GDPR Compliance Policy

1. Introduction

Purpose of the Policy
The purpose of this policy is to ensure that Youco complies with the General Data Protection Regulation (GDPR) and the UK Data Protection Act. It sets out how Youco processes personal data and the rights of individuals in relation to their personal information. The policy aims to protect the privacy of all data subjects and ensure transparency in how data is handled.

Scope and Legal Framework
This policy applies to all employees, contractors, and anyone processing personal data on behalf of Youco. It covers all data collection, storage, processing, and sharing activities carried out by Youco and is governed by the GDPR and the UK Data Protection Act.

---

2. Key Definitions

Personal Data
Any information that relates to an identified or identifiable individual (data subject). Examples include names, addresses, email addresses, identification numbers, and IP addresses.

Special Categories of Data
Sensitive personal data such as racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, and data concerning sexual orientation.

Data Controller and Data Processor

- **Data Controller**: The entity that determines the purposes and means of processing personal data.
- **Data Processor**: The entity that processes personal data on behalf of the data controller.

Data Subject
The individual to whom the personal data relates.

---

3. Principles of Data Protection

Youco adheres to the following GDPR data protection principles:

Lawfulness, Fairness, and Transparency
Personal data must be processed lawfully, fairly, and in a transparent manner. Data subjects must be informed of how their data is used.

Purpose Limitation
Personal data should only be collected for specified, explicit, and legitimate purposes. It should not be processed further for incompatible purposes.

Data Minimisation
Data collected must be adequate, relevant, and limited to what is necessary for the intended purpose.

Accuracy
Youco must take reasonable steps to ensure that personal data is accurate and kept up to date.

Storage Limitation
Personal data should be kept in a form that permits identification of data subjects only for as long as necessary.

Integrity and Confidentiality (Security)
Appropriate security measures must be in place to protect personal data against unlawful processing, accidental loss, destruction, or damage.

---

4. Lawful Bases for Processing Data

Youco must have a valid lawful basis for processing personal data. These include:

Consent
The data subject has given clear consent for Youco to process their personal data for a specific purpose.

Contractual Necessity
Processing is necessary for a contract Youco has with the individual, or because the individual has asked Youco to take specific steps before entering into a contract.

Legal Obligation
Processing is necessary to comply with a legal obligation (not including contractual obligations).

Legitimate Interests
Processing is necessary for the legitimate interests of Youco or a third party, unless overridden by the data subject's rights and freedoms.

---

5. Data Subject Rights

Data subjects have the following rights under GDPR:

Right to Access
Data subjects can request access to their personal data and receive information about how it is being processed.

Right to Rectification
Data subjects have the right to request correction of inaccurate or incomplete data.

Right to Erasure (Right to be Forgotten)
Data subjects can request the deletion of their personal data under certain circumstances, such as when the data is no longer necessary for the purpose for which it was collected.

Right to Data Portability
Data subjects have the right to obtain and reuse their personal data for their own purposes across different services.

Right to Restrict Processing
Data subjects can request the restriction of their personal data processing in certain cases.

Right to Object
Data subjects have the right to object to the processing of their data for reasons such as direct marketing or processing based on legitimate interests.

Rights in Relation to Automated Decision-Making and Profiling
Data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, which produces legal effects concerning them.

---

6. Data Protection Impact Assessments (DPIA)

When to Conduct a DPIA
A DPIA is required whenever processing is likely to result in a high risk to the rights and freedoms of data subjects, such as when using new technologies or conducting large-scale data processing.

Risk Assessment and Mitigation
Youco will assess potential risks to personal data and implement measures to mitigate those risks. The DPIA process includes identifying data flows, evaluating potential impacts, and implementing security and privacy measures.

---

7. Data Breach Management

Identifying a Data Breach
A data breach occurs when there is unauthorised access, loss, or destruction of personal data. This can include both accidental and deliberate incidents.

Reporting and Notification Procedures
Youco must report certain types of data breaches to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach. Data subjects must also be informed if the breach poses a high risk to their rights and freedoms.

Corrective Actions
Once a breach is identified, Youco will take immediate steps to contain and mitigate the impact of the breach, including recovery and restoring data integrity.

---

8. Third-Party Data Sharing and Processing

Contracts with Data Processors
When engaging third-party data processors, Youco will ensure that data processing agreements are in place, stipulating how the processor will handle personal data in compliance with GDPR.

International Data Transfers
Personal data transferred outside the European Economic Area (EEA) must comply with GDPR regulations regarding international transfers. Youco ensures that appropriate safeguards are in place when transferring data abroad.

9. Employee Responsibilities

Training and Awareness
All employees handling personal data must undergo regular GDPR training to understand their responsibilities. This ensures that all staff are aware of how to protect personal data and comply with GDPR.

Handling Personal Data
Employees are responsible for handling personal data securely and in accordance with the principles outlined in this policy. They must ensure that data is used appropriately and only for its intended purpose.

Reporting Suspected Breaches
Employees must report any suspected data breaches to the Data Protection Officer (DPO) or designated compliance officer immediately.

---

10. Data Retention and Disposal

Retention Periods for Personal Data
Youco will retain personal data only for as long as necessary to fulfil the purposes for which it was collected. Once the retention period has expired, the data will be securely deleted.

Secure Disposal of Data
Data that is no longer needed must be disposed of securely. This includes using shredding, secure deletion software, or other methods to ensure the data cannot be recovered.

---

11. Data Security Measures

Physical and Technical Security Controls
Youco implements both physical and technical controls to protect personal data. Physical controls include secure premises and document storage, while technical controls include encryption, firewalls, and secure access systems.

Access Controls
Access to personal data is restricted to authorised personnel only. Role-based access control (RBAC) systems are used to limit access to sensitive data based on job responsibilities.

Encryption and Anonymisation
Youco uses encryption to protect data at rest and in transit. Anonymisation and pseudonymisation techniques are used where possible to minimise the risk of exposure.

12. Review and Updates

Regular Policy Reviews
This policy will be reviewed on an annual basis or whenever there are significant changes to the data protection laws or regulations. Youco will ensure that all necessary updates are incorporated and communicated to relevant stakeholders.

Updates in Response to Legal or Regulatory Changes
If there are changes in GDPR or data protection regulations, Youco will update this policy and notify all employees of the changes.