LGL-029

Titomic Limited

Data Protection Policy and Procedure

Adopted by the Board: 17 December 2019
Last Review Date: 16 August 2021

Titomic Limited
ACN 602 793 644
Building 3, 270 Ferntree Gully Road, Notting Hill, VIC 3168 Australia
1300 108 122 | www.titomic.com | info@titomic.com

Data Protection Policy and Procedure

Definitions

Company	means **Titomic Limited**, a listed public company.
Personal Information	has the meaning set out in the Privacy Act.
Privacy Act	means the *Privacy Act 1988* (Cth) as amended from time to time.
Responsible Person(s)	means Company Secretary and Head of Human Resources.
Register of Systems	means a register of all systems or contexts in which Personal Information is processed by the Company.
Sensitive Information	has the meaning set out in the Privacy Act.

1. Data protection principles

The Company is committed to processing data in accordance with its responsibilities under the Privacy Act and the Australian Privacy Principles (**APPs**).

The APPs set out in Schedule 1 of the Privacy Act require that Personal Information will be:

a. managed in an open and transparent manner;

b. managed in a way that provides for individuals to be given the option of remaining anonymous or to use a pseudonym unless exceptions apply;

c. collected only where it is reasonably necessary for the Company's functions and activities and where the Company has taken reasonable steps to notify the individual of certain matters;

d. where it is also Sensitive Information, collected only where reasonably necessary for the Company's functions and activities and where the Company also has the individual's consent (unless an exemption applies);

e. collected by lawful and fair means and from the individual concerned, unless it is unreasonable or impractical;

f. only used or disclosed for a purpose for which it was collected, or for a secondary purpose if an exception applies;

g. not disclosed overseas unless certain conditions are met;

h. accurate, up to date and complete and in a manner that provides for correction and access to the Personal Information upon request of the relevant individual unless exemptions apply;

i. processed in a manner that ensures appropriate security of the Personal Information, including protection against misuse, interference, loss, unauthorised access, modification or disclosure;

j. managed in a way that allows for destruction or de-identification of the Personal Information in certain circumstances.

2. General provisions

a. This policy applies to all Personal Information processed by the Company.

b. The Responsible Person will take responsibility for the Company's ongoing compliance with this policy.

c. This policy will be reviewed at least annually.

3. Lawful, fair, and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Company will maintain a Register of Systems.

b. The Register of Systems will be reviewed at least annually.

c. Individuals have the right to access their Personal Information and any such requests made to the Company will be dealt with in a timely manner.

4. Lawful purposes

a. All Personal Information processed by the Company must be carried out by lawful and fair means.
b. The Company will note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent will be kept with the Personal Information.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be I place to ensure such revocation is reflected accurately in the Company's systems.

5. Data Minimisation

a. The Company will ensure that Personal Information is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
b. The Company collects Personal Information in the following situations:
    i. Website and all digital media access
    ii. Requests for information or quotations
    iii. Job applications for Company positions
    iv. Applications to invest in Titomic Limited
    v. Events and conferences where the Company exhibits
    vi. Subscriptions to receive Company information
    vii. Direct contact via telephone, email or in writing
c. The Company safely stores Personal Information electronically, protected from unauthorised access, accidental deletion and malicious hacking attempts. When Personal Information is stored on paper, it is kept in a secure place where unauthorised people cannot access it. Printouts are shredded and disposed of securely when no longer required.
d. The Company has defined technical and organisational measures to protect Personal Information appropriately depending on its nature, a data breach response plan, extent of processing and accessibility. These may for instance include data encryption, management of access right, of secure flows, etc. Respect for the

security and protection of Personal Information is required of all employees as well as Company partners and subcontractors.

6. Accuracy

a. The Company will take reasonable steps to ensure Personal Information is accurate.
b. Where necessary for the lawful basis on which data is processed, steps will be put in place to ensure that Personal Information is kept up to date.
c. Personal Information is held in as few places as necessary. Employees are instructed to not create any unnecessary additional data sets.
d. Employees take every opportunity to ensure Personal Information is kept current and updated periodically.
e. Personal Information will be updated as inaccuracies are discovered.

7. Archiving / Removal

a. To ensure that Personal Information is kept for no longer than necessary, the Company will put in place an archiving policy for each area in which Personal Information is processed and review this process annually.
b. The archiving policy will consider what data should/must be retained, for how long, and why.

8. Security

a. The Company will ensure that all electronically stored Personal Information is stored securely using modern software that is kept up-to-date.
b. Access to physically stored Personal Information will be restricted and secured at all times.
c. Access to Personal Information will be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
d. When Personal Information is destroyed or de-identified this should be done safely such that the data is irrecoverable or not able to be re-identified.
e. Appropriate back-up and disaster recovery solutions will be in place.

9. Breach

In the event of a potential breach of security leading to the accidental or unlawful misuse, interference, loss, unauthorised access, modification or disclosure of Personal Information, an impacted employee or person should raise a concern with either of the Responsible Person(s) listed in this Policy.

The Company will promptly assess whether this breach will result in serious harm to the affected individuals and is therefore a 'notifiable data breach' and will promptly make the required notifications with the timeframes prescribed by the Australian Government - Office of the Australian Information Commissions (OAIC) https://www.oaic.gov.au/privacy/data-breaches/.

- - - END OF POLICY - - -