DATA PROCESSING AGREEMENT

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

This Data Processing Agreement ("DPA") is entered into as of January 15, 2025, between TechCloud Solutions Inc. ("Processor") and Global Retail Corp. ("Controller").

1. DEFINITIONS AND INTERPRETATION

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, including collection, storage, use, disclosure, or deletion.

1.3 "Data Subject" means the individual to whom Personal Data relates.

1.4 "Supervisory Authority" means an independent public authority established by an EU Member State.

2. SCOPE AND DURATION

2.1 This DPA applies to all Processing activities performed by Processor on behalf of Controller in connection with the cloud hosting services described in the Master Services Agreement dated December 1, 2024.

2.2 The term of this DPA shall commence on the Effective Date and continue for the duration of the Master Services Agreement.

3. DATA PROCESSING OBLIGATIONS

3.1 Processor shall process Personal Data only on documented instructions from Controller, including with regard to transfers of Personal Data to a third country or international organization, unless required by applicable law.

3.2 Processor shall immediately inform Controller if, in its opinion, an instruction infringes GDPR or other applicable data protection provisions.

3.3 Processor shall ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. SECURITY MEASURES

4.1 Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:

(a) Encryption of Personal Data using AES-256 encryption for data at rest and TLS 1.3 for data in transit;

(b) Multi-factor authentication for all system access;

(c) Regular security assessments and penetration testing conducted quarterly;

(d) Pseudonymization and encryption of Personal Data where feasible;

(e) Ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems;

(f) Ability to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

(g) Regular testing, assessment and evaluation of the effectiveness of technical and organizational measures.

4.2 Access to Personal Data shall be restricted to authorized personnel on a need-to-know basis using role-based access controls.

5. SUB-PROCESSORS

5.1 Controller provides general authorization for Processor to engage sub-processors. Current sub-processors are listed in Annex A.

5.2 Processor shall inform Controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, giving Controller the opportunity to object.

5.3 Where Processor engages a sub-processor, Processor shall impose the same data protection obligations on the sub-processor via a written contract.

6. DATA SUBJECT RIGHTS

6.1 Processor shall assist Controller by implementing appropriate technical and organizational measures to fulfill Controller's obligation to respond to requests for exercising Data Subject rights, including:

(a) Right of access to Personal Data;

(b) Right to rectification of inaccurate Personal Data;

(c) Right to erasure ("right to be forgotten");

(d) Right to restriction of Processing;

(e) Right to data portability;

(f) Right to object to Processing.

6.2 Processor shall notify Controller within 48 hours of receiving any request from a Data Subject exercising their rights.

7. PERSONAL DATA BREACH NOTIFICATION

7.1 Processor shall notify Controller without undue delay after becoming aware of a Personal Data breach affecting Controller's data, and in any event within 24 hours of discovery.

7.2 The notification shall include, at a minimum:

(a) Description of the nature of the breach, including categories and approximate number of Data Subjects and Personal Data records concerned;

(b) Name and contact details of Processor's data protection officer or other contact point;

(c) Description of likely consequences of the breach;

(d) Description of measures taken or proposed to address the breach and mitigate its adverse effects.

7.3 Processor shall cooperate with Controller and provide all necessary assistance to enable Controller to notify the Supervisory Authority and affected Data Subjects as required by GDPR Article 33 and 34.

8. DATA PROTECTION IMPACT ASSESSMENT

8.1 Processor shall provide reasonable assistance to Controller with data protection impact assessments and prior consultations with Supervisory Authorities where required under GDPR Articles 35 and 36.

9. DELETION AND RETURN OF PERSONAL DATA

9.1 Upon termination of this DPA or upon Controller's written request, Processor shall, at Controller's choice, delete or return all Personal Data to Controller within 30 days, and delete existing copies unless storage is required by applicable law.

9.2 Processor shall provide written certification of deletion upon Controller's request.

10. AUDIT RIGHTS

10.1 Processor shall make available to Controller all information necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections, conducted by Controller or an auditor mandated by Controller.

10.2 Controller may conduct audits upon 30 days' prior written notice, during normal business hours, and no more than once per year unless there is reasonable suspicion of non-compliance.

11. INTERNATIONAL DATA TRANSFERS

11.1 Processor shall not transfer Personal Data outside the European Economic Area without Controller's prior written consent and implementation of appropriate safeguards under GDPR Chapter V.

11.2 Transfers to third countries shall be subject to Standard Contractual Clauses approved by the European Commission or other legally valid transfer mechanisms.

12. DATA RETENTION

12.1 Processor shall retain Personal Data only for the duration necessary to provide the services under the Master Services Agreement, unless longer retention is required by law.

12.2 Financial records and audit logs shall be retained for a minimum of seven years to comply with SOX requirements.

13. RECORDS OF PROCESSING ACTIVITIES

13.1 Processor shall maintain detailed records of all Processing activities carried out on behalf of Controller, including:

(a) Name and contact details of Processor and Controller;

(b) Categories of Processing;

(c) Categories of Data Subjects and Personal Data;

(d) Categories of recipients to whom Personal Data may be disclosed;

(e) Transfers to third countries;

(f) Time limits for deletion of different categories of data;

(g) Technical and organizational security measures.

14. COMPLIANCE WITH HIPAA (if applicable)

14.1 Where Processor processes Protected Health Information (PHI) as defined by HIPAA, Processor agrees to:

(a) Not use or disclose PHI except as permitted by this DPA or as required by law;

(b) Use appropriate safeguards to prevent unauthorized use or disclosure of PHI;

(c) Report to Controller any unauthorized use or disclosure of PHI within 24 hours of discovery;

(d) Ensure that any sub-contractors or agents that handle PHI agree to the same restrictions;

(e) Make PHI available to individuals as required under 45 CFR § 164.524;

(f) Make PHI available for amendment and incorporate amendments as required under 45 CFR § 164.526;

(g) Document disclosures of PHI and make information available as required under 45 CFR § 164.528.

15. LIABILITY AND INDEMNIFICATION

15.1 Processor shall indemnify and hold harmless Controller from any claims, damages, or fines resulting from Processor's breach of this DPA or applicable data protection laws.

15.2 Liability cap: Notwithstanding any limitation of liability in the Master Services Agreement, Processor's liability for breaches of this DPA shall not be capped and shall include all direct, indirect, and consequential damages.

16. TERM AND TERMINATION

16.1 This DPA shall remain in effect for the duration of the Master Services Agreement.

16.2 Controller may terminate this DPA immediately upon written notice if Processor materially breaches any provision and fails to cure within 15 days.

17. GOVERNING LAW AND JURISDICTION

17.1 This DPA shall be governed by the laws of Ireland and subject to the jurisdiction of Irish courts.

17.2 Any disputes arising from this DPA shall be subject to the exclusive jurisdiction of the supervisory authority in the Controller's EU Member State.

18. NOTICES

All notices under this DPA shall be sent to:

For Controller: Global Retail Corp. Data Protection Officer 123 Commerce Street, Dublin, Ireland Email: dpo@globalretail.com

For Processor: TechCloud Solutions Inc. Privacy Team 456 Tech Park, San Francisco, CA 94105, USA Email: privacy@techcloud.com

AGREED AND ACCEPTED:

CONTROLLER: Global Retail Corp. By: _____ Name: Sarah Johnson Title: Chief Privacy Officer Date: January 15, 2025

PROCESSOR: TechCloud Solutions Inc. By: _____ Name: Michael Chen Title: Chief Security Officer Date: January 15, 2025

ANNEX A - LIST OF SUB-PROCESSORS

1. AWS (Amazon Web Services) - Cloud infrastructure hosting (US-East-1, EU-West-1)

2. DataGuard Security Inc. - Security monitoring and intrusion detection 3. BackupPro Solutions - Automated backup and disaster recovery services 4. AnalyticsCo - Anonymized usage analytics and reporting

ANNEX B - TECHNICAL AND ORGANIZATIONAL MEASURES

1. Access Control - Role-based access control (RBAC) - Multi-factor authentication (MFA) mandatory - Unique user IDs for all system access - Automatic session timeout after 15 minutes of inactivity

2. Encryption - AES-256 encryption for data at rest - TLS 1.3 for data in transit - End-to-end encryption for sensitive communications - Hardware Security Modules (HSM) for key management

3. Network Security - Firewall protection with intrusion detection/prevention systems - Network segmentation and isolation - DDoS protection - Regular vulnerability scanning

4. Monitoring and Logging - 24/7 security operations center (SOC) - Real-time anomaly detection - Comprehensive audit logging (retained for 2 years) - Automated alerting for security incidents

5. Physical Security - SOC 2 Type II certified data centers - Biometric access controls - 24/7 on-site security personnel - Video surveillance with 90-day retention

6. Backup and Recovery - Daily automated backups - Geo-redundant backup storage - Recovery Time Objective (RTO): 4 hours - Recovery Point Objective (RPO): 1 hour

7. Incident Response - Documented incident response plan - Designated incident response team - Annual tabletop exercises - Post-incident review and remediation tracking

8. Employee Training - Annual data protection and security awareness training - Quarterly phishing simulation exercises - Background checks for all employees with data access - Confidentiality agreements signed by all personnel

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: _____