DATA PROTECTION POLICY

GAZA SOCIETY FOR SUSTAINABLE AGRICULTURE AND FRIENDLY ENVIRONMENT (SAFE) – OCTOBER 2025

DATA PROTECTION POLICY

1. INTRODUCTION

SAFE is committed to protecting the personal data of all stakeholders (beneficiaries, staff, partners, donors, etc.) in accordance with international standards. This policy sets out our framework for lawful, fair, and transparent data processing. It is rooted in the principles of respect for human dignity and the protection of vulnerable people. In the absence of a specific Palestinian data protection law (no comprehensive law has been enacted), SAFE adopts best-practice standards (GDPR principles, OECD Privacy Guidelines, ICRC/UN guidance) and will review alignment as local law evolves. This policy applies to all SAFE staff, volunteers, projects, and third parties handling SAFE data.

2. SCOPE AND APPLICABILITY

This policy covers *all* personal data ("any information relating to an identified or identifiable natural person") processed by SAFE, whether in electronic or paper form. It applies to data about beneficiaries, program participants, employees, volunteers, donors, suppliers, and other stakeholders. All SAFE personnel and data processors must comply.

3. DEFINITIONS

- **Personal Data:** Any information relating to an identified or identifiable individual.
- **Sensitive (Special-category) Data:** Personal data which, if disclosed, may lead to discrimination or repression (e.g. health, race, religion, political opinions). These require extra safeguards.
- **Data Subject:** The individual to whom personal data belongs.
- **Processing:** Any operation on personal data (collecting, storing, using, sharing, etc.).
- **Data Controller:** The person/organization determining the purposes and means of processing. (SAFE is the Controller for data it collects.)
- **Data Processor:** The person/organization processing data on behalf of the Controller (e.g. cloud providers or consultants). A **Sub-Processor** is engaged by a Processor to assist in processing.
- **Third Party:** Any entity other than the Data Subject, Controller, or Processor.

- **Data Protection Officer (DPO):** SAFE's appointed officer or office responsible for data compliance. (DPO is defined as SAFE's internal data protection office or officer.)
- **Data Breach:** Unauthorized access, disclosure, alteration or destruction of personal data.
- **Data Protection Impact Assessment (DPIA):** A risk assessment for high-risk processing projects.

4. LEGAL BASIS FOR PROCESSING

SAFE will only process personal data on legitimate legal grounds, consistent with GDPR and UN/ICRC guidance. Lawful bases include:

- **Consent:** A freely given, specific, informed indication of the subject's agreement. Consent is required for processing sensitive data (unless another legal basis applies) and must be documented.
- **Legitimate Interests:** Where SAFE has a genuine organizational need (e.g. sending newsletters, protecting its rights). For example, "SAFE has a legitimate interest" in processing donor data to administer donations.
- **Contract:** When processing is necessary to fulfill contractual obligations (e.g. employee contracts).
- **Legal Obligation:** Where SAFE is required by law (e.g. tax/accounting records).
- **Vital Interests:** In emergencies or to protect someone's life, especially in humanitarian crises.
- **Public Interest/Mission:** For core SAFE activities (e.g. identity registration in aid programs) – akin to "public interest" basis used by humanitarian agencies. However, even then, SAFE will respect consent and dignity.

All sensitive (special-category) data require either explicit consent **or** another strict condition (e.g. vital interest in emergencies). For example, health data of beneficiaries may be processed only with consent or in life-saving situations.

5. DATA CATEGORIES AND PURPOSES

SAFE will maintain an up-to-date data inventory. Personal data categories likely include:

- **Beneficiaries/Participants:** Names, contacts, demographics, project history. *Purpose:* Program registration, needs assessment, service delivery, monitoring.

- **Staff and Volunteers:** Identification, contact, employment/volunteer records, CVs, performance reviews. *Purpose:* HR management, payroll, security checks.
- **Donors and Partners:** Names, addresses, donation/payment history. *Purpose:* Fundraising, reporting, acknowledgement, contractual liaison.
- **Service Users/Public Contacts:** Newsletter/mailing list details. *Purpose:* Outreach, information provision.
- **Administrative/Finance Records:** Accounting data linking to individuals. *Purpose:* Financial management, audit.

Each data category is collected for **specific, explicit purposes** only. For example, beneficiary data collected for welfare assistance will not be repurposed without notice. SAFE will document the purpose at or before collection and inform data subjects (e.g. via privacy notices). This aligns with the *purpose limitation* principle and OECD's "purpose specification" principle.

6. LAWFUL PROCESSING PRINCIPLES

SAFE adheres to core data protection principles (mirroring GDPR Art.5):

1. **Lawfulness, Fairness, Transparency:** Data must be processed fairly and lawfully, and SAFE will be open with subjects about how their data is used. Privacy notices (website, forms) will explain collection purposes, sharing, and retention.
2. **Purpose Limitation:** Data shall be collected for clear purposes and not used beyond those purposes.
3. **Data Minimization:** Only the minimum data necessary for each purpose will be collected. "Personal data collected shall be adequate, relevant and not excessive". SAFE will regularly review data inventories to remove redundant data.
4. **Accuracy:** Data must be accurate and kept up to date. Procedures will allow subjects to request corrections.
5. **Storage Limitation:** Data will not be kept longer than necessary for the purpose. "Personal data should not be kept longer than is necessary". A retention schedule (below) defines periods. Data will be securely deleted or anonymized after retention expiry.
6. **Integrity and Confidentiality:** Data must be kept secure. SAFE will implement robust technical and organizational security measures (encryption, access controls, backups, etc.). Any person

accessing SAFE data must have authorization and appropriate safeguards (passwords, MFA, locked storage, confidentiality agreements).

7. DATA SUBJECT RIGHTS AND PROCEDURES

SAFE recognizes and will facilitate data subject rights (mirroring GDPR rights), including:

- **Right of Access:** Individuals may ask if their data are processed and obtain a copy. "Beneficiaries have the right to request access … to the data that are being processed". SAFE will verify requesters' identity and respond in writing (typically within 30 days).
- **Right to Rectification:** Individuals may correct inaccurate or incomplete data. SAFE will correct errors promptly upon validated request.
- **Right to Erasure ("Right to be forgotten"):** Individuals may request deletion of their data if no longer needed for the original purpose and no overriding SAFE need exists. As ICRC guidance notes, beneficiaries "should be able to rectify incorrect data… and, in certain circumstances, to have their data deleted". SAFE will assess each request, balancing data integrity against privacy, and erase data where justified (e.g. withdraw of consent, fulfillment of purpose).
- **Right to Restrict Processing:** Individuals may ask to limit processing while a dispute is resolved (e.g. pending rectification).
- **Right to Object:** Individuals may object to certain processing (e.g. direct marketing or processing based on legitimate interest). Such objections will be reviewed case-by-case.
- **Right to Data Portability:** If data were collected by automated means and the processing is based on consent or contract, individuals can request their data in a transferable format.
- **Right to Lodge Complaint:** Individuals can complain to SAFE's DPO or governing body about any privacy concern. They also may seek remedy from a relevant supervisory authority (if applicable) or through legal channels.

SAFE will establish clear procedures for rights requests (e.g. DPO email or web form). Requests will be logged, verified (to prevent fraud), and handled promptly (within statutory periods, e.g. 30 days) in a user-friendly manner.

8. CONSENT AND SPECIAL CATEGORIES

Where consent is used as the legal basis, it must meet the high standard of being freely given, specific, informed and unambiguous. SAFE will obtain explicit written or electronic consent where

required (e.g. for newsletters or photos), and will keep records of consent (who, when, for what purpose). Consent to sensitive data must be **explicit** and revocable at any time.

Whenever sensitive data are processed, SAFE will implement "privacy by design" safeguards and will restrict access (encryption, limited personnel). In emergency cases where consent cannot be obtained, SAFE will rely on a vital-interest basis (e.g. life-threatening health data) or public interest, but will still protect such data stringently.

9. DATA RETENTION SCHEDULE

Data Category	Example Data	Retention Period	Notes/Legal Basis
Beneficiary Records	Contact info, case files, assessments	5 years after case closure	Retain for program accountability; then securely deleted/anonymized.
Employee/Volunteer Files	Contracts, IDs, payroll records	7 years after termination/employment	Matches typical audit/legal needs; then purge personal info.
Financial & Tax Records	Invoices, receipts, donor gifts	7 years (per accounting norms)	Satisfies financial regulations; then destroy confidentially.
Donor Data	Names, contact, donation history	7 years after last donation or relationship	For donor relations and audit; subject to donor requests.
Partner/Contractor Data	Agreements, contact details	7 years after contract end	For contractual obligations and liability; then delete.
Marketing/Mailing Lists	Newsletter subscriptions	Until subscription ends or 3 years inactivity	Respect opt-out; periodic re-consent.
Surveillance/CCTV (if any)	Video/image recordings	30 days (unless incident requires longer)	Short-term for security; longer retention only if legal issues.
IT Logs, Backups	Audit trails, system logs	1 year (or as long as system lifecycle)	For security audits; securely overwrite when obsolete.

Data Category	Example Data	Retention Period	Notes/Legal Basis
Consent Forms	Signed consent documents	3 years after last use	For evidence of lawful basis; then destroy.

10. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

SAFE will implement appropriate safeguards to ensure confidentiality, integrity, and availability of personal data. These include:

- **Access Control:** Data access is restricted on a need-to-know basis. User accounts and passwords are unique; multi-factor authentication (MFA) is used where feasible. Physical access to archives or servers is controlled (locked offices/rooms, keycards). Confidentiality agreements (NDAs) are signed by relevant staff and contractors.
- **Encryption:** Sensitive data (especially personal identifiers or sensitive categories) must be encrypted both in transit (SSL/TLS for networks, HTTPS for web) and at rest (disk or database encryption). Portable devices (laptops, USB drives) must be encrypted. Encryption keys are securely managed and not shared.
- **Secure Systems:** All computers and servers are kept updated with security patches. Antivirus and firewall protection are in place on networks and devices. Regular backups are performed and encrypted; backups are tested for integrity.
- **Data Minimization Techniques:** Only necessary personal data fields are enabled in systems. Where possible, data are pseudonymized or anonymized (e.g. use ID codes instead of names) so that identities are not exposed to staff who do not need to know.
- **Disposal:** When data or equipment are no longer needed, SAFE will securely delete or destroy them (e.g. shredding paper, crypto-shredding electronic data) to prevent recovery.
- **Incident Response:** Staff are trained to report any suspected data breach immediately to the DPO or IT manager so that action can be taken quickly.
- **Physical Security:** Offices housing personal data are locked when unattended. Visitor access is logged and supervised.
- **Vulnerability Management:** SAFE will regularly assess systems (network scans, penetration tests) to detect and fix vulnerabilities. Service providers (cloud or software vendors) must demonstrate adequate security (e.g. ISO 27001, SOC 2 certifications). SAFE will review third-party security practices and require contractual assurances.

11. THIRD-PARTY AND PROCESSOR AGREEMENTS

When SAFE engages third-party processors (cloud services, data management firms, consultants), it will ensure they comply with this policy and with data protection standards. Each third-party contract will include:

- A data processing agreement binding the vendor to process data only on SAFE's instructions and to implement equivalent security measures.
- Confidentiality and non-disclosure clauses covering personal data (discretion clauses).
- Clear stipulations on breach notification: processors must notify SAFE promptly of any security incident.
- Requirements that any sub-processors are pre-approved by SAFE and are bound by similar obligations. (A **Sub-Processor** is defined as a third party engaged by a processor to process data.)
- Right to audit or demand security audits/certifications.

Before any data transfer to a new vendor, SAFE will evaluate the risks (e.g. location of data centers, local laws) and insist on measures (encryption, access restrictions). A table of key third-party relationships and risk levels will be maintained.

12. Data Breach Notification Procedures

In the event of a data breach, SAFE will follow these steps:

1. **Containment and Assessment:** Immediately secure systems to prevent further data loss. The DPO, IT manager, and senior management will convene a breach response team to assess the scope and severity. External forensic or legal assistance may be sought.
2. **Notification:** SAFE will notify the Board of Directors and executive management without undue delay. If local law requires (or if donors require notification), SAFE will notify the relevant data protection authority or regulator. Although Palestinian law has no specific DPA, SAFE will consider notifying international partners or donors as needed. Subject to legal advice, SAFE will also notify affected individuals if there is a high risk to their rights and freedoms (e.g. identity theft). Notifications to individuals will be prompt, transparent and in clear language, providing guidance on protective steps. (This follows the principle of notifying "affected individuals" promptly.)

3. **Documentation:** The DPO will document all details of the breach (what happened, data involved, actions taken) for accountability and future learning.
4. **Remediation:** SAFE will take corrective actions to fix vulnerabilities and improve safeguards. Policies/procedures will be updated to prevent recurrence.

13. DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

SAFE will conduct DPIAs for any new processing project likely to pose high privacy risks (e.g. large-scale collection of sensitive data, systematic monitoring). A DPIA (impact assessment) is defined as "an assessment that identifies, evaluates and addresses the risks to personal data". The DPIA process includes: describing the processing, assessing necessity and proportionality, identifying risks to individuals, and defining mitigation measures. The DPO will guide staff through DPIAs using the ICRC's decision framework or similar tools. Findings will be reviewed by management before launching the project. (See Annex C for a DPIA template.)

14. ROLES AND RESPONSIBILITIES

- **Board of Directors / Executive Management:** Overall accountability for SAFE's compliance. Approves the Data Protection Policy and ensures adequate resources are allocated (staffing, technology, training).
- **Data Protection Officer (DPO):** Oversees data protection program. Responsibilities include: monitoring compliance with this policy; advising on obligations and best practices; conducting audits and DPIAs; handling data subject requests and breach response; serving as contact point for authorities or partners. The DPO reports to senior management and has independence to act.
- **Program and Department Managers:** Implement policy in their areas (e.g. ensure project data is handled per this policy, support DPIAs, train teams). Approve data collection plans and ensure retention schedules are followed.
- **All Staff and Volunteers:** Must understand and follow this policy. They are responsible for securely handling data they use, reporting any breaches or concerns immediately, and respecting data subject rights (e.g. handing over data upon request). Training will emphasize individual duties.
- **IT and Security Team:** Maintain technical safeguards, access controls, and conduct security assessments.

15. TRAINING AND AWARENESS

SAFE will provide regular training for all staff and volunteers on data protection policies and procedures. New staff will receive data protection orientation on hiring. Annual refresher sessions (in-person or e-learning) will cover topics such as recognizing data breaches, secure data handling, and rights of individuals. Public awareness materials (posters, guidelines) will remind staff of good practices (e.g. locking computer screens, not sharing passwords).

16. AUDIT AND REVIEW SCHEDULE

SAFE's Data Protection compliance will be reviewed at least annually. The DPO will coordinate internal audits of data flows, retention practices, and security controls. Findings will be reported to management with recommendations for improvement. Policy and procedures will be updated as needed (e.g. to reflect new laws, technologies, or incidents). Major changes to processing (e.g. new database systems, significant projects) will trigger a policy review.

17. ACCOUNTABILITY AND GOVERNANCE

SAFE's governance of data protection is illustrated above. The Board/Executive Director has ultimate responsibility, delegating oversight to the DPO. The DPO works with a Data Protection Committee (comprising representatives of IT, HR, Programs, and Legal) to implement and monitor compliance. All major data-related decisions (new systems, major data sharing) must involve the DPO. This structure ensures that data protection is integrated into SAFE's decision-making and program management.

18. AUDIT, REVIEW, AND CONTINUOUS IMPROVEMENT

SAFE will maintain a regular audit cycle. The DPO will conduct or coordinate audits of data handling practices at least once per year. Audit findings and any incident investigations will be reported to the Board and used to refine the policy. Key performance indicators (KPIs) such as number of training sessions delivered, incidents reported, and DPIAs completed will be tracked. This ensures SAFE's data protection measures remain effective and adapt to new risks.