Boulevard Construction Limited

DATA PROTECTION POLICY

Contents

Introduction 3

Definitions 3

Policy 3

Non Compliance 4

Implementation of the Policy 4

Monitoring Policy 5

Reviewing Policy 5

Policy Amendments 5

Additional Information 5

Introduction

The aim of this policy is to comply with relevant legislation in regard to the keeping of employment records and customer data. The Company requires personal information relating to each individual in order to manage its business in an efficient and effective manner; this data is subject to the Data Protection Act 1998. The Company wishes to act and comply with the principles of this Act.

Definitions

Data: includes computerised data, manual data and any other form of accessible record that includes personal information held by the Company.

Personal data: is that which relates to a living individual who could be identified by the data.

Data Subject: A data subject is an individual that is the subject of any personal data.

GDPR: means the General Data Protection Regulation.

Policy

It is the intention of this Company to adhere to the principles of the Data Protection Act and GDPR provisions. Therefore the data protection policy applies to all employees and to any other party that handles data for or on behalf of the Company as follows:

1. 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; 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."

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 annually.

3. 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.

4. 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.

5. Security

a. The Company shall ensure that personal data is stored securely.
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.

6. Breach

a. 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 (more information on the ICO website).

Non Compliance

All employees have a role to play in enforcing the policy and are required to deal with any observed or reported breaches. Should employees feel apprehensive about their own safety in regard to addressing any breach, they should seek senior management support.

Failure to comply with this policy may lead to a lack of clarity over job role, learning needs or expected standards of performance, resulting in reduced effectiveness or efficiency, underperformance and putting service delivery at risk.

Any member of staff refusing to observe the policy will be liable to disciplinary action in accordance with the Company's Disciplinary Policy up to and including dismissal.

Implementation of the Policy

Overall responsibility for policy implementation and review rests with the Company senior management. However, all employees are required to adhere to and support the implementation of the policy. The Company will inform all existing employees about this policy and their role in the implementation of the policy. They will also give all new employees notice of the policy on induction to the Company.

This policy will be implemented through the development and maintenance of procedures for appraisals and one-to-one meetings, using template forms, and guidance given to both managers and employees on the process.

Monitoring Policy
The policy will be monitored on an on-going basis, monitoring of the policy is essential to assess how effective the Company has been.

Reviewing Policy
This policy will be reviewed and, if necessary, revised in the light of legislative or codes of practice and organisational changes. Improvements will be made to the management by learning from experience and the use of established reviews.

Policy review date: 6th January 2026

Policy Amendments
Should any amendments, revisions, or updates be made to this policy it is the responsibility of the Company senior management to see that all relevant employees receive notice. Written notice and/or training will be considered.

Additional Information
If you require any additional information or clarification regarding this policy, please contact your manager. In the unlikely event where you are unhappy with any decision made, you should use the Company's formal Grievance Procedure.

To the extent that the requirements of this policy reflect statutory provisions, they will alter automatically when and if those requirements are changed.

This Policy was approved & authorised by:

Name: Peter Brookes

Position: Operations Director

Date: 5th January 2025

Signature: 