subject to applicable law and limited exceptions):

- Right to be informed: individuals are told how their data is used at the point of collection.
- Right of access: individuals may request a copy of the personal data Slow holds about them.
- Right to rectification: individuals may request correction of inaccurate data.
- Right to erasure: individuals may request deletion of their data where there is no overriding legal basis for retention.
- Right to restrict processing: individuals may request that processing be restricted in certain circumstances.
- Right to data portability: where applicable, individuals may request their data in a portable format.
- Right to object: individuals may object to processing based on legitimate interests.

Requests should be directed to the Senior IT Technical Specialist. Slow will respond without undue delay and will not charge a fee for handling requests.

6. Data Collected in the Field

Slow collects personal data from farmers, workers, and community members in the course of its impact management activities. This includes household survey data, worker interview records, age verification forms, FPIC records, and grievance submissions. Special requirements apply:

- Informed consent or another valid legal basis is established before collection.
- Data is collected in the local language where possible.
- Purpose, use, and individuals' rights are explained in accessible terms at the point of collection.
- Data is anonymised or pseudonymised where individual identification is not necessary for the stated purpose.
- Worker interview records are stored with strict access controls; names are separated from responses where feasible.
- FPIC and grievance records that name individuals are held in restricted access folders.

Field staff receive training on data protection requirements relevant to their role per MGT-06.

7. Data Security

Slow takes appropriate technical and organisational measures to protect personal data. These include:

- Access controls: personal data is accessible only to staff with a legitimate need for it in their role.
- Encryption: sensitive personal data held digitally is encrypted at rest and in transit where technically feasible.
- Secure disposal: physical records are shredded; digital records are securely deleted at the end of the retention period.
- Vendor management: third-party processors (cloud storage, HR systems, survey platforms) are bound by data processing agreements that require equivalent security standards.

The Senior IT Technical Specialist maintains a record of key data processing activities and the security measures applied.

8. Data Breaches

A data breach is any security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. In the event of a suspected or confirmed breach:

- The incident is reported immediately to the Senior IT Technical Specialist and the CEO.
- Where the breach is likely to result in a risk to the rights and freedoms of individuals, Slow notifies the relevant supervisory authority within 72 hours of becoming aware.
- Where the breach is likely to result in a high risk to individuals, those individuals are notified without undue delay.
- All breaches, their impact, and the remediation actions taken are documented.

The escalation pathway for data breaches is set out in MGT-01 Section 3 (Escalation Pathways).

9. Transfers of Personal Data Outside the EEA

Where Slow transfers personal data to countries outside the European Economic Area (EEA) that do not have an adequacy decision, Slow relies on appropriate safeguards such as Standard Contractual Clauses (SCCs). Country-level data flows relevant to Slow's operations (Finland, Denmark, Germany, Singapore, Indonesia, Laos, Vietnam, Ethiopia) are mapped and documented by the CIO.

10. Retention

Personal data is retained only for as long as is necessary for its purpose. The full retention schedule is in MGT-07 Document Control SOP. Key periods:

- Employee HR records: duration of employment plus 7 years.
- Worker and farmer field data: 7 years from collection.
- Grievance records: 7 years from closure.
- FPIC records: permanent (or life of engagement plus 10 years).
- Age verification forms: 7 years from end of employment.

At the end of the retention period, personal data is securely deleted or anonymised.

11. Governance

The CIO is responsible for this Policy and for Slow's overall data protection compliance. The CIO acts as the designated data controller (and appoints a Data Protection Officer where legally required). Country Implementation Leads are responsible for compliance in field data collection activities.

12. Training

All staff complete annual data protection awareness training per MGT-06. Field staff receive specific training on handling personal data collected from farmers, workers, and communities.

13. Revision History

Version	Date	Author	Description of Changes
1.0	2026	Senior IT Technical Specialist	Initial release as Tier 3 Topic Policy. Establishes Slow's data protection framework in compliance with GDPR and applicable national laws. Particular attention given to personal data collected in field impact management activities (worker interviews, FPIC, grievances, age verification).

Sign-Off

Role	Name	Signature & Date
Senior IT Technical Specialist	Mark Nellemann	Signed by: Mark Nellemann 909AB71E931D445... Date: 6/1/2026
Chief Executive Officer	Sebastian Nielsen	Signed by: Sebastian Nielsen F57F8AB3E23746F... Date: 6/1/2026