Tiquo - Data Processing Addendum

EFFECTIVE DATE: 10 June 2026
VERSION: 1.6
CONTACT: privacy@tiquo.co

Introduction and Applicability

This **Data Processing Addendum** ("**DPA**") forms part of the **Tiquo Terms of Service** or any other written or electronic agreement between **Tiquo Ltd** ("**Tiquo**", the *Processor*) and the customer (the "**Controller**") governing the use of the Tiquo platform and related services (the "**Agreement**").

This DPA automatically applies to all customers who use the Tiquo services. By continuing to use the Tiquo platform after the Effective Date, the Controller agrees to this DPA.

This DPA is made pursuant to the UK GDPR, EU GDPR, Swiss revFADP, US state privacy laws (CCPA/CPRA, VCDPA, CPA, CTDPA, etc.), Canada PIPEDA and Quebec Law 25, Singapore PDPA, Hong Kong PDPO, Brazil LGPD, Japan APPI, Australia Privacy Act, India DPDPA, Thailand PDPA, Malaysia PDPA, New Zealand Privacy Act, South Africa POPIA, UAE PDPL, and all other applicable data protection laws in jurisdictions where Tiquo operates or processes personal data.

1. Parties

1. **Controller:** Any customer using the Tiquo platform, as identified in the Agreement.
2. **Processor: Tiquo Ltd**, incorporated in England and Wales with registered office at **180 Strand, London, England, WC2R 1EA**, company number **16500553**.

2. Background and Purpose

2.1 The Controller engages Tiquo to provide a unified management platform for service economy businesses (including hospitality, wellness, leisure, events, healthcare, transport, education and cultural venues such as hotels, restaurants, spas, gyms, clinics, cinemas, theatres, museums, training providers and private events), which requires Tiquo to process Personal Data on behalf of the Controller.

2.2 This DPA supplements and forms part of the Agreement. In the event of a conflict between this DPA and the Agreement, this DPA prevails to the extent of the conflict, except where the Agreement provides greater protection for Personal Data.

3. Definitions

Unless otherwise defined, terms in this DPA have the meaning given in the UK GDPR.

- **Applicable Data Protection Law:** All data protection and privacy laws applicable to a Party, including: (a) UK GDPR and UK Data Protection Act 2018; (b) EU GDPR; (c) Swiss revFADP (Revised Federal Data Protection Act); (d) US state privacy laws including CCPA, CPRA, VCDPA, CPA, CTDPA, TDPSA, OCPA, MCDPA, FDBR, ICDPA, TIPA, DPDPA, NJDPA, NHDPA, NDPA, MCDPA, MODPA, KCDPA, RIDTPPA, and any other applicable US state comprehensive privacy legislation; (e) Canada PIPEDA, Quebec Law 25, Alberta PIPA, and British Columbia PIPA; (f) Singapore PDPA; (g) Hong Kong PDPO; (h) Brazil LGPD; (i) Japan APPI; (j) Australia Privacy Act; (k) India DPDPA; (l) Thailand PDPA; (m) Malaysia PDPA; (n) New Zealand Privacy Act 2020; (o) South Africa POPIA; (p) UAE PDPL; (q) Mexico LFPDPPP; (r) Kenya Data Protection Act 2019; (s) Ghana Data Protection Act 2012; (t) Nigeria NDPA 2023; (u) Indonesia PDP Law 2022; (v) Philippines Data Privacy Act 2012 (RA 10173); and (w) any other applicable data protection or privacy laws in jurisdictions where Tiquo operates.

- **Controller**, **Processor**, **Data Subject**, **Personal Data**, **Personal Data Breach**, **Processing**, and **Supervisory Authority** have the meanings set out in the UK GDPR.

- **TOMs:** The technical and organisational measures described in **Annex 2**.

- **Sub-processor:** Any third party engaged by Tiquo to process Personal Data on behalf of the Controller.

- **SCCs:** The European Commission's Standard Contractual Clauses (Decision (EU) 2021/914) and, where applicable, the UK Addendum issued by the ICO; and, for transfers under Swiss revFADP, the transfer mechanisms recognised by the FDPIC including standard contractual clauses and adequacy decisions.

- **revFADP**: The Swiss Federal Act on Data Protection of 25 September 2020, as revised and in force from 1 September 2023, together with the Ordinance on Data Protection (DPO).

- **FDPIC**: The Swiss Federal Data Protection and Information Commissioner.

- **UK Addendum**: The Technical Addendum issued by the UK Information Commissioner's Office to the Standard Contractual Clauses.

- **CCPA**: California Consumer Privacy Act (Cal. Civ. Code - 1798.100 et seq.).

- **LGPD**: Brazil's Lei Geral de Protecao de Dados Pessoais.

- **PDPA**: Personal Data Protection Act (Singapore or Malaysia, as context requires).

- **APPI**: Japan's Act on the Protection of Personal Information.

- **LFPDPPP**: Mexico's Ley Federal de Proteccion de Datos Personales en Posesion de los Particulares.
- **POPIA**: South Africa's Protection of Personal Information Act 2013.
- **DPDPA**: India's Digital Personal Data Protection Act 2023.
- **PDPL**: UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data.
- **PDPO**: Hong Kong's Personal Data (Privacy) Ordinance (Cap. 486).
- **PDP Law**: Indonesia's Law No. 27 of 2022 on Personal Data Protection.
- **NDPA**: Nigeria's Data Protection Act 2023.
- **KDPA**: Kenya's Data Protection Act 2019.
- **Privacy Act 2020**: New Zealand's Privacy Act 2020.
- For the purposes of CCPA/CPRA, references to 'Personal Data' in this DPA shall be read as references to 'Personal Information' as defined under CCPA.

4. Roles and Scope of Processing

4.1 **Roles.** The Controller acts as the data controller; Tiquo acts as the data processor.
4.2 **Instructions.** Tiquo shall process Personal Data only on documented instructions from the Controller, as described in this DPA and the Agreement.
4.3 **Details of Processing.** The subject matter, nature and purpose, duration, types of data, and categories of data subjects are set out in **Annex 1**.
4.4 **Controller Responsibility.** The Controller is responsible for ensuring lawful collection and transfer of Personal Data and for configuring the Tiquo platform in a compliant manner.

5. Confidentiality and Personnel

5.1 Tiquo ensures that personnel authorised to process Personal Data are bound by confidentiality and trained in data protection.
5.2 Access to Personal Data is restricted to those with a legitimate business need.

6. Security Measures

Tiquo implements appropriate **technical and organisational measures (TOMs)** to ensure a level of security appropriate to the risk, as described in **Annex 2**. These measures may be updated to reflect technological progress without materially reducing protection.

7. Sub-Processing

7.1 The Controller grants Tiquo **general authorisation** to engage Sub-processors.
7.2 A current list of Sub-processors including their names, addresses, roles, and data categories processed, is available at https://tiquo.co/legals/subprocessor-policy. The sub-processor list includes the processing location and categories of personal data processed by each sub-processor. Tiquo will notify Controllers of new Sub-processors and provide a right to object on reasonable grounds.
7.3 Where a Sub-processor fails to fulfil its data protection obligations under the contract imposed on it by Tiquo in accordance with clause 7.1, Tiquo remains liable to the Controller for the performance of that Sub-processor's obligations, subject to the limitations of liability set out in the Platform Terms.

8. Assistance to the Controller

Tiquo assists the Controller, insofar as possible, with:

- Responding to Data Subject requests;
- Conducting or supporting Data Protection Impact Assessments (DPIAs), including impact assessments for AI-assisted analytics and automated processing features;
- Cooperating with Supervisory Authorities;
- Providing information and access for compliance verification (see Clause 11).

9. Personal Data Breaches

Tiquo shall notify the Controller **within 48 hours of confirming** a **Personal Data Breach** and shall provide information regarding the nature, consequences, and remedial actions. Tiquo shall cooperate to mitigate and remedy the breach.

10. International Transfers

Tiquo shall not transfer Personal Data to a jurisdiction that does not provide an adequate level of protection except where lawful transfer mechanisms are in place, including adequacy decisions, SCCs, UK Addendum, Swiss revFADP mechanisms, APEC Cross-Border Privacy Rules (CBPR), and other recognised and legally compliant transfer mechanisms as described in Annex 4.

11. Audits and Information Requests

Tiquo will make available all information reasonably necessary to demonstrate compliance. The Controller may request audits under reasonable notice and frequency.

Independent third-party certifications (e.g., ISO 27001, SOC 2) may satisfy audit requirements.

12. Deletion or Return of Personal Data

Upon termination or expiry of the Agreement, Tiquo will delete or return all Personal Data within the timeframes in **Annex 6**, unless retention is required by law.

13. Liability

Each Party's liability under this DPA is subject to the limitations in the Agreement, except where prohibited by Applicable Data Protection Law.

14. Updates and Changes

Tiquo may update this DPA (including Annexes) to reflect legal or operational changes by providing prior written or public notice. Continued use of the services after such notice constitutes acceptance of the updated DPA.

15. Sector-Specific Regulations

The Services may be used by Customers operating across a range of sectors. Where a Customer's use of the Services involves processing personal data subject to sector-specific regulations (including but not limited to healthcare privacy laws such as HIPAA, regulations governing the processing of children's personal data such as COPPA and the ICO Age Appropriate Design Code, and transport sector passenger data regulations), the Customer remains solely responsible for ensuring its own compliance with those regulations and must not use the Services in a manner inconsistent with them. Tiquo does not, by providing the Services, assume obligations under sector-specific regulations that would otherwise apply only to the Customer, and does not offer a Business Associate Agreement or equivalent sector-specific addendum as part of the standard Services. Customers requiring such arrangements should contact Tiquo before processing regulated data on the platform.

16. Governing Law and Jurisdiction

This DPA is governed by the laws of **ENGLAND AND WALES**. Any disputes shall be subject to the exclusive jurisdiction of the courts of **ENGLAND AND WALES**.

Annex 1 – Details of Processing

Subject Matter: Provision of the Tiquo platform and related support and professional services.

Duration: For the term of the Agreement and any data return/deletion period.
Nature and Purpose: Hosting, storage, transmission, reporting, analysis, AI-assisted analytics, automated processing, backup, configuration, and related processing required to deliver the Tiquo services.
Types of Personal Data: Names, contact details, booking and membership data, preferences, payment identifiers (tokenised), staff data, device data, AI-generated insights and analytics derived from processing, and any data entered by the Controller.
Special Category Data: Not intentionally processed. The Controller must ensure a lawful basis if entered.
Categories of Data Subjects: End-users, staff, and other individuals.
Processing Locations: Customer Personal Data is replicated across AWS eu-west-1 (Ireland) and AWS us-east-1 (Virginia). Transfers to us-east-1 are covered by the EU-US Data Privacy Framework, Standard Contractual Clauses, and the UK International Data Transfer Agreement as applicable. Data is replicated durably across multiple physical availability zones using secure database technologies and architectures.

AI and Automated Processing

The Tiquo platform includes optional AI-enabled features that process Personal Data for the purposes of generating insights, recommendations and operational analytics. These features are configurable by the Controller and may be enabled or disabled at the Controller's discretion. Where AI features are enabled, the following processing may occur:

(a) AI-generated analytics insights and write-ups based on anonymised analytics data;

(b) AI-generated customer overview summaries;

(c) automatic name inference from email addresses during data import;

(d) AI-generated document and form templates;

(e) AI-assisted email campaign drafting;

(f) natural language to segment rule conversion.

The Controller retains full control over which AI features are active and is responsible for ensuring an appropriate lawful basis and, where required, conducting a DPIA before enabling high-risk AI processing features.

Annex 2 – Technical and Organisational Measures (TOMs)

Tiquo maintains a security programme aligned to recognised standards (e.g., ISO/IEC 27001):

1. **Access Control:** Role-based access, least privilege, SSO/MFA.
2. **Encryption:** In transit (TLS 1.2+) and at rest (AES-256 or equivalent).
3. **Secure Development:** Secure SDLC, code review, vulnerability scanning.

4. **Monitoring:** Centralised logging, anomaly detection, alerting.
5. **Business Continuity:** Backups, disaster recovery, tested restoration.
6. **Sub-Processor Oversight:** Due diligence and contractual controls.
7. **Physical/Cloud Security:** Reputable data centres, certification alignment.
8. **Incident Response:** Defined procedures and 24/7 escalation.
9. **Privacy by Design:** Product reviews ensuring minimisation and compliance.
10. **AI Governance:** Model input/output logging, human oversight mechanisms, bias monitoring, and configurable feature controls enabling Controllers to enable or disable AI processing.

Annex 3 – Sub-Processors

Tiquo uses certain third-party Sub-processors to provide hosting, infrastructure, and related services. A current and up-to-date list of Sub-processors is maintained at:

https://tiquo.co/legals/subprocessor-policy

Annex 4 – International Transfers

For transfers outside the UK/EEA/Switzerland without an adequacy decision, the SCCs (Module 2: Controller to Processor and Module 3: Processor to Sub-processor) apply. Details required by Annexes I–III of the SCCs are provided in Annexes 1–3.
Tiquo conducts transfer risk assessments where required. The UK Addendum applies for transfers from the UK. For transfers from Switzerland, the SCCs apply as recognised by the FDPIC, with the necessary Swiss-specific modifications (Swiss FDPIC as competent authority, Swiss revFADP as governing law for the data protection clauses).

Tiquo maintains Transfer Impact Assessments for sub-processors located in jurisdictions without an adequacy decision. These are available to Controllers on request.

Annex 5 – Security Incident Response

1. **Detection & Notification:** Breaches notified within 48 hours of confirmation.
2. **Investigation:** Root cause analysis, mitigation, corrective actions.
3. **Communication:** Updates provided as new information becomes available.
4. **Post-incident Review:** Lessons learned, policy updates.

In addition to standard incident response procedures, Tiquo assists the Controller with jurisdiction-specific supervisory authority notifications, including:

- ICO (UK Information Commissioner's Office) - UK GDPR breaches
- Relevant EU DPA - EU GDPR breaches
- FDPIC (Swiss Federal Data Protection and Information Commissioner) - revFADP breaches
- PDPC Singapore - PDPA breaches
- PCPD (Hong Kong) - PDPO breaches
- OAIC (Office of the Australian Information Commissioner) - Privacy Act breaches
- OPC Canada (Office of the Privacy Commissioner of Canada) - PIPEDA breaches
- OIPC Alberta (Office of the Information and Privacy Commissioner of Alberta) - Alberta PIPA breaches
- OIPC BC (Office of the Information and Privacy Commissioner for British Columbia) - BC PIPA breaches
- ANPD (Autoridade Nacional de Protecao de Dados) - LGPD breaches
- PPC (Personal Information Protection Commission) - APPI breaches (Japan)
- DPBI (Data Protection Board of India) - DPDPA breaches
- INAI (Instituto Nacional de Transparencia, Acceso a la Informacion y Proteccion de Datos Personales) - LFPDPPP breaches (Mexico)
- JPDP (Department of Personal Data Protection) - PDPA breaches (Malaysia)
- OPC New Zealand (Office of the Privacy Commissioner) - Privacy Act 2020 breaches (New Zealand)
- Information Regulator - POPIA breaches (South Africa)
- UAE Data Office - PDPL breaches (UAE)
- ODPC (Office of the Data Protection Commissioner) - KDPA breaches (Kenya)
- DPC (Data Protection Commission) - DPA breaches (Ghana)
- NDPC (Nigeria Data Protection Commission) - NDPA breaches (Nigeria)
- MCIT / Supervisory Institution - PDP Law breaches (Indonesia)
- NPC (National Privacy Commission) - Data Privacy Act breaches (Philippines)
- PDPC Thailand (Personal Data Protection Committee) - PDPA breaches (Thailand)

Annex 6 – Data Retention & Deletion

1. Personal Data retained for the term of the Agreement.
2. On termination, the Controller may request data export within 30 days. If no export is requested within 30 days, Tiquo will proceed to deletion.
3. Deletion within 90 days from backups following export completion or expiry of the 30-day export window, whichever is earlier.
4. Deletion certificate available upon request.

Annex 7 - Jurisdiction-Specific Provisions

1. United States (CCPA/CPRA)

Tiquo is a 'Service Provider' under CCPA/CPRA. Tiquo does not: (a) sell or share Personal Information; (b) retain, use, or disclose Personal Information for any commercial purpose except as necessary to perform services; or (c) combine Personal Information from the Controller with other sources, except as permitted under CCPA.

1A. United States (State Privacy Laws - VCDPA, CPA, CTDPA, TDPSA, and others)

For the purposes of applicable US state comprehensive privacy laws beyond CCPA/CPRA, Tiquo acts as a Processor. Tiquo shall:

(a) not sell, share, or process Personal Data for targeted advertising except as instructed by the Controller;

(b) not retain, use, or disclose Personal Data for any purpose other than performing the services specified in the Agreement;

(c) not combine Personal Data received from the Controller with Personal Data received from other controllers or collected directly from consumers, except as permitted by applicable law;

(d) assist the Controller in responding to Data Subject rights requests, including requests for access, correction, deletion, portability, and appeals of denied requests, within the timeframes required by each applicable state law;

(e) provide the information necessary for the Controller to conduct and document data protection assessments as required under applicable state laws;

(f) upon reasonable request, provide the Controller with information necessary to demonstrate compliance with applicable state privacy obligations;

(g) require any sub-processor engaged under Section 7 to comply with obligations no less protective than those set out in this section.

2. Canada (PIPEDA and Quebec Law 25)

Tiquo processes Personal Information in compliance with PIPEDA and Quebec Law 25. Tiquo implements reasonable safeguards, obtains Controller consent for processing beyond the Agreement scope, and provides reasonable privacy assistance.

2A. Canada (Alberta PIPA and British Columbia PIPA)

Tiquo processes Personal Information in compliance with the Alberta Personal Information Protection Act (PIPA) and the British Columbia Personal Information Protection Act (PIPA). Tiquo implements reasonable safeguards as required by both provincial statutes, assists Controllers with Data Subject access and correction requests within the applicable response timelines (45 days for Alberta, 30 business days for British Columbia), and cooperates with the respective provincial Information and Privacy Commissioners.

3. Singapore (PDPA)

Tiquo is a Processor under Singapore PDPA. Personal Data may be transferred to third countries only where PDPC-approved mechanisms are in place or where consent has been obtained. Tiquo assists Controllers in meeting notification and transfer obligations.

4. Hong Kong (PDPO)

Tiquo does not require registration with the Hong Kong Privacy Commissioner (not required for Processors). Tiquo complies with PDPO including cross-border transfer provisions. Controllers are responsible for obtaining lawful basis for disclosures; Tiquo provides reasonable assistance.

5. Brazil (LGPD)

Tiquo operates as an Operator (Operador) under LGPD. Tiquo appoints a DPO equivalent and participates in LGPD notification with ANPD. Tiquo cooperates on Data Subject rights requests and notifications.

6. Japan (APPI)

Tiquo processes Personal Information under APPI. For cross-border transfers, Tiquo obtains Controller consent or ensures lawful basis and provides transfer documentation (adequacy or contractual).

7. Australia (Privacy Act)

Tiquo complies with Australian Privacy Principles (APPs), including APP 8 (cross-border disclosure). Tiquo discloses Personal Information to overseas recipients only where the Controller has consented or it is required by law.

8. India (DPDPA)

Tiquo operates as a Processor under DPDPA. Tiquo ensures compliance with data principal consent, implements security safeguards, and handles breach notifications

consistently with DPDPA requirements. Tiquo assists with cross-border transfer documentation.

9. UAE (PDPL)

Tiquo processes Personal Data in compliance with UAE Personal Data Protection Law. Tiquo complies with local transfer requirements and assists Controllers with Government Authority requests and notifications.

10. Mexico (LFPDPPP)

Tiquo operates as a Processor ("encargado") under the LFPDPPP. The Controller is responsible for providing a compliant privacy notice ("aviso de privacidad") and obtaining any required consent, including express consent for sensitive or financial data. Tiquo assists with ARCO rights requests (access, rectification, cancellation, opposition) within the 20-business-day statutory timeline. Tiquo notifies the Controller without undue delay of any security breach affecting Personal Data.

11. China (PIPL)

Processing of Personal Information subject to China's PIPL is **DEFERRED** to a future phase. Tiquo will address PIPL compliance separately upon market readiness. Until then, Tiquo does not process or store Personal Information subject to PIPL.

12. Ghana (Data Protection Act 2012)

Tiquo processes Personal Data in compliance with the Ghana Data Protection Act 2012 (Act 843). Tiquo implements appropriate safeguards for cross-border transfers and assists Controllers with Data Subject access and correction requests. Tiquo notifies the Controller without undue delay of any security breach.

13. Indonesia (PDP Law 2022)

Tiquo operates as a Processor under Law No. 27 of 2022 on Personal Data Protection. Tiquo complies with cross-border transfer requirements, including any notification obligations to MCIT. Tiquo assists Controllers with Data Subject rights requests and breach notifications.

14. Kenya (Data Protection Act 2019)

Tiquo processes Personal Data in compliance with the Kenya Data Protection Act 2019. Tiquo implements appropriate safeguards for cross-border transfers under Section 48 and assists Controllers with Data Subject rights requests and ODPC notifications.

15. Malaysia (PDPA 2010, as amended 2024)

Tiquo operates as a Processor under the Malaysian Personal Data Protection Act 2010 (as amended). Tiquo complies with cross-border transfer provisions under Section 129 and assists Controllers with Data Subject rights requests, including portability and erasure rights introduced by the 2024 Amendment.

16. New Zealand (Privacy Act 2020)

Tiquo processes Personal Information in compliance with the New Zealand Privacy Act 2020 and the Information Privacy Principles. Tiquo discloses Personal Information to overseas recipients only where comparable privacy protections apply or the individual has authorised the disclosure (IPP 12). Tiquo assists Controllers with breach notifications to the OPC.

17. Nigeria (NDPA 2023)

Tiquo processes Personal Data in compliance with the Nigeria Data Protection Act 2023 and the General Application and Implementation Directive. Tiquo assists Controllers with Data Subject rights requests, breach notifications to the NDPC, and annual Compliance Audit Returns.

18. Philippines (Data Privacy Act 2012)
Tiquo operates as a Personal Information Processor under Republic Act No. 10173. Tiquo complies with cross-border transfer requirements and assists Controllers with Data Subject rights requests and NPC breach notifications within the 72-hour statutory window.

19. South Africa (POPIA)

Tiquo operates as an Operator under the Protection of Personal Information Act 2013. Tiquo implements appropriate safeguards for cross-border transfers under Section 72 and assists Controllers (Responsible Parties) with Data Subject access, correction, and deletion requests and Information Regulator notifications.

20. Thailand (PDPA 2019)

Tiquo processes Personal Data in compliance with the Thailand Personal Data Protection Act B.E. 2562. Tiquo ensures appropriate transfer safeguards are in place for data stored in regions not on the PDPC whitelist. Tiquo assists Controllers with Data Subject rights requests and PDPC breach notifications within the 72-hour statutory window.

Annex 8 - Data Protection Lead and Representatives

Data Protection Lead: privacy@tiquo.co

EU Art. 27 Representative: Appointed representative based in Paris, France - privacy@tiquo.co

Swiss revFADP Art. 14 Representative: Appointed representative based in Switzerland - privacy@tiquo.co