Data Protection Policy

1. PURPOSE

This policy sets out Nimble's approach to data protection following the Data Protection Act (DPA) 1998 and the updated requirements of the General Data Protection Regulations (GDPR) with effect from May 2018.

2. WHAT THE LAW SAYS

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

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

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

3. GENERAL PROVISIONS

a. This policy applies to all personal data processed by Nimble.
b. The Responsible Person shall take responsibility for Nimble's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. Nimble shall register with the Information Commissioner's Office as an organisation that processes personal data.

4. LAWFUL, FAIR AND TRANSPARENT PROCESSING

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

5. LAWFUL PURPOSES

a. All data processed by Nimble must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
b. Nimble 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 Nimble and third-party systems.

6. DATA MINIMISATION

a. Nimble shall ensure that personal data are adequate, relevant and limited to what is necessary for the purposes they are processed.
b. Nimble shall require third-party systems to maintain compliance with GDPR legislation.

7. ACCURACY

a. Nimble 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.
c. Nimble shall take reasonable steps to ensure personal data in third-party systems is accurate.

8. ARCHIVING/REMOVAL

a. To ensure that personal data is kept for no longer than necessary, Nimble shall maintain an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

9. SECURITY

a. Nimble shall ensure that personal data is stored securely using modern software that is 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 information sharing.
c. When personal data is deleted, this should be done safely such that the data is irrecoverable.
d. Appropriate backup and disaster recovery solutions shall be in place.

10. DATA BREACH

a. All potential personal data breaches **must immediately** be reported to the Data Protection Officer.
b. The Data Protection Officer will notify their equivalent at the Controller organisation as soon as they are made aware and where they consider that a breach may have occurred.
c. The Data Controller organisation is obliged to report the breach to the ICO within 72 hours of notification.

11. INFORMATION COMMISSIONER'S OFFICE

For further detail on the Data Protection Act 1998 and the General Data Protection Regulations 2018 visit The Information Commissioner's Office: https://ico.org.uk/.

Version: 19 October 2021

END OF POLICY