

GDPR Compliance Policy Draft Structure

1. Introduction

Brief overview of the purpose and scope of the policy.

2. Definitions

- Personal Data
- Processing
- Data Subject
- Data Controller
- Data Processor
- Supervisory Authority

3. Data Protection Principles

- Lawfulness, Fairness, and Transparency
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

4. Legal Bases for Processing

Description of conditions under which data processing is lawful, such as consent, contract, legal obligation, vital interests, public task, and legitimate interests.

5. Data Subject Rights

- Right to be Informed
- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Restrict Processing
- Right to Data Portability
- Right to Object
- Rights Related to Automated Decision-Making and Profiling

6. Data Collection and Processing

Details regarding the collection, use, and management of personal data.

7. Data Retention

Policies on how long different types of data are retained.

8. Data Security

- Technical and Organizational Measures
- Breach Notification Procedures

9. Third-Party Processors

Guidelines for working with third parties, including data sharing and data processing agreements.

10. International Data Transfers

Mechanisms for transferring data outside the EEA, such as Standard Contractual Clauses.

11. Data Protection Impact Assessments

Requirements for conducting DPIAs where relevant.

12. Data Protection Officer

Roles, responsibilities, and contact information if applicable.

13. Staff Training and Awareness

Outline of data protection training and awareness programs for employees.

14. Policy Review and Updates

Procedures for reviewing and updating the GDPR compliance policy.