GDPR Compliance Policy – ExampleCorp Ltd.

Purpose

This policy establishes how ExampleCorp Ltd. complies with the European Union's General Data Protection Regulation (GDPR). The company is committed to protecting the privacy and rights of all individuals whose personal data it processes.

Scope

This policy applies to all employees, contractors, and third-party vendors who process personal data on behalf of ExampleCorp Ltd. It covers all systems, processes, and data handling activities, including storage in cloud environments.

Lawful Basis for Processing (GDPR Article 6)

All personal data shall be collected and processed lawfully, fairly, and transparently. ExampleCorp identifies one or more lawful bases before processing personal data, such as consent, contractual necessity, or legitimate interest. Where consent is relied upon, individuals must be able to withdraw consent as easily as it was given.

Data Minimization and Retention (GDPR Articles 5 & 13)

Personal data collected shall be adequate, relevant, and limited to what is necessary. Data retention schedules are established by the Data Protection Officer (DPO), and personal data is deleted or anonymized when no longer required. Automated scripts remove outdated records from customer systems every 90 days.

Data Subject Rights (GDPR Chapter 3)

ExampleCorp provides mechanisms for individuals to exercise their rights under GDPR, including: the right of access to their personal data, the right to rectification of inaccurate information, the right to erasure ("right to be forgotten"), the right to data portability, and the right to object to automated decision-making. All requests are logged, verified, and resolved within 30 days of receipt.

Security and Technical Safeguards (GDPR Article 32)

All personal data is encrypted in transit and at rest. Access to personal data is restricted through multi-factor authentication. Annual penetration testing is performed by certified third-party vendors. Incident response procedures ensure that any data breach is reported to the supervisory authority within 72 hours.

Vendor and Third-Party Management (GDPR Article 28)

ExampleCorp ensures that all vendors with access to personal data sign Data Processing Agreements (DPAs). Vendor audits are conducted annually to verify GDPR compliance. Third parties are not allowed to subcontract processing without written authorization.

Data Transfers Outside the EU (GDPR Chapter V)

Where personal data is transferred outside the European Economic Area (EEA), ExampleCorp uses Standard Contractual Clauses (SCCs) approved by the European Commission. Additional safeguards such as encryption and pseudonymization are applied to mitigate transfer risks.

Data Protection Impact Assessments (GDPR Article 35)

High-risk processing activities undergo a Data Protection Impact Assessment (DPIA) prior to implementation. The DPO reviews and approves all DPIAs and maintains records of the assessments.

Breach Notification and Response (GDPR Articles 33–34)

Any employee discovering a potential personal data breach must report it immediately to the DPO. Incident reports include affected systems, data categories, and remediation actions. If required, affected individuals are notified without undue delay.

Training and Awareness

All employees undergo annual GDPR training. Records of attendance and completion are maintained by the HR department. New hires must complete privacy training within 30 days of joining.

Continuous Improvement

This policy is reviewed annually and updated as necessary to reflect changes in regulation, business processes, or technology.