General Data Protection Regulation (GDPR)

Policy & Procedures

Version History and Document Approval

Version History:

Version	Date	Author	Reason
1.0	Mar 2018	SRB – Ignition Development	Initial Procedure to comply with GDPR
1.1	Apr 2018	SRB – Ignition Development	Document Updated & Proposed for Review

Document Approval:

Status	Name	Date	Signed
Reviewed:	Theresa Clewes	1st May 2018	Theresa Clews
Approved:	Redmond Cosgrove	1st May 2018	
Reviewed:	Redmond Cosgrove	30th Dec 2022	

Table of Contents

Policy Statement

Central Power takes the issue of compliance with GDPR very seriously and is committed to ensuring all activities carried out by the company and its employees adhere to the principles set out in the regulation. All members of staff will receive full training in respect of the regulation to ensure they are made aware of their obligations and responsibilities when handling personal data. The Directors fully support this policy and appropriate disciplinary action for non-compliance.

Background

The Act

The current Data Protection Act which came into force in 1984, and was later amended in 1998 is to be replaced by the GDPR on the 25th May 2018 in the UK. The main purpose of the regulation is to protect the personal data of Natural Persons residing within the EU, and ensure that it is handled fairly and properly. It also provides individuals with the right to access personal data that is held in both computer and paper-based records.

This is done through setting out 6 Principles that must be adhered to when dealing with personal data; these are that Personal Data must be:

- fairly and lawfully processed;
- collected and processed for the specified purposes;
- accurate and, where necessary, kept up to date;
- not kept for longer than is necessary;
- limited to what is necessary;
- kept secure

It was in 1998, that an amendment to the original Data Protection Act led to the establishment of the Information Commissioners Office, which was given the responsibility of enforcing the Data Protection Act and now has the responsibility of enforcing the GDPR. It gained extensive legal powers allowing it to investigate and prosecute any individual, employee or organisation that it found to be in breach of the regulation, with many facing significant fines, a criminal record and imprisonment.

Use of Personal Data

Central Power may transfer personal data to other companies or to third parties acting on our behalf, for administrative purposes, processing or for the operation and maintenance of your employment with us. If the companies to whom we transfer personal data are not in the European Economic Area, we will ensure that those companies are bound by obligations to hold data securely and use it only for the purposes specified in the agreement with Central Power. Central Power may disclose personal details and/or transfer data to third parties to whom we propose to assign our rights under this agreement.

Associated Legislation

The Information Commissioners Office does cover other areas of legislation including:

- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Privacy and Electronic Communications Regulations 2003 as amended (PECR)

The only direct marketing carried out by Central Power is of a business to business nature. However, in the future direct marketing maybe conducted by other electronic means such as email, SMS and social media. Any direct marketing via electronic means conducted will comply with GDPR, PECR and any legislation that amends or replaces PECR.

Definitions

Data

Data refers to any information that can be held as a record. For Central Power this would include all information that is held in our own records, whether it be electronic or as part of the paper filing system. This would cover information relating to Suppliers, Contractors and Business Customers.

Personal Data

Personal Data refers to any information relating to a natural person, who can be identified from that information. This also includes any expression of opinion and indications of intentions in relation to the individual by Central Power or any other person. This therefore would cover all information regarding Employees of Central Power and Sole Traders but not information specific to Business Customers.

Sensitive Data

Sensitive Data refers to personal data consisting of information such as:-

1. the racial or ethnic origin of the data subject;
2. their political opinions;
3. their religious beliefs or other beliefs of a similar nature;
4. whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
5. their physical or mental health or condition;
6. their sexual life;
7. the commission or alleged commission by them of any offence; or
8. any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Processing

Processing refers to how the data is used. This would include, the obtaining of information at the initial application stage for new employees, recording it manually and onto the system for the duration of employment and deleting the information after the retention period has expired.

Natural Person

Natural Person refers to an individual residing in the EI who is the subject of personal data. This would cover all employees and sole traders who are individual people but not companies or businesses of any form.

Data Protection Officer

Data Protection Officer refers to the person or organisation that decides how any personal data is processed or used. For Central Power this is Theresa Clewes .

Data Processor

Data Processor refers to a person or organisation that processes or uses personal data on behalf of the data controller. This would for example be a HR services provider or a Payroll provider, who would be using information on behalf of Central Power **for a specific purpose**.

Recipient

Recipient refers to any person or organisation to whom data is disclosed from the data controller. This would for example be a Government body or Police Officer who have received information from Central Power.

Third Party

Third party refers to any person other than the data subject, the data controller, or any data processor or other person authorised to process data for the data controller or processor.

Security of Personal Data

Clear Desk Policy

Central Power operates a Clear Desk Policy with regards to all GDPR relevant data to ensure all personal information is stored securely when not in use by employees. This applies to all personal information that is in hard copy, so unless the documentation is in use, it must be locked away in the filing storage units provided. If you do not have access to secure filing storage units, please contact the Data Protection Officer who will arrange access.

External Windows

Due to the location of the Central Power office space, being close to a residential area of Birmingham with lots of passers by and buildings within close proximity of the ground floor a significant risk of a data protection breach is posed by the high volume of non-employees passing the building on a daily basis. Despite the main office where data is stored being located on the first floor of the building which prevents the office from being viewed externally, it is not 100% effective, especially at night. As such it is essential that all employees ensure no personal information can be viewed through any external windows, whether it is in hard copy or on computer screen. If you believe that your computer screen is in view of an external window, please re-position your workstation correctly.

Shredding

When disposing of paperwork that contains personal information it is essential that it is disposed of securely to ensure that there is not a security breach once the documentation has left the premises. To prevent such a breach occurring Central Power has invested in a confidential waste facility that will shred all paperwork securely. Therefore all paperwork regardless of size or quality that contains any amount of personal information (e.g. Employee name or bank details or address), must be disposed of using the confidential waste bin located in the main office of the building. If you have any queries regarding the location of a confidential waste bin, please contact the data protection officer. If you have any queries regarding what should and should not be disposed of confidentially, please contact the Data Protection Officer who can offer further advice.

Computers & Passwords

All Central Power systems and files are password protected for each individual user that has access to them, to allow that employee to be identified accurately. It is therefore important that all passwords used by an individual employee are not shared with other employees or family & friends as this may lead to a data protection breach. It is also necessary that when you have been using any computer to access Central Power systems and files that you either log off or lock the computer before you move away from your workstation regardless of the distance you are moving, however short.

Visitors

All visitors can enter through the warehouse or main entrance of Unit 1. If they enter via the warehouse they should be directed to the reception area in the main entrance. They must then be signed in and out of the premises from the front desk. Visitors that are allowed access will be escorted and accompanied at all times by an employee.

Data Retention

As specified in the GDPR principles, Central Power will not keep data for longer than necessary. All personal data will be held for the minimum time necessary whilst ensuring compliance with its legal obligations. Whilst it is being held all personal data will be held securely either electronically or on-site in a secure storage facility. When the necessary period has expired, all personal information will be disposed of securely.

Where a employee requests that their data is removed, and we can do so (i.e. employee record is older than the Retention Periods required by law), we will destroy all manual records confidentially and archive all electronic records.

Building Access

All staff are issued with the Access Control code for the main office where personal data is stored. All staff are responsible for the security of this code and as such, must ensure that it is not disclosed outside of the organisation. If you suspect a non-Central Power employee has access to the control code, please inform the Data Protection Officer who will arrange for the access code to be updated.

Communication

When communicating with employees via telephone, it is important that the only information disclosed is the personal information relating specifically to them. It is essential that you have performed sufficient identity checks with the individual you are speaking to, before referring to any personal information. This does apply to both incoming and outgoing calls.

The identity checks involve the individual confirming their identity – such as: name, address, employee number, payroll number, DOB etc.

Requests for the Disclosure of Personal Data

Subject Access Requests

Any individual whose personal data is held by Central Power in its role as a Data Controller, has the right to access the data, to be told for what purpose it is being held and to whom it may be disclosed. To access their personal data, an individual is required to make a Subject Access Request to the Data Protection Officer. Upon receiving this request Central Power are required to respond within 30 days; otherwise we will be in breach of the regulation.

When a Subject Access Request is received it is the responsibility of the Data Protection Officer to respond, therefore all requests must be referred immediately.

Central Power takes every measure necessary to ensure the accuracy of its data, if however, the individual receiving the Subject Access Request believes any data to be inaccurate, we will make every effort to correct the issue straight away.

Law Enforcement Agencies

There are a number of exceptions contained within the GDPR that recognise the need for the disclosure of personal data when it is in the public interest, which otherwise may be in breach of the Act.

An example of this would be for the purposes of preventing crime and taxation fraud, which can be used by Law Enforcement Agencies to aid them in their investigations. These agencies include the Police, NCA, HM Revenue & Customs and the Department of Work & Pensions.

However, there are strict requirements on what personal data can be disclosed by the Data Protection Officer, to the third party requesting the information to ensure that only relevant information is shared.

When Law Enforcement Agencies contact Central Power to request personal information, it will most likely be via telephone or email. In either circumstance it is essential that no information is communicated, due to the strict criteria governing personal data disclosure. It is the responsibility of the Data Protection Officer; therefore, all requests must be referred to this person immediately.

Information Commissioners Office Notification

Notification is the process by which a data controller informs the Information Commissioner of certain details about their processing of personal information. These details are used by the Information Commissioner to make an entry describing the processing in a register that is available to the public for inspection.

The principal purpose of having notification and the public register is transparency and openness. It is a basic principle of data protection that the public should know (or should be able to find out) who is carrying out the processing of personal information, as well as other details about the processing (such as the reason it is being carried out).

Central Power as a data controller has a legal obligation to notify the Information Commissioners Office that it is a data controller and provide a general description of the purposes for which it processes that data. Central Power has informed the Information Commissioners Office that it processes data for the following purposes:

- Staff Administration
- Accounts & Records
- Crime Prevention and Prosecution of Offenders

The Information Commissioners Office will be made aware of any change of information within 28 days.

Staff Awareness & Training

The training of all staff will take place on a yearly basis and will be delivered electronically using the online training system Peritus. The training material will include a presentation featuring sufficient information to ensure that staff are aware of what they need to do to comply with the GDPR. This will be followed by a multiple-choice test which will be used to assess employee's understanding of the regulation and highlight any subsequent training needs.

Complaints

All complaints and potential breaches relating to the GDPR must be referred to the Data Protection Officer as soon as possible. They will be responsible for conducting investigations into the particular incident, reporting their findings to Central Power's Directors and if deemed necessary, authorities where appropriate.

Expectations of Staff

In the course of their daily duties, Central Power expects its staff to remain compliant with GDPR at all times and must abide by all guidance contained within this policy. This will include the following practices:

- To collect only the personal information that is required by Central Power.
- To update records promptly – for example, changes of address.
- To delete any personal information that Central Power no longer requires.
- That you will be committing an offence if you release customer/employee records to third parties without consent from the Data Protection Officer or the Directors of the business.

Designated Data Controller

The Data Protection Officer is responsible for ensuring compliance with GDPR and the implementation of this policy. If any aspects of this policy or the GDPR remain unclear, please refer all queries in the first instance to the Data Protection Officer and in their absence the Directors of Central Power.

Theresa Clewes Office Manager Tel: 0121 358 1142 Email: Theresa@centralpower.co.uk	**Redmond Cosgrove** Managing Director Tel: 0121 358 1142 Email: Redmond.cosgrove@centralpower.co.uk