# **GDPR Compliance Policy**

**Purpose**:

This policy outlines ACompany's commitment to compliance with the General Data Protection Regulation (GDPR) and sets out the principles by which personal data is managed, protected, and processed.

**Scope:**

This policy applies to all employees, contractors, and third-party service providers of ACompany who handle the personal data of individuals residing in the European Union (EU) or European Economic Area (EEA).

1. Key GDPR Principles

ACompany is committed to ensuring that personal data is:

1. Lawfully, fairly, and transparently processed
2. Collected for specified, explicit, and legitimate purposes
3. Adequate, relevant, and limited to what is necessary
4. Accurate and up-to-date
5. Stored only as long as necessary
6. Processed securely using appropriate technical and organizational measures

2. Legal Basis for Processing

ACompany will only process personal data when one or more of the following conditions apply:

* Consent has been given
* Processing is necessary for contract performance
* Legal obligation compliance
* Protection of vital interests
* Performance of a task in the public interest
* Legitimate business interest that is not overridden by individual rights

3. Data Subject Rights

ACompany respects the rights of data subjects, including:

* Right to access their data
* Right to rectification
* Right to erasure ("right to be forgotten")
* Right to restrict processing
* Right to data portability
* Right to object to processing
* Right to withdraw consent at any time

Requests can be sent to: `privacy@acompany.com`

4. Data Security

* All data is stored in secure environments with encryption-at-rest and encryption-in-transit.
* Access to personal data is limited to authorized personnel only.
* Regular audits and risk assessments are conducted.

5. Data Breach Response

* Any suspected personal data breach must be reported within **1 hour** to `security@acompany.com`.

* The Data Protection Officer (DPO) will assess and, if necessary, notify authorities within **72 hours**.

6. Data Processors and Third Parties

* Third parties handling personal data on behalf of ACompany must sign a **Data Processing Agreement (DPA)**.

* All third parties are vetted for GDPR compliance.

7. Training and Awareness

* Annual GDPR training is mandatory for all employees.

* New hires must complete data protection onboarding within 2 weeks of joining.

8. Data Protection Officer (DPO)

For questions, complaints, or requests, contact:

* **Name**: Jane Doe

* **Email**: `dpo@acompany.com`

* **Phone**: +1-800-555-0199

Failure to comply with this policy may result in disciplinary action, including termination and legal liability.