Trendie

PRIVACY AND DATA RETENTION POLICY AND PROCEDURES

Purpose

The purpose of this Privacy Policy and Procedure is to safeguard the personal information entrusted to Trendie by our employees, clients, suppliers, and other stakeholders. This policy outlines our commitment to privacy, detailing how we collect, use, disclose, retain, and protect personal information in accordance with the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth).

Scope

This policy applies to all personal information collected, used, stored, and retained by Trendie. It covers the information of employees, clients, customers, suppliers, and other individuals with whom we interact. This includes but is not limited to information collected through our website, during business operations, and from third-party sources.

Definitions

- **Personal Information:**

  Any information or opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not, and whether recorded in a material form or not.

- **Sensitive Information:**

  A subset of personal information that includes information about an individual's racial or ethnic origin, political opinions, religious beliefs, sexual orientation, health information, or criminal record.

- **Consent:**

  Voluntary agreement to some act, practice, or purpose. Consent can be express or implied.

Trendie

Privacy Principles

- **Collection of Personal Information:**
  - Trendie will only collect personal information that is necessary for our business functions and activities or to comply with legal or regulatory obligations.
  - Information will be collected directly from the individual wherever possible, unless it is unreasonable or impracticable to do so.
  - Individuals will be informed about the purpose of collection, the types of information collected, and their rights regarding their information.
- **Use and Disclosure of Personal Information:**
  - Personal information will only be used or disclosed for the primary purpose for which it was collected or for a related secondary purpose that an individual would reasonably expect.
  - We may disclose personal information to third parties, including service providers, regulatory bodies, or other entities, as required by law or with the individual's consent.
- **Data Quality and Security:**
  - Trendie will take reasonable steps to ensure that the personal information we collect is accurate, complete, and up-to-date.
  - We will implement appropriate security measures to protect personal information from misuse, interference, loss, unauthorised access, modification, or disclosure.
  - Access to personal information will be restricted to authorised personnel only.
- **Access and Correction:**
  - Individuals have the right to request access to their personal information held by Trendie. Requests will be processed in accordance with applicable laws and our internal procedures.
  - Individuals may also request corrections to their personal information if they believe it is inaccurate, incomplete, or out of date.

- **Anonymity and Pseudonymity:**
    - Wherever it is lawful and practicable, individuals have the option of not identifying themselves or using a pseudonym when dealing with Trendie.
- **Cross-Border Disclosure:**
    - Before disclosing personal information to an overseas recipient, Trendie will take reasonable steps to ensure that the recipient does not breach the APPs or equivalent privacy laws.
- **Complaints Handling:**
    - Individuals who believe their privacy has been breached can submit a complaint in accordance with our Complaints Handling Procedure. All complaints will be taken seriously and investigated promptly.

Data Retention Procedures

- **Data Retention:**
    - Personal information will only be retained for as long as necessary to fulfil the purposes for which it was collected, or as required by law. Retention periods will be determined based on legal requirements, business needs, and best practices.
    - A data retention schedule will be maintained, specifying the types of personal information held, the retention period for each type, and the justification for the retention period.
- **Review of Retained Data:**
    - Regular audits will be conducted to ensure that personal information is not retained longer than necessary. Any information that no longer serves a legitimate business purpose or is not required by law will be securely disposed of.
- **Data Disposal:**
    - Personal information that is no longer required will be securely destroyed or de-identified. Secure disposal methods include shredding physical documents, permanently deleting electronic files, and using secure disposal services for electronic storage devices.

- Employees responsible for data disposal must ensure that all copies, including backups and duplicates, are also securely destroyed.

- **Archiving:**
  - Certain data may need to be archived for historical, research, or compliance purposes. Archived data will be securely stored and access will be restricted to authorised personnel only.
  - Archived data will be periodically reviewed to determine if it can be disposed of in accordance with this policy.

- **Data Anonymisation:**
  - In cases where data retention is required but identification of individuals is not necessary, personal information will be anonymised to protect individual privacy. Anonymisation will involve removing or altering personal identifiers in such a way that the individual can no longer be identified.

Responsibilities

- **Employees:**
  All employees are responsible for understanding and adhering to this Privacy Policy and the data retention procedures. They must ensure that personal information is handled and retained in accordance with this policy and report any potential breaches to their manager or the Privacy Officer.

- **Managers:**
  Managers are responsible for ensuring their teams comply with this policy and that employees understand their obligations regarding the handling, retention, and disposal of personal information.

- **Privacy Officer:**
  The Privacy Officer is responsible for overseeing the implementation of this policy, managing privacy-related inquiries and complaints, and ensuring compliance with applicable privacy laws and regulations. They will also monitor data retention practices and conduct regular audits to ensure compliance.

Procedures

- **Collecting Personal Information:**
    - Obtain personal information directly from the individual wherever possible. If collecting from a third party, ensure the individual has consented or is aware of the collection.
    - Inform individuals about the purpose of collection, the types of information collected, how it will be used, and how they can access and correct their information.
- **Storing and Securing Personal Information:**
    - Store personal information securely, whether in electronic or physical form. Implement security measures such as encryption, access controls, and secure disposal methods for records no longer required.
    - Regularly review and update security practices to safeguard against unauthorised access, modification, or disclosure.
- **Accessing and Correcting Personal Information:**
    - Individuals wishing to access or correct their personal information must submit a written request to the Privacy Officer.
    - The Privacy Officer will verify the individual's identity before providing access or making corrections. Requests will be processed within a reasonable timeframe.
- **Disclosing Personal Information:**
    - Ensure any disclosure of personal information is for the primary purpose for which it was collected or a related secondary purpose. Obtain the individual's consent for any other disclosures unless required by law.
    - When disclosing information to third parties, ensure appropriate agreements are in place to protect the privacy of the information.
- **Data Breach Response:**
    - Immediately report suspected data breaches to the Privacy Officer.
    - Implement corrective actions to prevent future breaches.

- The Privacy Officer will assess the breach to determine if it qualifies as an eligible data breach under the Notifiable Data Breaches (NDB) scheme.
- If the breach is likely to result in serious harm, notify affected individuals and the Office of the Australian Information Commissioner (OAIC) promptly.

- **Handling Complaints:**
  - Individuals can lodge a privacy complaint by contacting the Privacy Officer in writing. The complaint should include details of the alleged breach and any supporting evidence.
  - The Privacy Officer will acknowledge receipt of the complaint within 5 business days and conduct a thorough investigation. A written response outlining the findings and any corrective actions will be provided within 30 days.

Review and Amendments

This policy, including data retention procedures, will be reviewed annually to ensure its effectiveness and compliance with current laws and practices. Any amendments will be communicated to all employees.

Implementation

All new employees will receive training on this Privacy Policy and data retention procedures as part of their induction. Existing employees will receive regular training and updates to ensure ongoing compliance. This policy will be accessible to all staff and stakeholders via the company intranet and website.

By adhering to this Privacy Policy and Procedure, Trendie demonstrates its commitment to protecting personal information and maintaining the trust and confidence of our employees, clients, and other stakeholders.