Pulse Business Energy Limited
DATA PROTECTION & RETENTION POLICY

We, Pulse Business Energy Limited (the "**Company**") collect and use (i.e. process) personal data in the course of our activities. We are obliged to comply with the law, in particular the Data Protection Act and the EU General Data Protection Regulation (GDPR), when acquiring and processing personal data.

The aim of this policy is to guide the Company and its personnel so that they meet their legal and contractual obligations in relation to personal data.

Collection & Processing of personal data

Personal data is information relating to an identifiable individual person.

We only collect and process personal data for lawful reasons. Details are in the GDPR, Article 6. In our case we collect various categories of personal data relating to individuals who are:

- Customers of the Company
- Potential customers with whom we have some contact
- Suppliers and other third parties with whom we have dealings
- Directors, employees and consultants

We collect personal data:

- To comply with our legal obligations, for performance of contracts and for other legitimate reasons
- To deal with enquiries from customers and potential customers
- To keep in touch with customers and others for the purpose of providing news and information and for marketing, by use of our blog, newsletters, emails, text, social media and other communications
- To perform a specific activity for which the individual has given us consent.

In the case of customers who buy our products and services and third parties with whom we have contractual arrangements, we need to keep records of sales etc. for tax purposes and for dealing with complaints, queries and after-sales service.

In the case of directors and employees we have statutory obligations.

When providing news and information as well as marketing to customers and other third parties, we need the written consent of the individuals.

All customers and others who give consent are free to withdraw that consent at any time and every email or other communication must give the recipient the right to withdraw consent by clicking on an 'unsubscribe' button.

In any special case, we will obtain consent in writing (preferably by email) before proceeding further.

Data that we collect

The personal data we collect should be adequate, relevant and limited to what is necessary for our purposes. This means we only collect from:

- customers and potential customers:
  Name and address (email and/or physical address)
  Phone number

- suppliers, and third parties who provide us with goods and services:
  name, address, bank details plus copies of contracts entered into by them with us and relevant correspondence with them.

- directors and employees
  name, address, contract details, date of birth and related material as well as any appraisals and/or correspondence with them and related documents – e.g. references from a third party.

We should take appropriate steps to ensure that all personal data is accurate, accessible (subject to password and authority level controls), complete and compliant with our legal duties.

As a company we will avoid collecting sensitive data except when considered appropriate or necessary by the board of directors.

Security of Data

Any personal data relating to customers, suppliers and other third parties stored on our website is on a secure server in the UK.

Some personal data is also held on our premise server and on our email system and accessed by authorised users. The information perimeter security for this site is managed by a High Availability WatchGuard Firewall which is running the full total security license.

Personal data of employees and of third parties with contractual arrangements with the Company and related correspondence is held on network attached storage at our office. Again, this is protected by the WatchGuard firewall.

All end points are password protected with acceptable levels of anti-malware controls. Reviews and updates of our security are routinely carried out.

Paper records are confined primarily to signed contracts with suppliers and consultants and other third parties. These are kept secure in our office.

As far as possible, personal data should be stored electronically and not in hard copy paper form.

The Company operates a ‘clean desk policy’ and no personal data should be left on desks or accessible on unattended pcs or laptops.

Third Party Processors

Some personal data we obtain is processed or held by third parties – in particular:

- Data that is made available to third party service providers who comprise:
  - IT Systems and Services
  - Legal Services
  - Human Resources
  - Direct Marketing Services
  - Service Support Providers

We undertake due diligence to check that these organisations are competent to deal with personal data and comply with the data protection regulations.

We need agreements with all data processors. These need to be checked for compliance with the law and for acceptability for our organisation before being signed. This will be dealt with at directors’ level.

Retention of Data

We only keep and process data that is necessary for legal and contractual reasons for as long as necessary. Generally, this means:

- In the case of customers, for 6 full tax years from the date of purchase, and thereafter until the individual withdraws consent to receiving information from us
- Where the data relates to a contract we have with the individual, for the duration of the contract plus 6 years limitation period,
- Where individuals have agreed to receive newsletters etc., until they unsubscribe or withdraw their consent
- Feedback forms will normally be destroyed once the data has been collated and anonymised
- Other personal data not specified in this section will be destroyed as soon as it is no longer of relevance to our activities.

A review of this policy and our Erasure and Retention Policy and of personal data will be conducted no less often than yearly and data that is no longer relevant will be destroyed.

Anonymised Data

We may retain data indefinitely in a form that does not include the identity of any individuals – e.g. records of sales of different products, or geographical location of customers - once it has been anonymised or pseudonymised.

Destruction & Disposal of Data

Personal data stored in digital or electronic form will be removed when it is no longer required in a manner that makes it irrecoverable, as far as reasonably practicable.

Personal data in hard copy form that is no longer required will be destroyed by shredding at a suitable organisation.

Rights of Individuals and Procedures for dealing with them
Information to be provided to the individual

When obtaining personal data, it is necessary for us to provide:

- Our name and contact details
- The reasons for processing and the legal basis for it
- Who will be receiving the data (if relevant)
- How long we will keep the data
- Information on the individual's right to access, rectify or require deletion of the information we hold and
- The right to lodge a complaint with the ICO
- Contact details of the data protection officer (if relevant).

We do this online via our Privacy Notice and by asking the individual to consent to our processing their data.

In the case of dealings with third party individuals, the same or similar and relevant information should be provided, and a consent form signed if we are to maintain contact with them.

Also, when we do not receive personal data from the individual concerned but from another source, we should give this information to the individual whose data we receive. But we must not provide them with information if that would be in breach of a confidentiality obligation.

Our obligations to provide/rectify/erase information when requested:

If an individual requests information on what personal data we hold on them, we should provide that information within 30 days of the request. This is known as a 'subject access request'. We will usually require the request in writing and we should take steps to verify that the request is coming from the person he/she claims to be.

If requested by an individual to erase their personal data, we should comply with that request without undue delay. However, if we are required for legal reasons to retain the information (e.g. for tax reasons or because litigation is threatened or in progress), we should inform the individual what data we consider it is necessary to retain for legitimate reasons and only erase it when we consider it is safe to do so.

If consent for retaining personal data is withheld, we should erase the data, subject to the legal points in the previous paragraph. No fee will be charged to an individual for providing/rectifying or erasing personal data. However, if anyone makes repeated requests for personal data we may require a £10 fee before providing it.

A subject access request form can be found on our website.

Data Breaches

Any breach of security is a serious matter and any data breach may need to be reported to the police and the ICO.

If a data breach is detected, the Data Protection Officer should immediately be informed. The Board of Directors will be consulted as soon as possible, and will monitor all actions to be taken by way of reporting the breach to the police and/or Information Commissioner and overcoming the problems that arise.

Training & Review

All personnel having access to personal data will be given a training session on the GDPR and our Data Protection arrangements.

This Policy will be subject to regular review, not less frequently than once a year. That review will include all aspects of the policy and how it is working in practice.