POWERSYSTEMS™
HIGH VOLTAGE SPECIALISTS
An Employee Owned Business

DOCUMENT REF. POL-28

Powersystems Data Protection Policy

Author: **CP Data Protection** Date: **30/01/2025**

POWERSYSTEMS DATA PROTECTION POLICY

AMENDMENT HISTORY		
Version	**Purpose**	**Date**
1.0	Initial Issue	10.01.20
2.0	Revised & re-dated	01.01.19
3.0	Review & change of Managing Director	15.01.19
4.0	Rebranded and versioned	23.03.20
5.0	Annual update	31.03.21
6.0	Update in line with new legislation	12.07.21
7.0	Annual review – Brand update	27.06.22
8.0	Data Protection document update and changes by consultants CP Data	14.06.24

DOCUMENT ISSUE RECORD		
Task/Name	**Position**	**Date**
Prepared by CP data Protection	GDPR Consultants	14.06.24
Reviewed by Jacqui Hallett	Project Administrator	18.08.24
Approved by Rachel Berry	Finance Director	30.01.25

Table of Contents

Powersystems Data Protection Policy

DOCUMENT REFERENCE POL-28

1. The data protection policy and handbook:

The Data Protection Policy and Handbook highlights what you need to be aware of to comply with Data Protection Legislation and reduce the risks of mishandling information about people.

The Summary and Policy Statement sections are the most important sections to read and understand, if you need more support to apply any of the legal requirements, please contact the Financial Director on 01454 318000.

Glossary of some Data Protection terms

Data Controller = the legal entity (i.e. usually our Company) that decides the purposes for collecting, using, and so on, Personal Data.

Data Processor = businesses or contractors that will handle Personal Data on our behalf as part of the paid work they do for our Company.

Data Subject = the living person whose data is being processed.

Personal Data = any information that identifies (either directly or indirectly by adding other information to it) a living person.

Processing = anything that can be done with data, from collecting it through using it, sharing it, storing it, to deleting or destroying it.

2. Summary:

Handling personal data properly and upholding the rights of data subjects (the people whose data we hold, including our customers and colleagues) is inextricably linked with our aims as a responsible business, and we cannot carry out our work without handling personal data.

In general terms, if people are at risk, Data Protection legislation allows us to process and share personal data appropriately.

To comply with Data Protection legislation and uphold individuals' data rights:

- We will only process personal data when we have a clear and fair legal basis and we are transparent about the processing (unless an exemption to transparency applies)
- We use appropriate security measures, including technical and company measures
- Personal data will only be shared with our contractors, suppliers or other third parties where appropriate due diligence has been carried out and a legally compliant contract is in place where required
- We will respond without delay to any request or enquiry from a data subject

3. Policy Statement:

To protect the personal data and rights of the people whose data we collect, hold, and use, we will aim, at all times, to comply with all relevant data protection laws and follow best practice. We value the people we work with, and endeavor to be open and transparent, and act with integrity in all of our working relationships.

Relevant laws:

- UK General Data Protection Regulation – **(UK)GDPR**
- Data Protection Act 2018 – **DPA 2018**
- The Privacy and Electronic Communications Regulations (EC Directive) – **PECR**
- The common law duty of **confidentiality**
- Any updated or additional laws or regulations relating to data protection or privacy.

In particular we will aim to make sure that personal data is always:

- Processed **fairly, lawfully** and in a **transparent** manner.
- Processed for **specified, explicit and legitimate purposes** and not in a manner that is incompatible with those purposes.
- **Adequate, relevant and limited** to what is necessary for the purpose for which it is being processed.
- **Accurate** and, where necessary, kept **up to date**.
- **Not kept longer than necessary** for the purposes for which it is being processed.
- Processed in a **secure manner**, by using appropriate technical and company measures.
- Processed **in keeping with the rights of data subjects** regarding their own personal data.

- Processed on our behalf only by **Data Processors** who provide sufficient guarantees that they will process data securely and will comply with relevant laws.
- **Not transferred outside of the UK** unless appropriate safeguards or exemptions apply.

In addition, we will:

- Build **'Privacy by Design'** into our processes as appropriate, by considering data-related risks at the earliest stages of planning new policies or projects.
- **Report data security breaches** to the regulator and to data subjects as required.
- **Demonstrate our compliance** with legal requirements, to comply with the legal requirement for accountability.

4. Responsibilities:

Business: The business and all colleagues are responsible for the business complying with Data Protection legislation.

Individuals: In addition, an individual who obtains or retains personal data or purposefully identifies an individual from anonymised data, when they have no authorisation from the business to do so, may be committing an offence under the DPA 2018. Also, an individual who purposefully withholds data from a Subject Access Request (see the section on data rights) may be committing a DPA 2018 offence.

5. Personal data processing

5.1 Data and data subjects

5.1.1 A Data Subject is a person whose data we process (which means to do anything with data.) In the course of our work, we process information about:

- People we work with, or will potentially work with, including contractors, consultants and suppliers.
- People who buy/will potentially buy from us.
- Our colleagues, including applicants, employees, work experience, students, Trustees, Board consultants.
- Next of kin/emergency contacts, beneficiaries, named additional drivers
- Other business contacts, including visitors.

5.1.2 We collect and process a range of information about different data subjects as appropriate, including amongst other things; name, contact details, date of birth, and other information including data produced during our interactions. Full details are included in our **Privacy Notice (PSUK_POL27)**.

5.1.3 In some cases, we process information known as **'special categories'** of data. This type of personal data can only be processed under strict conditions and includes information about:

- Race or ethnic origin, religious, or other beliefs, physical or mental health and trade union membership
- Information relating to **criminal** proceedings or offences or allegations is also subject to strict rules around processing
- Other data, such as financial details, may be regarded as **sensitive**, but is not included in the legal definition 'special categories'

5.2 Data protection principles

Fair, lawful and transparent processing is achieved by making sure that we only process personal data when the reason for the processing meets a **legal basis** listed in the GDPR (or two legal bases, in the case of special categories data or criminal information), and by **explaining** that processing to data subjects.

5.2.1 Legal basis for processing

Processing of personal data is lawful when the purpose meets one of the legal bases, as listed in Article 6 in the GDPR:

- The processing is necessary for a **contract** with the data subject; (including employment contracts).
- The processing is necessary for us to comply with a **legal obligation**.
- The processing is necessary to protect someone's **life** (known as 'vital interests').
- the processing is necessary for us to perform a task in the **public interest**, and the task has a clear basis in law (this applies to public authorities whose tasks are laid down in UK law).
- The processing is necessary for our **legitimate interests** or those of a third party, unless these are overridden by the legitimate interests, rights and freedoms of the data subject (this applies to data processing such as obtaining customer feedback, or sending hard copy marketing materials, for example).
- If none of the other legal bases apply, the processing will only be lawful if the data subject has given their clear, specific, freely given **consent**. *(Consent should generally be the last resort for a legal basis but* **is** *the only available legal basis for sending "unsolicited direct electronic marketing" and for setting non-essential Cookies, under the PECR – see below).*

5.2.2 Consent for direct electronic marketing

Under the PECR, **direct electronic marketing** to **individuals' email accounts or phones** – as opposed to accounts run and owned by businesses/companies – requires GDPR-standard of consent.

"Marketing" includes fundraising and promoting our aims or free services as well as selling goods or services, and recruitment.

"Electronic" includes email and SMS text message.

The only exception is that we can send electronic marketing messages to current/previous customers (or people who have entered into negotiations to buy from us) without obtaining separate consent – this is known as "soft opt-in".

All "marketing" messages must include an "unsubscribe" link or method.

Marketing Telephone calls must NOT be made to any numbers registered on the individual Telephone Preference Service (TPS) or the business Telephone Preference Service.

5.2.3 Consent for non-essential website cookies

Under the PECR, **non-essential website cookies** should only be placed on a website visitor's device with their freely given consent, by way of a pop-up or banner and Cookie settings function on the website, which allows visitors to consent or decline non-essential cookies. Non-essential means cookies that aren't needed to make the website work properly for the **visitor**.

5.2.4 In addition, when processing **special categories** of personal data, to be lawful the purpose must also meet one **extra legal basis**, this time from those listed in Article 9 of the GDPR. These bases include, amongst others, where:

- The processing is necessary for carrying out our obligations, or for the exercising of rights, under **employment law, or social security law, or social protection law** *(including the Health & Safety at Work Act).*
- The processing is necessary for protecting the vital interests of an individual when the data subject is incapable of giving consent (e.g. in emergency, **life or death situations**)
- The processing relates to personal data that is manifestly made public by the data subject.
- The processing is necessary for pursuing or defending **legal claims**.
- The processing is necessary for the **substantial public interest**, for purposes with a basis in law, specifically the **DPA 2018** (see 5.2.5 below).
- The processing is necessary for **medicine or healthcare**, including preventative or occupational medicine/health, subject to conditions – the processing is carried out by or under the supervision of a health professional and they are obliged to keep confidentiality under the law or their professional body.
- If none of these or the other Article 9 legal bases apply, the processing will be lawful only if the data subject has given their **explicit**, clear, specific, freely given **consent**. *(Consent should generally be the last resort for a legal basis N.B. The standard of consent required for special categories of data is a higher standard – it is "explicit consent").*

5.2.5 Purposes for which we process **special categories** of personal data or **criminal information** where it is necessary for the **substantial public interest, as listed in the DPA 2018**, include the following, all of which have particular criteria in order to be relied upon:

- Statutory and government purposes.
- Equality of opportunity or treatment (regarding different: race or ethnic origins; religious or similar beliefs; health status; sexual orientation).
- Promoting or maintaining racial or ethnic diversity at senior management levels.
- Preventing or detecting unlawful acts.
- Protecting the public against dishonesty, malpractice, incompetence and similar.
- Preventing fraud.
- Making disclosures about suspicions of terrorist financing or money laundering.
- Providing confidential advice, support or another similar service provided confidentially.
- Safeguarding of children and adults at risk, including safeguarding of economic well-being.
- Insurance purposes.
- Occupational pensions.
- Responding to requests made by Elected Representatives e.g. Members of Parliament on behalf of individuals.Making disclosures about suspicions of terrorist financing

5.3 Privacy notices

5.3.1 When personal data is collected directly from the data subject, we inform them, in our Privacy Notice, and as far as reasonably possible at the time of the data collection, about:

- Who we are and how to contact us.
- The reasons for which we process their personal data, and each legal basis for the processing.
- Where the legal basis is legitimate interests, we will explain those legitimate interests.
- If the data is needed for a contract or for a statutory requirement, we will explain the possible consequences of failing to provide it.
- Any automated data processing and decision making where the outcome could have a significant effect on an individual (including profiling), and its possible consequences.
- Who we will share the data with, or the types of companies/people we will share it with.
- If we plan to store or transfer personal data outside of the UK, the fact that this will happen, and the safeguards that are in place.
- How long the data will be stored, or how we will decide how long we will keep the data
- The legal rights that data subjects have.
- The right to withdraw consent at any time, if we are relying on consent as the legal basis for the processing.
- The right to complain to the UK's Data Protection regulator, the Information Commissioner's Office (ICO).

5.3.2 When personal data is collected via a third party, we will also inform the data subjects about:

- The categories of personal data concerned.
- The source of the personal data.

We will provide this information in writing no later than 1 month after we receive the data, unless a legal exemption applies.

5.4 Purpose limitation

We will only process personal data for the purposes which we've explained in our Privacy Notice, or for compatible purposes.

If we need to assess whether a new processing purpose is a compatible purpose, we will consider, amongst other things, the context in which the data was collected, what the data subject might expect us to do with their data, the link between the original processing purpose and the proposed new purpose, the nature of the data, the consequences and risks of the new processing, and appropriate safeguards.

5.5 Data minimisation

Our data collection processes and forms are designed to collect only the personal data that is required.

We will not collect more than we need or anything "just in case."

5.6 Data accuracy

Personal data will be kept accurate and up to date, as necessary and to the level that is appropriate to the risks of inaccurate or out of date personal data being processed.

5.7 Data retention

Our retention periods are based on the requirements of the purposes for processing, legal requirements, and official guidance or good practice in our sector. See PSUK-GDPR-013 Record of Processing (Data Retention) Form, held by our finance team.

5.8 Data security

We use appropriate technical and company measures to ensure personal data is processed securely, including protecting it from unauthorised or unlawful processing, or from accidental loss or damage.

Measures include, where possible and appropriate: technical systems security, access controls, disaster recovery measures, regular testing of security measures, physical security of our premises and data, policies, procedures, training and audits. We will take into account the risks to data subjects which could result from a data breach, and the costs and quality of available measures. *(See section 6 on Managing Risk for more on security).*

5.9 Data subjects' rights

5.9.1 We process personal data in line with data subjects' rights to:

- Request **access** to their personal data held by us - this is known as a **(Data) Subject Access Request**, or a DSAR, or a SAR.
- Ask to have inaccurate personal data in our records **rectified**.
- **Restrict** processing, in certain circumstances.
- **Object** to processing, in certain circumstances – if the processing being objected to is the sending of hard copy **marketing** materials, we must stop the processing **immediately**.

- Data portability, in certain circumstances, which means to receive their data, or some of their data, in a format that can be easily used by another company or person
- **Not be subject to automated decisions or profiling**, where it would have a legal or similarly significant effect on the data subject.
- **Withdraw consent** when we are relying on their consent for the processing.

5.9.2 All data subjects' rights are provided free of charge, and we will fulfil all valid requests to exercise rights as soon as possible, and within one month at the latest, unless there is good reason to, and we can lawfully extend that timescale, by up to an extra two months.
(If we receive a request from a data subject, see the ICO website or contact **Data Protection** *consultant for support and information).*

5.10 Data sharing

5.10.1 Data processors

Contractors or Suppliers who will (or could) process personal data as part of the work they are doing on our behalf are our 'Data Processors'. Regardless of the monetary value of the contract, when working with Data Processors we will carry out appropriate due diligence checks to ensure they guarantee they will comply with data protection legislation.

We will require Data Processors to sign a contract that includes the GDPR-compliant terms. This could be their own contract (if it is already compliant) or it could be using **our own Data Processing Agreement template (PSUK-GDPR-002)**.

Data Processor contracts, and compliance, should continue to be monitored throughout the contract period.

5.10.2 Third parties

Personal data will only be shared with any other third parties, including other data controllers, when the sharing has one or more appropriate legal bases, and is carried out in keeping with the data protection principles and while upholding the rights of data subjects. If faced with a data sharing request, we will not share until we have established the validity of the request and the identity of the requestor.

5.10.3 Data transfers outside the UK

Personal data will not be transferred outside the UK – including using Data Processors or cloud storage services that physically store data on servers located outside of the UK, or the company is based outside the UK – unless one of the following applies:

- It's an EEA [inside the European Economic Area] country
- It's a non-EEA country that has been given an "adequacy decision" by the UK (see the ICO website for the current list of countries and territories with an adequacy decision)
- It's a non-EEA country without an adequacy decision but we carry out a Risk Assessment and sign a contract that includes an "IDTA" (International Data Transfer Agreement).

6. Managing risk and accountability

6.1 Privacy by design

6.1.1 We will build 'Privacy by Design' into our new processes and systems as appropriate, which means we will consider and control any Data Protection related risks before we introduce any new processes or systems that involve the handling of personal data.

6.1.2 If the new process or system seems to present a high risk to our Data Subjects, we will carry out a Data Protection Impact Assessments (DPIA) before implementing the new process/system.

6.2 Data security breaches

6.2.1 All Data Security Breaches, including any loss or leak of personal data, should be reported internally immediately to the Data Protection Lead, and then logged, investigated, and appropriate corrective and preventive action taken as soon as possible, by following the Data Breach reporting form (PSUK-GDPR-016)

6.2.2 Specifically, any personal data breach that is likely to result in a risk to data subjects should be reported to the ICO within 72 hours of us becoming aware of the breach.
(See the ICO website for more information.)

6.2.3 If a data breach is likely to cause a **high** risk to data subjects, we will also inform the data subjects, as soon as possible, to allow them to take any appropriate action that may help to protect them and their data, such as changing their passwords or reporting a loss of their bank details to their own bank.

6.3 Accountability

6.3.1 We demonstrate our compliance with legal requirements (also known as 'accountability'), by keeping records of the regular data processing we carry out, having appropriate policies in place, also registering with the ICO is required, and accessing appropriate Data Protection support when required.

6.3.2 Records of processing include information about how and why we are processing personal data, what data we hold, and the legal basis for the processing, as well as any third parties the data is shared with, including any transfers outside of the UK, and the safeguards in place if data is transferred outside the UK.

6.3.3 We pay the required annual fee to the ICO as required.
(See the ICO website for more information).

Powersystems Data Protection Policy

6.4 General security measures and good practice

6.4.1 Paper

- Keep as few paper records that contain personal data as possible.
- All paper records containing personal data should be stored in a locked filing cabinet when not in use.
- Scraps of paper containing names or other personal data should be treated as carefully as if they were a more official document.
- Paper containing personal data should be shredded when being disposed of.

6.4.2 Emails

- It is **very easy** to make a mistake when sending emails and cause a data breach.
- Work email addresses should always be used for official work purposes, and work-related information not forwarded to a personal/home email address.
- Use "reply all" with caution. Double-check all the recipients are authorised to receive the information you have included in your response to the original email.
- If sending emails to groups of individuals, use "BCC" (blank carbon copy) or Mail merge from a Word document or a mass email sending system.
- Clear out auto-fill options on a frequent basis to remove external names or those you rarely email.

6.4.3 Phones

- Any mobile phone used for business, including personal phones, must have a lock.
- Wherever phone calls are taking place, care should be taken to make sure you can't be overheard when discussing confidential information.

6.4.4 IT equipment

- Any IT equipment used to hold personal data or otherwise confidential information, e.g. laptops, memory sticks, DVD's or external hard drives, should be encrypted and password protected.
- Laptops and storage media should not be left unaccompanied in public. When travelling by car laptops and other storage devices must be carried in the boot and not left in a vehicle overnight.
- Care should always be taken to make sure your screen can't be seen by anyone without authority. This is especially important if working in cafes, on trains or in any other public places.

6.4.5 Postal services

- Any hard copy documents containing sensitive personal data or otherwise confidential information, for example sensitive health-related information or original ID documents should be sent using tracked delivery where possible.
- A "return to sender" address should be included on the outside of the envelope.

6.4.6 Archiving and retention

- Once the appropriate data retention period has elapsed, the personal data should be securely destroyed or deleted.
- Paper records should be shredded.
- Secure deletion of electronic files includes permanently removing all back-up copies of the data too.