Estonian Refugee Council's Data Protection Policy

1. Introduction

The Estonian Refugee Council (ERC) is committed to safeguarding the personal data of its beneficiaries, staff, partners, individual donors, and other stakeholders. This Data Protection Policy outlines the principles and procedures that govern the collection, processing, storage, and disposal of personal data in compliance with applicable EU and national legislations as well as humanitarian principles. This policy applies to all personal data processed by the ERC, regardless of the medium or format, and to all individuals and entities acting on behalf of the ERC.

2. Data protection principles

ERC adheres to the following data protection principles:

- **Lawfulness, fairness, and transparency:** Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- **Purpose limitation:** Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data minimisation:** Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.
- **Storage limitation:** Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Integrity and confidentiality:** Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. Purpose of processing personal data

ERC processes personal data in order to provide services which are requested by individuals and to fulfil its legal obligations which is reasoned by relevant laws and

regulations. ERC approaches any personal data in line with its mission of providing humanitarian assistance to people in need and processing activities are limited to specified purposes. The term “processing activities” refers to any operation or set of operations performed on personal data by ERC; which includes storing, collecting, retrieving, using, combining, erasing and destroying personal data, and can involve automated or manual operations.

4. Personal data that ERC processes

ERC processes the following personal data through lawful and transparent means and obtains the consent of data subjects where necessary. Categories of personal data that ERC depends on type of engagement of data subjects with the organization:

- **Beneficiaries:** Basic personal data including but not limited to full name, contact details, identification numbers, nationality, gender, age, family composition, health information, financial information, and any other data necessary to provide humanitarian assistance services.
- **Employees, volunteers, members:** Personal data in order for ERC to maintain its legal obligations and employer responsibilities including but not limited to full name, contact details, identification numbers, banking information, employment history, educational background, emergency contact details, criminal record history (if applicable).
- **Individual donors:** Full name, national ID number (if person has indicated need for tax return), contact detail, donation records, and any other data related to the engagement with ERC.
- **Individual contractors, implementing partners and service providers:** Full name, national ID number, contact detail, financial information, professional background, banking information, criminal record history and/or sanctions check (if applicable).

Specific rules regarding data protection and privacy per each ERC’s platform are outlined in Annex 1.

5. Data subject rights

ERC respects and upholds the following rights of data subjects:

- **Right to information:** Data subjects have the right to be informed about the collection and use of their personal data, as described in GDPR Article 12-14.
- **Right of access:** Data subjects have the right to access their personal data and obtain information about how it is being processed, as foreseen in GDPR Article 15.

- **Right to rectification:** Data subjects have the right to have inaccurate personal data corrected or completed if it is incomplete, as foreseen in GDPR Article 16.
- **Right to erasure:** Data subjects have the right to have their personal data erased under conditions and limitations foreseen in GDPR Article 17.
- **Right to data portability:** Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format and have the right to transmit those data to another controller without hindrance in accordance with GDPR Article 20.
- **Right to object:** Data subjects have the right to object to the processing of their personal data as described in GDPR Article 21.
- **Right to confidentiality of electronic communications:** Data subjects have the right to confidentiality and privacy in their electronic communications.

6. Data Protection Officer

ERC appoints a staff member in the capacity of Data Protection Officer (DPO) who is responsible for overseeing data protection strategy and implementation to ensure compliance with legal requirements. DPO is registered officially in the Estonian Business Registry (Äriregister).

In case of any questions, concerns, or requests regarding this policy or the protection of data subjects' personal data, contact should be established with the designated DPO at dpo@pagulasabi.ee.

7. Data security measures

ERC implements appropriate technical and organisational measures to ensure the security of personal data, including:

- **Access controls:** Restricting access to personal data to authorised personnel only.
- **Security audits:** Conducting regular security audits (by ERC's own staff or external) to assess the effectiveness of data protection measures.
- **Incident reporting:** Establishing procedures to detect, report, and respond to data breaches promptly (see below).

8. Data management and confidentiality

ERC maintains strict controls within its data management processes to ensure compliance with data protection and confidentiality rules, including:

- **Data classification:** Classifying data based on sensitivity and implementing handling procedures accordingly.

- **Secure storage:** Storing physical and electronic documents containing personal data securely to prevent unauthorised access.
- **Retention and disposal:** Retaining documents containing personal data only for as long as necessary and disposing of them securely when no longer required.

Specific rules regarding data protection and privacy per each ERC's platform are outlined in Annex 1.

9. Incident reporting

ERC is committed to responding promptly to any data protection incidents or breaches. In case of a data incident:

- **Incident detection and notification:** Staff must report suspected or confirmed data breaches immediately to the DPO (preferably using the incident report template available on Siseveeb).
- **Assessment:** The DPO will assess the severity of the incident and determine the appropriate response.
- **Containment and remediation:** Immediate actions will be taken to contain the breach and prevent further unauthorised access.
- **Notification:** Affected individuals will be notified if their personal data is at risk, in compliance with legal requirements.
- **Documentation:** All incidents are documented, and lessons learned are used to improve security measures.

10. Training and awareness

ERC is committed to ensuring that all staff and partners (if they have access to any of the tools and platforms) are aware of their data protection responsibilities through:

- **Training:** Providing regular training sessions on data protection principles, policies, and procedures.
- **Policy accessibility:** Ensuring that data protection policies and procedures are readily accessible to all staff and associates.
- **Ongoing awareness:** Promoting a culture of data protection awareness through continuous communication and updates.

11. Monitoring and policy review

This policy is reviewed annually or as required to ensure its relevance and effectiveness in light of any legal or organisational changes. Regular audits and assessments are conducted to monitor adherence to this policy.

Annex 1: Data protection and privacy regulations for ERC's online tools and platforms

This document outlines the different online platforms used by the Estonian Refugee Council (ERC), the personal data stored in each platform, and the data protection regulations pertaining to the use and storage of that data.

---

1. ERC Website (www.pagulasabi.ee)

- **Purpose of data collection:** To facilitate communication and engagement through newsletter subscriptions and to accept donations.
- **Personal data collected:**
    - Newsletter subscriptions: E-mail address
    - Donations: Name, e-mail address, personal code (but possible to remain anonymous)
- **Grounds for data collection:** Personal data is collected only with explicit consent (opt-in for newsletter subscriptions). Data is used exclusively for sending newsletters or donation receipts.
- **Data storage:** SQL database.
- **Access restrictions:** Subscription and donor data is only accessible to authorised staff handling communications and donor relations.
- **Data retention:**
    - Newsletter subscription data: retained until the user unsubscribes.
    - Donation records: retained for seven years as per financial record-keeping obligations, anonymised thereafter.

---

2. Cash Assistance Platform (register.pagulasabi.ee and cash.pagulasabi.ee)

- **Purpose of data collection:** To manage applications for cash assistance and process eligibility.
- **Personal data collected:**
    - Name, contact details (phone number, e-mail address)
    - Home address
    - Details of household members (names, ID numbers)
    - Passport copies and other identification documents
    - Documents proving vulnerability (e.g., medical certificates, financial records)
    - Bank account details

- **Grounds for data collection:** Personal data is processed based on the applicant's explicit consent and in accordance with legal obligations.
- **Data storage:** SQL database, secure file system.
- **Access restrictions:** Data access is strictly limited to authorised caseworkers and programme administrators through a secure online system with two-factor authentication (TFA) for access. All uploaded documents are encrypted and securely stored in ERC servers.
- **Data retention:** Application data is retained for the duration of programme eligibility plus three years after programme closure for audit purposes.

---

3. Livelihoods Platform (livelihoods.pagulasabi.ee)

- **Purpose of data collection:** To manage applications for livelihoods and economic recovery programmes.
- **Personal data collected:**
    - Name, contact details (phone number, e-mail address)
    - Application form details (e.g., employment history, educational background)
    - Supporting documents (e.g., CVs, proof of eligibility)
- **Grounds for data collection:** Personal data is processed based on the applicant's explicit consent and in accordance with legal obligations. Personal data is used exclusively for programme enrolment and support.
- **Data storage:** SQL database, secure file system.
- **Access restrictions:** Data access is restricted to programme administrators and livelihoods officers through a secure online system with two-factor authentication (TFA) for access.
- **Data retention:** Application data is retained for the duration of programme eligibility plus three years after programme closure for audit purposes.

---

4. Protection Platform (www.asyluminestonia.ee)

- **Purpose of data collection:** To facilitate registration for protection-related events (e.g., community engagement events, trainings and workshops, information sessions).
- **Personal data collected:**
    - Name
    - Contact details (phone number, e-mail address)
    - Home address
    - Details of household members (names, ID numbers)
    - Case management journal entries

- **Grounds for data collection:** Personal data is collected with the beneficiary's consent.
- **Data storage:** SQL database, secure file system.
- **Access restrictions:** Data access is limited to protection and empowerment officers and their managers through a secure online system with two-factor authentication (TFA) for access.
- **Data retention:**
    - Case management: retained for the duration of programme eligibility plus three years after programme closure for audit purposes.
    - Event registration details: retained until the event concludes plus 1 year for reporting purposes.

---

5. HR Platform

- **Purpose of data collection:** To manage job applications and recruitment processes.
- **Personal data collected:**
    - Name
    - Contact details (phone number, e-mail address)
    - Curriculum Vitae (CV) and other supporting documents
- **Grounds for data collection:** Personal data is processed as part of the recruitment process based on the applicant's explicit consent.
- **Data storage:** SQL database, secure file system.
- **Access restrictions:** Access is limited to HR personnel and hiring managers.
- **Data retention:**
    - Unsuccessful applications: retained for 24 months after the hiring decision.
    - Successful applicants: data transferred to the internal management system (Siseveeb) upon hiring.

---

6. Internal Management System *Siseveeb* (siseveeb.pagulasabi.ee)

- **Purpose of data collection:** To retain employee records and other internal documentation.
- **Personal data collected:**
    - Name
    - Contact details (phone number and e-mail address)
    - Home address
    - Bank account information
    - Employment contract and all of its annexes

    - Scanned copy of passport or ID
    - Scanned copies of educational diplomas and certificates
    - Emergency contact
- **Grounds for data collection:** Personal data is processed during the onboarding process of a new employee based on legitimate interest (contact information, education) or in accordance with legal obligation (submitting employee taxes to the tax office, etc).
- **Data storage:** SQL database, secure file system.
- **Access restrictions:** Access is limited to the HR and Finance departments of particular Country Offices for their own staff members. Head office HR and Finance departments have access to all staff records.
- **Data retention:** Employee records are retained as per national legislation.

---

7. Complaint and Feedback Mechanism (cfm.pagulasabi.ee)

- **Purpose of data collection:** To collect feedback and complaints from stakeholders.
- **Personal data collected:**
    - Name (optional)
    - Contact details (optional phone number or e-mail address)
    - Content of feedback or complaint (may include personal details)
- **Grounds for data collection:** Submission of personal data is voluntary; anonymous submissions are accepted. Personal data is used solely for follow-up and resolution of the complaint or feedback.
- **Data storage:** SQL database, secure file system.
- **Access restrictions:** Access is restricted to the feedback/complaints management team (under MEAL). Designated HR staff have access to sensitive complaints (as described in the Complaint and Feedback Mechanism).
- **Data retention:** Feedback/complaint records are retained for 24 months after resolution for accountability and reporting purposes.