Data Protection Policy

Purpose
The purpose of the Data Protection Policy is to ensure FlexEnable and its team members, contractors and any associated third-party providers are aware of the responsibilities associated with and, as such, can fully comply with The General Data Protection Regulations (GDPR), effective on 25th May 2018.

Responsibility for Data Protection
All team members, contractors and associated third-parties are responsible for Data Protection. FlexEnable will ensure information on the responsibilities is freely available and full training is provided.

As a small business, FlexEnable does not require a Data Protection Officer. Should any team member have a concern in relation to FlexEnable compliance with the GDPR they should raise this with the HR Director.

Definitions

Business Purpose	The purpose for which personal data may be used by us: HR, recruitment, administrative, financial, regulatory, payroll, travel visas and business development purposes Business purposes can include the following: ➢ Compliance with our legal, regulatory and corporate governance obligations and good practice ➢ Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests ➢ Ensuring business policies are adhered to (such as policies covering email and internet use) ➢ Investigating complaints ➢ Conducting occupational health assessments ➢ Checking references, ensuring safe working practices, monitoring and managing team access to systems and facilities and team absences, administration and assessments ➢ Monitoring team conduct, disciplinary and grievance matters ➢ Providing employment benefits, for example the company pension scheme, for employees and any family members as appropriate ➢ Obtaining travel and business sponsorship visas for employees and business visitors
Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other team members, clients, suppliers and marketing / sales contacts. Personal data we gather may include: individual's contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title and CV.
Sensitive personal data	GDPR defines sensitive personal data as genetic and biometric data as well as data regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), health, sex life, sexual orientation and criminal offences or related proceedings. Sensitive personal data will be strictly controlled in accordance with this policy. In most cases the processing of such data will require explicit consent to do so unless exceptional circumstances apply or it is a legal requirement, for example, to comply with legal obligations to ensure health and safety at work.

Scope and Monitoring

This policy applies to all team members, contractors and third-party providers working with FlexEnable. As an individual you must be familiar with this policy and comply with its terms. Adherence to this policy will be regularly monitored to ensure compliance. This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new modified policy will be circulated to the team before being adopted.

Data Protection Principles

FlexEnable will adhere to the following principles in relation to Data Protection. All data will be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
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.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
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 are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for Health and Safety Executive requirements, 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 individuals; and
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.

Processing Data

FlexEnable will process data in accordance with the above principles at all times. Certain departments / functions require the collation, analysis, storage and processing of data. This can be for:

1. Compliance with a legal obligation (such as HMRC and HSE)
2. Performance of a contract
3. Purpose of the legitimate interests of the employer or a third party.

Processing Sensitive Personal Data

FlexEnable will ensure the processing of any sensitive personal data is restricted to what is required for one or more of the three reasons for processing data as outlined above. Any queries on the correct processing of sensitive personal data should be addressed to the HR Director.

Retention

Area	Detail	Retention Period	Security considerations
Occupational Health	Health surveillance reports	40 years	Stored separately and securely
	H&S training records	6 years + 1 (post leaving)	
	Medical reports		
	Occupational health records		
Employment applications (unsuccessful)	Curriculum Vitae	6 months	Stored separately and securely
	Application forms		

HR records	Employment details	6 years (post leaving)	Stored securely
HMRC income tax / NI	Records	6 years + 1 (post leaving)	Stored securely
	Correspondence with HMRC		
Accident Book		3 years	Stored securely
Employee wage / salary		6 years + 1 (post leaving)	Stored securely
Pension	Individual pension information	12 years	Stored securely
	Pension scheme		
Shareholder information	Contact details	permanently	Stored securely
	Share information		
Senior Management Team	Officers of the company	Permanently	Stored securely
Customer information	Contact details	Permanently	Stored securely
Inventor information	IP database	20 years	Stored securely
Business visitors	Visa applications (copy of passport)	3 years	Stored securely

Data will be held securely and separately as appropriate in line with the above retention periods. After which time it will be securely destroyed.

Individual rights

Under the General Data Protection Regulations (GDPR) individuals have the following rights:

- Information Right – the right to receive the information contained in this policy and our data collection forms about the way we process personal data.
- Personal Data Access Right – the right to know that we are processing personal data and, in most circumstances, to have a copy of the personal data that we hold. An individual can also ask for certain other details such as what purpose we process data for and how long we hold it.
- Personal Data Correction Right – An individual has the right to request that we correct inaccurate data or complete incomplete data that we hold.
- Personal Data Erasure Right – Known as the Right to be forgotten. In certain circumstances an individual may request that we erase personal data held by us.
- Personal Data Restriction Right – An individual has the right to restrict the way we process personal data in certain circumstances, for example if: an individual contests the accuracy of the data, if our processing is unlawful, to pursue legal claims, where we are relying on legitimate interests to process data.
- Data Processing Objection Right – An individual has the right to object to us processing data for (i) direct marketing purposes (ii) scientific or historical research or statistical purposes and (iii) purposes of profiling related to direct marketing or based on our legitimate interests or on the performance of a task in the public interest
- Data Portability Right – An individual has the right to receive a copy of certain personal data or to have it transferred to another organisation in some circumstances

Sharing Data with a third party

FlexEnable will never share information with third parties for their own purposes, unless this is explained at the time the data is collected, express permission is given, or FlexEnable is legally required to do so. For example, FlexEnable is legally required to provide data to HMRC in relation to earnings for tax and National Insurance purposes.

FlexEnable also use suppliers known as 'data processors' to process data, for example, to manage the workplace pension scheme and obtain business and travel visas. When enlisting the services of such suppliers the company will ensure that they are under a contractual obligation to only use individual information in accordance with

instructions and for no other purposes.

Subject Access Requests
Individuals have the right to request copies of personal information that is held by FlexEnable. This is known as a Subject Access Request. FlexEnable will ensure any Subject Access Request is forwarded to the HR Team and is responded to within one month. FlexEnable may need to conduct proof of identity checks to ensure that the request can be complied with. All Subject Access Requests will need to be submitted in writing via email to privacy@flexenable.com or letter providing a postal address to which the information is to be sent. Should the copies contain supplementary information not relevant to the individual who has submitted the Subject Access Request this information will be deleted / blacked out as appropriate. If this is not possible, only data relevant to the individual will be released.

Reporting a breach in data protection
All team members, contractors and third-parties are responsible for data protection which includes a duty to report any potential breach. Should any individual be concerned that there has been a breach they should report it to the HR Director. The report should include as much information as possible to enable a full investigation to take place. It is the responsibility of the HR Director to decide when the potential breach should be reported to the ICO.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

When a personal data breach has occurred, the HR Director will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is decided there is no need to report the breach a full report will be created as record of the incident.

Training
All team members, contractors and third-parties will be required to undergo training on data protection obligations under GDPR. Any individual who will be handling personal data and / or sensitive personal data will undergo an additional level of training to include detailed understanding of the internal processes in place to support compliance with GDPR. Any individual may request a refresher of the training and should make this request to the HR Team.

Privacy Notice
Being transparent and providing accessible information to individuals about how we use their personal data is important. FlexEnable has Privacy Notices on its website and on team noticeboards. In addition, there is a Data Control Log [Appendix A] which is owned and updated by the HR Director.

The Data Control Log contains information on what data is held, where it is stored, how it is used, who is responsible and any retention timeframes that may be relevant. This Data Control Log will be audited on a regular basis to manage and mitigate any risks associated with data protection. It is held on SharePoint in People/Privacy.

Consent
Data that is collected is subject to active consent by the data subject. This consent can be revoked at any time unless the data that has been collected is required in order for FlexEnable to exercise a legal obligation.

Criminal Record Checks
Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability
Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may request that their data is transferred directly to another system. This will not incur an administration fee.

Right to be forgotten
A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies, for example the data must be held in order to comply with a legal obligation or in relation to the contract of employment.

Privacy by design and default
Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The HR Director will be responsible for conducting Privacy Impact Assessments and ensuring that all projects that involve personal / sensitive data commence with a privacy plan, for example, introducing a new customer relationship management system or a new payroll management system.

International data transfers
With the exception of the agreed contract in place with PTL Group it is not anticipated that FlexEnable will undertake an international data transfer. Should a further requirement arise, HR Director will be involved in any discussion where data is to be transferred to a country out of the EEA, for example, the provision of personal data to obtain a visa for international travel. Prior to transfer, specific consent must be obtained from the data subject.

For reference data is protected in the EU / EEA under GDPR and in the USA under The Privacy Shield. Further information is available on www.ico.org.uk. for countries not listed above.

Consequences of failing to comply with this policy
FlexEnable takes compliance with this policy very seriously. Failure to comply puts individuals and the company at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary actions under our Disciplinary and Grievance Policy which may result in dismissal.

Individual Consent

Name	
Job Title	
Date	

I hereby confirm that I have read and fully understand the terms of the FlexEnable Data Protection Policy. I agree to comply with the policy at all times and confirm that I understand how to raise concerns about any potential breach of this policy. I understand I have the right to receive regular training and updates on data protection.

Signed	

[COPY TO BE HELD ON PERSONAL FILE, VISA FILE OR CONTRACT FOR SERVICES FILE]