Customer Data Storage, Handling and Disclosure Policy (AU and NZ)

1. Purpose

TEG is committed to protecting the privacy and security of customer data. This policy sets out clear guidelines for the secure handling, storage, and sharing of customer data by TEG Pty Ltd and its controlled subsidiaries in Australia and New Zealand (together "**TEG**"). It applies to TEG entities with operations in Australia or New Zealand including Ticketek, TEG Live, TEG Dainty, TEG Van Egmond, TEG Sport, SXSW Sydney, Ovation, Life Like Touring, Handsome Tours Australia, The Entertainment Store, the Brickman Exhibitions, St Jerome's Laneway, and Fan Plus International.

The purpose of this policy is to ensure consistent compliance with applicable data protection laws and regulations across TEG, while maintaining the trust and confidence of our customers. TEG recognises the significant risks posed by data breaches to both our customers, clients and our organisation and we stress our collective responsibility to mitigate these risks and adhere to industry standards and regulations. This policy aims to safeguard data integrity, ensure consistent compliance with data protection laws, reduce the risk of data incidents, and maintain the trust and confidence of our customers and clients.

2. Scope

Who must comply with this policy? All employees, directors, contractors and labour hire workers, apprentices, trainees and volunteers (collectively referred to throughout as **Workers**) are required to comply.

Whose data does this policy apply to? This policy applies to the **data of our customers**. A **customer** is any individual that interacts with one of our business units as a consumer of our goods or services. **Examples** of customer interactions include:

- An individual creates an account with Ticketek or Ticketek Marketplace.
- An individual signs up to Ticketek Rewards or Purkle and provides personal information through surveys.
- TEG Live receives the data of patrons from a venue in connection with an event.
- An individual subscribes to a TEG Live or Ticketek "event waitlist".
- An individual lodges a query with customer support.

This means the policy covers data collected from customers of any ticketing, promoter, or other service offered by TEG. It applies to all data collected, processed, and stored by TEG by any channel, including data collected through websites, mobile applications, customer service interactions, at events and from third-parties such as venues or co-promoters.

This policy addresses two types of customer data: (1) customer personal information and data (**Customer PI**); and (2) customer transaction data (**Transaction Data**).

Customer PI	**Transaction Data**
Customer PI includes any information or data about a customer that on its own or when combined with other information, could identify an individual. This includes: • Username • Customer ID • Password • First name • Last name • Email Address • Postal Address (excluding postcode) • Street Address (excluding postcode) • Date of Birth • Home Phone number • Business Phone number • Mobile Phone Number • Any "member" number fields	Transaction Data is information about the customer's transactions which cannot be used to identify an individual. This includes: • Transaction Order ID • Event Details • Ticket Pricing • Ticket Fees • Ticket Seat Details • Ticket Barcode

Certain business units (such as Ticketek and SXSW Sydney) also collect payment information, such as credit and debit card details, when processing transactions. This information is handled in strict accordance with the Payment Card Industry Data Security Standard (PCI DSS) which outlines robust security measures for the protection of cardholder data. In addition, TEG applies its internal *Guidelines for all Computer Systems Handling Credit Card Numbers*, which set out specific technical and procedural controls to ensure secure processing, storage, and transmission of payment information across TEG systems.

3. Storage

Approved Platforms and Programs for Storing Customer PI

Data Storage Platforms: These platforms are used to store data, including Customer PI, transaction history, marketing preferences and event details. Customer PI must only be stored on approved data storage platforms that meet TEG's data protection and regulatory compliance standards. These systems must be assessed by IT for their security features, including encryption, access controls, and secure infrastructure.

Approved systems for storing Customer PI include:

- Redshift (data warehouse)
- MongoDB (NoSQL database)
- Snowflake (cloud native data platform)
- Lotus (SQL)
- Braze, Brevo, Audience Republic (customer engagement platforms)
- Origin

Customer PI must not be stored on personal devices (such as laptops or PCs), in email applications (such as Outlook), or in unauthorised cloud storage platforms (such as SharePoint or OneDrive).

Cloud Infrastructure: This refers to the underlying technology that hosts and supports TEG systems, enabling them to run securely and efficiently. TEG has approved and currently uses **Amazon Web Services (AWS)** as its cloud infrastructure provider.

Data Processing Applications: These applications, such as **Insight**, are used to analyse, interpret or transform data. They **do not store personal information long-term**. Instead, they are used to generate reports, dashboards and insights, or to facilitate the movement of data between systems in real time or through scheduled workflows.

Geographical location

Customer PI must be stored in one of the approved locations, in accordance with the requirements below: Australia, United States Singapore, Hong Kong, Ireland, and United Kingdom.

TEG adheres to data residency requirements imposed by local laws and regulations. Where specific data residency requirements exist, data will be stored and processed within the required geographical boundaries to ensure compliance.

Regional Data Storage:

Subject always to any data residency requirements articulated in applicable laws, and unless otherwise approved by IT in writing, the following regional data storage rules should apply:

- **Australia and New Zealand**: Customer PI collected in Australia and New Zealand will be stored in data centers located in Australia;
- **Asia**: Data collected in Asia will be stored in data centers located in Singapore and Hong Kong; and
- **European Union**: Data collected in the European Union will be stored in data centers located in Ireland and the United Kingdom.

Excluded Data Storage Regions:

Certain countries have strict data localisation laws or other regulatory, security, or privacy concerns that make them unsuitable for storing Customer PI. TEG does not store Customer PI in the following jurisdictions:

- Russia
- China
- India
- Brazil
- Turkey

The exclusion of these jurisdictions is based on:

- Inadequate data protection laws and regulations.
- High risk of data breaches or unauthorised access.
- Political or economic instability that may compromise data security.
- Specific legal or regulatory requirements that prohibit data storage in these regions.

4. Internal Access

Access Control Principles

Access to Customer PI is governed by the following principles and restricted to the following roles within TEG.

Workers	Access Level	Responsibilities
Privacy Officer and Legal Team	Full access to all Customer PI on an as-needs basis for example to manage complaints, data incidents, customer feedback etc.	Oversee data protection policies, ensure compliance with regulations, and manage data breach response.

IT Department (Tech Ops, Enterprise IT and Event IT, QA and Dev Teams)	Access to Customer PI is in accordance with IT access controls procedures. Limited access to the production environment to manage customer inquiries.	Implement and maintain technical security measures, manage access controls, and support data handling activities.
Data Analysts	Read-only access to anonymised Customer PI.	Analyse data for business insights while ensuring data privacy and security.
Customer Support Representatives	Limited access to Customer PI relevant to their support cases.	Assist customers with inquiries and issues while maintaining data confidentiality.
Marketing Team	Access to aggregated and anonymised Customer data for campaign analysis. Limited access to Customer PI for Workers approved on a case-by-case basis, as relevant to marketing activities.	Develop and optimise marketing strategies based on data insights.

5. Access Request and Approval Process

- **Request Submission**: Employees must submit an access request form to their manager and to the IT Department specifying the required access level and justification.
- **Approval Workflow**: Access requests are reviewed and approved by the employee's manager, the and the IT Department.
- **Access Provisioning**: Once approved, access is granted by the IT Department.

6. Disclosure of Customer PI and Transaction Data

When and to whom can TEG share data?

TEG must not disclose Customer PI to third parties without the customer's consent, unless required or authorised by law. Where we have the customers' consent, TEG will only share relevant Customer PI and/or Transaction Data with third parties under the following circumstances:

1. **To Venues**: Where the disclosure is made in accordance with a signed Ticketing Services Agreement

that includes appropriate data sharing provisions (including that the Venue is required to adhere to applicable privacy laws), and the disclosure is aligned with the primary purpose for which the data was collected.

2. **To Promoters, Artists/Performers, and Other Third Parties (including Partners)**: Where there is:
    - A signed Data Sharing Agreement (also referred to as a privacy agreement); or
    - A signed Ticketing Services Agreement that contains appropriate data sharing provisions, and the disclosure is aligned with the primary purpose for which the data was collected or a secondary purpose permitted under applicable privacy laws.

Data Sharing Agreements for Ticketek can be found on the intranet here and for Ovation found here.
Without either a signed Ticketing Services Agreement or Data Sharing Agreement that addresses data sharing or a specific data sharing agreement, TEG cannot disclose data to any third party.

When the Ticketek purchasing journey includes a bespoke consent that incorporates the third party's privacy policy and any applicable terms and conditions (a "**Bespoke Opt-in**"), the third-party recipient can use and share data in accordance with that privacy policy, provided that the customer has consented to the Bespoke Opt-in. In the absence of that express consent, data sharing will only be with the third party and not with their subsequent data processors, in accordance with TEG's privacy policy. Furthermore, TEG should not receive data unless there is an equivalent agreement in place OR without the direct consent of the customer.

Any Data Sharing Agreement, Ticketing Services Agreement or Privacy Agreement, must include requirements for the third party to comply with relevant privacy laws. These privacy laws must be of a comparable standard to Australian privacy laws, such as the Australian Privacy Principles (APPs) under the Privacy Act 1988. This ensures that any third-party data recipients handle the data with the same level of protection and accountability as required in Australia.

How can TEG share data externally?

At TEG, all data transfers must be conducted using secure, approved methods to uphold our data protection standards. Unsecure tools such as Outlook emails, Microsoft Word documents or Excel spreadsheets must not be used for transferring data. The following secure transfer methods are approved for use at TEG:

- Encrypted Streams
- SFTP (Secure File Transfer Protocol)
- S3 Buckets
- Kinesis Stream
- Azure Event Hub Storage

- Kiteworks

Customer PI must not be transferred to any external organisation using unapproved methods. For clarity, email is not an approved or secure method for transferring Customer PI.

7. Monitoring and Auditing

- **Continuous Monitoring**: Access to Customer PI is continuously monitored using advanced security information and event management systems.

- **Regular Audits**: Periodic audits are conducted to review access permissions, identify any unauthorised access, and ensure compliance with access control policies, including audits for the purposes of ASAE and ISO compliance.

- **Incident Response**: Any suspicious activity or potential data breaches are promptly investigated and addressed by the Privacy and Data Governance Lead, the Legal Team and IT Department in accordance with our Data Incident Response Plan.

8. Training and Awareness

- **Employee Training**: All employees undergo regular training on data protection policies, access control procedures, and security best practices.

- **Awareness Programs**: Ongoing awareness programs are conducted to reinforce the importance of data security and compliance with access control measures.

Document Information

Version Number	1
Last Update	20/3/2025
Author	Tane Oakes
File Name	Customer Data Storage, Handling and Disclosure Policy
Responsible Executive (Role Position)	Chief Technology Officer

Document Revision History

Version	Issue Date	Author	Approved By

1	20/03/2025	Ashley Brown	Ashley Brown
1	3/06/2025	Ashley Brown	Tane Oakes