General Data Protection Regulation (GDPR) Policy

Statement

This policy sets out the requirements for the management of data in relation to the collection, storage and use relating to the business.

The 'Company' shall abide by the principles of the GDPR by:

- Processing personal data lawfully, fairly and in a transparent manner;
- Collecting only for specified, explicit and legitimate purposes and not further processed in an incompatible manner;
- Collecting minimal data that is adequate, relevant and limited to what is necessary;
- Keeping only accurate and up-to-date data;
- Not keeping, any longer than necessary, and in a form which permits identification of a data subject;
- Providing appropriate security ensuring protection against unauthorised or unlawful processing and against accidental loss, destruction nor damage.

The scope of this policy covers the personal, operational and business data related to the Company in compliance with the General Data Protection Regulation.

System shall be incorporated within the existing integrated management system for ease of management and efficiency.

Responsibilities

It is the responsibility of:

- The 'Company' (Managing Director and Director jointly) to assume the role of Data Controller. As Data Controller the 'Company' is responsible for establishing policies and procedures in order to comply with the regulation.
- A member or members of the Project Office to assume the roles of Data Processors, as nominated by the 'Company' responsible for:
    - Providing guidance, giving advice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information;
    - The appropriate compliance with subject access rights and ensuring that data is released in accordance with subject access legislation under the regulation;
    - Ensuring that any data protection breaches are resolved, documented and reported appropriately in a swift manner and in line with guidance from the Information Commissioners Office;
    - Investigating and responding to complaints regarding data protection including requests to cease processing personal data.
    - Those members who process personal data must comply with the requirements of this policy.
- Employees are responsible for ensuring that their personal data provided to the 'Company' is accurate and up-to-date, of any changes to information previously provided i.e. change of address, health status that may affect their day to day work or errors in the information provided.
- Contractors and third parties working on behalf of OTL shall ensure that any data provided by them is accurate and up-to-date in compliance with the regulation. Managers who employ contractors shall ensure that they are vetted for the data that they are processing or using on behalf of the 'Company' and, ensure that:
    - Any personal data collected or processed in the course of the work is kept securely and confidentially;
    - All personal data is returned to the 'Company' on completion of the work, including any copies that may have been made or, alternately, the data is destroyed and the 'Company' notified;
    - The 'Company' receives prior notification of an disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;
    - Any personal data made available by the 'Company', or collected in the course of the work, is neither stored nor processed outside the UK unless written comment to do so has been received from the 'Company'.
    - All practical and reasonable steps are taken to ensure that contractors do not have access to any personal data beyond what is essential for the work to be carried out properly.

Subject Access Requests

The 'Company' shall, upon agreement with the MD and/or the Director, permit access to an individual's personal data. Any individual wishing to exercise this right shall do so in writing using the appropriate form obtainable from the Project Office. The 'Company' aims to comply with any request for access to personal information as soon as possible and within the confines of the regulation.

A requester shall:

- Know what personal information we are processing or have processed;
- Why we have processed your personal data – the reason(s) and purpose(s) for the processing of your personal information;
- Know if we have shared your personal information and if so, with whom and for what purpose(s).

Individuals will not be entitled to access information to which any of the exemptions of the regulation applies. However, only those specific items of information to which the exemption applies will be withheld and determining the application exemptions will be with the MD and/or Director.

Data Protection Breaches

Where a data protection breach occurs, or is suspected, it should be reported immediately to the MD and/or the Director and include full and accurate details of the incident including who is reporting the incident and what data is involved. All incidents will be managed under the Non-conformance procedure.

Data Security

Data relating to operational and business is held in the integrated management system located on the server, accessible to authorised persons only and backed up on hard drives by the Project Office. Data stored on the server is encrypted

We may need to share your information with third parties (client and Achilles/NQA audits) but will always be to enable us to undertake our statutory functions, to regulate effectively and/or to comply with our legal and regulatory obligations.

When personal data is shared it will be done so in line with the regulation. The employee is entitled to know why and how the 'Company' is sharing your personal information and the organisation or individual receiving your personal information will be required to protect your information in accordance with the regulation.

Backup (portability): Hard drives taken off site shall not be used off site, it is only for the purpose of recovery and not for use by the holder or anyone else. Those who are found to use this data, unless otherwise agreed by the MD and/or Director in writing, shall be subject to the disciplinary procedure. Hard drives will be encrypted or otherwise protected to ensure that, if lost or stolen, data cannot be recovered, seen and used.

Personal: Employees, contractors and other persons acting on behalf of OTL shall, where personal data is to be collected, stored and used, shall give their consent for their data to be stored and used. Whenever an individual's data is to be shared with a third party this shall not happen without the explicit agreement, in writing, of that individual. Where personal data has been stolen or lost the individual shall be informed of the situation and, with management, identify and agree what corrective actions are required to control and rectify the situation.

Where an individual refuses collection, storage and use of his/her data then this shall be discussed with the MD and/or Director to ascertain the reasons why and if, agreement could be reached with agreed limitations. However, where this information is required for business or legislative (employment and the right to work in the UK) purposes and refusal cannot be acceptable, a suitable and sufficient resolution shall be identified and agreed, if not, then OTL shall need to review the situation and the terms of employment.

Existing personal data that it no longer valid or required shall be shredded, only data that is current and required shall be held.

Personal data, in paper format, shall be held in a locked filing cabinet and accessible only by authorised personnel with limited access to keys.

Personal data held electronically (intended to replace paper copies) shall be available to only those who have been authorised access. Access by others not authorised shall be prohibited.

It will be a disciplinary offence where personal data is left in view whilst not in use, once that use has expired personal data shall be returned to the filing cabinet and locked.

Client, Supplier and Third Party: Data related to clients, suppliers and other third parties associated with the business/project shall be retained as agreed by the client, supplier or third party in a secure location either in the OTL office or client site office and available only to authorised persons.

Disposal shall be with the agreement of the document owner, minimal documentation shall be retained.

CCTV: Images taken and stored with the CCTV surveillance cameras shall be stored electronically, locked in the server cabinet upstairs and only available to authorised persons as agreed by the MD and/or Director. The keys to the cabinet shall be available to authorised persons only.

The Information Commissioner's Office

The Information Commissioner's Office (ICO) is "the UK's independent authority set up to uphold information rights in the public interest, prompting openness by public bodies and data privacy for individuals and responsible for administering the provisions of the regulation.

Signed: 

S Edwards

Managing Director

O.T.L. Electrical Services Limited

Date: **January 2022**