DATA PROCESSING AGREEMENT 2

40% Compliant

Effective Date: November 14, 2025
Document Type: Data Processing Agreement
Version: 1.0
Status: Sample Document for Compliance Testing

DISCLAIMER: *This is a sample contract generated for compliance testing purposes only. It should not be used as an actual legal agreement without proper legal review and customization for your specific requirements.*

DATA PROCESSING AGREEMENT - 40% GDPR COMPLIANT

This Data Processing Agreement ("Agreement") is entered into between the Controller and Processor.

1. DEFINITIONS

1.1 "Personal Data" means any information relating to an identified or identifiable natural person.

1.2 "Processing" means any operation performed on Personal Data.

1.3 "Controller" means the entity which determines the purposes and means of Processing.

1.4 "Processor" means the entity which Processes Personal Data on behalf of the Controller.

2. SCOPE AND PURPOSE

2.1 The Processor shall Process Personal Data only on documented instructions from the Controller.

2.2 Processing shall be for the purposes specified in Annex A.

2.3 The Processor shall inform the Controller if instructions appear to infringe data protection laws.

3. DATA PROTECTION PRINCIPLES (ARTICLE 5)

3.1 Personal Data shall be:

(a) Processed lawfully, fairly and in a transparent manner.

(b) Collected for specified, explicit and legitimate purposes.

(c) Adequate, relevant and limited to what is necessary.

(d) Accurate and kept up to date.

(e) Kept for no longer than necessary.

(f) Processed securely with appropriate technical and organisational measures.

4. LAWFULNESS OF PROCESSING (ARTICLE 6)

4.1 The Controller confirms that Processing has a lawful basis under Article 6:

(a) Consent from the Data Subject

(b) Necessary for contract performance

(c) Necessary for legal compliance

(d) Necessary to protect vital interests

(e) Necessary for public interest tasks

(f) Necessary for legitimate interests

5. CONSENT (ARTICLE 7)

5.1 Where Processing relies on consent:

(a) Consent shall be freely given, specific, informed and unambiguous.

(b) Data Subjects can withdraw consent at any time.

(c) Withdrawal shall be as easy as giving consent.

6. SPECIAL CATEGORIES OF DATA (ARTICLE 9)

6.1 Processing of special categories requires explicit consent or other legal basis under Article 9(2).

6.2 Enhanced security measures apply to special category data.

7. TRANSPARENCY (ARTICLES 12-14)

7.1 Information about Processing shall be provided in concise, transparent, intelligible form using clear language.

7.2 When collecting directly from Data Subjects (Article 13):

(a) Controller identity and contact details

(b) DPO contact details if applicable

(c) Purposes and legal basis for Processing

(d) Recipients of Personal Data

(e) Retention periods

(f) Data Subject rights (Articles 15-22)

(g) Right to withdraw consent

(h) Right to lodge complaint with supervisory authority

8. DATA SUBJECT RIGHTS (ARTICLES 15-22)

8.1 The Processor shall assist the Controller in responding to Data Subject requests:

(a) Right of access (Article 15): Confirmation of Processing and copy of data.

(b) Right to rectification (Article 16): Correction of inaccurate data.

(c) Right to erasure (Article 17): Deletion when no longer necessary.

(d) Right to restriction (Article 18): Limiting Processing in certain circumstances.

(e) Right to data portability (Article 20): Receiving data in machine-readable format.

(f) Right to object (Article 21): Objecting to Processing on legitimate interest grounds.

8.2 Requests shall be responded to within one month.

9. PROCESSOR OBLIGATIONS (ARTICLE 28)

9.1 The Processor shall:

(a) Process only on documented Controller instructions.

(b) Ensure personnel confidentiality.

(c) Implement appropriate security measures.

(d) Engage Sub-processors with Controller consent.

(e) Assist Controller with Data Subject requests.

(f) Assist with security and breach obligations.

(g) Delete or return data upon termination.

(h) Provide information to demonstrate compliance.

10. SUB-PROCESSORS

10.1 The Processor shall not engage Sub-processors without prior authorization.

10.2 Approved Sub-processors are listed in Annex B.

10.3 The Processor shall inform Controller of Sub-processor changes.

10.4 Sub-processor agreements shall impose equivalent obligations.

11. INTERNATIONAL TRANSFERS (CHAPTER V)

11.1 Transfers outside the EEA require:

(a) Adequacy decision; or

(b) Appropriate safeguards (Standard Contractual Clauses, Binding Corporate Rules)

11.2 Standard Contractual Clauses apply to transfers listed in Annex B.

12. SECURITY (ARTICLE 32)

12.1 The Processor shall implement appropriate technical and organisational measures:

(a) Pseudonymisation and encryption

(b) Ongoing confidentiality, integrity, availability and resilience

(c) Ability to restore availability after incidents

(d) Regular testing and evaluation of measures

12.2 Security measures are detailed in Annex C.

13. DATA BREACH NOTIFICATION (ARTICLES 33-34)

13.1 The Processor shall notify the Controller without undue delay upon becoming aware of a breach.

13.2 Notification shall describe:

(a) Nature of the breach

(b) Categories and numbers affected

(c) Likely consequences

(d) Measures to address the breach

13.3 The Controller shall notify the supervisory authority within 72 hours if required.

13.4 Data Subjects shall be notified if the breach poses high risk.

14. DATA PROTECTION IMPACT ASSESSMENT (ARTICLE 35)

14.1 The Controller shall conduct DPIA for high-risk Processing.

14.2 The Processor shall assist by providing:

(a) Description of Processing operations

(b) Assessment of necessity and proportionality

(c) Risks to Data Subject rights

(d) Mitigation measures

15. DATA PROTECTION OFFICER (ARTICLES 37-39)

15.1 The Processor has designated a Data Protection Officer:

Contact: dpo@processor.com

15.2 The DPO shall:

(a) Inform and advise on GDPR obligations

(b) Monitor compliance

(c) Advise on DPIAs

(d) Cooperate with supervisory authority

(e) Act as contact point

16. RECORDS OF PROCESSING (ARTICLE 30)

16.1 The Processor shall maintain records of Processing activities including:

(a) Name and contact details

(b) Categories of Processing

(c) International transfers

(d) Security measures description

17. AUDIT RIGHTS

17.1 The Controller may audit the Processor's compliance.

17.2 The Processor shall provide access to documentation, facilities and personnel.

17.3 Reasonable notice shall be provided unless urgent circumstances exist.

18. LIABILITY (ARTICLE 82)

18.1 The Processor is liable for damage caused by non-compliance or unauthorized Processing.

18.2 The Processor shall indemnify the Controller for fines and compensation arising from Processor breach.

19. TERM AND TERMINATION

19.1 This Agreement continues for the duration of Processing services.

19.2 Upon termination, the Processor shall delete or return all Personal Data.

20. GOVERNING LAW

20.1 This Agreement is governed by [Jurisdiction] law.

ANNEX A: PROCESSING DETAILS

Subject Matter: Customer data processing Duration: Term of commercial agreement

Nature and Purpose: - Data storage and hosting - Transaction processing - Customer support - Service analytics

Types of Personal Data: - Contact information (name, email, phone) - Account credentials - Transaction records - Usage data - IP addresses

Categories of Data Subjects: - Customers - Customer employees - End users

Retention Periods: - Active data: Duration of relationship - Transaction logs: 7 years - Analytics: 2 years - Backups: 90 days

ANNEX B: SUB-PROCESSORS

1. Cloud Provider Location: Ireland (EEA) Service: Infrastructure hosting Safeguards: ISO 27001, GDPR DPA

2. Email Provider Location: Germany (EEA) Service: Email communications Safeguards: SOC 2, Standard Contractual Clauses

3. Analytics Provider Location: United States Service: Data analytics Safeguards: Standard Contractual Clauses

ANNEX C: SECURITY MEASURES

Technical Measures: - Encryption: AES-256 at rest, TLS 1.3 in transit - Access controls: Multi-factor authentication, role-based access - Network security: Firewalls, intrusion detection - Monitoring: 24/7 security operations center - Backups: Daily backups with geo-redundant storage

Organisational Measures: - ISO 27001 certified - SOC 2 Type II compliant - Employee confidentiality agreements - Annual security training - Background checks for personnel with data access - Incident response procedures - Business continuity plan

Physical Security: - Biometric access controls - 24/7 surveillance - Secured data centers

Recovery: - RTO: 4 hours - RPO: 1 hour - Quarterly DR testing

---

END OF AGREEMENT

SIGNATURE PAGE

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

CONTROLLER	PROCESSOR
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____