INNOVA
GLOBAL LIMITED

Data Security Policy

1. Introduction

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

The Company acts as a **data controller** for personal data processed in the course of its business activities.

1.1 Scope of Data

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

It applies regardless of:

- The format or storage medium of the data;
- 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 must 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;
- Staff must complete relevant training and understand their responsibilities;

1.4 Internal Use

This Policy is an internal document and must not be shared externally without prior authorization 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 must be interpreted in accordance with such laws, including the **General Data Protection Regulation (GDPR)**.

---

2. Scope and Responsibility

The Company recognizes that lawful and secure handling of personal data is essential for maintaining trust and ensuring business continuity.

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

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 cases involving:

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

---

3. Data Protection Principles

The Company adheres to the core principles of GDPR, 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 when 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 Data Subject rights);

Each processing activity must have a 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 silence);
- It must be as easy to withdraw as it is to give;
- Records of consent must be maintained;

Explicit consent may be required for:

- Sensitive personal data;
- Automated decision-making;
- Cross-border data transfers;

5. Purpose Limitation

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

- Personal data must not be used for new or different 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 when required for their job duties;
- Avoid collecting excessive or unnecessary data;
- Ensure data is deleted or anonymized when no longer required;

---

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 at the point 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 purposes or legal requirements;
- 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, risk exposure, and resources;
- Use measures such as encryption and pseudonymization where appropriate;
- Regularly test and evaluate security controls;

Employees must:

- Follow all internal security procedures;
- Protect sensitive data from unauthorized access or disclosure;
- Only share data with authorized third parties that meet security requirements;

Core Security Principles

- **Confidentiality** – Data is accessible only to authorized individuals;
- **Integrity** – Data is accurate and reliable;
- **Availability** – Data is accessible when needed by authorized users;

Reporting a Personal Data Breach

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

In the event of a suspected breach:

- Do not investigate independently;
- Immediately report 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 following rights:

- To withdraw consent at any time;
- To access their personal data;
- To request correction or deletion of data;
- To restrict or object to processing;
- To opt out of direct marketing;
- To challenge automated decision-making;
- To be informed of data breaches;
- To lodge complaints with supervisory authorities;
- To request data portability (in applicable cases);

Employees must:

- Verify the identity of the requester;
- Immediately forward any request to the Compliance Manager;
- Ensure no unauthorized disclosure of personal data;

11. Accountability

The Company must implement appropriate technical and organizational measures to ensure compliance with data protection principles and must be able to **demonstrate such compliance** at all times.

The Company is responsible for:

- Ensuring adequate resources and controls are in place;
- Appointing a responsible individual for data protection oversight;
- Integrating data protection into all internal policies and processes;
- Conducting regular training for staff;

- Performing audits and compliance reviews;

Record Keeping

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

- Data controller details;
- Types of personal data processed;
- Categories of Data Subjects;
- Processing purposes and activities;
- Third-party recipients;
- Storage locations and transfers;
- Retention periods;
- Security measures;

Records must also include:

- Evidence of consent;
- Data flow mapping;

Training and Audits

- All staff must complete mandatory data protection training;
- The Company must maintain records of training attendance;
- Systems and processes must be regularly reviewed to ensure compliance;

Privacy by Design and DPIAs

The Company must apply **privacy by design** principles when processing personal data.

This includes:

- Implementing appropriate technical measures (e.g., pseudonymization);
- Considering risks to Data Subjects before processing;
- Evaluating cost, scope, and impact of processing activities;

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 of public areas;

A DPIA must include:

- Description of processing and purposes;
- Assessment of necessity and proportionality;
- Risk analysis;
- Risk mitigation measures;

Automated Decision-Making (ADM)

Automated decision-making is generally prohibited where it significantly affects individuals unless:

- The Data Subject has given explicit consent;
- It is authorized by law;
- It is necessary for a contract;

In such cases, the Company must:

- Inform Data Subjects about automated processing;
- Explain the logic and consequences;
- Provide the right to human intervention;
- Allow individuals to challenge decisions;

A DPIA must be conducted before implementing such processing.

Direct Marketing

When conducting direct marketing:

- Prior consent is required for electronic marketing (email, SMS, etc.);
- “Soft opt-in” may apply for existing customers under specific conditions;
- Data Subjects must be able to easily opt out;
- Opt-out requests must be honored immediately;
- Suppression lists must be maintained to respect preferences;

Sharing Personal Data

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

Internal Sharing

Data may be shared within the Company only if:

- There is a legitimate business need;
- The recipient is authorized;

External Sharing

Data may be shared with third parties only if:

- It is necessary for service provision;
- It complies with the Privacy Notice;
- Consent is obtained where required;
- The third party implements adequate security measures;
- Cross-border transfer rules are respected;
- A valid GDPR-compliant contract is in place;