Data Security Policy

1. Introduction

This Data Protection Policy outlines how E-Finance (the “Company”) processes and protects personal data relating to customers, suppliers, employees, and other third parties (the “Data Subjects”).

The Company acts as a data controller in relation to personal data processed during its business operations.

1.1 Scope of Data

This Policy applies to all personal data, defined as any information that identifies or may be used to identify a Data Subject, either directly or indirectly.

It applies irrespective of:

- The format or storage medium in which the data is held;
- Whether the data relates to past or present individuals;

1.2 Applicability

This Policy applies to:

- Employees;
- Contractors;
- Consultants;
- Directors and management;
- Any individual processing data on behalf of the Company;

All such persons are required to comply with this Policy when handling personal data.

1.3 Compliance

Compliance with this Policy is mandatory;

Failure to comply may result in disciplinary action;

All staff must complete relevant training and understand their responsibilities under this Policy.

1.4 Internal Use

This Policy is intended for internal use only and must not be disclosed externally without prior approval from the Compliance Manager.

1.5 Amendments

The Company reserves the right to amend this Policy at any time.

1.6 Legal Framework

This Policy does not override applicable national data protection laws and shall be interpreted in accordance with such laws, including the General Data Protection Regulation (GDPR).

---

2. Scope and Responsibility

The Company recognizes that the lawful and secure processing of personal data is essential to maintaining trust and ensuring business continuity.

Failure to comply with applicable data protection laws may result in regulatory penalties and reputational harm.

Management is responsible for:

- Implementing appropriate controls and procedures;
- Ensuring staff training and awareness;
- Monitoring compliance with this Policy;

Any questions or concerns must be directed to the Compliance Manager, particularly in relation to:

- Determining the lawful basis for processing;
- Use of consent;
- Drafting privacy notices;
- Personal data breaches;
- Data Subject rights requests;
- New or modified processing activities (including DPIA requirements);
- Direct marketing compliance;

---

3. Data Protection Principles

The Company adheres to the core GDPR principles, including:

- Lawfulness, fairness, and transparency;
- Purpose limitation;
- Data minimization;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality;
- Accountability;

The Company must be able to demonstrate compliance with these principles at all times.

---

4. Lawfulness, Fairness, and Transparency

Lawful Processing

Personal data must be processed lawfully, fairly, and transparently. Processing is permitted only where a valid legal basis exists, including:

- Consent of the Data Subject;
- Performance of a contract;
- Compliance with legal obligations;
- Protection of vital interests;
- Legitimate interests (where not overridden by the rights of the Data Subject);

Each processing activity must have a clearly documented legal basis.

Consent

Where consent is relied upon:

- It must be freely given, specific, informed, and unambiguous;
- It must involve a clear affirmative action (no pre-ticked boxes or implied consent);
- It must be as easy to withdraw as it is to provide;
- Records of consent must be maintained;

Explicit consent may be required for:

- Processing sensitive personal data;
- Automated decision-making;
- Cross-border data transfers;

---

5. Purpose Limitation

Personal data must be collected for specified, explicit, and legitimate purposes and must not be processed in a manner incompatible with those purposes.

Data must not be used for new purposes unless the Data Subject has been informed and, where required, has provided consent.

---

6. Data Minimization

Personal data must be:

- Adequate;
- Relevant;
- Limited to what is necessary for the intended purpose;

Employees must:

- Process personal data only where required for their duties;
- Avoid collecting excessive or unnecessary data;
- Ensure data is deleted or anonymized when no longer needed;

---

7. Accuracy

Personal data must be accurate and kept up to date.

Inaccurate or outdated data must be corrected or deleted without delay.

Reasonable steps must be taken to verify accuracy both at the time of collection and periodically thereafter.

---

8. Storage Limitation

Personal data must not be retained longer than necessary.

Data must only be stored for legitimate business or legal purposes.

The Company must implement retention policies to ensure timely deletion.

Data Subjects must be informed of retention periods.

Third parties must also comply with deletion requirements where applicable.

---

9. Security, Integrity, and Confidentiality

Protection of Personal Data

Personal data must be protected using appropriate technical and organizational measures against:

- Unauthorized or unlawful processing;
- Accidental loss, destruction, or damage;

The Company will:

- Implement safeguards proportionate to its size and risk exposure;
- Use measures such as encryption and pseudonymization where appropriate;
- Regularly test and review security controls;

Employees must:

- Follow internal security procedures;
- Prevent unauthorized access or disclosure of data;
- Share data only with authorized parties that meet security standards;

Core Security Principles

- **Confidentiality** – Access is limited to authorized individuals;
- **Integrity** – Data remains accurate and reliable;
- **Availability** – Data is accessible when required;

Reporting a Personal Data Breach

A personal data breach includes any unauthorized access, disclosure, loss, or compromise of personal data.

In the event of a suspected breach:

- Do not attempt to investigate independently;
- Immediately report the incident to the Compliance Manager;
- Preserve all relevant evidence;

The Company will notify regulators and affected individuals where required by law.

---

10. Data Subject Rights

Data Subjects have the right to:

- Withdraw consent at any time;
- Access their personal data;
- Request correction or deletion;
- Restrict or object to processing;
- Opt out of direct marketing;
- Challenge automated decision-making;
- Be informed of data breaches;
- Lodge complaints with supervisory authorities;
- Request data portability where applicable;

Employees must:

- Verify the identity of the requester;
- Immediately escalate requests to the Compliance Manager;
- Ensure no unauthorized disclosure occurs;

---

11. Accountability

The Company must implement appropriate technical and organizational measures to ensure compliance and must be able to demonstrate such compliance.

The Company is responsible for:

- Maintaining adequate resources and controls;
- Appointing a responsible data protection lead;
- Integrating data protection into internal processes;
- Conducting staff training;
- Performing audits and compliance reviews;

Record Keeping

The Company must maintain accurate records of processing activities, including:

- Data controller details;
- Categories of personal data and Data Subjects;
- Processing purposes;
- Third-party recipients;
- Storage and transfer details;
- Retention periods;
- Security measures;

Records must also include:

- Evidence of consent;
- Data flow documentation;

Training and Audits

- All staff must complete mandatory data protection training;
- Training records must be maintained;
- Systems and processes must be regularly reviewed;

Privacy by Design and DPIAs

The Company must apply privacy by design principles when processing personal data, including:

- Implementing appropriate technical safeguards;
- Assessing risks prior to processing;
- Evaluating scope, cost, and impact;

A Data Protection Impact Assessment (DPIA) must be conducted for high-risk processing, including:

- Use of new technologies;
- Automated decision-making or profiling;
- Large-scale processing of sensitive data;
- Monitoring public spaces;

A DPIA must include:

- Description of processing activities;
- Necessity and proportionality assessment;
- Risk analysis;
- Risk mitigation measures;

Automated Decision-Making

Automated decision-making is generally restricted unless:

- Explicit consent is obtained;
- It is authorized by law;
- It is necessary for contract performance;

In such cases, the Company must:

- Inform Data Subjects;
- Explain the logic and consequences;
- Provide the option for human intervention;
- Allow decisions to be challenged;

A DPIA must be completed prior to implementation.

Direct Marketing

For direct marketing:

- Prior consent is required for electronic communications;
- “Soft opt-in” may apply for existing customers under certain conditions;
- Data Subjects must be able to opt out easily;
- Opt-out requests must be processed immediately;
- Suppression lists must be maintained;

Sharing Personal Data

Personal data may only be shared where appropriate safeguards are in place.

Internal Sharing
Permitted only where there is a legitimate business need and authorized access.

External Sharing
Permitted only where:

- It is necessary for service delivery;
- It complies with privacy obligations;
- Consent is obtained where required;
- Adequate security measures are implemented;
- Cross-border transfer rules are followed;
- A valid GDPR-compliant agreement is in place;