LOWRY

Building & Civil Engineering

GENERAL DATA PROTECTION REGULATION

PRIVACY STATEMENT

January 2024

Policy Statement

Lowry Building & Civil Engineering Ltd (the Company) recognises the importance of respecting the personal privacy of clients, employees and others, and the need to implement appropriate safeguards relating to the processing of personal data.

Data protection regulates the way in which organisations use and store personal data about individuals such as clients, suppliers or employees to protect those individuals from unauthorised use or disclosure of their personal information.

The Company is fully committed to abiding by all current UK legislation and this policy is to ensure that the Company fully complies with General Data Protection Regulation (GDPR) laws.

HELEN LOWRY
Director

January 2024

Policy

The Company currently fully complies with all GDPR requirements and in order to maintain compliance with the current Data Protection Act the Company will:

1. Operate in compliance with data protection principles.
2. Ensure any exemptions are applied accurately in accordance with the law.
3. Periodically review and action the guidance and standards issued by the Information Commissioner.
4. Take note of applicable codes of practice and provide relevant data protection training.

Principles

The Act stipulates that anyone processing personal data must comply with Eight legally enforceable Principles of good practice. These principles require that personal information shall:

1. Be processed fairly and lawfully, and in particular, shall not be processed unless specific conditions are met.
2. Be obtained only for one or more specified and lawful purposes and not be further processed in any manner which is incompatible with those lawful purposes.
3. Be adequate, relevant, and not excessive in relation to the purpose/s for which it is processed.
4. Be adequate and where necessary kept up to date.
5. Not be kept for longer than is necessary for that purpose.
6. Be processed in accordance with the rights of data subjects under the Act.
7. Be kept secure to an appropriate level.
8. Not be transferred to a country / territory outside the EU unless it ensures adequate level of data protection.

The Act also provides conditions for processing personal data, and makes distinction between personal and ‘sensitive’ personal data:

1. Personal data is defined as relating to a living individual who can be identified from that data
2. Sensitive personal data is defined as relating to that individual’s:
    - Race
    - Political opinion
    - Religious beliefs
    - Trade union membership
    - Physical or mental health
    - Sexual life
    - Criminal proceedings or convictions

Collection & Retention

The Company collects and uses personal data about individuals in order to carry on its business. Any personal data processed will have the appropriate safeguards applied to ensure compliance with the Act.

Collection

- The Company will only collect personal data that is relevant to carrying out its legitimate purposes in a manner that does not prejudice the interests of individuals.
- The Company will ensure that data collection is as accurate as possible given the methods used in collection and will collect no more data than is necessary for the purpose declared.

Retention

- The Company will keep all personal data up to date and when no longer required for its legitimate purposes, will archive, or destroy the data as appropriate.
- Personal data will be reviewed periodically to check accuracy and whether retention of that data is necessary.

Sensitive Personal Data

- The Company will handle sensitive personal data with particular care and will ensure that appropriate notification will be given to individuals and required consent obtained before collecting or processing such data.

Responsibilities for Handling Sensitive Data

- The Company will ensure that any employee permitted to handle sensitive data (Data Controllers & Processors) comply with the principles set out in the previous section.

Disclosure & Third-Party Processing

The Company will not allow data collected from individuals to be disclosed to third parties except where, for example:

- The individual has consented to the disclosure.
- The Company is legally obliged to disclose the data.
- There is a business requirement to disclose the data which does not prejudice the interests of individuals or breach the Act.
- All requests for disclosure of personal data to third parties should be referred to the Data Protection Officer.

Where data is disclosed to a third party for processing, the Company will obtain written confirmation to ensure that the processor will:

- act only on the Company's instructions,
- not disclose personal data without specific authority
- provide appropriate operational and technical security.
- allow the Company to check compliance.

Security

Data processing will be allowed where there is a clear purpose for any activity which meets the purpose of the Act. Any other purposes for processing will be disclosed to the individual.

Personal data should not be transferred outside the Company and in particular not to a country outside the UK:

- except with the data subject's consent, or
- unless that country's data protection laws provide an adequate level of protection, or
- adequate safeguards have been put in place in consultation with the Company.

Security procedures include - entry controls, secure lockable cupboards, safe disposal methods e.g. shredding and secure IT equipment and systems including firewalls controlled and maintained by IT Department.

Employee data is held by HR (Human Resources) for the duration of their employment. Seven years after an employee's employment terminates, personal data held will be destroyed.

Employee Communications

The Company has put in place appropriate technical, physical and operational security measures to ensure the security of personal data against unauthorised or unlawful processing, and against the accidental loss, destruction or damage of personal data:

Personal information should:

- be kept locked in a filing cabinet, drawer or safe
- if computerised be encrypted or password protected on both local hard drive and on a network drive which is regularly backed up
- if a copy is retained on any removable storage device that device itself should be kept locked away

Data stored on portable electronic or removable devices is the responsibility of the individual member of staff who operates the equipment, who should ensure that:

- suitable regular backups of the data exist
- sensitive data is appropriately encrypted or password protected
- sensitive data is not copied onto portable storage devices without first consulting the IT department and Data Controller to ensure protection measures
- electronic devices such as laptops, storage media etc are not left unattended when offsite

Training

The Company will provide GDPR training for employees as relevant and required for their role.

Breaches of this Policy

Communication is essential to the operation of the Company's business:

- How you communicate with people reflects on you as an individual but also on the Company
- The Company invests substantially in information technology and communication systems which enable you to work more efficiently, and trusts you to use them responsibly and in accordance with Company policies
- The Company may take disciplinary action against you if you fail to comply with Company policies.