MGRL-POL-0007

DATA PROTECTION POLICY

APPROVED BY		
NAME	**SIGNATURE**	**DATE**
Andrew Tilson		13/02/2020

REVISION HISTORY

REVISION	DATE	DETAIL	AUTHOR
V1	26/02/2019	New	K.Lamb
V2	13/02/2020	Organisational Change – updated and reviewed External parties are now included. Section 16 - CCTV added Reference to new forms: MGRL-FOR-0026 Subject Access Request Form and MGRL-FOR-0027 Data Breach Register	R Prendeville

Contents

1 INTRODUCTION

We may have to collect and use information about people with whom we are engaged with internally or externally. These can include Customers, Suppliers, Employees and other people the company has a relationship or contact with. This personal information must be collected, handled, stored and dealt with securely, to meet data protection requirements and to comply with the law.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources function as described below. It also covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of job applicants, existing and former employees, customers, their residents, sub-contractors, consultants, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

2 DEFINITIONS

“Personal data” is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person’s name, identification number, location, online identifier. It can also include pseudonymised data.

“Special categories of personal data” is data which relates to an individual’s health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

“Criminal offence data” is data which relates to an individual’s criminal convictions and offences.

“Data processing” is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3 DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

- processing will be fair, lawful and transparent
- data be collected for specific, explicit, and legitimate purposes
- data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
- data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
- data is not kept for longer than is necessary for its given purpose

- data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- we will comply with the relevant GDPR procedures for international transferring of personal data

4 TYPES OF DATA HELD

We keep several categories of personal data on our employees and other relevant individuals in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

Specifically, we hold the following types of data:

- personal details of relevant individuals such as name, address, phone numbers, email addresses
- information gathered via the recruitment process such as that entered a CV or included in a CV cover letter, references from former employers, details on education and employment history etc
- details relating to pay administration such as National Insurance numbers, bank account details and tax codes
- relevant individuals' medical or health information
- information relating to employment with us, including:
  - job title and job descriptions
  - employee's salary
  - employee's wider terms and conditions of employment
  - details of formal and informal proceedings involving employees such as letters of concern, disciplinary and grievance proceedings, annual leave records, appraisal and performance information
  - internal and external training modules undertaken
- employee's criminal offence data
- relevant individual's personal data received from our customers and/or their residents

All the above information is required for our processing activities and progressing works instructed by our customers and/or their residents. More information on those processing activities are included in our privacy notice for employees, which is available from their manager.

5 RELEVANT INDIVIDUAL RIGHTS

You have the following rights in relation to the personal data we hold on you:

- the right to be informed about the data we hold on you and what we do with it;
- the right of access to the data we hold on you. More information on this can be found in the section headed "Access to Data" below and in our guidance notes on our Subject Access Request form.
- the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
- the right to have data deleted in certain circumstances. This is also known as 'erasure';
- the right to restrict the processing of the data;
- the right to transfer the data we hold on you to another party. This is also known as 'portability';
- the right to object to the inclusion of any information;
- the right to regulate any automated decision-making and profiling of personal data;

For further information on each of these rights, including the circumstances in which they apply, see the guidance from the UK Information Commissioner's Office (ICO) on individual's rights under the General Data Protection Regulations (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/).

6 RESPONSIBILITIES

The Company is overall responsible for protecting all data including internal, external/ client data/information. In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

The Company will review and monitor the effect of this policy and reserve the right to review, amend as required.

7 LAWFUL BASES OF PROCESSING

We acknowledge that processing may be only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the relevant individual's consent in order to process data.

However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Relevant Individuals will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

8 ACCESS TO DATA

As stated above, relevant individuals have a right to access the personal data that we hold on them. To exercise this right, relevant individual should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in the guidance notes on our Subject Access Request form (MGRL-FOR-0026).

9 DATA DISCLOSURES

The Company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties;
- disabled individuals - whether any reasonable adjustments are required to assist them at work;
- individuals' health data - to comply with health and safety or occupational health obligations towards the relevant individual;
- for Statutory Sick Pay purposes;
- HR management and administration - to consider how a relevant individual's health affects his or her ability to do their job;
- the smooth operation of any employee insurance policies or pension plans;
- to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

These kinds of disclosures will only be made when strictly necessary for the purpose.
Any disclosures of client or their resident's data will be subject to the client's policy and/or contract.

10 DATA SECURITY

All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary.
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
- ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

11 THIRD PARTY PROCESSING

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Company's commitment to protecting data.

12 INTERNATIONAL DATA TRANSFERS

The Company does not transfer personal data to any recipients outside of the EEA.

13 REQUIREMENT TO NOTIFY BREACHES

All data breaches will be recorded on our Data Breach Register (MGRL-FOR-0027). Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

Further guidance on breach notification is available from the UK Information Commissioner's Office (ICO) (https://ico.org.uk/for-organisations/report-a-breach/.

14 TRAINING

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the Company are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect relevant individuals' personal data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

15 RECORDS

The Company keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities.

16 CCTV

We may use CCTV for the protection of employees and third parties, and to protect against theft, vandalism and damage to goods and property. Generally, recorded images are routinely destroyed and not shared with third parties unless there is a suspicion of crime, in which case they may be turned over to the Police or any other appropriate government agency or authority.

17 DATA PROTECTION COMPLIANCE

Our Data Protection Officer is:
Rosemarie Prendeville
rosemarie@MGRL.co.uk
07922 897004