Obie.ai Data Protection Policy

Definitions

Company	means Tasytt Inc. operating as Obie or Obie.ai
GDPR	means the General Data Protection Regulation
Responsible Person	means Alexander Sopinka, CTO
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Company

Data Protection Principles

The Company is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. 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 not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. 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;

5. 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. 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.

General Provisions

1. This policy applies to all personal data processed by the Company.
2. The Responsible Person shall take responsibility for the Company's ongoing compliance with this policy.
3. This policy shall be reviewed at least annually.

Lawful, Fair and Transparent Processing

1. To ensure its processing of data is lawful, fair and transparent, the Company shall maintain a Register of Systems.
2. The Register of Systems shall be reviewed at least annually.
3. Individuals have the right to access their personal data and any such requests made to the Company shall be dealt with in a timely manner.

Lawful Purposes

All data processed by the Company is done on a lawful contractual basis upon subscription activation for the Company's product(s).

Data Minimization

The Company shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

1. The Company shall take reasonable steps to ensure personal data is accurate.
2. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Archiving / Removal

1. To ensure that personal data is kept for no longer than necessary, the Company has an archiving policy for each area in which personal data is processed and reviews this process annually.
2. All client data, personal or otherwise, is kept for 5 years after a subscription is terminated, unless otherwise requested for deletion immediately.

Security

1. The Company shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
2. Access to personal data is limited to personnel who need access and appropriate security is in place to avoid unauthorised sharing of information.
3. When personal data is deleted this shall be done safely such that the data is irrecoverable.
4. Appropriate back-up and disaster recovery solutions are in place.

Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Company shall promptly assess the risk to people's rights and freedoms, and notify affected clients in a timely manner.

Last Updated: May 28, 2019
By: Alex Sopinka