POWERSYSTEMS™
HIGH VOLTAGE SPECIALISTS

DOCUMENT REF. POL-28

Powersystems Data Protection Policy

Author: **Clarke Willmott (Consultants)** Date: **27/06/2022**

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

DOCUMENT ISSUE RECORD		
Task/Name	**Position**	**Date**
Prepared by Sophie Hardwick	HSEQ Administration	23.03.20
Reviewed by Sophie Hardwick	HSEQ Administration	23.03.20
Approved by Chris Jenkins	Managing Director	23.03.20

Table of Contents

1. Introduction 2
2. The Data Protection principles 2
3. Lawful, fair and transparent data processing 2
4. Process for specified, explicit and legitimate purposes 3
5. Adequate, relevant and limited data processing 3
6. Accuracy of data and keeping data up to date 3
7. Timely processing 3
8. Secure processing 3
9. Accountability 3
10. Privacy impact assessments 3
11. The rights of data subjects 4
12. Keeping data subjects informed 4
13. Data subject access 4
14. Rectification of personal data 5
15. Erasure of personal data 5
16. Restriction of personal data processing 5
17. Data portability 5
18. Objections to personal data processing 5
19. Automated decision making 6
20. Profiling 6
21. Processing data activities 6
22. Data protection measures 7
23. Organisational measures 8
24. Transferring personal data to a country outside the EEA 8
25. Data breach notification 9
26. Implementation of policy 9
27. Changes to this policy 9

Powersystems Data Protection Policy

DOCUMENT REFERENCE POL-28

1. Introduction:

This Policy sets out the obligations of Powersystems (the "Company") regarding data protection and the rights of customers both old and new and members of staff, whether existing or not ("Data subjects"), in respect of their personal data under the Data Protection Act 1998 (DPA) and General Data Protection Regulation (the "Regulation").

The Regulation defines personal data as any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company. Any breach of this Policy may result in disciplinary action. This Policy does not form part of an employee's contract of employment and may be amended at any time.

The Company is committed not only to legal compliance, but also to the spirit of the law and places of 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. The Data Protection principles:

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which anyone handling personal data must comply. All personal data must be:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject
- Collected for specific, 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 will 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, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as it 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 Regulation in order to safeguard the rights and freedoms of the data subject
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

3. Lawful, fair and transparent data processing:

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 will be lawful if at least one of the following applies:

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract 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
- Processing is necessary for compliance with a legal obligation to which the Company is subject
- Processing is necessary to protect the vital interests of the data subject or of another natural person

Powersystems Data Protection Policy

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company
- Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

4. Process for specified, explicit and legitimate purposes

The Company collects and processes the personal data set out in section 21 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and data received from third parties (for example, HMRC and Child Support Services).

The Company only processes personal data for the specific purposes set out in section 21 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be communicated to the data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

5. Adequate, relevant and limited data processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose(s) communicated to the data subjects in accordance with section 3.

6. Accuracy of data and keeping data up to date

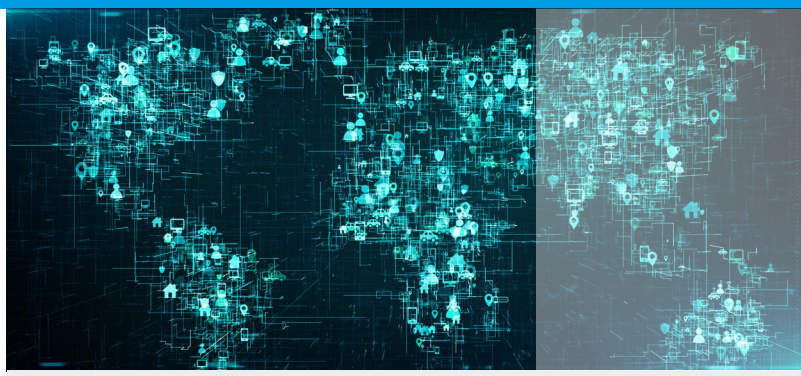
The Company will ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of personal data will be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date personal data is found, all reasonable steps will be taken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

7. Timely processing

The Company will not keep personal data for any longer than is necessary in light of the purposes for which that personal data was originally collected and processed. When the personal data is no longer required, all reasonable steps will be taken to erase it without delay.

8. Secure processing

The Company will ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which will be taken are provided in sections 22 and 23 of this Policy.



9. Accountability

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

- The name and details of the Company, its Data Compliance Team, and any applicable third party data controllers
- The purposes for which the Company 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 (and categories) of any third parties that will receive personal data from the Company and on what basis. A copy of any agreement purporting to transfer personal data must be kept and reviewed prior to signing to ensure processing provisions are compliant with the Regulation. Please contact the Data Compliance Team before entering into any contract
- 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
- Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

10. Privacy impact assessments

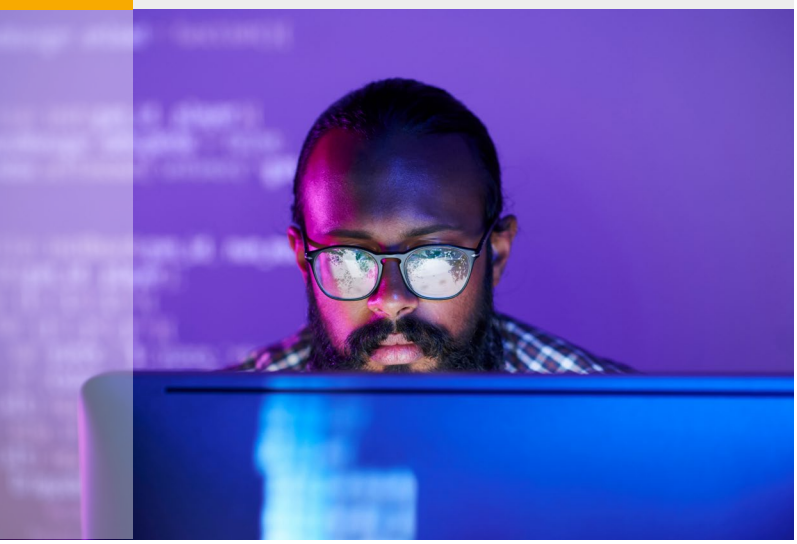
The Company will carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments will be overseen by the Data Compliance Team who will address the following areas:

- The purpose(s) for which personal data is being processed and the processing operations to be carried out on that personal data
- Details of the legitimate interests being pursued by the Company
- An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed
- An assessment of the risks posed to individual data subjects
- Details of the measures in place to minimise and handle risks, including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation

11. The rights of data subjects

The Regulation sets out the following rights applicable to data subjects:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (also known as the 'right to be forgotten')
- The right to restrict processing
- The right to data portability
- The right to object
- Rights with respect to automated decision-making and profiling.



12. Keeping data subjects informed

The Company will ensure that the following information is provided to every data subject when personal data is collected:

- Details of the Company including, but not limited to, the identity of its Data Compliance Team
- The purpose(s) for which the personal data is being collected and will be processed, and the legal basis justifying that collection and processing
- Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data
- Where the Personal data is not obtained directly from the data subject, the categories of personal data collected and processed
- Where the personal data is to be transferred to one or more third parties, details of those parties
- Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see clause 24 of this Policy for further details concerning such third country data transfers)
- Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined)
- Details of the data subject's rights under the Regulation
- Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time
- Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation)
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it
- Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

The information set out above in clause 0 will be provided to the data subject:

- Where the personal data is obtained from the data subject directly, at the time of collection
- Where the personal data is not obtained from the data subject directly (i.e. from another party)
- If the personal data is used to communicate with the data subject, at the time of the first communication
- If the personal data is to be disclosed to another party, before the personal data is disclosed
- In any event, not more than one month after the time at which the Company obtains the personal data.

13. Data subject access

A data subject may make a subject access request ("**SAR**") at any time to find out more about the personal data that the Company holds on them. The Company is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests and, in such cases, the data subject will be informed of the need for the extension.

All subject access requests received must be forwarded to the Data Compliance Team within 24 hours of receipt.

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.

14. Rectification of personal data

If a data subject informs the Company that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question will be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject will be informed of the need for the extension).

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

15. Erasure of personal data

Data subjects may 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 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) (see clause 18 of this Policy for further details concerning data subjects' rights to object)
- 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 will be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject will be informed of the need for the extension).

In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties will be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. 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 will retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

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

17. Data portability

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 legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).

To facilitate the right of data portability, the Company will make available all applicable personal data to data subjects in the following format[s]:

- Secure PDF format

Where technically feasible, if requested by a data subject, personal data will be sent directly to another data controller.

All requests for copies of personal data will be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject will be informed of the need for the extension).

18. 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 statistics purposes.

Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company will cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or 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 will cease such processing forthwith.

Where a data subject objects to the Company processing their personal data for statistics purposes, the data subject must, under the Regulation, '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.

19. Automated decision making

In the event that the Company uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.

The right described in clause 0 does not apply in the following circumstances:

- The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject
- The decision is authorised by law
- The Data subject has given their explicit consent.

20. Profiling

Profiling is a form of automated processing that is intended to evaluate certain personal aspects of an individual, in particular to analyse the performance at work, health, personal preferences, reliability, location, movements etc. Where the Company uses personal data for profiling purposes, the following will apply:

- Clear information explaining the profiling will be provided, including its significance and the likely consequences
- Appropriate mathematical or statistical procedures will be used
- Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected will be implemented
- All personal data processed for profiling purposes will be secured in order to prevent discriminatory effects arising out of profiling.

21. Processing data activities

The following personal data may be collected, held, and processed by the Company:

PERSONNEL DATA			
Type of Data	Purpose of Processing	Type of recipient to whom Personal data is transferred	Retention Period
Name	Legal Identification	HMRC, Pension, Auditor, HR, Client.	7 years
Address	Correspondence	HMRC, Pension, Auditor, HR	7 years
National Insurance No.	Payroll	HMRC, Pension, Auditor, HR	7 years
D.O.B.	Legal Identification	HMRC, Pension, Auditor, HR	7 years
Salary	Payroll	HMRC, Pension, Auditor, HR	7 years
PAYE Information	HMRC, Tax, Payroll	HMRC, Pension, Auditor,	7 years
Tax Information	HMRC, Payroll	HMRC, Pension, Auditor,	7 years
Passport or proof of residence	Proof of legal UK residence	HMRC, Pension, Auditor, HR	7 years
Email	Correspondence	Pension, HR,	7 years
Phone Numbers	Correspondence	Pension, HR	7 years
Bank Information	Payroll	HMRC, Pension, Auditor	7 years
Other Financial Information	Payroll	HMRC, Pension, Auditor	7 years
Qualifications and Experience	Proof of competence	Auditor, HR, Client	7 years
Photo ID	Legal Identification	Auditor, HR, Client	7 years
Driving Licence and History	Company and Personnel Insurances	Auditor, HR	7 years
Medical Information and Next of Kin	Health and Safety	Auditor, HR	7 years
Location in regards to Company Vehicles by Tracking software	Company Insurance	Auditor, HMRC Compliance	7 years
Car Insurance	Company Insurance	Auditor, HR	7 years
Sample Signatures	Legal Identification	Auditor	7 years
Basic information (Name, Address, NINO, DOB, Employment dates, Job title)	Employers liability insurance claims	Insurers	Unlimited

SUPPLIER DATA			
Type of Data	Purpose of Processing	Type of recipient to whom Personal data is transferred	Retention Period
Name	Legal Identification	Auditor, Client	7 years
Address	Correspondence, Payment	Auditor	7 years
Email	Correspondence	Auditor	7 years
Phone Numbers	Correspondence	Auditor	7 years
Bank Information	Payment	Auditor	7 years
Public Liability	Health and Safety	Auditor, Client	7 years
Professional Indemnity Insurances	Health and Safety	Auditor, Client	7 years
Unique Tax Reference Number	HMRC	HMRC, Auditor	7 years
National Insurance Number	HMRC	HMRC, Auditor	7 years
Company Registration	HMRC, Payment	HMRC, Auditor	7 years

RECRUITMENT DATA			
Type of Data	Purpose of Processing	Type of recipient to whom Personal data is transferred	Retention Period
Name	Legal Identification	N/A	6 Months
Address	Correspondence	N/A	6 Months
Email	Correspondence	N/A	6 Months
Phone Numbers	Correspondence	N/A	6 Months
Qualifications	Proof of competence	N/A	6 Months

22. Data protection measures

All employees, agents, contractors, or other parties working on the Company's behalf must comply with the following when working with personal data:

- All emails containing personal data relating to payroll and confidential information must be encrypted using Microsoft Outlook Trust Centre
- 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 using company approved secure deletion software
- 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 sent by facsimile transmission, the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data. Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using a secure courier service
- No personal data may be shared informally and if an employee, 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 the Data Compliance Team
- 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 relating to payroll and confidential information may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the Data Compliance Team
- Personal data must be handled with care at all times and should not be left unattended or on view by unauthorised employees, agents, sub-contractors or other parties at any time
- 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 relating to payroll and confidential information 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 Data Compliance Team 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
- No personal data relating to payroll and confidential information should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken)
- All personal data stored electronically is backed up automatically with backups stored onsite and offsite. All backups are protected using the Datto File Firewall and encrypted while stored, alongside connection encryption while communicating with the backup servers
- All electronic copies of personal data should be stored securely using passwords and behind the server's Virtual Private Network
- All passwords used should be unique to the user
- Users consent to IT staff and 3rd party IT support having access to passwords for legitimate reasons such as hardware and software updates and repairs. Under no circumstances should any passwords be written down or shared between other employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset securely via the IT administration team
- Where personal data held by the Company is used for marketing purposes, it will be the responsibility of The Data Compliance Team to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked at least every 24 months.

23. Organisational measures

The Company will ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, agents, contractors, or other parties working on behalf of the Company will be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy, and will be provided with a copy of this Policy
- Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly will have access to said personal data held by the Company
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised
- Methods of collecting, holding and processing personal data will be regularly evaluated and reviewed
- The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be evaluated and reviewed regularly
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract
- All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation
- Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party will indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

24. Transferring personal data to a country outside the EEA

The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

The transfer of personal data to a country outside of the EEA will take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data

Powersystems Data Protection Policy

- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority
- The transfer is made with the informed consent of the relevant data subject(s)
- The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject)
- The transfer is necessary for important public interest reasons
- The transfer is necessary for the conduct of legal claims
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent
- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

25. Data breach notification

All personal data breaches must be reported immediately to the Company's Data Compliance Team.

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 Compliance Team 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 (that is, a higher risk than that described under clause 0) to the rights and freedoms of data subjects, the Data Compliance Team must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications will 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 Compliance Team (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.

26. Implementation of policy

This Policy will be deemed effective as of 25/5/2018. No part of this Policy will have retroactive effect and will thus apply only to matters occurring on or after this date.

27. Changes to this policy

The Company reserves the right to change this Policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

Chris Jenkins
Managing Director

POWERSYSTEMS™
HIGH VOLTAGE SPECIALISTS

For more information

T 01454 318000

www.powersystemsuk.com