TREASURY WINE ESTATES

DATA PROTECTION POLICY

A Treasury Wine Estates Limited Policy

1. INTRODUCTION / CONTEXT

As one of the world's leading wine producers and sellers of premium wine, Treasury Wine Estates (**TWE**) handles a wide variety of information to operate its business. The information TWE handles includes "personal information" (also referred to as data) about our employees, job applicants, consumers, customers, suppliers, shareholders and other individuals we deal with during the course of our business activities. TWE understands that personal information is valuable, important and sensitive and is committed to protecting the privacy and security of this information and complying with data protection laws and any data security standards applicable to TWE.

This Policy sets out how we ensure that the personal information of individuals is collected, used, transferred, stored and disposed of appropriately and lawfully. It also refers to specific guidelines which apply when TWE accepts payment for its goods via credit cards. As credit cards are an accepted form of payment across all channels, TWE is required to comply with the Payment Card Industry Data Security Standards (PCI DSS) in all jurisdictions in which it operates.

You must read, understand and comply with this Policy when processing any personal information on TWE's behalf.

2. WHO THIS POLICY APPLIES TO

This policy is a global policy and applies to all TWE employees, directors, agency workers, consultants and contractors in all jurisdictions in which TWE operates.

3. POLICY STATEMENT

TWE will comply with the following general data protection principles when processing personal information.

We will:

- process personal information lawfully, fairly and in a transparent manner;
- collect personal information for specified and legitimate purposes only;
- only process personal information that is adequate and necessary for the purposes for which it is processed;
- ensure that personal information is accurate and kept up to date;
- not keep personal information longer than is necessary;
- take appropriate measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage; and
- not transfer data to another country without appropriate safeguards being in place.

Specifically in relation to credit card data, we will

- ensure that any activity involving the collection, storage, transmission or payment processing of credit card information shall adhere to the PCI DSS (as published by the PCI Council www.pcisecuritystandards.org) as detailed in the *Credit Card Data Management Guidelines;* and
- aim to minimise any involvement or contact with credit card information. Where PCI approved outsourced suppliers and solutions are available, they shall be utilised as a method of transferring risk and reducing the overall number of compliance controls required within TWE.

4. DEFINITIONS

PCI	Payment Card Industry representing the major card schemes of Visa, AMEX, Mastercard, JCB and Discover
PCI DSS	The Payment Card Industry Data Security Standard is the information security standard for organisations that handle branded credit cards from major card schemes.
Personal Information	Any information about a person who can be identified (directly or indirectly) from that information – see section 6 for examples of personal information
Privacy Notice or Information Notice	means a notice which sets out the type of personal information that TWE may collect about individuals, the purposes for which it is collected and how it is handled.
Sensitive Personal Information	means Personal Information about an individual's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

5. RESPONSIBILITIES

CFO	Owner of the Data Protection Policy. All changes must be approved by the CFO. The CFO will report any significant information security risks, lapses in compliance controls and breaches to the Risk Compliance and Governance Committee. The CFO is also responsible for managing/updating this document and will review it annually or in the event of any change to TWE's strategy that may impact the scope of cardholder data environment .
CIO	Responsible for ensuring implementation, monitoring, review and assurance of global compliance with the relevant technical IT related data protection, security or PCI controls outlined in this Policy.
Chief People & Communications Officer	Responsible for ensuring implementation, monitoring, review and assurance of compliance with this Policy as it relates to employee personal information and HR's use of personal information.
Chief Marketing Officer	Responsible for ensuring implementation, monitoring, review and assurance of compliance with this Policy as it relates to consumer personal information and technical requirements and controls required to comply with this Policy.
Director, Direct to Consumer Channel for each operating region	Each region within which TWE operates will have different providers of payment devices which are capable of capturing card payment information. The Director, Direct to Consumer Channel for each region will hold overall responsibility for the acquisition, operations, maintenance and disposal of these terminals in accordance with the *Credit Card Data Management Guidelines*. The Director of Direct to Consumer Channel is also responsible for all non-technical PCI requirements that are related to sales, for example Order Forms, Telephone Orders etc.
Group Treasurer	Responsible for reporting significant security risks, lapses in governance controls and breaches of this Policy as it relates to compliance with PCI DSS to the CFO
IT Security Manager	The IT Security Manager is responsible for: ○ Implementation and maintenance of any relevant technical requirements and controls required to comply with this Policy and the attached Guidelines. ○ Informing the CIO (and Group Treasurer as it relates to credit card data) of any potential security events or issues of non-compliance that could potentially affect TWE's business operations.

IT Service Desk	The IT Service Desk is responsible for managing information security incidents to resolution, including recording, dispatching, escalating and reporting incidents to the IT Security Manager.
All Personnel	All personnel at TWE, including temporary and permanent employees, directors, agency workers, secondees, consultants and contractors shall comply with this policy and any applicable guidelines, standards and procedures.

6. WHAT IS PERSONAL INFORMATION?

Personal information or personal data means any information about a person who can be identified from that information. It includes:

- contact details such as name, address, telephone number or email;
- a person's salary, bank account or financial details, including a credit card number;
- purchase, income and credit histories
- pictures, photographs or videos of a person;
- opinions, preferences, memberships and religious or political affiliations of a person
- a person's medical details or health information
- details about a person's religious or sexual preferences.

This Policy applies to all personal information TWE processes regardless of how that data is stored or whether it relates to past or present employees, job applicants, consumers, customers, suppliers, shareholders or any other individual.

7. YOUR OBLIGATIONS REGARDING PERSONAL INFORMATION

Your obligations regarding third party personal information

In your role with TWE, you may have access to the personal information of other TWE employees, or of TWE's consumers, customers, suppliers, shareholders, job applicants and other third parties. If so, TWE expects you to help meet its data protection obligations to those individuals. If you do have such access to personal information, you must:

- only access or obtain the personal information that you have a job-related need and authority to access or obtain, and only for authorised and lawful purposes;
- only allow other TWE staff to access or obtain personal information if they have a job-related need to access that information, appropriate authorisation and a lawful reason for doing so;
- only allow individuals who are not TWE staff to access personal information if you have specific authority to do so from your manager and suitable safeguards and contractual arrangements have been put in place (see **Information Security** above for more information);
- ensure that the personal information we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it;
- keep personal information secure (e.g. by complying with our rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in TWE's *Information Security Policy*);
- not remove personal information, or devices containing personal information from TWE's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection);
- not store personal information on local drives or on personal devices that are used for work (or other) purposes; and

- comply with this Policy and our related policies and procedures

If you are concerned or suspect that one of the above obligations has not been complied with (or is likely to not complied with), you should contact the IT Service Desk immediately.

Your obligations regarding your own personal information

You should let the HR department know as soon as possible if the personal information you have provided to TWE changes (for example if you move house or change your banking details) by using MyHR on the intranet.

Collecting personal information and using Information Notices

Whenever TWE collects personal information directly from an individual (such as when a consumer provides us with their personal information), we must ensure that an appropriate Information Notice (sometimes called a Privacy Notice or a privacy collection notice) is provided to them. You must contact the Legal Department responsible for your region for further guidance whenever TWE is collecting (whether directly or indirectly) or using personal data to ensure we comply with our obligations to provide information.

If you are a TWE employee and also an EU citizen, TWE may also issue you with an Information Notice from time to time informing you about the personal information that TWE collects, how you can expect your personal information to be used and for what purposes**.**

Rights of Individuals

Every individual (including you as a TWE employee and others such as TWE's consumers, customers and shareholders), has certain rights in relation to their personal information including but not limited to, a right:

- to be informed about how and why their personal information is processed;
- to make an access request to obtain a copy of their personal information; and
- to have that data corrected and updated and in certain circumstances, to have it erased (for example, if it is no longer necessary for the purpose for which it was collected).

Individuals who are EU citizens also have a number of other rights available to them which include but are not limited to, a right;

- to restrict the processing of personal information in certain circumstances;
- to ask to obtain a portable copy of their personal data in certain circumstances; and
- to object to processing in certain circumstances.

If you, as a TWE employee, wish to exercise any of the rights listed above or have any questions, please email your local HR team member in your region.

If you receive a written request of the nature set out above (for example, a request from a job applicant, customer, consumer or shareholder), you should forward it to your manager and also the Legal Department responsible for your region immediately.

Credit card information

As credit cards are an accepted form of payment across all channels, TWE must comply with the Payment Card Industry (PCI) Data Security Standards (DSS). Any individual handling and managing credit card payments or dealing with third party service providers who capture credit card information must comply with the *Credit Card Data Management Guidelines*.

Information security and the role of third party providers

TWE will use appropriate technical and organisational measures in accordance with TWE's Information Security Policy to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

- making sure that, where appropriate, personal information is pseudonymised or encrypted;
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

- ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Where TWE uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered or extended, the relevant staff must seek guidance from the Legal Department and ensure we are meeting all of our data protection obligations in relation to that information. This includes a requirement that service providers who will be procuring and/or processing credit card transactions on TWE's behalf are certified as being PCI DSS compliant.

Storage and retention of personal information

Personal information (including Sensitive Personal Information) must be stored securely in accordance with TWE's Information Security Policy and must not be retained in an identifiable format for any longer than needed. The length of time for which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained and any relevant legal or business considerations. You should follow TWE's Document Retention Policy which set out the relevant retention periods. After those retention periods have expired, Personal information (and Sensitive Personal Information) that is no longer required must be deleted permanently from our information systems and any hard copies must be securely destroyed.

Data breaches

A data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information by a TWE employee or a third party;
- loss of data resulting from an equipment or systems failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

If required by law, TWE will:

- notify relevant authorities of the data breach; and
- also notify the affected individuals (for example, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law).

If you know or suspect that a data breach has occurred, you must immediately contact the IT Help Desk and the Legal Department responsible for your region. Do not attempt to investigate the matter yourself. You should preserve all evidence relating to the potential data breach.

International transfers outside of the European Economic Area

Personal information is transferred to another country when it is sent, transmitted, viewed or accessed in or to a different country. If TWE transfers the personal data of an EU citizen outside the European Economic Area (EEA), it must only do so on the basis that that receiving country, territory or organisation provides an adequate level of protection, such as having adequate safeguards by way of standard data protection clauses in place.

You may only transfer EU personal information outside the EEA where one of the above conditions applies. Before sending any personal data outside the EEA, you should contact the legal team for advice.

Lawful reasons for processing personal information

In relation to any processing activity undertaken by TWE (such as collecting personal data) we must before the processing starts and then regularly while it continues:

- review the purposes of the particular processing activity, and identify the most appropriate lawful reason for that processing, which may include:
    - that the data subject has consented to the processing;
    - that the processing is necessary for TWE to perform a contract with the individual (ie we are selling wine to a consumer);
    - that the processing is necessary for compliance with a legal obligation to which TWE is subject;
- satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
- include information about both the purposes of the processing and the lawful basis for it in our relevant Information Notice(s) and provide a copy of this to the individual(s) that the information relates to where appropriate;
- where Sensitive Personal Information is processed, also identify a lawful special condition for processing that information (see **Sensitive Personal Information** below) and document it.

Where you process personal information on TWE's behalf, you must ensure that you comply with the above requirements in order to help TWE meet its obligations. We must keep a record of our processing activities in accordance with our obligations.

Sensitive Personal Information

Sensitive Personal Information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'. TWE may from time to time need to process Sensitive Personal Information. We must only process Sensitive Personal Information if:

- we have a lawful reason for doing so (e.g. it is necessary for the performance of the employment contract) and
- one of the special conditions for processing Sensitive Personal Information applies, e.g. processing is necessary for the purposes of exercising the employment rights or the obligations of TWE or the data subject;

.

In order to help TWE meet its obligations, if you process Sensitive Personal Information as part of your role, you must ensure that you comply with the requirements set out above and elsewhere in this Policy. If you are in any doubt about whether the information can be lawfully processed, please contact your manager.

Criminal records information

TWE will only collect, store and use information about criminal convictions and offences in line with the requested disclosure of these as per TWE's Motor Vehicle Policy and some TWE contracts of employment. If you are a TWE employee in the EU, your Information Notice gives further details about how we use disclosed criminal records. Where TWE processes criminal records information, we will follow this Policy and our related policies and procedures to ensure that we comply with the data protection principles set out above.

Training

TWE aims to ensure that its global workforce is suitably trained on their data protection responsibilities as part of their compliance training when joining and at regular intervals thereafter.

8. CONSEQUENCES FOR BREACH OF THIS POLICY

A breach of any of the provisions of this Policy may constitute a disciplinary offence and will be dealt with in accordance with TWE's disciplinary procedures. Depending on the gravity of the offence, it may be treated as misconduct and could render you liable to summary dismissal or termination.

Any breaches of this policy must be reported immediately to your line manager and/or in accordance with the Whistle-blower Policy. Failure to report such breaches could expose TWE to an unacceptable level of risk.

Breaches or non-compliance by third parties will be handled according to terms and conditions contained in the relevant contracts between the parties.

9. RELATED TWE DOCUMENTS

This Policy should be read in conjunction with the following documents:

- TWE Credit Card Data Management Guidelines
- TWE Information Security Policy
- TWE Information Security Manual
- TWE Document Retention Policy
- TWE Procure to Pay Policy
- TWE Code of Conduct Policy
- TWE Social Media Policy
- TWE Mobile Device Policy
- TWE Incident Management Plans

10. APPROVAL

Approval of this Policy is required annually by the CFO.

11. VERSION CONTROL

Last Edited by:	Policy Owner:	Date Published:
Fiona Anderson	Matt Young	May 2018