**Privacy Policy**

**GDPR Policy**

For the balance of this document **Badger Power Electronics Limited** will be shortened to **BPE**

**Contents:**

1. **GDPR Statement of Readiness**
2. **Customer Privacy Notice**

**III. Data Protection Policy**

1. **Data Security**
2. **Staff Privacy Notice**
3. **BPE : GDPR Statement of Readiness**

BPE is committed to data protection and data privacy. With the General Data Protection Regulation (GDPR) becoming enforceable on the 25th May 2018, we have undertaken a GDPR readiness programme to review our entire company, the way we handle data and the way in which we use it to provide our services.

Our GDPR readiness programme is looking at the following areas:

* **Staff training and awareness** – how GDPR, the Data Protection Bill and the ePrivacy Regulation will impact clients, employees and the supply chain
* **Supplier management** – ensuring all appropriate security, organisational controls and governance processes meet the demands of our clients and of BPE as it continues to grow
* **Development** – ensuring we maintain our commitment to best practice and developing systems which meet recognised security standards and making sure we meet our commitment to privacy by design
* **Individuals rights** – refining our approach to handling requests for data, or the handling of data, to meet the new demands of GDPR (including the right of subject access, cease processing requests and erasure of personal data)
* **Data mapping** – a full review of all processes and systems to truly understand the customer experience, the data we hold and the way in which it is used
* **Data retention** – confirming data retention periods meet contractual, legal and organisations requirements.
* **Privacy notices** – reviewing all notices to inform clients and employees of the way we handle their data
* **HR** – preparing our HR department to incorporate important aspects of GDPR for our employees

BPE has a designated Data Protection Officer who oversees our information governance practices and coordinates the company’s efforts to ensure we continue to manage personal data in the way our clients expect.

Here at BPE we are fully committed to the principles of data protection and to safeguarding our data and that of our clients – as such we confirm that all reasonable efforts will be taken to comply with the applicable GDPR rules and regulations.

Any queries should be addressed to Llion Rowlands (Director) at the following email address: Llion@badgerpowerelectronics.com or GDPR@badgerpowerelectronics.com

1. **BPE – Customer Privacy Notice**

BPE holds personal data on its Customers, and their employees, to provide its services. This Customer Data Privacy Notice details the personal data BPE may retain, process and share with third parties relating to your business and its employees. BPE is committed to ensuring that your information is secure, accurate and relevant. To prevent unauthorised access or disclosure, we have implemented suitable physical, electronic, and managerial procedures to safeguard and secure personal data we hold.

This policy will be subject to periodic review and it is recommended that you review this document from time to time to ensure that you are aware of any amendments applicable to the retention, processing and sharing of personal data.

See **www.badgerpowerelectronics.com** for current version.

**Introduction**

We respect the privacy rights of individuals and are committed to handling personal information responsibly and in accordance with applicable law. This Notice sets out the personal information that we collect and process as a data processor, the purposes of the processing and the rights connected with it. BPE are also considered a Data Controller for some personal data, including data we store in relation to the creation and access of user accounts, administration, the methods of processing and service access.

If you are in any doubt regarding the applicable standards, or have any comments or questions about this Notice, please contact Llion Rowlands (Director) at the following email address: Llion@badgerpowerelectronics.com or GDPR@badgerpowerelectronics.com

**Types of personal information we collect**

During your engagement with BPE, or during negotiations with BPE, we may process personal information about you, your employees and other individuals whose personal information has been provided to us. The data we process will depend on the services we provide your company.

The types of personal information we may process include:

* Identification data – such as name, gender, photograph.
* Contact details – such as home and business address, telephone/email addresses.
* Employment details – such as job title/position, office location.
* IT information – information required to provide access to BPE systems and networks such as IP addresses, log files and login information.

Generally, we try not to collect or process any Sensitive Personal Data relating to Customers and their employees, unless authorised by law or where necessary to comply with applicable laws.

**Purposes for processing personal information**

Our legal basis for collecting and using the personal information described above will depend on the personal information concerned and the specific context in which we collect it.

However, we will normally collect personal information from you only where we have your consent to do so, where we need the personal information to perform a contract with you or your employer (i.e. provision of services), or where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms. In some cases, we may also have a legal obligation to collect personal information from you or may otherwise need the personal information to protect your vital interests or those of another person.

We have policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed without authorisation and only accessed or used for specific legal purposes.

If you have questions about or need further information concerning the legal basis on which we collect and use your personal information, please contact BPE.

**Contractual purposes**

We use this personal information when it is necessary for the provision of our services, in line with the purposes agreed upon between our Customer and BPE.

**Legal purposes**

We may use personal information where we consider it necessary for complying with laws and regulations, including collecting and disclosing staff member personal information as required by law or under judicial authorization, or to exercise or defend the legal rights of the companies within BPE.

**Legitimate interest**

We may also collect and use personal information when it is necessary for other legitimate purposes, such as to help us conduct our business more effectively and efficiently – for example, for general IT security management when auditing access of our platforms. We may also process your personal information to investigate violations of law or breaches of our own internal policies.

We may also collect and process personal information where we consider it necessary for BPE’s legitimate interest, including:

* recording all telephone calls made to, or from, our advice centre
* marketing similar services to our Customers

**Who we share personal information with**

We take care to allow access to personal information only to those who require such access to perform their tasks and duties in relation to the provision of our services, and to third parties who have a legitimate purpose for accessing it to support these purposes. Whenever we permit a third party to access personal information, we will implement appropriate measures to ensure the information is used in a manner consistent with this notice and that the security and confidentiality of the information is maintained.

**Transfers to third-party service providers**

In addition, we make certain personal information available to third parties who provide services to us. We do so on a “need to know” basis with appropriate security measures in place – this is done in accordance with applicable data privacy law.

**Transfers to other third parties**

We may also disclose personal information to third parties on other lawful grounds, including:

* To comply with our legal obligations, including where necessary to abide by law, regulation or contract, but not limited to, a subpoena, government audit or search warrant
* In response to lawful requests by public authorities (including for national security or law enforcement purposes)
* As necessary to establish, exercise or defend against potential, threatened or actual litigation
* Where necessary to protect the vital interests of our employees or another person
* In connection with the sale, assignment or other transfer of all or part of our business; or with your expressed consent

**Transfer of personal information abroad**

We may need to transfer personal information to countries other than the ones in which the information was originally collected. When we export your personal information to a different country, we will take steps to ensure that such data exports comply with applicable laws. For example, if we transfer personal information from the European Economic Area to a country outside it, such as the United States, we will implement an appropriate data export solution such as entering into EU standard contractual clauses with the data importer or taking other measures to provide an adequate level of data protection under EU law.

**Data retention periods**

Personal information will be stored in accordance with applicable laws and kept for as long as needed to carry out the purposes described in this Notice or as otherwise required by applicable law. Generally, this means your personal information will be retained until the termination of the relationship with BPE plus a reasonable period of time thereafter.

**Data privacy rights**

The following rights are available under applicable data protection law:

* Access, correct, update or request deletion of personal information
* Object to processing of personal information, ask us to restrict processing of personal information or request portability of personal information.
* If we have collected and process personal information using a person’s consent, then this can be withdrawn at any time. Withdrawing consent will not affect the lawfulness of any processing we conducted prior to withdrawal, nor will it affect processing of personal information conducted in reliance on lawful processing grounds other than consent.
* You have the right to complain to a data protection authority about our collection and use of personal information. For more information, please contact your local data protection authority. In the United Kingdom, the data protection authority is the Information Commissioner’s Office whose website is https://ico.org.uk/
* We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws. You can read more about these rights at: https://ico.org.uk/for-the-public/is-my-information-being-handled-correctly/

**Updates to this Notice**

This Notice may be updated periodically to reflect any necessary changes in our privacy practices. In such cases an updated version of this notice shall be uploaded on www.greendisti.com. Any significant changes to the policy shall be publicised directly. We encourage you to check this notice periodically to be aware of the most recent version.

**Contact details**

Any queries should be addressed to Llion Rowlands (Director) at the following email address: Llion@badgerpowerelectronics.com or GDPR@badgerpowerelectronics.com

**III. BPE : Data Protection Policy**

**Introduction**

This Policy sets out the obligations of BPE (“the Company”) regarding data protection and the rights of employees, customers, suppliers, complainants and enquirers (“data subjects”) in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation (“GDPR”).

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, 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 the Company’s obligations regarding the collection, processing, transfer, storage, and disposal of 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.

The Company is committed to apply all reasonable efforts to comply not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

**Data Protection Principles**

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

2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.2 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.

2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4 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 it is processed, is erased, or rectified without delay.

2.5 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 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 GDPR in order to safeguard the rights and freedoms of the data subject.

2.6 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.

**The Rights of Data Subjects**

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

3.1 The right to be informed (Part 12).

3.2 The right of access (Part 13);

3.3 The right to rectification (Part 14);

3.4 The right to erasure (also known as the ‘right to be forgotten’) (Part 15);

3.5 The right to restrict processing (Part 16);

3.6 The right to object (Part 17); and

**Lawful, Fair, and Transparent Data Processing**

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

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;

4.1.2 The 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 with them;

4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;

4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;

4.1.5 The 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 data controller; or

4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller 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.

**Specified, Explicit, and Legitimate Purposes**

5.1 The Company collects and processes the personal data set out in Part 18 of this Policy. This includes:

5.1.1 Personal data collected directly from data subjects, for example contact details used when a data subject communicates with us.

5.1.2 Personal data obtained from third parties, for example contact details used from a 3rd party data provider for marketing purposes or sales leads provided by our product partners.

5.2 The Company only collects, processes, and holds personal data for the specific purposes set out in Part 18 of this Policy (or for other purposes expressly permitted by the GDPR).

5.3 Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

**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 or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 18, below.

**Accuracy of Data and Keeping Data Up-to-Date**

7.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.

7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

**Data Retention**

8.1 The Company shall 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.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

**Secure Processing**

The Company shall 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. Further details of the technical and organisational measures which shall be taken are provided in Parts 19 to 24 of this Data Protection Policy (GDPR) v2.1 4

**Accountability and Record-Keeping**

10.1 The Director of BPE is responsible for managing the policies and processes and can be contacted at the following email address: Llion@badgerpowerelectronics.com or GDPR@badgerpowerelectronics.com

10.2 The Director shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company’s other data protection-related policies, and with the GDPR and other applicable data protection legislation.

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

10.3.1 The name and details of the Company, its Director, and any applicable third-party data processors;

10.3.2 The purposes for which the Company collects, holds, and processes personal data;

10.3.3 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;

10.3.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

10.3.5 Details of how long personal data will be retained by the Company (please refer to the Company’s Data Retention Policy); and

10.3.6 Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

**Data Protection Impact Assessments**

11.1 The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data.

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

11.2.1 The type(s) of personal data that will be collected, held, and processed;

11.2.2 The purpose(s) for which personal data is to be used;

11.2.3 The Company’s objectives;

11.2.4 How personal data is to be used;

11.2.5 The parties (internal and/or external) who are to be consulted;

11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

11.2.7 Risks posed to data subjects;

11.2.8 Risks posed both within and to the Company; and

11.2.9 Proposed measures to minimise and handle identified risks.

**Keeping Data Subjects Informed**

12.1 The Company shall provide the information set out in Part 12.2 to every data subject:

12.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

12.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

1. a) if the personal data is used to communicate with the data subject, when the first communication is made; or
2. b) if the personal data is to be transferred to another party, before that transfer is made; or

12.2 The following information shall be provided:

12.2.1 Details of the Company including, but not limited to, the identity of its Director;

12.2.2 The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 18 of this Policy) and the legal basis justifying that collection and processing;

12.2.3 Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

12.2.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

12.2.5 Where the personal data is to be transferred to one or more third parties, details of those parties;

12.2.6 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 Part 25 of this Policy for further details);

12.2.7 Details of data retention;

12.2.8 Details of the data subject’s rights under the GDPR;

12.2.9 Details of the data subject’s right to withdraw their consent to the Company’s processing of their personal data at any time;

12.2.10 Details of the data subject’s right to complain to the Information Commissioner’s Office (the “supervisory authority” under the GDPR);

12.2.11 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; and

12.2.12 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

**Data Subject Access**

13.1 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.

13.2 Data subjects wishing to make a SAR may do so in writing to the Company’s Director at the following address: Badger Energy, Unit 15, Enterprise House, Manchester Science Park, M15 6SE

13.3 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.

13.4 All SARs received shall be handled by the Company’s Director.

13.5 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**

14.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

14.2 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.

14.3 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**

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

15.1.1 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;

15.1.2 The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

15.1.3 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 Part 17 of this Policy for further details concerning the right to object);

15.1.4 The personal data has been processed unlawfully;

15.1.5 The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

15.2 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.

15.3 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**

16.1 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.

16.2 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).

**Objections to Personal Data Processing**

17.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling).

17.2 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.

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

**Personal Data Collected, Held, and Processed**

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

18.1 **Names of Individuals** – Will include contact names of customers, suppliers, staff and those in our marketing database (including job titles). The names are stored and used to facilitate contact to those individuals. Names of staff are held in HR files together with other personal data required to process payroll.

18.2 **Postal addresses** – Personal addresses for staff are held in the HR files to facilitate contact for payroll and pension purposes. No personal addresses are held in respect of other contacts.

18.3 **Email addresses** – Collected and held in the course of communicating with contacts and those in our marketing database.

18.4 **Telephone numbers** – Collected and held in the course of communicating with contacts and those in our marketing database.

**Data Security – Transferring Personal Data and Communications**

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

19.1 All emails containing personal data must be encrypted.

19.2 All emails containing personal data must be marked “restricted”;

19.3 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

19.4 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;

19.5 Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent via recorded delivery.

**Data Security – Storage**

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

20.1 All electronic copies of personal data should be stored securely using passwords and data encryption;

20.2 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;

20.3 All personal data stored electronically should be backed up. All backups should be encrypted;

20.4 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of the director responsible for the safekeeping of that information 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; and

20.5 No personal data 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 GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

**Data Security – Disposal**

When 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. For further information on the deletion and disposal of personal data, please refer to the Company’s Data Retention Policy.

**Data Security – Use of Personal Data**

The Company shall ensure that the following measures are taken with respect to the use of personal data:

22.1 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 from the director responsible for the safekeeping of that information;

22.2 No personal data 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 director responsible for the safekeeping of that information;

22.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

22.4 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; and

22.5 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Marketing Manager to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

**Data Security – IT Security**

The Company shall ensure that the following measures are taken with respect to IT and information security:

23.1 Passwords are used to protect personal data, in line with our Information Security Management System.

23.2 Under no circumstances should any passwords be written down or shared between any 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 using the applicable method.

23.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company’s IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so.

**Organisational Measures**

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

24.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company’s responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

24.2 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 shall have access to personal data held by the Company;

24.3 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

24.4 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

24.5 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

24.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

24.7 All personal data held by the Company shall be reviewed periodically, as set out in the Company’s Data Retention Policy;

24.8 The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

24.9 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 GDPR and this Policy by contract;

24.10 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 GDPR; and

24.11 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 shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

**Transferring Personal Data to a Country Outside the EEA**

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

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

25.2.1 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;

25.2.2 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 GDPR); 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;

25.2.3 The transfer is made with the informed consent of the relevant data subject(s);

25.2.4 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);

25.2.5 The transfer is necessary for important public interest reasons;

25.2.6 The transfer is necessary for the conduct of legal claims;

25.2.7 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; or

25.2.8 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.

**Data Breach Notification**

26.1 All personal data breaches must be reported immediately to the Company’s Data Protection Officer.

26.2 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.

26.3 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 Part 26.2) 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.

26.4 Data breach notifications shall include the following information:

26.4.1 The categories and approximate number of data subjects concerned;

26.4.2 The categories and approximate number of personal data records concerned;

26.4.3 The name and contact details of the Director (or other contact point where more information can be obtained);

26.4.4 The likely consequences of the breach;

26.4.5 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.

**Implementation of Policy**

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

1. **BPE Client Data Security Statement**

All data captured by BPE is processed to enable us to provide you with our services.

**Data Security Measures**

All client related data are held either securely in an onsite secure environment or offsite in enterprise-grade highly secure data centres.

Off-site data centres are protected by layers of ‘defence-in-depth’ security that include perimeter fencing, video cameras, security personnel, secure entrances, and real-time communication networks. This multi-layered security model is in use throughout every area of the facility, including each physical server unit.

Technical controls that are in place include, but are not limited, to the following:

The access to servers are restricted to BPE network using dedicated hardware firewalls

The access lists on firewalls are based on specific open ports for applications only. All other ports are blocked

The web servers are highly secure, which have inbuilt features capable of protecting various threats

Servers and PCs are protected and regularly scanned with best available updated antivirus / spyware/ malware which are updated in line with our patching policies and processes

Servers and PCs have inbuilt features e.g. dynamic rules-based policies to protect shared folders and files and hard drive encryption to enhance data security and management

Security auditing is enabled as a risk assessment feature, which helps identify attacks (successful or not) that pose a threat to our network, or attacks against resources

Data held in is encrypted at rest and in transit; this includes files stored on our servers and the use of opportunistic TLS, at a minimum, for all email traffic.

**System Access**

Access to data is strictly controlled through our Role Based Access Controls, which are maintained in line with our policies.

**Training and Awareness**

All BPE employees with access to either personal or client data are given appropriate data protection and information security training. This is supported with awareness campaigns to promote best practice and promote good information governance.

**Information Governance and IT Security – Frequently Asked Questions**

**Governance and Standards**

Q: Is a mechanism in place to ensure your employees and contractors receive appropriate information security awareness training upon appointment, and regular updates to organisational policies and procedures, as relevant for their job function?

A: Yes. BPE has Data Protection and Information awareness and eLearning courses for relevant staff; this is supported with additional a variety of communications on data protection and information security. eLearning courses include assessments; poor performance is recorded and followed up on to ensure that staff responsibilities are understood.

Training is incorporated as part of induction process and bespoke training is provided for specific roles and departments.

Q: Are security operating procedures in place governing the use of your ICT systems?

A: BPE has policies, processes and procedures to address the following areas (this is not exhaustive):

* home and mobile working
* data protection
* information security
* acceptable use
* risk management
* incident management
* data breach management
* business continuity and disaster recovery
* asset management
* software development

These polices are made available to all staff and are reviewed either whenever a change is required or, at a minimum, once every 12 months.

Q: Are policies and controls in place to ensure IT systems are protected from malicious and mobile code and are patched against known vulnerabilities in a timely manner?

A: Yes, BPE has policies, processes (including patch automation) to ensure that systems are patched against known vulnerabilities and protect systems from malicious threats.

Q: Do BPE’s policies and procedures cover the control, protection, secure usage and destruction of electronic storage media?

A: Yes

Q: Are policies and controls in place to manage the risks of working in non-secure environments?

A: Yes

Q: Does your company have a senior individual responsible for the security of our information within your custody?

A: Information Governance (including data protection and information security) are the responsibility of the Director. The technical implementation of security is the responsibility of the Heads of IT.

Q: Are the security roles and responsibilities of your employees clearly defined and documented in accordance with your organisations information security policy?

A: Yes, all responsibilities are defined and documented across all policies within the Information Governance Framework, including Information Security, Data Protection and the IT Policy.

Q: Is a corporate approach to risk management in place which enables the escalation of project risks to programme and/or organisational level risk registers?

A: The running of risk management activities is conducted by the IT Management Team with all corporate risks incorporated into BPE’s Corporate Risk Register. The Board has full oversight of risks and sufficient levels of escalation routes exist to effectively manage any risks which are above/outside of the organisation’s risk appetite.

**Business Continuity / Disaster Recovery and Backups**

Q: Do you have a BCP (Business Continuity Pan) and DRP (Disaster Recovery Plan) in place?

A: Yes – BPE continually reviews these plans when updating services, processes to ensure that all aspects of our services are included within its scope. Our data is backed up both on premises and remotely.

Q: Is data backup encrypted and to what standard?

A: Backup data is encrypted.

**Data Management**

Q: Is there a process to ensure that media is erased securely at disposal?

A: All physical hardware containing personal data is securely disposed of using approved WEEE vendors who are assessed against BPE’s security standards.

Q: Has an owner been assigned to all information assets which require protection?

A: Yes

**Security Assessment and Incident Management**

Q: Are there regular vulnerability scans performed?

A: Vulnerability scans are conducted regularly against all key systems, to ensure that BPE continues to protect the data it holds. This includes, but is not limited to, the following:

* Port Scanning
* Services Probing
* Exploit Research
* Application Layer Testing
* Password Strength Testing
* Manual Vulnerability Testing and Verification
* Manual Configuration Weakness Testing and Verification
* Database Security Controls Testing

Any risks or vulnerabilities identified are immediately rectified by appropriate remedial actions.

Q: Are security assessments undertaken at regular intervals?

A: Both Internal and external assessments are regularly conducted as part of our information security and data protection programmes to monitor the effectiveness of our controls. Areas covered include, but are not limited to, the following:

* Perimeter Security
* Access Control
* Secure areas and/or cabinets for the storage of sensitive assets.

Q: Is there a security incident procedure?

A: Our incident management policy and process contain additional provisions for data breaches and security incidents. This includes the identification of a breach/incident, established scope, notification to third parties/data subjects and all investigative efforts and remedial actions.

**Software Development and Security**

Q: Has the application been developed in compliance with any structured frameworks or guidelines?

A: All software development is conducted appropriately and incorporates the “privacy by design” principle to ensure that all aspects of the development are secure and meet legal obligations and client expectations relating to data protection and information security.

Q: Is a process in place to manage change to systems i.e. capacity management and separation of testing environments?

A: All software development is conducted in line with BPE’s Data Protection Policy and Software Development Policy. These policies ensure that all data is processed in line with legal requirements and that test environments are separated from live environments. A Change Control Process is used to monitor and review all proposed changes to systems – any changes impacting personal data are also assessed against the requirements for data protection impact assessments.

Q: Are user passwords hashed / how are they stored?

A: Passwords are hashed and encrypted.

**Access Controls & Administrator Management**

Q: Are access controls in place to ensure information is only available to system users who require access?

A: Yes, BPE follows the principle of Role Based Access Control to ensure that data is only accessible to those who require access as part of their core activities.

Q: For access via the Internet, are the administrators or privileged accesses protected appropriately.

A: A variety of authentication and technologies, including IP restrictions, are utilised to further limit access to data.

**Remote Working and Mobile Device Management**

Q: In relation to the ICT systems used to deliver your service, which of the following is true?

We permit remote working

We allow staff to connect their own devices to our ICT systems

A: Security controls and strict processes are in place to ensure that the risks of remote working are minimised, this includes device encryption, secure VPN traffic and the use of mobile device management software to set organisations controls on remote devices. Only approved devices, which have been supplied by BPE, are permitted to be used on our ICT infrastructure.

**Network Security**

Q: Are network security boundaries defined and enforced to group users, services and information that require different levels of protection?

A: Yes, permissions and access are assigned based on roles and responsibilities.

Q; Are processes and controls in place to ensure that equipment and cabling is protected and maintained to preserve the confidentiality, integrity and availability of our assets?

A: Yes, these assets are protected to meet industry best practice.

**Staff Management**

Q: Are background verification checks carried out on employees and contractors who have access to our assets?

A: All staff have routine verification checks conducted prior to employment, including checks of identification, right to work and verification of previous employment.

Q: Are non-disclosure agreements in place with all staff who have access to our assets?

A: Yes, these are built into the terms of employment and BPE’s company policies.

Q: Is a disciplinary process in place for employees and contractors who have committed a security breach?

A: Yes, any breach of company policies and procedures may be subject to disciplinary action.

Q: Upon termination of employment is there a process in place to ensure assets are returned and rights to assets revoked?

A: Yes, this is part of the standard staff management process.

**Data Processing**

Q: If data is stored outside of the EU what provision do you provide to assure that you comply with the GDPR requirements to protect it?

A: Strict contractual obligations are placed on all third-party data processes; these also include the right for BPE to audit compliance with the terms in question. Appropriate due diligence is conducted on all potential suppliers, including data protection and information security practices and processes.

1. **BPE : Staff Privacy notice**

We process personal data relating to those we employ to work as, or are otherwise engaged to work as, part of our workforce. We do this for employment purposes, to assist in the running of the business and/or to enable individuals to be paid.

The personal data we process may include, but may not be limited to, the following:

* data relating to your identity (including name, data of birth, gender, photographs, passport, National Insurance Number, immigration status, marital status, dependants),
* contact details (business and home address, telephone numbers, email addresses, emergency contact details),
* employment details (position, office location, terms of employment, performance and disciplinary records, sickness and holidays),
* background information (CV, previous experience, qualifications and certifications, criminal records check (for vetting purposes, where permissible and in accordance with applicable law)),
* financial information (bank details, tax information, salary, benefits, expenses),
* IT information – information related to your access to our systems (login details, IP addresses, log files, access/times/duration of use, location).

The collection of this information will benefit us by:

* improving the management of workforce data across the business,
* enabling development of a comprehensive picture of the workforce and how it is deployed,
* informing the development of recruitment and retention policies,
* allowing better financial modelling and planning,
* ensuring compliance with our policies and procedures and our legal obligations,
* enabling monitoring of selected protected characteristics.

We will not share information about you with third parties without your consent unless the law allows or requires us to do so.

Under the data protection legislation you have the right to:

* object to processing of personal data that is likely to cause, or is causing, damage or distress,
* prevent processing for the purpose of direct marketing,
* object to decisions being taken by automated means,
* in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed,
* claim compensation for damages caused by a breach of the data protection legislation.

If you would like to find out more about our data retention policy and how we use your personal data, or if you want to see a copy of the information about you that we hold, please contact Llion Rowlands (Director) at the following email address: Llion@badgerpowerelectronics.com.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner’s Office at https://ico.org.uk/concerns/