SG CIVIL ENGINEERING LTD

Privacy, Confidentiality & Data Protection Policy

2024 – 2025

Table of Contents

Section

1.0 Introduction

1.1 This Policy sets out the obligations of SG Civil Engineering Ltd ("the Company") regarding data protection and the rights of workers, clients and business contacts ("data subjects") in respect of their personal data under the General Data Protection Regulations ("the Regulation").

1.2 The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly.

1.3 In addition, the Policy sets out the procedures that are to be followed when dealing with personal data and confidentiality. The procedures and principles set out herein must be followed at all times by the Company, its workers, agents, contractors, or other parties working on behalf of the Company.

1.4 The Company is committed not only to the legal requirements, but also places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2.0 Lawful & Transparent Data Processing

2.1 The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

- The individual has given consent to the processing of his or her personal data for one or more specific purposes;
- Processing is necessary for the performance of a contract (i.e. Suppliers etc) to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- Specific processing is necessary for compliance with a legal obligation;
- It is necessary to protect the vital interests of the data subject or of another natural person;
- It is necessary for the performance of a task carried out in the public interest.

3.0 Personal Data the Company Collects

3.1 As a business, we are required to keep information relating to each, worker, Service Provider (Suppliers) and any Subcontractors. We need this information to communicate with them for various business purposes and to carry out any necessary checks to ensure compliance. We also hold information that allows us to pay salaries, material supplies and work with other payroll and pension providers.

3.2 Information we may hold about workers, sub-contractors etc may include the following;

- Name and contact details (Inc Telephone Numbers & email addresses), next of Kin details;
- Proof of eligibility of working within the UK (Passport, National Insurance Number);
- Details of individual experience, qualifications, skills (including CSCS etc);
- Details of any training additional training received;
- Copies of driving licenses (if you drive a fleet vehicle) are also required to adhere to the company insurance policy;
- Business contact details and information;

- Bank Details.

3.3 All workers are required to complete a Health Questionnaire, through the appointed Occupational Health Provider. The information within this form the Company classify as special data and enables the business to support individuals with any specific health needs in relation to work.

4.0 Data Protection Measures (Security)

4.1 Everyone within the Company who handles personal data must ensure it is held securely to protect against unlawful or unauthorised processing and accidental loss or damage these groups include;

- Workers (Inc all levels of Management and workers);
- Accounts / Payroll;
- Pension providers.

4.2 The Company will further take appropriate steps to ensure all personal data is secure by ensuring

- All emails containing personal data are encrypted;
- That where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely;
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient;
- No personal data may be shared informally and if a worker, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the director of the company.
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;
- No personal data may be transferred to any workers, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the director of the company;
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise (without the formal written approval of the director of the company and, in the event of such

approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary);

- Under no circumstances should any passwords be written down or shared between any employees, agents, subcontractors, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. The HR / IT Department do not have access to passwords.

5.0 Data Retention

5.1 The Company only holds relevant information and as such are required by law to retain information for different periods of time for varying different purposes.

5.2 The Company shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required or it is outdated, all reasonable steps will be taken to ensure it is destroyed (by means of secure shredding) without delay.

6.0 Accessing & Updating Personal Data

6.1 All individuals have the right to review and amend any information we hold about you as a person. Therefore, they are entitled to ask the Company, in writing, for a copy of this data. In respect of this request the Company will not charge a monetary fee and will respond to the individual request within one calendar month (this can be extended by up to two months in the case of complex requests, and in such cases the individual shall be informed of the need for the extension).

6.2 The Company shall ensure that all personal data collected and processed is kept accurate and up to date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7.0 Confidentiality

7.1 Every individual involved with the Company has the right to confidentiality and respect.

7.2 In the course of its work the Company will be in possession of confidential information about individuals involved with the business and will do its utmost to protect that confidentiality. Any information obtained about individuals, which could reasonably be expected to be confidential, will be stored securely and only used for the purpose for which it was intended.

7.3 The Company may be required to share confidential information with others for the purpose of providing support for the worker in the realms of professional enhancement, or for the purposes of ensuring personal safety. Depending on the circumstances of the situation the Company will either endeavour to obtain the individual's permission before sharing confidential information with others or we will endeavour to inform the individual we have done so or will do so. Individuals will have access to information held about them.

7.4 The Company also expects all individuals engaged in work be it on the business premises or on a transient work site will **not** create or transmit material that might be defamatory or incur liability for the company particularly in respect of social media and should always apply the requirements of the Company 'Social Media Acceptable Use Policy'.

7.5 In addition to the Company position, all individuals must respect the contractual requirements between the Company, Principal Contractor and / or Clients in relation to the sharing of comments or material that breach client / principal contractor confidentiality. Furthermore, all individuals must respect the contractual requirements in relation to the transmission of defamatory comments or material which is posted on social media and as stated in 7.4 individuals should always apply the requirements of the Company 'Social Media Acceptable Use Policy'.

8.0 Third Parties

8.1 The Company will not disclose any personal information we collect about each individual to a third party without specific consent from the individual concerned. This personal information will, in those cases, be passed directly to the relevant contact within the company.

9.0 Data Breaches

9.1 If any data breaches emerge the Company has the duty to report such incidences to the Information Commissioner's Office (ICO). If individuals feel there has been a serious breach of how their data is stored, they are in the first instance to contact their Supervisor.

10.0 Accountability

10.1 The Company's Data Protection Officer is the HR Manager, however if you require further specific information or have any questions regarding how personal data may be used within the Company, please contact the office at enquiries@sgcivilengineering.co.uk

10.2 This policy document and associated documentation will be brought to the attention of all employees and subcontractors and will be reviewed on a regular basis being no less frequently than annually.

S Gallagher
Operations Director
SG Civil Engineering Ltd

1st June 2024