Penny Engineering Ltd – Privacy Policy

PH_CW_PD_009 Rev 2

The General Data Protection Regulations (GDPR) gives rights to individuals (data subjects) whose personal data we collect, process, store, share and dispose of and this Policy sets out the Company's obligations, principles and policies with which it will comply in relation to personal data.

The regulations require that any personal data held should be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject;
- 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.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and kept up to date. All reasonable steps will be taken to ensure personal data that is inaccurate is erased or rectified without delay.
- Held securely, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- Kept in a form that permits identification of data subjects, for no longer than is necessary, for the purposes of 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 legislation.

The regulations also give employees certain rights. For employment purposes, the most important rights are the right to be informed, the right to access the personal data held about the employee and the right to be forgotten.

Purposes for which Personal Data may be Held

Employee personal data will be collected to comply with our statutory requirements as an employer, to fulfil the performance of the employment contract and the legitimate business use of maintaining a successful employment relationship. Examples include:

- Recruitment, promotion, training, redeployment and/or career development;
- Administration and payment of wages;
- Calculation of certain benefits including pensions;
- Disciplinary or performance management purposes;
- Performance review;
- Recording of communication with employees and their representatives;
- Compliance with legislation;
- Provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers; and
- Staffing levels and career planning.

The Company considers that the following, falls within the categories set out above:

- Personal details including name, address, age, status and qualifications. Where specific monitoring systems are in place, ethnic origin and nationality will also be deemed as relevant;
- References and CVs;

- Emergency contact details;
- Notes on discussions between management and the employee;
- Appraisals and documents relating to grievance, discipline, promotion, demotion or termination of employment;
- Training records;
- Salary, benefits and bank/building society details; and
- Absence and sickness information.

Employees or potential employees will be advised by the Company of the personal data which has been obtained or retained, its source, and the purposes for which the personal data may be used or to whom it will be disclosed, as well as how long we will keep it for. For more information, please refer to the Company's Privacy Notice.

The Company will review the nature of the information being collected and held on an annual basis to ensure there is a legitimate reason for requiring the information to be retained.

Special Category (Sensitive) Personal Data

Sensitive personal data includes information relating to the following matters. This type of data will only be processed where it is necessary for the purpose of carrying out our obligations and exercising our rights and that of the data subject in the field of employment.

- The employee's racial or ethnic origin;
- His or her political opinions;
- His or her religious or similar beliefs;
- His or her trade union membership;
- His or her physical or mental health or condition, and other medical data
- His or her sex life; or
- The commission or alleged commission of any offence by the employee.

Responsibility for the Processing of Personal Data

The Company will appoint a Data Protection Lead as the named individual responsible for ensuring all personal data is controlled in compliance with the General Data Protection Regulations (GDPR).

Employees who have access to personal data must comply with this Policy and adhere to the procedures laid down by the Data Protection Lead. Failure to comply with the Policy and procedures may result in disciplinary action up to and including summary dismissal.

Use of Personal Data

To ensure compliance with the General Data Protection Regulations (GDPR) and in the interests of privacy, employee confidence and good employee relations, the disclosure and use of information held by the Company is governed by the following conditions:

- Personal data will only be used for one or more of the purposes specified in this Policy and only shared with third parties who satisfy our checks for GDPR compliance and who have a legitimate reason to have access to this data.
- Company documents may only be used in accordance with the statement within each document stating it's intended use; and
- Provided that the identification of individual employees is not disclosed, aggregate or statistical information may be used to respond to any legitimate internal or external requests for data (e.g., surveys, staffing level figures); and
- Personal data will not be disclosed, either within or outside the Company, to any unauthorised recipient.

Disclosure of Personal Data

Personal data may only be disclosed outside the Company where disclosure is required by law, in order to facilitate performance of the employment contract, where there is immediate danger to the employee's health or when explicit consent has been received.

Consent

Where the company is relying on an employee's consent to process their data, the employee has a right to restrict processing or withdraw their consent for their data to be processed. Please speak to the Data Protection Lead or a member of management for further queries or to exercise your rights.

Accuracy of Personal Data

The Company will review personal data regularly to ensure that it is accurate, relevant and up to date.
In order to ensure the Company's files are accurate and up to date, and so that the Company is able to contact the employee or, in the case of an emergency, another designated person, employees must notify the Company as soon as possible of any change in their personal details (e.g., change of name, address; telephone number; loss of driving licence where relevant; next of kin details, etc.).

The Company will review personal details records from time to time for the purposes of ensuring the data is up to date and accurate. Employees will be entitled to amend any incorrect details and these corrections will be made to all files held on the Company's information systems. In some cases, documentary evidence, e.g., qualification certificates, will be requested before any changes are made.

Once completed, these records will be stored in the employee's personnel file.

Data Retention

The Company will not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

Secure Processing

The Company will ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. For further information about how we keep personal data secure, please refer to our Information Security Policy and our Acceptable IT Use Policy.

Accountability and Record-Keeping

The Company's Data Protection Lead is XXXX.

The Data Protection Lead is responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, other data protection-related policies and with the General Data Protection Regulations.

The Company will keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;
- The purposes for which the Company collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy); and
- Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data (please refer to the Company's Information Security Policy and Acceptable IT Use Policy.

Data Protection Impact Assessments

The Company will carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

Data Protection Impact Assessments shall be overseen by the Data Protection Lead and shall address the following:

- The type(s) of personal data that will be collected, held, and processed;
- The purpose(s) for which personal data is to be used;
- The Company's objectives;
- How personal data is to be used;
- The parties (internal and/or external) who are to be consulted;
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- Risks posed to data subjects;
- Risks posed both within and to the Company; and
- Proposed measures to minimise and handle identified risks.

THE RIGHTS OF DATA SUBJECTS

Keeping Data Subjects Informed

The Company shall provide information to every data subject in line with the requirements of the GDPR via a Privacy Notice.

Data Subject Access

Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Data Protection Lead at 8 Hanbury Close, Balby, Doncaster, DN4 9AW, United Kingdom

Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

All SARs received shall be handled by the Company's Data Protection Lead.

The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of Personal Data

Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.
The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

Erasure of Personal Data

Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
- The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so)
- The personal data has been processed unlawfully;
- The personal data needs to be erased in order for the Company to comply with a particular legal obligation:
    - Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
    - In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

Restriction of Personal Data Processing

Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Data Portability

The Company processes personal data using automated means.

Where data subjects have given their consent to the Company to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the data

subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects when requested, when it is appropriate and in a format that is reasonable and manageable. Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

Objections to Personal Data Processing

Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

Personal Data Collected, Held, and Processed

Personal data is collected, held, and processed in line with the Company's Data Retention Policy and Schedule.
Data Security

For full details of the organisational and technical measures the Company has taken please refer to the Information Security Policy.

Data Breach Notification

All personal data breaches must be reported immediately to the Company's Data Protection Lead.

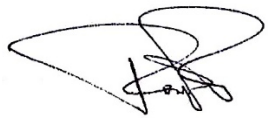
If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Signed
T. Penny MD



Date 19/01/2026