General Data Protection Policy (GDPR)

Aarsleff Ground Engineering Ltd and its UK group of companies including Centrum Pile Ltd and Avoncross Ltd T/A Cannon Piling (the Company) expect their employees to demonstrate honesty, integrity and fairness in all aspects of their duties carried out on behalf of the Company. Similarly, relationships with all stakeholders including clients and suppliers will be at all times conducted professionally and to high ethical standards.

The contents of this policy and all revisions which may be made will be brought to the notice of all employees.
The Company will operate a 'zero tolerance' approach to any breach of this policy. Any such breach will be treated as gross misconduct.

This policy will form part of the Integrated Management System and be formally reviewed annually by Senior Management.

Purpose

This General Data Protection Policy sets out how the Company handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

Target Group

This Policy applies to all Company employees. You must read, understand, and comply with policy when processing personal data on our behalf and attend training on its requirements. This policy sets out what we expect from you for the Company to comply with applicable law. Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

Where you have a specific responsibility in connection with processing such as capturing consent, reporting a personal data breach, conducting a Data Privacy Impact Assessment DPIA as referenced in this data protection policy or otherwise then you must comply with the related policies and privacy guidelines.

Scope

The Company recognises that the correct and lawful treatment of personal data maintains confidence in the organisation providing successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of GDPR.

The Personal Data Controller (PDC) (Finance Director) has responsibility for ensuring all Company employees comply with this Policy and appropriate IT systems practices, processes, controls and training are in place to ensure that compliance.

The Data Protection Officer (DPO) is responsible for overseeing this policy in practice. That post is held by Head of Human Resources. HR@aarsleff.co.uk

AARSLEFF

You must always contact the DPO in the following circumstances:

- If you are unsure of the lawful basis which you are relying on to process personal data (including the legitimate interests used by the Company)
- If you need to rely on Consent and/or need to capture Explicit Consent (see Paragraph 6 below);
- If you need to draft Privacy Notices (see Paragraph 7 below);
- If you are unsure about the retention period for the Personal Data being Processed (see Paragraph 11 below);
- If you are unsure about what security or other measures you need to implement to protect Personal Data (see Paragraph 12.1 below);
- If there has been a Personal Data Breach (Paragraph 13 below);
- If you are unsure on what basis to transfer Personal Data outside the EEA (see Paragraph 14 below);
- If you need any assistance dealing with any rights invoked by a Data Subject (see Paragraph 15);
- Whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see Paragraph 19 below) or plan to use Personal Data for purposes other than what it was collected for;
- If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see Paragraph 20 below);
- If you need help complying with applicable law when carrying out direct marketing activities (see Paragraph 21 below); or
- If you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see Paragraph 22 below).

Personal Data Protection Principles

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require personal data to be:

- Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
- Collected only for specified, explicit and legitimate purposes (Purpose Limitation);
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation);
- Accurate and where necessary kept up to date (Accuracy);
- Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);
- Not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and
- Made available to data subjects and allow data subjects to exercise certain rights in relation to their personal data (Data Subject's Rights and Requests).
- We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

Lawfulness, Fairness, Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

- You may only collect, process, and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing but ensure that we process personal data fairly and without adversely affecting the data subject.
- GDPR allows processing for specific purposes, some of which are set out below:
- The data subject has given his or her consent;
- The processing is necessary for the performance of a contract with the data subject;
- To meet our legal compliance obligations;
- To protect the data subject's vital interests;

- To pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The purposes for which we process personal data for legitimate interests need to be set out in applicable privacy notices.

Consent

- A controller must only process personal data on the basis of one or more of the lawful bases set out in the GDPR, which include consent.
- A data subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing e.g. a signature.
- Data Subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented.
- When processing special category data or Criminal Convictions Data, we will usually rely on a legal basis for
- processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.
- You will need to evidence consents captured and keep records of all consents in accordance with related policies and privacy guidelines so that the Company can demonstrate compliance with consent requirements.

Transparency (Notifying Data Subjects)

The processing of personal data must be transparent. Therefore, we provide information on how personal data is processed. As a principle we only collect personal data directly from the relevant person. During the processing of personal data, we will provide information about:

- Contact details of the personal data controller
- The purpose of the processing and the legal basis for the processing
- The recipients or categories of recipients of the personal data
- Data transfers to a third country (if relevant)
- How long the processing lasts
- The rights of the data subject
- The right to withdraw consent
- The right to complain to the Information Commissioners Office
- Automated profiling if this is used.

The requirement to inform about the processing of personal data is provided with the IMS area on Sharepoint in so far as concerns our own employees and on our website in so far as concerns external parties. New employees will get an Employee Handbook at point the employment contract is offered with information about the processing of personal data at our Company during their employment.

Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

You cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the data subject of the new purposes and they have consented where necessary.

Data Minimisation

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. You may only process personal data when performing your duties where your role requires it. You cannot process personal data for any reason unrelated to your job duties.

You may only collect personal data that you require for your job duties: do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes.

You must ensure that when personal data is no longer needed or legally required for specified purposes, it is deleted or anonymised if legally possible in accordance with the Company's data retention guidelines.

Accuracy

Personal data must be updated so ensure accuracy. Data subject may contact data controllers to update personal data if they are unable to this for themselves on our IT portal systems.

Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

The Company will maintain retention procedure and register to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time. You must comply with the Company's guidelines on data retention.

You must not keep personal data in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which it was originally collected, including for the purpose of satisfying any legal, accounting or reporting requirements.

The PDC will take all reasonable steps to destroy or erase from our systems all personal data that the Company no longer requires in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.

A register is maintained of storage limitation periods for personal data. Data Subjects can access the register on application to the DPO.

Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental/deliberate act of loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data. The PDC, DPO and the processor are responsible for protecting the personal data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. The Company exercises particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

Processors must follow all procedures and technologies the Company puts in place to maintain the security of all personal data from the point of collection to the point of destruction. The processor may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

The Processor must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it;

- Integrity means that personal data is accurate and suitable for the purpose for which it is processed; and
- Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

Reporting a Personal Data Breach

The GDPR requires PDCs to notify any personal data breach to the applicable the ICO and, in certain instances, the data subject.

The Company will deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

If employees know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO who will instigate the necessary processes to deal with the data breach. You should preserve all evidence relating to the potential personal data breach.

Transfer Limitation

If personal data is transferred to third parties, it must be ensured that the required lawful basis exists. If it is assessed that a third party will become an independent data controller in connection with, this should be informed in connection with the transfer.

Any personal data to be transferred outside of the EEA will require special processing and consents so these potential transfers are to be reported to the DPO who will ensure that the correct process is followed in accordance with the ruling Regulations at the time.

The Rights of Data Subjects

Data subjects of our Company have rights that must observed when handling their personal data.

These rights are:

- Withdraw consent to processing at anytime;
- Request access to the personal data we hold on the data subject
- Rectification of errors in personal data
- Prevention of use for direct marketing purposes
- Erasure of their data
- Object to the processing of their data
- Object to decisions based solely on Automated Processing
- Portability of data
- Be notified of a personal data breach

Data subjects can exercise their right by contacting the DPO

Right to Access

A data subject can request from the DPO the right to access their personal data and copy of the data must be supplied. Refer to the ICO portal for the timescale to provide this at any given time, usually in one month.

The DPO will respond by providing the data and detailing;

- The purpose of holding/processing the data
- Categories of processed data
- From where the data was received
- Categories of data recipients
- The period the data is held
- Remind the data subject of their right to erasure

Records will be held of any such requests and how they were handled.

Accountability

The PDC must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The DPC is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Company must have adequate resources and controls in place to ensure and to document GDPR compliance including:

- Appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;
- Integrating data protection into internal documents and processes;
- Training employees on the GDPR, this Data Protection Policy, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by employees; and
- Test the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

Record-Keeping

GDPR requires the Company to keep full and accurate records of all our data Processing activities.

- Keep and maintain accurate corporate records reflecting our processes including records of Data Subjects' Consents and procedures for obtaining consents in accordance with the Company's record keeping guidelines.
- Records should include, at a minimum, the name and contact details of the Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the
- Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

Changes to this Data Protection Policy

The Company will regularly review this policy at a minimum annually.

Annex 1 – Definitions as defined by the General Data Protection Regulation

Definitions:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company name: Aarsleff Ground Engineering Ltd, Centrum Pile Ltd, Avoncross Ltd T/A Cannon Piling.
Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, members, and others.
Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.
Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.
Criminal Convictions Data: means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.
Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.
Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.
Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.
EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.
Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).
General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.
Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.
Privacy Notices or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.
Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

Signed on behalf of the Board of Directors:

Signed:

Kevin Hague - Managing Director, Aarsleff Ground Engineering Ltd

Date: March 2023