Data Protection Policy

API Stone Ltd

Last updated	15/08/2018
Approved by board	22/08/2018
Next update due	21/08/2021

Definitions

Company	means APIStone Ltd, Company No. 07404408 (registered in England and Wales).
GDPR	means the General Data Protection Regulation.
Responsible Person	means Emma Longford, an employee of the Company
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Company.

1. Purpose of Policy

a. Complying with the law
b. Following good practice
c. Protecting clients, staff and other individuals
d. Protecting the organisation

2. 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:

e. processed lawfully, fairly and in a transparent manner in relation to individuals;
f. 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;

g. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
h. 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;
i. 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
j. 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."

2. General provisions

a. This policy applies to all personal data processed by the Company.
b. The Responsible Person shall take responsibility for the Company's ongoing compliance with this policy.
c. This policy shall be reviewed at least once every three years.

3. Lawful, fair and transparent processing

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

4. Lawful purposes

a. All data processed by the Company must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
b. The Company shall 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 shall be kept with the personal data.

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 in place to ensure such revocation is reflected accurately in the Company's systems.

5. Data minimisation

a. 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.

6. Accuracy

a. The Company shall take reasonable steps to ensure personal data is accurate.
b. 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.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Company has put in place an archiving policy for each area in which personal data is processed and will review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.
c. The Company recognises that individuals could be harmed through data being inaccurate or insufficient and will take reasonable steps to prevent this from happening.

8. Security

a. The Company shall ensure that personal data is stored securely using modern methods that are kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.
e. The Company recognises that individuals could be harmed through data getting into the wrong hands, through poor security or inappropriate disclosure of information and will take reasonable steps to prevent this from happening.

9. Staff Training

a. Training shall be provided to all of the Company's employees about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

b. All of the Company's employees whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy will receive additional training to help them understand their duties and how to comply with them.
c. Access to personal data shall not be granted to any individual who does not agree to abide by the Company's data protection policy.

10. 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 if appropriate report this breach to the ICO. The Company's board of directors is ultimately responsible for ensuring that the organisation complies with its legal obligations.

END OF POLICY