Data Processing Agreement

This Data Processing Agreement ("Agreement") is an addendum to the Supply Agreement between:

(1) Quick SMS Limited, incorporated and registered in Jersey with company number 133441, whose registered office is at 54 Bath Street, St Helier, JE1 1FW (the "Company" or "Data Processor");

and

(2) "The Customer" as defined in the Terms and Conditions (the "Customer" or "Data Controller"),

each a "Party" and collectively the "Parties".

1. Compliance with Applicable Laws and Accreditations

1.1 Quick SMS Limited ensures compliance with relevant data protection, procurement, and security standards applicable to the jurisdictions in which the Company operates, including:

United Kingdom:

- UK General Data Protection Regulation (UK GDPR): Mirrors the EU GDPR post-Brexit, providing a framework for data processing, data subject rights, and data transfers.
- Data Protection Act 2018: Supplements the UK GDPR and includes additional provisions for data processing.
- Privacy and Electronic Communications Regulations (PECR): Governs electronic communications, including the use of cookies.
- NHS Data Protection Regulations: Ensures data handling complies with NHS Act 2006, Health and Social Care Act 2012, and standards set by NHS Digital and the DSP Toolkit.

European Union:

- General Data Protection Regulation (EU GDPR): Establishes requirements for data processing, data subject rights, data transfers, and data security.
- ePrivacy Directive: Complements GDPR by regulating electronic communications and the use of cookies.

United States:

- California Consumer Privacy Act (CCPA): Provides comprehensive data rights for California residents, including the right to know, delete, and opt-out of data sales.
- FTC Act: Protects consumers against unfair or deceptive practices, including data privacy issues.
- State-specific privacy laws: Variations exist, such as the Virginia Consumer Data Protection Act (VCDPA) and Colorado Privacy Act (CPA), providing similar rights to the CCPA.

United Arab Emirates:

- Federal Decree-Law No. 45 of 2021 (PDPL): Sets the framework for personal data protection, aligning with international data protection standards.
- DIFC Data Protection Law No. 5 of 2020 and ADGM Data Protection Regulations 2021: Specific to free zones, these regulations provide comprehensive data protection guidelines.
- Federal Law No. 6 of 2023 on Public Procurement: Governs procurement involving data processing in the public sector.

2. Key Data Protection and Accreditation Requirements

2.1 The Company adheres to the following standards to align with the Privacy and Cookie Policy:

- ISO 27001: Ensures comprehensive risk management, incident response, and continuous improvement of the Information Security Management System (ISMS).
- Cyber Essentials and Cyber Essentials Plus: Validates robust cybersecurity measures to guard against common cyber threats.
- NHS DSP Toolkit: Compliance ensures the Company meets NHS Digital's standards for data security and patient data protection.

3. Scope and Commitment

3.1 This Agreement applies to data processing activities, covering client data, website data, customer information, and patient data. It ensures compliance with:

- UK GDPR, EU GDPR, and regional laws for data protection.
- ISO 27001, Cyber Essentials, and NHS data protection regulations.

4. Breakdown of Data Protection Requirements Per Country

4.1 United Kingdom:

- Data Processing:
- Comply with UK GDPR for data subject rights such as access, rectification, and erasure.
- Secure data processing with encryption and access controls.
- Data Transfer and Storage:
- Data stored at Rackspace data centres in London.
- Transfers outside the UK only occur with proper safeguards, such as adequacy decisions or Standard Contractual Clauses (SCCs).
- Additional Requirements:
- NHS patient data must comply with the DSP Toolkit and Caldicott Principles.

4.2 European Union:

- Data Processing:
- Comply with EU GDPR for lawful, transparent processing and data subject rights.
- Implement data minimization and secure processing methods.
- Data Transfer and Storage:
- Data stored within the EU or transferred under GDPR-compliant mechanisms.
- ePrivacy Compliance:
- Obtain cookie consent and provide transparent cookie use notifications.

4.3 United States:

- Data Processing:
- Comply with CCPA for rights such as data access, deletion, and opt-out.
- Adhere to state-specific regulations where applicable.
- Data Transfer and Storage:
- Data stored on servers within the USA, with no cross-border transfers unless compliant with legal requirements.
- FTC Compliance:
- Ensure practices align with consumer protection standards against deceptive practices.

4.4 United Arab Emirates:

- Data Processing:
- Comply with PDPL for data processing and data subject rights like access and rectification.
- Adhere to DIFC and ADGM data protection laws when processing data in those free zones.
- Data Transfer and Storage:
- Data stored on local servers within the UAE. Cross-border transfers are restricted and require consent and appropriate safeguards.
- Procurement Compliance:
- Public procurement practices involving data processing must align with Federal Law No. 6 of 2023.

5. Data Transfer and Storage Practices

5.1 Region-Specific Data Storage:

- UK and Europe: Data is stored in London, adhering to GDPR and UK GDPR requirements. Transfers use legal safeguards for cross-border data flows.
- USA: Data is retained locally within the USA, and transfers outside the region are compliant with state and federal laws.
- UAE: Data storage is confined to local servers, with strict control on transfers to ensure PDPL compliance.

6. Data Security Measures

6.1 The Company's data security measures include:

- ISO 27001: Comprehensive security management, including regular audits and risk assessments.
- Cyber Essentials: Technical controls to prevent unauthorized access.
- NHS Compliance: Alignment with the DSP Toolkit and Caldicott Principles for patient data.

7. Third-Party Service Providers

7.1 The Company ensures that third-party service providers comply with:

- ISO 27001, Cyber Essentials, and Cyber Essentials Plus standards.
- Data transfer and storage policies that align with regional regulations (e.g., GDPR, CCPA, PDPL).

8. Data Subject Rights and Compliance

8.1 The Company supports data subject rights as mandated by:

- GDPR and UK GDPR: Right to access, rectify, erase, and restrict processing.
- CCPA: Right to know, delete, and opt-out.
- PDPL: Rights for UAE data subjects, including data access and rectification.

9. Governing Law and Jurisdiction

9.1 This Agreement is governed by the laws of England and Wales, taking into account international data protection laws. Disputes will be managed under the jurisdiction relevant to the applicable regulations.

10. Miscellaneous

10.1 Amendments must be in writing and signed by both Parties.

10.2 If any provision is deemed invalid, the remaining provisions remain effective.