
PRIVACY AND PERSONAL DATA PROTECTION POLICY

Contents

1	INTRODUCTION	2
2	PRIVACY AND PERSONAL DATA PROTECTION POLICY	2
2.1	THE GENERAL DATA PROTECTION REGULATION	2
2.2	DEFINITIONS.....	2
2.3	PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA	3
2.4	RIGHTS OF THE INDIVIDUAL.....	4
2.5	CONSENT	4
2.6	PRIVACY BY DESIGN	4
2.7	TRANSFER OF PERSONAL DATA	5
2.8	DATA PROTECTION OFFICER	5
2.9	BREACH NOTIFICATION	5
2.10	ADDRESSING COMPLIANCE TO THE PRIVACY ACT.....	5
2.11	OUR OBLIGATIONS AS A CLOUD SERVICE PROVIDER	6

List of Tables

<i>TABLE 1 – TIMESCALES FOR DATA SUBJECT REQUESTS</i>	<i>4</i>
-------------------------------------------------------------	----------

1 Introduction

In its everyday business operations BrewAI makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Customers
- Users of its websites
- Subscribers
- Other stakeholders

In collecting and using this data, the organization is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps BrewAI is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to BrewAI systems.

The following policies and procedures are relevant to this document:

- *Information Classification Procedure*
- *Information Labelling Procedure*
- *Acceptable Use policy*
- *Electronic Messaging Policy*
- *Internet Acceptable Use Policy*
- *Information Security Incident Response Procedure*
- *Information Security Roles, Responsibilities and Authorities*

2 Privacy and Personal Data Protection Policy

2.1 The General Data Protection Regulation

The **Privacy Act 1988 (Privacy Act)** is one of the most significant pieces of legislation affecting the way that BrewAI carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the **Privacy Act**, which is designed to protect the personal data of citizens of Australia. It is BrewAI's policy to ensure that our compliance with the **Privacy Act** and other relevant legislation is clear and demonstrable at all times.

2.2 Definitions

However, the most fundamental definitions with respect to this policy are as follows:

'BrewAI' refers to:

BrewAI Group Pty Ltd and its wholly owned subsidiaries.

Personal data is defined as:

any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more

factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'processing' means:

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'controller' means:

the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

2.3 Principles Relating to Processing of Personal Data

There are a number of fundamental principles upon which the **Privacy Act** is based.

These are as follows:

1. *Personal data shall be:*
 - (a) *processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*
 - (b) *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with **Privacy Act**, not be considered to be incompatible with the initial purposes ('purpose limitation');*
 - (c) *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*
 - (d) *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*
 - (e) *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with **Privacy Act**) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');*
 - (f) *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*
2. *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').*

BrewAI must ensure that it complies with all of these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems. The operation of an information security management system (ISMS) that conforms to the ISO/IEC 27001 international standard is a key part of that commitment.

2.4 Rights of the Individual

The data subject also has rights under the **Privacy Act**. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to restrict processing
5. The right to data portability
6. The right to object
7. Rights in relation to automated decision making and profiling.

Each of these rights must be supported by appropriate procedures within BrewAI that allow the required action to be taken within the timescales stated in the **Privacy Act**. These timescales are shown in Table 1.

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not specified

Table 1 – Timescales for data subject requests

2.5 Consent

Unless it is necessary for a reason allowable in the **Privacy Act**, explicit consent must be obtained from a data subject to collect and process their data. In case of children below the age of 16 parental consent must be obtained. Transparent information about our usage of their personal data must be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge.

If the personal data are not obtained directly from the data subject then this information must be provided within a reasonable period after the data are obtained and definitely within one month.

2.6 Privacy by Design

BrewAI has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more privacy impact assessments.

The privacy impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymisation will be considered where applicable and appropriate.

2.7 Transfer of Personal Data

Transfers of personal data outside the Australia must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the **Privacy Act**. This depends partly on the Australian Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

2.8 Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the **Privacy Act** if an organization is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on these criteria, BrewAI requires a Data Protection Officer to be appointed.

2.9 Breach Notification

It is BrewAI's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the **Privacy Act**, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within scope. This will be managed in accordance with our *Information Security Incident Response Procedure* which sets out the overall process of handling information security incidents.

Under the **Privacy Act** the relevant supervisory authority has the ability to impose a range of fines for infringements of the regulations.

2.10 Addressing Compliance to the Privacy Act

The following actions are undertaken to ensure that BrewAI complies at all times with the accountability principle of the **Privacy Act**:

- The legal basis for processing personal data is clear and unambiguous
- A Data Protection Officer is appointed with specific responsibility for data protection in the organisation (TBD)
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively

- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
 - Organization name and relevant details
 - Purposes of the personal data processing
 - Categories of individuals and personal data processed
 - Categories of personal data recipients
 - Personal data retention schedules
 - Relevant technical and organisational controls in place

These actions will be reviewed on a regular basis as part of the management review process of the information security management system.

2.11 Our Obligations as a Cloud Service Provider

In addition to holding personal data on our own account, BrewAI also stores and processes the personal data of our cloud customers. In doing so, there are a number of additional obligations that must be fulfilled to allow our customers to stay within the law. Our policy in this area is informed by *ISO/IEC 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors* which, as well as recommending specific enhancements to ISO/IEC 27001 controls, also provides the following policy guidance:

- We must provide our customers with the facilities to meet their obligations under law in activities such as accessing, amending and erasing individuals' PII
- We must only use the cloud customer's PII for their purposes, not our own
- The customer must be informed if we are required by law to disclose any of their data, unless we are prohibited from doing so
- Details of disclosures must be recorded
- We must tell our customers if we use sub-contractors to process their PII
- We must tell our customers if their PII is subject to unauthorized access
- It must be clear in which country or countries the customer's PII is stored

Additional recommendations stated in ISO/IEC 27018 are also included in the relevant policies and procedures within the ISMS.

Policy Version: 1.0
Approved: 25th November 2021