

## HR-DP-GDPR Data Protection Policy

Marbank Construction Ltd are registered with the ICO (Information Commissioner's Office)

### General Statement and Scope

Marbank process relevant personal data regarding members of staff and some clients, contractors and suppliers as part of its operation and shall take all reasonable steps to do so in accordance with this Policy and the GDPR (General Data Protection Regulations)

### Data Protection Controller

Marbank is the Data Controller and has appointed its Compliance Manager as the Data Protection Lead (DPL) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the GDPR

### The Principles

Marbank shall so far as is reasonably practicable ensure that all personal data is:

- Fairly and lawfully processed
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure

### Sensitive Personal Data

Marbank have no need or requirement to process sensitive personal data with the possible exception of medical information where that may affect the individual's health or safety at work

### Rights of Access to Information

Data subjects have the right of access to information held on them by Marbank

Any data subject wishing to access their personal data should put their request in writing to the DPL

Marbank will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within 31 days for access to records and 21 days to provide a reply to an access to information request

### Accuracy

Marbank will endeavour to ensure that all personal data held in relation to all data subjects is accurate

Data subjects must notify the data processor of any changes to information held about them

### Enforcement

If an individual believes that Marbank has not complied with this Policy or acted otherwise than in accordance with the GDPR this should be reported to the DPL as soon as practicably possible

### Data Security

Marbank will take appropriate technical and organisational steps to ensure the security of personal data

All staff will be made aware of this policy and their duties under the GDPR via email or the company Intranet Staff are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data

An appropriate level of data security must be deployed for the type of data and the data processing being performed

## **External Processors**

Marbank must ensure that data processed by external processors, for example, service providers, Cloud services including storage, web sites etc. are compliant with this policy and the relevant Legislation

## **Secure Destruction**

When data held in accordance with this policy is destroyed, it must be destroyed securely in accordance with best practice at the time of destruction.

## **Retention of Data**

Marbank may retain data for differing periods of time for different purposes as required by statute, best practices, statutory obligations, legal processes and enquiries

Retention periods are recorded in the GDPR matrix document.

## **CCTV**

Some Marbank sites operate CCTV networks for the purposes of crime prevention, detection, and Safeguarding

Where a data subject can be identified, images must be processed as personal data.

**END**