Data Protection Policy

This Policy sets out how Manage My Block Limites (the Company) processes the personal data that it holds relating to clients, staff and third parties. It outlines the companies' responsibilities under data protection legislation and regulation, setting out how it will comply, and provides instruction for staff handling personal data.
The Policy applies to all members of staff employed by the company
Date of publication: May 2023

Introduction

The protection of individuals via the lawful, legitimate, and responsible processing and use of their personal data is a fundamental human right. Individuals may have a varying degree of understanding or concern for the protection of their personal data and the company must respect their right to have control over their personal data and ensure it acts in full compliance with legislative and regulatory requirements at all times.
The General Data Protection Regulation (GDPR), as supplemented by the Data Protection Act DPA 2018 (DPA), is the main piece of legislation that governs how the company collects and processes personal data.
This Policy sets out how the Company will process the personal data of its staff, customers and third parties and applies to all personal data that the company processes regardless of the format or media on which the data are stored or who it relates to.
Compliance with this Policy and the related policies and procedures set out in Schedule 2 is mandatory. Any breach of this Policy and any related policies and procedures may result in disciplinary action. All members of staff must read, understand, and comply with this Policy when processing personal data in the course of performing their tasks and must observe and comply with all controls, practices, protocols and training to ensure such compliance.

Data Protection Principles

The GDPR is based on a set of core principles that the company must observe and comply with at all times from the moment that personal data are collected until the moment that personal data are archived, deleted or destroyed. The company must ensure that all personal data are:
1. Processed lawfully, fairly and in a transparent manner (Lawfulness, fairness, and transparency)
2. Collected only for specified, explicit and legitimate purposes (Purpose limitation)
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is to be processed (Data minimisation)
4. Accurate and where necessary kept up to date (Accuracy)
5. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (Storage limitation)
6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage (Security, integrity and confidentiality)

Additionally, the Company must ensure that:
1. Personal data are not transferred outside of the EEA (which includes the use of any website or application that is hosted on servers located outside of EEA) to another country without appropriate safeguards being in place (see Transfers of personal data outside of the EEA)
2. The Company allows data subjects to exercise their rights in relation to their personal data (see Data subject rights and requests). The Company is responsible for, and must be able to demonstrate compliance with, all the above principles (see Accountability and record-keeping).
Lawfulness, fairness, and transparency

Lawfulness and fairness: In order to collect and process personal data for any specific purpose, the Company must always have a lawful basis for doing so. Without a lawful basis for processing, such processing will be unlawful and unfair and may also have an adverse impact on the affected data subjects.
No data subject should be surprised to learn that their personal data has been collected, consulted, used, or otherwise processed by the company.

Processing personal data will only be lawful where at least one of the following lawful bases applies:
1. The data subject has given their consent for one or more specific purposes
2. The processing is necessary for the performance of a contract to which the data subject is a party (for instance a contract of employment or registration with the company)
3. To comply with the company's legal obligations
4. To protect the vital interests of the data subject or another person (this will equate to a situation where the processing is necessary to protect the individual's life)
5. To perform tasks carried out in the public interest or the exercise of official authority
6. To pursue the Company's legitimate interests where those interests are not outweighed by the interests and rights of data subjects (only available to the Company in some circumstances). The Company must identify and document the lawful basis relied upon by it in relation to the processing of personal data for each specific purpose or group of
related purposes. Consent as a lawful basis for processing. There is no hierarchy between the lawful bases for processing above, of which a data subject's consent is only one.

Consent may not be the most appropriate lawful basis depending on the circumstances. In order for a data subject's consent to be valid and provide a lawful basis for processing, it must be:
• specific (not given in respect of multiple unrelated purposes)
• informed (explained in plain and accessible language)
• unambiguous and given by a clear affirmative action (meaning opt-in: silence, inactivity or pre-ticked boxes will not be sufficient)
• separate and unbundled from any other terms and conditions provided to the data subject
• freely and genuinely given (there must not be any imbalance in the relationship between the Company and the data subject and consent must not be a condition for the provision of any product or service). A data subject must be able to withdraw their consent as easily as they gave it. Once consent has been given, it will need to be updated where the Company wishes to process the personal data for a new purpose that is not compatible with the original purpose for which they were collected.

Unless the Company is able to rely on another lawful basis for processing, a higher standard of explicit consent (where there can be no doubt that consent has been obtained, for example a signed document or a Yes/No option accompanied by clear consent wording) will usually be required to process special categories of personal data, for automated decision-making and for transferring personal data outside of the EEA.

Where the Company needs to process special categories of personal data, it will generally rely on another lawful basis that does not require explicit consent; however, the Company must provide the data subject with a fair processing notice explaining such processing. If the Company is unable to demonstrate that it has obtained consent in accordance
with the above requirements, it will not be able to rely upon such consent