MJL Contractors Ltd

HELSTON OFFICE
Unit 6, Hellys Court, Water Ma Trout Industrial Estate, Helston, Cornwall TR13 0EW
Telephone Helston 01326 574444 **Fax** 01326 572200
Email : enquiries@mjl-ltd.com
EXETER OFFICE
Unit 16, Basepoint Business Centre, Yeoford Way, Marsh Barton Trading Estate, Exeter, Devon EX2 8LB
Telephone Exeter 01392 826044

GDPR COMPLIANCE POLICY

1. Introduction

1.1. The General Data Protection Principles (GDPR), which came into force in May 2018, increased the level of regulation surrounding the processing of information relating to individuals. The existing requirements under the Data Protection Act will be replaced by GDPR and thus this policy aims to ensure MJL's continued compliance with applicable legislation.

1.2. GDPR is concerned with obtaining, holding, using or disclosing of personal data. This includes data gathered for various purposes, including but not limited to marketing, sales of goods or services, employment and research.

1.3. In this policy, the Company is primarily concerned with the collection and processing of:

a. Employee information;
b. Customer information;
c. And information provided to the Company as a third party to enable us to deliver services to our customers, i.e. Information regarding their employees and/or contractors.

1.4. The legislation covers computerised records as well as manual filing systems.

1.5. MJL is committed to holding the minimum personal information necessary to enable it to perform its functions. All such information is confidential and therefore must be treated with care to comply with the law.

1.6. Any breach of this Policy, whether deliberate, or through negligence, may lead to disciplinary action being taken or even a criminal prosecution.

2. Summary of Data Protection Principles

2.1. The principles of GDPR state 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 is inaccurate, having regard to the purposes for which they are processed, 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 is 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.

2.2 MJL and all staff who process or use personal data ensure that they abide by these principles at all times. This Policy has been developed to help ensure this happens.

3. Lawful Grounds for Processing Personal Data

3.1. Lawful grounds for processing personal data include:

a. **Consent:** Where the Employee provides their express agreement to your obtaining and processing their personal data.
b. **A contract with the individual**: for example, to supply goods or services they have requested, or to fulfil an obligation under an employment contract.
c. **Compliance with a legal obligation**: when processing data for a particular purpose is a legal requirement, e.g. providing information to HMRC.
d. **Vital interests**: for example, when processing data will protect someone's physical integrity or life (either the data subject's or someone else's).
e. **A public task**: for example, to complete official functions or tasks in the public interest. This will typically cover public authorities such as government departments, schools and other educational institutions; hospitals; and the police.
f. **Legitimate interests**: when a private-sector organisation has a genuine and legitimate reason (including commercial benefit) to process personal data without consent, provided it is not outweighed by negative effects to the individual's rights and freedoms.

3.4 Where consent is considered to be the most appropriate way to demonstrate lawful processing of data, the Employer must also bear in mind that consent can be withdrawn by the Employee.

3.5 If the withdrawal of consent prevents the Employer from carrying out its legitimate business, then the consent was, in any case, arbitrary and therefore not an appropriate method of demonstrating lawful grounds for processing of data. In order for consent to be effective, it must be on the basis that the data subject has real choice over how their data is collected and used.

4. Individual Rights

4.1. The GDPR provides the following rights for individuals in respect of their own personal information:

a. The right to be informed;
b. The right of access;
c. The right to rectification;
d. The right to erasure;
e. The right to restrict processing;
f. The right to data portability;
g. The right to object;
h. Rights in relation to automated decision making and profiling.

5. Data Protection Officer

5.1. Large scale data-processors, public authorities and organisations who process specific types of sensitive data, such as criminal convictions and offences, are required to appoint a Data Protection Officer (DPO).

5.2. It is therefore not necessary for MJL to appoint a DPO under the provisions of GDPR, however MJL reserves the right to appoint such a role should this be considered in the best interests of the business.

5.3. It is the responsibility of the Data Protection Officer to:

a. To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;
b. To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits;
c. To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

5.4. It is NOT the responsibility of the Data Protection Officer to apply the provisions of the Data Protection Act or GDPR. This is the responsibility of everyone within the Company who are individual collectors, keepers and users of personal data. Therefore, all staff are required to be aware of the provisions of the Data Protection Act and GDPR, such as keeping records up to date and accurate, and its impact on the work they undertake on behalf of Company.

5.5. The Company will ensure that:

a. The DPO reports to the highest management level;
b. The DPO operates independently and is not penalised for performing their task;
c. Adequate resources are provided to enable the DPO to meet their GDPR obligations.

6. Data Security

6.1. All staff are responsible for ensuring that:

a. Any personal data they hold, whether in electronic or paper format, is kept securely, particularly from casual observation.
b. Personal information is not disclosed deliberately or accidentally either verbally or in writing to any unauthorised third party. If in doubt, do not disclose the information and check with the Data Protection Officer.

6.2. Records will normally be kept for a minimum of three years following completion of any work or requirement for the information to be kept, or in the case of employment records, for a minimum of six years following the termination of the Employee's employment with the Company.

7. Sharing Data with Third Parties

7.1. It may be necessary for MJL Contractors to share personal data with third parties, for example either to enable MJL to manage employment effectively or in order to comply with a legal obligation.

7.2. Third parties with whom Employee data may be shared include:

a. HM Revenue and Customs;
b. Health and Safety Executive (HSE);
c. HR Consultancy Services;
d. Legal advisors;
e. Insurance providers;
f. Child Maintenance Services;
g. External IT providers;

h. Law Enforcement e.g. Police;
i. Information Commissioner;
j. Health surveillance providers, ie: Occupational Health practitioners; health surveillance clinics and health professionals engaged by clients of MJL on whose sites we operate in accordance with our contractual obligations to them.

8. Subject Access Requests

8.1. Staff, clients and members of the public have the right to access personal data that is being kept about them, insofar as it falls within the scope of the GDPR.

8.2. Any person wishing to exercise this right should make their request in writing to the Data Protection Officer, or to a Director if a DPO has not been appointed.

8.3. The information will normally be provided free of charge, unless the request is manifestly unfounded or excessive, or it is repetitive. In such cases the Company reserves the right to either:

a. Charge a reasonable fee to cover the administrative costs associated with providing the information. If the Company considers it reasonable to charge a fee for providing information, the Employee or data subject will be notified in advance of this, and payment will be required before the request is processed.
b. Refuse to respond to the request by setting out, in writing, to the data subject, why they have refused.

8.4. If the Company refuses to respond to a subject access request, the data subject has the statutory right to raise a complaint to the supervisory authority.

8.5. MJL aims to comply with request for access to personal information as quickly as possible, but company must comply with a subject access request within one month of receipt or the request, or if later, within one month of the receipt of the identity information required, the completed subject access request form and the relevant fee (if appropriate).

8.6. The Company will normally respond to such requests in hard copy but can provide electronic copies if required, upon request.

9. Breach Reporting

9.1. The GDPR requires that any breach of security of personal data be reported to the relevant authority within 72 hours of becoming aware of the breach, where feasible.

9.2. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Company will also inform those individuals without undue delay.

9.3. The Company will also keep a record of any personal data breaches, regardless of whether we are required to notify any external authority.

Signed: **Dated** **28th February 2019**

Managing Director: Matthew Lugg