DATA PROCESSING ADDENDUM

Last Updated: 02 April 2026

This Data Processing Addendum ("**DPA**") forms part of the **Master Services Agreement** ("**Agreement**") between **Reg X Innovations Ltd.** ("**Processor**" or "**Reg X**") and the customer identified in the Agreement ("**Controller**" or "**Customer**").

This DPA sets out the parties' obligations with respect to the Processing of Personal Data in accordance with applicable Data Protection Laws, including Regulation (EU) 2016/679 ("**GDPR**"), the **UK GDPR**, the **Data Protection Act 2018**, and any applicable implementing, successor, or replacement legislation.

---

1. Scope and Roles

1.1 Roles

For the Personal Data processed under the Agreement, Customer acts as the **Controller** and Reg X acts as the **Processor**.

1.2 Instructions

Reg X shall process Personal Data only on documented instructions from Customer, including as necessary to provide, secure, operate, and improve the Services and to comply with applicable law. Where Processing is required by law, Reg X shall inform Customer in advance unless legally prohibited.

1.3 Customer Responsibility

Customer is responsible for the accuracy, quality, and legality of Personal Data and for ensuring that it has provided all required notices and obtained all necessary consents or lawful bases for Processing.

---

2. Processing Details

2.1 Subject Matter

Reg X provides regulatory reporting and compliance technology solutions, including data processing necessary for automation, reporting, analytics, and compliance support.

2.2 Duration

The duration of Processing shall be the term of the Agreement plus any applicable post-termination data retention period set out in this DPA.

2.3 Nature and Purpose

Processing includes hosting, storage, transmission, analysis, monitoring, support, billing, security, regulatory reporting, and permitted service improvements.

2.4 Types of Personal Data

- Identification data (e.g., name, job title)
- Contact details (e.g., email address, phone number)
- Professional data (e.g., company, role)
- System usage data (e.g., login credentials, IP address, activity logs)
- Regulatory reporting data where required for compliance

2.5 Categories of Data Subjects

- Employees
- Authorized users
- Client representatives
- End customers of the Customer

2.6 Special Categories of Data

None.

---

3. Compliance and Cooperation

3.1 Compliance

Reg X shall comply with its obligations under the GDPR, UK GDPR, and all applicable Data Protection Laws when acting as a Processor.

3.2 Assistance

Taking into account the nature of the Processing, Reg X shall reasonably assist the Customer, **at Customer's cost**, with:

- responding to Data Subject requests (Articles 12–23 GDPR);
- meeting security and risk-management obligations (Articles 32–36 GDPR);
- conducting Data Protection Impact Assessments; and
- consultations with supervisory authorities.

3.3 Data Subject Requests

If a Data Subject submits a request directly to Reg X, Reg X shall promptly notify Customer and shall not respond unless required by law or instructed in writing by Customer.

---

4. Confidentiality and Personnel

4.1 Reg X shall ensure that personnel authorized to process Personal Data are subject to appropriate confidentiality obligations and receive regular data protection and information security training.

4.2 Access to Personal Data shall be limited to personnel who require such access to perform the Services.

---

5. Security

5.1 Technical and Organizational Measures

Reg X implements appropriate technical and organizational measures ("**TOMs**") to ensure a level of security appropriate to the risk, including encryption in transit and at rest, access controls, least-privilege principles, multi-factor authentication for administrative access, logging and monitoring, secure development practices, vulnerability management, and business continuity and disaster recovery controls.

5.2 Documentation

The TOMs are described in **Annex II** and may be updated over time, provided that any update does not materially reduce the overall level of protection.

---

6. Sub-processors

6.1 Authorization

Customer provides Reg X with general authorization to engage Sub-processors to support the Services.

6.2 List and Changes

Reg X shall maintain a current list of Sub-processors available at: https://trust.reg-x.co.uk/. Reg X shall provide at least thirty (30) days' prior notice before adding or replacing a Sub-processor.
Customer may object to a new Sub-processor on reasonable data protection grounds by providing written notice within the notice period.

6.3 Liability

Reg X shall remain fully liable for the acts and omissions of its Sub-processors.

---

7. International Data Transfers

7.1 Transfer Mechanisms

Where Personal Data is transferred outside the EEA, United Kingdom, or Switzerland to a jurisdiction without an adequacy decision, the parties rely on the **Standard Contractual Clauses (EU 2021/914)**, supplemented by the **UK International Data Transfer Addendum** and Swiss adaptations where applicable, as set out in **Annex III**.

7.2 Supplementary Measures

Reg X shall implement appropriate supplementary technical, contractual, and organizational measures to ensure an essentially equivalent level of protection.

7.3 Certified Frameworks

Where applicable, participation in approved data-transfer frameworks (e.g., EU-U.S. Data Privacy Framework) may be relied upon without prejudice to the SCCs.

---

8. Personal Data Breaches

Reg X shall notify Customer of a Personal Data Breach **without undue delay and, where feasible, within seventy-two (72) hours** after becoming aware of the breach, and shall provide information reasonably required under Articles 33 and 34 GDPR.

---

9. Audits and Reports

9.1 Upon request, Reg X shall provide available third-party security certifications, audit reports, or responses to standardized security questionnaires.

9.2 Where required by law or a competent supervisory authority, Customer may conduct an audit no more than once annually, with reasonable prior notice, at Customer's cost, subject to reasonable confidentiality, security, and safety requirements.

9.3 Audits shall be limited in scope to systems used to process Customer Personal Data and shall avoid intrusive testing of shared or multi-tenant infrastructure.

---

10. Data Retention and Deletion

Customer Personal Data shall be retained for six (6) months following termination of the Agreement, **unless otherwise agreed in writing or required by applicable law**. Upon expiry of the retention period, Reg X shall delete or irreversibly anonymize the Personal Data.

---

11. Government and Third-Party Requests

11.1 Reg X shall not disclose Personal Data to public authorities unless legally compelled.

11.2 Where legally permitted, Reg X shall notify Customer of such requests and challenge unlawful or disproportionate demands.

11.3 Disclosures shall be limited to the minimum legally required information, and records of disclosures shall be maintained.

---

12. Liability and Order of Precedence

12.1 Each party's liability under this DPA is subject to the liability limitations in the Agreement, except where liability cannot be limited under applicable law.

12.2 In the event of a conflict, the **Standard Contractual Clauses prevail**, followed by this DPA, and then the Agreement.

---

13. Contact Details

Reg X Innovations Ltd. – Data Protection Contact
Email: **privacy@reg-x.co.uk**
Address:
30 Churchill Place
Canary Wharf Estate
London E14 5RE
United Kingdom

Data Protection Officer: Not applicable
EU Representative: Subbu Loganathan
UK Representative: Not applicable

Annex I – Details of Processing (GDPR Art. 28)

A. List of Parties

Data Exporter (Controller): Customer identified in the Agreement.
Contact: As specified in the Master Service Agreement

Data Importer (Processor): Reg X Innovations
Contact: privacy@reg-x.co.uk

B. Description of Transfer & Processing

Data Subjects:
Employees, authorized users, client representatives, and end customers.

Categories of Personal Data:
Identification data, contact details, professional info, system usage data, regulatory reporting data.

Sensitive Data:
No

Frequency: Continuous as required for the Services

Nature of Processing:
Hosting, storage, transmission, analysis, log processing, support, security monitoring.

Purposes of Transfer:
Service delivery, support, billing, security, service improvement (as permitted), compliance.

Retention:
6 months (as per Section 10)

Subprocessors:
https://trust.reg-x.co.uk/

C. Competent Supervisory Authority

Determined per GDPR Art. 56 and the exporter's establishment/representative.

Annex II – Technical & Organizational Measures (Security)

Reg X maintains TOMs including (non-exhaustive):

1. **Governance & Risk Management**
    - Information Security Management System (ISMS) aligned with ISO 27001, risk assessments at least annually.
2. **Access Controls**
    - Role-based access, least privilege, MFA for privileged accounts, SSO, strong password policies, periodic access reviews.
3. **Encryption**

- TLS 1.2+ in transit; AES-256 at rest; encryption key management with restricted access and rotation.

4. **Network & Infrastructure Security**
    - Segmentation, firewalls, WAF/CDN, DDoS protections, vulnerability scanning, timely patching, hardened baselines, container security.
5. **Application Security**
    - Secure SDLC, code reviews, dependency scanning, SAST/DAST, secret scanning, change management, pre-prod isolation.
6. **Monitoring & Logging**
    - Centralized logging, SIEM, anomaly detection, time sync, log retention with tamper-resistance.
7. **Incident Response**
    - Documented IR plan with defined RACI, regular tabletop exercises, 24×7 escalation.
8. **Business Continuity & Disaster Recovery**
    - Multi-AZ/region redundancy (where applicable), backups with periodic restore testing, RPO/RTO targets defined.
9. **Physical Security**
    - Data centers with industry-standard controls (badging, CCTV, visitor logs) via vetted providers.
10. **Vendor & Sub-processor Management**

- Security due diligence, DPAs/SCCs, continuous monitoring, contractual enforcement.

11. **Privacy by Design & Default**

- Data minimization, pseudonymization where feasible, configurable retention, privacy reviews for new features.

12. **Employee & Contractor Controls**

- Background checks where lawful, confidentiality agreements, security & privacy training at onboarding and annually.

(Reg X may update TOMs without materially diminishing protection.)

Annex III – Standard Contractual Clauses (EU 2021/914)

This Annex incorporates by reference the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 establishing Standard Contractual Clauses ("SCCs") for the transfer of personal data to third countries pursuant to GDPR Article 46. The full SCC text is available at the official EU source. The parties agree as follows:

1) Modules. The SCCs (Module 2 – Controller to Processor, and/or Module 3 – Processor to Processor, as applicable) apply to all transfers of Customer Personal Data to third countries lacking an adequacy decision.

2) Parties & Roles. For the SCCs, the Customer is the Data Exporter and Reg X Innovations is the Data Importer. Sub-processors engaged by Reg X may become additional data importers as permitted by the SCCs (Docking Clause applies).

3) Annex Mapping. The SCC Annexes are completed by reference to this DPA:
- SCC Annex I(A) – List of Parties → DPA Annex I(A)
- SCC Annex I(B) – Description of Transfer → DPA Annex I(B)
- SCC Annex I(C) – Competent Supervisory Authority → DPA Annex I(C)
- SCC Annex II – Technical & Organizational Measures → DPA Annex II
- SCC Annex III – List of Sub-processors → DPA Annex I(B)

4) Sub-processors (Clause 9). Customer consents to the use of Sub-processors as described in Section 6 of the DPA, Annex IV and Annex V. Reg X remains fully liable for their performance and will provide at least thirty (30) days' prior notice of changes.

Governing Law and Jurisdiction: The parties select the law of England and Wales and the courts of England and Wales for Modules 2 and/or 3, as applicable.

6) Transfer Impact Assessment & Supplementary Measures. The parties will assess relevant laws and practices of the destination country and implement appropriate supplementary measures (e.g., encryption at rest and in transit, access controls, data minimisation, and contractual commitments) to ensure a level of protection essentially equivalent to that in the EEA.

7) Government Access Requests. The Data Importer will notify the Data Exporter (where legally permitted) of legally binding requests for access to personal data, challenge unlawful or over-broad requests, and disclose only the minimum necessary to comply with such requests.

8) Conflicts. In case of conflict between this DPA and the SCCs, the SCCs prevail to the extent of the conflict.

9) UK & Swiss Add-ons. For UK transfers, the parties incorporate the UK Information Commissioner's Office International Data Transfer Addendum ("UK Addendum") to

the SCCs. For Swiss transfers, references to GDPR are deemed references to the Swiss FADP as required; the competent authority is adjusted accordingly.