

DATA PROTECTION POLICY

Definitions

The Company	Means Western Blueprint Limited.
GDPR	Means the General Data Protection Regulation.
Responsible Persons	Means Richard Russell and Thomas Lowe.
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:

- 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;
- 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 is inaccurate is 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; 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.

General provisions

- a. This policy applies to all personal data processed by the Company.
- b. The Responsible Persons shall take responsibility for the Company's ongoing compliance with this policy.
- c. This policy shall be reviewed as deemed necessary.

Lawful, fair and transparent processing

- a. To ensure that 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 as deemed necessary.

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

- 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 shall be clearly available and systems shall be in place to ensure such revocation is reflected accurately in the Company's systems.

Data minimisation

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

Accuracy

- a. The Company shall take reasonable steps to ensure that 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.

Archiving / removal

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

Security

- a. The Company 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 shall be in place to avoid unauthorised sharing of information.
- c. When personal data is deleted, this shall be done safely such that the data is irrecoverable.
- d. Appropriate back-up and disaster recovery solutions shall be 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 if appropriate report this breach to the Information Commissioner's Office.

Review

The effectiveness of this policy and associated arrangements will be reviewed annually under the direct supervision of the Directors.



Richard Russell
Director



Thomas Lowe
Director

Date: 12 August 2024