P4 S1 DATA PROTECTION POLICY 2019

Section 1 - DATA PROTECTION POLICY

PURPOSE

This policy establishes an effective, accountable and transparent framework for ensuring compliance with the requirements of the GDPR.

SCOPE

This policy applies to all Forus Training employees and all third parties responsible for the processing of personal data on behalf of Forus Training.

POLICY STATEMENT

Forus Training is committed to conducting its business in accordance with all applicable data protection laws and regulations.

This policy sets out the expected behaviours of Forus Training employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to a Forus Training contact (i.e. the data subject).

Forus Training, as a Data Controller, is responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose Forus Training to complaints, regulatory action, fines and/or reputational damage.

Forus Training's leadership is fully committed to ensuring continued and effective implementation of this policy, and expects all Forus Training employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

Data Protection Impact Assessments (DPIA) are used to identify and mitigate against any data protection related risks arising from new project, service, product, or process which may affect the organisation (Data Controller) or the individuals (Data Subjects).

Data Retention - The need to retain personal data varies widely with the type of data. Some personal data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. This Data Retention Policy provides guidelines to ensure that all applicable regulations and Forus Training rules on personal data retention are consistently applied throughout the organisation.

Any staff member who suspects that a breach of security leading to the accidental or unlawful destruction, loss, alteration unauthorised disclosure of, or access to, personal data might have occurred, must immediately notify the **Data Protection Officer** and provide a description of the circumstances. Notification of the incident can be made via email, by telephone, or in person.

The Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Officer will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved. For severe personal

data breaches, Forus Training's Executive Team will initiate and chair an emergency response team to coordinate and manage the personal data breach response.

Forus Training services/entities may transfer personal data to internal or third party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third countries), they must be made in compliance with an approved transfer mechanism. Forus Training services/entities may only transfer personal data where one of the transfer scenarios list below applies:

- The data subject has given Consent to the proposed transfer,
- The transfer is necessary for the performance of a contract with the data subjecT,
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request,
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject,
- The transfer is legally required on important public interest grounds,
- The transfer is necessary for the establishment, exercise or defence of legal claims,
- The transfer is necessary in order to protect the vital interests of the data subject.

DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data.

Data Processor: the entity that processes data on behalf of the Data Controller.

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Data subject: a natural person whose personal data is processed by a controller or processor.

Personal data: any information related to a natural person or 'data subject', which can be used to directly or indirectly identify the person.

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

Regulation: a binding legislative act that must be applied in its entirety across the Union.

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

Governance

Data Protection Officer

To demonstrate our commitment to data protection, and to enhance the effectiveness of our compliance efforts, Forus Training has appointed a Data Protection Officer. The Data Protection Officer operates with independence and is supported by suitability skilled individuals granted all necessary authority. The Data Protection Officer reports to Forus Training's MD. The Data Protection Officer's duties include:

- Informing and advising Forus Training and its employees who carry out processing pursuant to data protection regulations, national law or European Union based data protection provisions;
- Ensuring the alignment of this policy with data protection regulations, national law or European Union based data protection provisions;
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);
- Determining the need for notifications to one or more DPAs as a result of Forus Training's current or intended personal data processing activities;
- Making and keeping current notifications to one or more DPAs as a result of Forus Training's current or intended personal data processing activities;
- The establishment and operation of a system providing prompt and appropriate responses to data subject requests;
- Informing senior managers, officers, and directors of Forus Training of any potential corporate, civil and criminal penalties which may be levied against Forus Training and/or its employees for violation of applicable data protection laws.

Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any third party who:

- provides personal data to Forus Training
- receives personal data from Forus Training
- has access to personal data collected or processed by Forus Training

Data Protection by Design

To ensure that all data protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing. Forus Training must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Officer, for all new and/or

revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the MD for review and approval. Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the Data Protection Officer to assess the impact of any new technology uses on the security of personal data.

Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by all Forus Training services/entities in relation to this policy, the Data Protection Officer will carry out an annual data protection compliance audit for all such services/entities. Each audit will, as a minimum, assess:

- Compliance with policy in relation to the protection of personal data, including:
- The assignment of responsibilities.
  - ✔ Raising awareness.
  - ✔ Training of employees.
- The effectiveness of data protection related operational practices, including:
  - ✔ Data subject rights.
  - ✔ Personal data transfers.
  - ✔ Personal data incident management.
  - ✔ Personal data complaints handling.
  - ✔ The level of understanding of data protection policies and privacy notices.
  - ✔ The currency of data protection policies and privacy notices.
  - ✔ The accuracy of personal data being stored.
  - ✔ The conformity of data processor activities.

The adequacy of procedures for redressing poor compliance and personal data breaches. The Data Protection Officer, in cooperation with key business stakeholders from Forus Training, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies and good practice identified will be reported to, monitored and shared by the Forus Training executive team.

Data Protection Principles

Forus Training has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

No.	Principle
1	**Lawfulness, Fairness and Transparency**. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, Forus Training must tell the data subject what processing will occur (**transparency**), the processing must match the description given to the data subject (**fairness**), and it must be for one of the purposes specified in the applicable data protection regulation (**lawfulness**).

2	**Purpose Limitation.** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means Forus Training must specify exactly what the personal data collected will be used for and limit the processing of that **personal data to only what is necessary** to meet the specified purpose.
3	**Data Minimisation.** Personal data shall be **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed. This means Forus Training must not store any personal data beyond what is strictly required.
4	**Accuracy.** Personal data shall be accurate, and kept up to date. This means Forus Training must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.
5	**Storage Limitation.** Personal data shall be 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. This means Forus Training must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.
6	**Integrity & Confidentiality.** Personal data shall be 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. Forus Training must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.
7	**Accountability.** The Data Controller shall be responsible for, and be able to demonstrate compliance. This means Forus Training must **demonstrate** that the six data protection principles (outlined above) are met for all personal data for which it is responsible
8	Personal data shall not be transferred to any other country outside of the EEA unless that country can ensure an adequate level of protection.

Data Collection

Data Sources

Personal data should be collected only from the data subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the personal data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent serious loss or injury to another person.

If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:

- The data subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation.
- A national law expressly provides for the collection, processing or transfer of the personal data.

Where it has been determined that notification to a data subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the personal data
- At the time of first communication if used for communication with the data subject
- At the time of disclosure if disclosed to another recipient.

Data subject Consent

Forus Training will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, Forus Training is committed to seeking such consent. The Data Protection Officer, in cooperation with other relevant business representatives, shall establish a system for obtaining and documenting data subject consent for the collection, processing, and/or transfer of their personal data.

Data Subject Notification

Forus Training will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide data subjects with information as to the purpose of the processing of their personal data. When the data subject is asked to give consent to the processing of personal data and when any personal data is collected from the data subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The data subject already has the information;
- A legal exemption applies to the requirements for disclosure and/or consent. The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Data Protection Officer. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

External Privacy Notices

Each external website provided by Forus Training will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

Data Use

Data processing

Forus Training uses the personal data of its contacts for the following broad purposes:

- The general running and business administration of Forus Training.
- To provide services to Forus Training's stakeholders.
- The ongoing administration and management of customer services.

We process personal information to enable us to provide education and training to our customers and clients; to promote our services, to maintain our own accounts and records and to support and manage our employees.

We process information relevant to the above reasons/purposes. This may include:

a) personal details

b) business activities of the person whose personal information we are processing

c) financial details

d) education and employment details
e) family details
f) lifestyle and social circumstances
g) training details
h) goods and services

We process personal information about:

a) customers
b) students
c) employees
d) professional advisers and consultants
e) clients
f) trainers
g) suppliers
h) complainants
i) enquirers

The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a contact's expectations that their details will be used by Forus Training to respond to a contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that Forus Training would then provide their details to third parties for marketing purposes.

Forus Training will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, Forus Training will not process personal data unless at least one of the following requirements are met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- 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.
- 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 interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child).

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Data Protection Officer before any such processing may commence.

- In any circumstance where consent has not been gained for the specific processing in question, Forus Training will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected: Any link between the purpose for which the personal data was collected and the reasons for intended further processing.
- The context in which the personal data has been collected, in particular regarding the relationship between data subject and the Data Controller.
- The nature of the personal data, in particular whether special categories of data are being processed, or whether personal data related to criminal convictions and offences are being processed.
- The possible consequences of the intended further processing for the data subject.
- The existence of appropriate safeguards pertaining to further processing, which may include encryption, anonymisation or pseudonymisation.

Special Categories of Data

Forus Training will only process special categories of data (also known as **sensitive data**) where the data subject expressly consents to such processing or where one of the following conditions apply:

- The processing relates to personal data which has already been made public by the data subject.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is specifically authorised or required by law.
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health.

In any situation where special categories of data are to be processed, prior approval must be obtained from the Data Protection Officer, and the basis for the processing clearly recorded with the personal data in question. Where special categories of data are being processed, Forus Training will adopt additional protection measures.

Sensitive data may include:

a) Racial or ethnic origin.

b) Religious beliefs.

c) Physical or mental health.

d) Criminal records.

e) Political opinions.

f) Trade Union membership.

g) Sexual life.

h) Court sentences.

Children's Data

Children under the age of 14 are unable to consent to the processing of personal data for information society services (any service normally provided for payment, by electronic means and at the individual request of a recipient of services). Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

Data Quality

Forus Training will adopt all necessary measures to ensure that the personal data it collects and processes is complete and **accurate** in the first instance, and is updated to reflect the current situation of the data subject. The measures adopted by Forus Training to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.
- Restriction, rather than deletion of personal data, insofar as:
  - ✔ a law prohibits erasure.
  - ✔ erasure would impair legitimate interests of the data subject.
  - ✔ the data subject disputes that their personal data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

Profiling & Automated Decision Making

Forus Training will only engage in profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the data subject or where it is authorised by law. Where a Forus Training service/entity utilises profiling and automated decision-making, this will be disclosed to the relevant data subjects. In such cases the data subject will be given the opportunity to:

- Express their point of view.
- Obtain an explanation for the automated decision.
- Review the logic used by the automated system.
- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision.

Object to the automated decision-making being carried out. Forus Training service/entity must also ensure that all profiling and automated decision-making relating to a data subject is based on accurate data.

1.1.1. Digital Marketing

As a general rule Forus Training will not send promotional or direct marketing material to a Forus Training Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their consent. In the case where a member of staff/representative of Forus Training wishes to carry out a digital marketing campaign without obtaining prior Consent from the data subject must first have it approved by the Data Protection Officer. Where personal data processing is approved for digital marketing purposes, the data subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes. If the data subject puts forward an objection, digital marketing related processing of their personal data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

1.2. Data Retention

To ensure fair processing, personal data will not be retained by Forus Trainingfor longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which Forus Training needs to retain personal data is set out in Forus Training '*Data Retention Policy*'. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

1.3. Data Protection

Forus Training will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary

Data subject Requests

The Data Protection Officer will establish a system to enable and facilitate the exercise of data subject rights related to:

j) Information access.

k) Objection to processing.

l) Data portability.

m) Data rectification.

n) Objection to automated decision-making and profiling.

o) Restriction of processing.

p) Data erasure. If an individual makes a request relating to any of the rights listed above.

Forus Training will consider each such request in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature data subjects are entitled to obtain, based upon a request made in writing/email to: **certification@forustraining.ie**

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights. Detailed guidance for dealing with requests from data subjects can be found in Forus Training's '*Data Subject Access Rights Policy and Procedure*' document.

1.4. Data Sharing

We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons. Where necessary or required we share information with:

a) business associates and other professional advisers

b) current, past or prospective employers

c) processing

d) financial organisations

e) debt collection and tracing agencies

f) persons making an enquiry or complaint

g) central government

h) educators and examining bodies

i) family, associates and representatives of the person whose personal data we are

j) employment and recruitment agencies

k) credit reference agencies

l) suppliers and service providers;

Personal information is traded and shared as a primary business function. For this reason the information processed may include name, contact details, family details, financial details, employment details, and goods and services. This information may be about customers and clients. The information may be traded or shared with business associates and professional advisers, agents, service providers, customers and clients, and traders in personal data.

1.5. Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

a) The prevention or detection of crime.

b) The assessment or collection of a tax or duty.

c) The apprehension or prosecution of offenders.

d) By the order of a court or by any rule of law.

Forus Training processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If any Forus Training receives a request from a court or any regulatory or law enforcement authority for information relating to a Forus Training contact, you must immediately notify the Data Protection Officer who will provide comprehensive guidance and assistance.

1.6. Data Protection Training

All Forus Training employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, Forus Training will provide regular Data Protection training and procedural guidance for their staff.

1.7. Data Transfers

Forus Training may transfer personal data to internal or third party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third countries), they must be made in compliance with an approved transfer mechanism. Forus Training may only transfer personal data where one of the transfer scenarios list below applies:

- The data subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the data subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject

Complaints handling

Data subjects with a complaint about the processing of their personal data should put forward the matter in writing to the Data Protection Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the data subject and the Data Protection Officer, then the data subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Data Protection Officer providing a description of what occurred. Notification of the incident can be made via e-mail or by phone. The Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Officer will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved. For severe personal data breaches, Forus Training Executive Team will initiate and chair an emergency response team to coordinate and manage the personal data breach response.

DATA SECURITY AND PROTECTION
BACKGROUND

Forus Training needs to keep certain information about its employees, clients, prospective clients and other persons to allow it to carry out its business. Information such as this which identifies living individuals is known as 'Personal Data'. The way in which personal data can be used or processed is specified by the Data Protection Act 1998 (the Act). This document is designed to increase your understanding and awareness of the Act, the obligations it places on individuals and organisations and the way it affects your work here at Forus Training.

The Data Protection Act 1998

Introduction

Data Protection is an important issue for both organisations and individuals who store and process personal data held on living individuals and in turn have it stored and processed about them. Technological developments make it easier for organisations like Forus Training to collect, process, store and distribute information. The Act sets rules for processing personal information (i.e. information about living, identifiable individuals) and applies to paper records as well as those held on computers (automated data). The Act works in two ways, it gives individuals certain rights, whilst requiring those who record and use personal information to be open about how it is used and to follow the eight Principles (section 6 below) of 'good information handling' set out in the Act.

What is Covered By The Act?

Personal data is information which identifies a living individual. This data may include:

- personal details (name, address)
- employment details (job title)
- financial details (bank account number, sort code)
- lifestyle indicators (shopping habits, leisure pursuits, holiday habits)

The Act is concerned with how data is processed, however, processing covers virtually every activity connected with the collection, use, alteration, distribution, or destruction of personal data. Where there is personal data, you may therefore assume that the processing of it takes place. ForusTraining uses this personal data for many different purposes, which can include:

- Staff administration (payment of salary, pensions, contact details)
- Advertising, marketing and public relations (new products, updated products, customer and staff opinion surveys)
- Accounts and records (tax, national insurance, payment details).

- Research (competitors, customer requirements)
- Student processing

Who IS Covered By The Act?

It is a condition of employment with Forus Training that employees will abide by the rules and policies made by the firm. Forus Training's data protection policy therefore applies to all employees and any failure to follow the policy could result in disciplinary action.

Sensitive Personal Data

Some personal data is classified under the Act as sensitive. This personal data is covered by much stricter rules about the way it is processed and disclosed. Sensitive Data falls can include:

a) racial or ethnic origin

b) religious beliefs

c) physical or mental health

d) court sentences

e) political opinions

f) trade Union membership

g) criminal records

Within Forus Training there may be a need to collect sensitive personal data about individuals (e.g.HR).

Great care should be taken when handling sensitive personal data. You must have explicit consent from the data subject to process this information.

Data Protection Breaches

What Constitutes A Breach Of the Act?

The following actions, whether taken by an individual or organisation, are examples of breaches of the Act:

- Making unauthorised or unlawful disclosure of personal data without consent
- Using personal data for anything other than the registered purpose
- Inviting others to make unauthorised or unlawful disclosure of personal data
- Using inaccurate personal data or fails to correct data
- Failing to keep personal information confidential and secure

Remember that all employees of Forus Training, including Directors, Senior Managers and other staff can be liable for breaches of the Act.

Reporting a Breach

All Forus Training staff have a duty to ensure that any data protection breach is reported to the DPO. If you are in any doubt as to whether a breach has occurred, please consult with your Line Manager.

Staff must inform their Line Managers of any data protection breach in the first instance. It is the responsibility of each Line Manager to ensure that all breaches raised by their team are appropriately reported. Similarly it is the responsibility of each Line Manager to work with the member of their team involved to resolve any weaknesses or shortcomings that have contributed to the breach (where applicable).

Breaches and incidents must be reported to the DPO as soon as possible after they are identified. Reports should be made in writing, either by email or in hard copy, providing all necessary information to the DPO to understand the issue.

Data Security and Protection Policy – Data Protection Principles

The Act lists the eight Data Protection principles in the following terms:

VERIFICATION OF IDENTITY

Forus Training holds substantial amounts of information collected from various sources. This information ranges from basic name and address records to much more personal information including financial details. We are obliged to exercise care in holding and disclosing all data.

You should always ensure information is only given to a person who is entitled to it.

Prior to providing any personal data to an individual we must undertake checks by collecting basic factual information such as their:

- Full name
- Full address (including postcode)

Wherever possible we should also ask for some information that is more specific to their dealings with Forus Training, such as a piece of factual information that only they could have provided.

These checks allow us to confirm that callers are who they claim to be and that they are entitled to the information they request.

You must obtain the information required to verify the caller's identity without disclosing any personal data held in Forus Training's records.

If you fail to follow proper procedure and disclose personal data to someone who is not entitled to it, you can be individually prosecuted.

- Never volunteer information, or prompt for correct answers.
- Only disclose personal data to which the caller is entitled.
- Never leave confidential information on an answer phone without the customer's express instructions.

Security - Under the Data Protection Act there must be appropriate measures in place to ensure that there is no unlawful or unauthorised processing of personal data or accidental loss, destruction or damage to personal data.

Cloud Services-Forus Training hosts its application and data in industry-leading Cloud Services, whose data centres have been tested for security, availability and business continuity.

User ID and Passwords

Forus Training's staff are given a unique User ID to gain access to the systems they need to do their jobs. The User ID is protected by a password, which you must keep secret. This ensures that everyone is directly accountable for any actions under their User ID. We all need to be aware of who is around when we are working with personal data and should take care that it is not accidentally disclosed to someone who is not entitled to see it.

Clear Desk Policy

Forus Training operates a clear desk policy. The clear desk policy ensures that desks are kept clear of papers that are not being used. To achieve this:

- File documents in a lockable drawer or filing cabinet when your work on them is completed.
- Put documents in locked drawers at the close of business.
- Clear your in-tray regularly.

Spot checks of working areas are carried out on a regular basis to monitor adherence to the clear desk policy, and should items containing personal data be found, they will be removed and stored securely.

Disposal of Data

Careless disposal and distribution of data can put personal data at risk. At ForusTraining we have measures in place to minimise this risk.

Confidential waste bins are provided in several locations around the office. Where documents or print outs which contain personal data need to be disposed the confidential waste bins should always be used.

Email Security

Sending personal data via email is not always a secure method of distribution. Emails can be intercepted and read or amended by people who are not entitled to do so.

Emails should not be used for confidential communications unless the consent of the person to whom the information relates has been obtained, both in relation to the content of the email and the form in which it is transmitted (i.e. encrypted or unencrypted). If you need to send or receive important information via email, check with the IT team about encryption, password protecting documents you attach (sending the password separately or using We Transfer) and virus checking software.

Data On Your Laptop And Email

Where possible, personal data that can identify a person should not be stored/saved on your laptop or email.

Saving Data

Data should be stored in centrally managed locations so when a data request is made a formal procedure is followed.

Data in written format

Where possible, personal data that can identify a person, should not be stored in hard copy. Data should be transferred to an appropriate location (e.g. CRM or a specific drive/folder that's used by your business areas as part of a formal procedure) – documents could be scanned/stored as PDFs or manually typed up.

Offices

The Forus Training offices ensure only authorised individuals have access to the building and the Forus Training office. A policy has been implemented to approve and regulate visitor access to the building (e.g. manned reception, visitors books, passcode or smartcards required).

Fire alarms and water sprinklers are in place to detect and mitigate damage in the unlikely event of a fire. Regular fire drills are also conducted by the premises management team to educate employees about emergency evacuation procedures.

Key Points to Remember About Data Security

- Keep your password secure; do not write it down for others to see.
- If you suspect someone knows your password – change it and report your suspicions.
- Lock your workstation when leaving your desk for any period of time
- Make sure your desk is clear of paperwork and the documents are filed or locked away before leaving your desk.
- Dispose of documents by shredding or placing in the confidential waste bins or bags.

Reporting Issues And Threats

If you have found any issues or flaws impacting the data security or privacy of Forus Training users, please write to certification@forustraining.ie with the relevant information so we can get working on it right away.

Your request will be looked into immediately. We might ask for your guidance in identifying or replicating the issue and understanding any means to resolve the threat right away. Please be clear and specific about any information you give us. We deeply appreciate your help in detecting and fixing flaws in Forus Training, and will acknowledge your contribution to the world once the threat is resolved.

Record Management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised Forus Training's recordkeeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

SECTION 2: DATA PROTECTION IMPACT ASSESSMENT

When is DPIA necessary

DPIA is necessary:

- Before the implementation of new technologies or processes, or before the modification of existing technologies or processes;
- Data processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals;
- Large scale processing of special categories of data or personal data relation to criminal convictions or offences;
- Large scale, systematic monitoring of public areas (CCTV).

Should the Regulator be consulted on completion of the DPIA

If, during the DPIA process, the Data Controller has identified and taken measures to mitigate any risks to personal data, it is not necessary to consult with the Regulator before proceeding with the changes.

If the DPIA suggests that any identified risks cannot be managed and the residual risk remains high, you must consult with the Regulator before moving forward with the project.

Regardless of whether or not consultation with the Regulator is required, your obligations of retaining a record of the DPIA and updating the DPIA in due course remain.

Even if consultation is not required, the DPIA may be reviewed by the Regulator at a later date in the event of an audit or investigation arising from your use of personal data.

PROCEDURE

Steps for conducting DPIA

Describe data flows. Identify how personal information will be collected, stored, used and deleted as part of the new (or modified) system or process. Identify what kinds of data will be used as part of the new (or modified) system or process and who will have access to the data. *Populate Section 1 of the Data Protection Impact Assessment (DPIA) Form.*

Identify data protection and related risks. Identify all risks to Data Subjects or to the organization (Data Controller) that are related to personal data protection. For each risk assign a risk category (High/Medium/Low) and *populate the appropriate columns in Section 2 of the Data Protection Impact Assessment (DPIA) Form.*

Assign risk mitigation measures. For each risk assign risk mitigation measures. Focus on mitigating measures for risks with the High and Medium impact category. *Populate the last column in Section 2 of the Data Protection Impact Assessment (DPIA) Form.*

Further actions. Consider if the Regulator should be consulted for the DPIA. Plan regular DPIA reviews and updates.

SECTION 3: DATA RETENTION

Reasons for data retention

Some personal data must be retained in order to protect the company's interests, comply with regulatory requirements, preserve evidence, and generally conform to good business practices. Personal data may be retained for one or several of the following reasons:

a) Business requirements

b) Possible litigation

c) Security incident investigation

d) Regulatory requirements

e) Accident investigation

f) Intellectual property preservation

Data processed by Quality and Qualifications Ireland (QQI) for the purposes of certification, provider approval and programme validation

Forus Training as data controllers must be clear about the length of time for which personal data will be kept and the reasons why the information is being retained.

In determining appropriate retention periods, regard must be had for any statutory obligations imposed on a data controller.

If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner.

It may also be anonymised to remove any personal data. Anonymisation must be irrevocable; removing names and addresses may not necessarily be sufficient.

In order to comply with this legal requirement, Forus Training has assigned specific responsibility for implementation of GDPR.

Procedures have been introduced for ensuring that files are purged regularly and securely and that personal data is not retained any longer than is necessary.

All records will be periodically reviewed in light of experience and any legal or other relevant indications.

Information on Disposal and Certification - David White

Source **Purpose**	**Publicly accessible**	**Provided by private person themselves**
Marketing - Lead Staging Life-cycle		Interests, Questions asked Learner Requirements – Goals Hopes and Dreams Email address, Contact telephone number(s) Job Title, Home Addre
Initiation of business		ID, PPS, DOB, Gender, Contact Information, Proof of Identification Training Needs Analysis: Job Title, Professional experience, Educati Professional Qualifications Professional experience Programme on which currently enrolled (learner representative) rol Credit / Debit Card details ❶ Bank details in the case of Direct Debits / Refunds
Learning Life-cycle **inc. Access Transfer and Progression**	Aggregate scores / gender breakdown appear on QQI website Infographics	Correspondence Registration Forms ❼ ₡ Name of Programme Award type, Award Name, Award Code, Award Year of programme Date of commencement, Number of Years completed Entry standard to programme Highest qualification Garda vetting form & outcome - Learners ❶ ₡

		Psychological assessments ⍰ Special Education Needs' files, reviews, correspondence ⍰ Individual Education Plans ⍰ Sensitive Learner information - Accident reports ⍰
		Sensitive Learner information - Records of complaints Ω or ❼* ₡
		Sensitive Learner information - Appeal Applications ❼ ₡
		Fee Status - Exempt - Not Exempt
HR Records Life-cycle		ID, PPS, DOB, Contact Information, Proof of Identification correspondence
		Unsuccessful Applications & CVs of candidates called for interview ⓲ Unsuccessful Database of applications ⓲₡ Unsuccessful Selection criteria ⓲₡ Unsuccessful Applications of candidates not shortlisted ⓲₡ Unsuccessful Unsolicited applications for jobs ⓲₡ Unsuccessful Candidates shortlisted but unsuccessful at interview ⓲ Unsuccessful Candidates shortlisted and are successful but do not ac Unsuccessful Interview board marking scheme & board notes ⓲₡ Unsuccessful Panel recommendation by interview board ⓲₡
		Staff personnel files - e.g. applications, qualifications, references, re specification FD+❼₡ Staff personnel files - contract, records of staff training etc. FD+❼₡ Staff personnel files - Application &/CV **FD**+❼₡ Staff personnel files - Qualifications FD+❼₡ Staff personnel files - References FD+❼₡ Staff personnel files - Interview: database of applications (section rel only) FD+❼₡ Staff personnel files - Emergency contact FD+❼₡ Staff personnel files - Selection criteria FD+❼₡ Staff personnel files - Interview board marking scheme & board note Staff personnel files - Panel recommendation by interview board FD Staff personnel files - Recruitment medical FD+❼₡ Staff personnel files - Job specification/ description FD+❼₡ Staff personnel files - Contract/Conditions of employment FD+❼₡ Probation letters/forms FD+❼₡ Staff personnel files - POR applications and correspondence (whethe FD+❼₡

		Staff personnel files - Leave of absence applications FD+❼₡ Staff personnel files - Job share FD+❼₡ Staff personnel files - Career Break FD+❼₡ Staff personnel files - Maternity leave FD+❼₡ Staff personnel files - Paternity leave FD+❷ or FD+❼ ₡ Staff personnel files - Parental leave** ❽ or FD+❷₡ Staff personnel files - Force Majeure leave ❽ or FD+❷₡ Staff personnel files - Carers leave*** ❽ ₡ Staff personnel files - Working Time Act (attendance hours, holidays, Staff personnel files - Allegations/complaints Ω Staff personnel files - Grievance and Disciplinary records***** ❼₡ Staff personnel files - Sickness absence records/certificates ❼₡ or ⍰ Staff personnel files - Pre-employment medical assessment ❼₡ or ⍰ Staff personnel files - Occupational health referral ❼₡ or ⍰ Staff personnel files - Correspondence re retirement on ill-health gro Staff personnel files - Accident/injury at work reports ❿ or FD+❼₡ Staff personnel files - Medical assessments or referrals ❿ or FD+❼₡ Staff personnel files - Sick leave records (sick benefit forms) ❿ or FD
Accounting records		

Classification – Retention Period UNCLEAR **– Should be predetermined Mapping of data classes to retention periods needed to ensure erasing the right data at the right time**

₡ Confidential Shredding

❶Delete immediately

❼ ₡ Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)

♾ Retain indefinitely. Archive following RAP for Period

⓬ ₡ Record of outcome retained for 12 months. School to retain the reference number and date of disclosure on file, which can be checked with An Garda Siochana in the future.

Indefinitely. Administrative log and does not relate to any one employee in particular: the monthly reports are not structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily

accessible. Not a “relevant filing system”.

♾ Retain indefinitely Never destroy

Ω Depends entirely on the nature of the complaint. If it is child-safeguarding, a complaint relating to trainer-handling, or an accident, then retain indefinitely. Never destroy.

FD+❼Retain for duration of employment (Finish Date FD) plus 7 years (6 years in which to take a claim against the company plus 1 year for proceedings to be served on the company)

❼Retain for 7 years

⓲months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.

**Must be kept for 8 years - Parental Leave Act 1998

***Must be kept for 8 years - Carer's Leave Act 2001

****Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school). There is a statutory requirement to retain for 3 years

*****note the relevant HR policy re Disciplinary Procedures in relation to the period of time for which a warning remains “active” on an employee’s record.

⑩Delete 10 years after the account becomes inactive

❼¢ Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual’s duties within the school, in which case, do not destroy.

❿ or FD+❼¢ Retain for 10 years, or the duration of the employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), whichever is the greater (unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual’s duties within the school, in which case, do not destroy).

⑥Delete 6 years after account becomes inactive

On centre closure, records should be transferred as per Records Retention in the event of school closure/amalgamation. A decommissioning exercise should take place with respect to archiving and recording data.

FD+or FD+Retain for 2 years following retirement/resignation or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater).

❼✆ or ⍰ Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy

Retention of encrypted data - If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

Data duplication - When identifying and classifying Forus Training's personal data, it is important to also understand where that data may be stored, particularly for duplicate copies, so that this policy may be applied to all duplicates of the information.

Data destruction - When the retention timeframe expires, Forus Training will actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of Forus Training's senior management team.

The company specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to himself or herself or destroying data in an attempt to cover up a violation of law or company policy is particularly forbidden.

SECTION 4: DATA TRANSFERS

Transfers between Forus Training's services/entities

In order for Forus Training to carry out its operations effectively across its various services/entities, there may be occasions when it is necessary to transfer personal data internally or to allow access to the personal data from an overseas location. Should this occur, Forus Training sending the personal data remains responsible for ensuring protection for that personal data.

Protection of enrolled learners needs to be addressed here

Transfers to Third Parties

Forus Training will only transfer personal data to, or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where third party processing takes place, Forus Training will first identify if, under applicable law, the third party is considered a data controller or a data processor of the personal data being transferred.

Where the third party is deemed to be a data controller, Forus Training will enter into, in cooperation with the Data Protection Officer, an appropriate agreement with the controller to clarify each party's responsibilities in respect to the personal data transferred. Where the third party is deemed to be a data processor, Forus Training will enter into, in cooperation with the Data Protection Officer, an adequate processing agreement with the data processor. The agreement must require the data processor to protect the personal data from further disclosure and to only process personal data in compliance with the Forus Training instructions. In addition, the agreement will require the data processor to implement appropriate technical and organisational measures to protect the personal data as well as procedures for providing notification of personal data breaches.

The Forus Training has a 'Standard Data Processing Agreement' document that should be used as a baseline template. When Forus Training is outsourcing services to a third party (including cloud computing services), they will identify whether the third party will process personal data on its behalf and whether the outsourcing will entail any third country transfers of personal data. In either case, it will make sure to include, in cooperation with the Forus Training Data Protection Officer, adequate provisions in the outsourcing agreement for such processing and third country transfers.

Data Transfers Policy –Responsibilities

Compliance, monitoring and review

The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing data transfers activities at Forus Training rests with the Data Protection Officer.

All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant Forus Training policies and procedures.

Records management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised Forus Training recordkeeping system.
All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

SECTION 5: DATA SUBJECT ACCESS REQUESTS

The GDPR details rights of access to both **manual data and electronic data** for the data subject. This is known as a Data Subject Access Request (DSAR).
Under the GDPR, organisations are required to respond to subject access requests within **one month.** Failure to do so is a breach of the GDPR and could lead to a complaint being made to the Data Protection Regulator.
This policy informs staff of the process for supplying individuals with the right of access to personal data and the right of access to staff information under the General Data Protection Regulation (hereinafter called GDPR).
Specifically:

- All staff need to be aware of their responsibilities to provide information when a data subject access request is received. When a subject access request is received, it should immediately be reported to the Data Protection Officer to log and track each request.
- Requests must be made in writing to head office but a prospect can request the information verbally - If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are.
- The statutory response time is one month.
- Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the GDPR, information relating to the individual must only be disclosed to them or someone with their written consent to receive it.
- No fee can be charged for initial DSAR for all types of records, whether manual or electronic format.

How should DSARs be processed after receiving

When a subject access request is received from a data subject it should immediately be reported to the Data Protection Officer who will log and track each request. If you are asked to provide information, you will need to consider the following before deciding how to respond:

g) Under GDPR Articles 7(3), 12, 13, 15-22 data subjects have the following rights:

h) to be informed;

i) to rectification;

j) to restriction of processing;

k) to data portability;

l) to object to automated decision making.

m) to access their own data;

n) to erasure (Right to be Forgotten);

o) to be notified;

p) to object;

- Requests must be made in writing. All DSARs received by email, mail, fax, social media, etc. must be processed.
- The type of access you must provide and the fee you are allowed to charge may vary depending on how the records are held. It does not have to state ‘subject access request’ or ‘data protection’ to constitute a request under the GDPR.
- If a request has already been complied with and an identical or similar request is received from the same individual a fee can be charged for the second request unless a reasonable interval has elapsed.

- The statutory response time is one month.
- Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the GDPR, information relating to the individual must only be disclosed to them or someone with their written consent to receive it.
- Before processing a request, the requestor's identity must be verified. Examples of suitable documentation include:
    - Valid Passport
    - Valid Driving Licence
    - Valid Identity Card
    - Birth Certificate along with some other proof of address e.g. a named utility bill (no longer than 3 months old)

Fees

No fee can be charged for providing information in response to a data subject access request, unless the request is 'manifestly unfounded or excessive', in particular because it is repetitive.

If Forus Training receives a request that is manifestly unfounded or excessive, it will charge a reasonable fee taking into account the administrative costs of responding to the request. Alternatively, Forus Training will be able to refuse to act on the request.

Subject access requests made by a representative or third party

Anyone with full mental capacity can authorise a representative/third party to help them make a data subject access request. Before disclosing any information, Forus Training must be satisfied that the third party has the authority to make the request on behalf of the requestor and that the appropriate authorisation to act on their behalf is included (see *Data Request Form*).

Complaints

If an individual is dissatisfied with the way Forus Training have dealt with their subject access request, they should be advised to invoke the Forus Training complaints process. If they are still dissatisfied, they can complain to the Data Protection Regulator.

Forms to assert your rights under the Act:

Data Subject Rights Under GDPR

5.1 Right of Access

The Data Subject has the right to obtain/request confirmation from FORUS as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

· The purposes of the processing;

· The categories of personal data concerned;

· Notification of recipients or categories of recipient to whom the personal data have been or will be disclosed; FORUS Data Protection Policy and Privacy Statement V1.0 Page 3 of 6

· Notification of period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

· Where the personal data is not collected from the data subject, any available information as to their source.

5.2 Right to Rectification

The Data Subject has the right to obtain from FORUS without undue delay, the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the Data Subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

5.3 Right to Erasure

Under Article 17 of the GDPR, Data Subjects have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances. Data Subjects have the right to have their personal data erased by FORUS if:

· The personal data is no longer necessary* for the purpose which FORUS originally collected or processed it for;

· The Data Subject withdraws consent;

· The Data Subject objects to the processing of personal data for direct marketing purposes; · The personal data has been unlawfully processed (i.e.in breach of the lawfulness requirement of the 1st principle);

· The personal data have to be erased for compliance with a legal obligation;

· The personal data have been collected to offer information society services to a child. *Data Subjects are reminded that though FORUS's business activity as a provider of Further Education and Training Services, that in some instances information/personal data regarding the certification outcome of a learner, trainee or apprentice may be retained into the long-term or indefinitely as applicable. FORUS may decline a request for the erasure of personal data where processing activity is necessary:

· For FORUS to comply with a legal obligation;

· The performance of a task related to the public interest or in exercise of official authority;

· The establishment, exercise or defense of legal claim(s);

· Public health reasons;

· For exercising the right to freedom of expression and information.

5.4 Right to Restriction of Processing

Article 18 of the GDPR gives Data Subjects the right to restrict the processing of their personal data in certain circumstances. This means that a Data Subject can limit the way FORUS uses their data. This is an alternative to requesting the erasure of a Data Subject's personal data. Data Subjects have the right to restrict FORUS processing their personal data where they have a particular reason for wanting the restriction. This may be because the Data Subject has issues with the content of the information held, or how FORUS have processed their data. This restriction may in FORUS Data Protection Policy and Privacy Statement V1.0 Page 4 of 6 some cases be time bound. The following grounds apply to a request from a Data Subject to restrict the processing of their personal data:

· The Data Subject contests the accuracy of their personal data, in such cases FORUS will ensure a restriction to processing of the personal data, whilst the case is under review by the FORUS Data Protection Officer;

· The personal data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the Data Subject opposes erasure and requests restriction instead;

· FORUS no longer need the personal data but the individual requires FORUS to keep it in order to establish, exercise or defend a legal claim; or the individual has objected to FORUS processing their data under Article 21(1). In all instances where FORUS lift a restriction of processing, the Data Subject will be notified in writing to include the date of lifting of the restriction. FORUS will only continue to process the personal data if:

· Consent is provided by the Data Subject;

· The processing is necessary for the defense or exercise of legal claims/process;

· The processing is necessary for the public interest;

· The processing is with regard to the protection of rights of other individuals or legal persons.

5.5 Right to Data Portability The right to Data Portability

Under GDPR provides Data Subjects the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. This also includes the transmission of the Data Subject's personal data to another controller. With regard to FORUS's business operations, this right applies to personal data a Data Subject has provided to FORUS, and to personal data generated by a Data Subject's activity. This right does not extend to data generated by FORUS. In practice, Data Portability will only be facilitated by FORUS when:

· Consent is provided by the Data Subject or for the performance of a contract;

· The processing is managed by automated means (i.e. excluding paper files). Data that is provided to a Data Subject or controller through Data Portability norms will not culminate in the erasure to the personal Data on FORUS systems. Furthermore, this will also not affect the original retention period applying to the Data Subject's personal data.

5.6 Right to Object

Article 21 of the GDPR provides an explicit outline that a Data Subject has the right to object to the processing of their personal data. This right allows the opportunity for Data Subjects to request FORUS to stop processing their personal data. However, this right only applies in certain limited circumstances. Data Subjects have the absolute right to object to the processing of their personal data for direct marketing purposes/initiatives. Data Subjects may also object to FORUS processing their personal data if the processing is carried out in the public interest, or in the exercise of an official authority vested in FORUS Data Protection Policy and Privacy Statement V1.0 Page 5 of 6 our organisation. FORUS are cognisant that significant legislation governs contemporary Data Protection Law. That said, FORUS always welcome any request by a Data Subject to better understand how FORUS process their personal data. This process may ultimately culminate in the Data Subject exercising their right to object. FORUS will ensure to process such applications in a timely manner.

5.7 Right to Object to Automated Decision-Making,

Including Profiling Under GDPR, processing of Data Subjects' personal data by FORUS is restricted in instances where decision-making processes have no human involvement. However unlikely this scenario is with regard to FORUS's data processing, and FORUS business activity, the regulations in this regard must still be made explicit to Data Subjects. In limited instances, where automated decision making is in existence within FORUS, the Data Subject will be duly notified of the nature of same with regard the processing of a Data Subject's sensitive personal data. Article 22(3) of the GDPR outlines that Data Subjects will be provided "at least the right" to express their perspective and contest the decision.

5.8 Right to Withdraw Consent

The right to withdraw consent allows a Data Subject to exercise their right to withdraw their consent of a controller to process their personal data at any juncture. Article 7(3) specifically states, “The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.” Withdrawal of consent by a Data Subject may still allow the processing of personal data by FORUS if:

· Processing is necessary for compliance with a legal obligation;

· Processing is necessary for the performance of a contract which includes the Data Subjects as a party to same;

· Processing is necessary in order to protect a natural person or the Data Subject;

· Processing is necessary for aiding a task in the public interest. 7. Data Access Request Forms available from FORUS.

1. FORUS Data Protection Form 1 Subject Access Request Download from FORUS website.
2. FORUS Data Protection Form 2 Right to Rectification Download from FORUS website
3. FORUS Data Protection Form 3 Right to Erasure Download from FORUS website
4. FORUS Data Protection Form 4 Right to Restrict Processing Download from FORUS website
5. FORUS Data Protection Form 5 Right to Data Portability Download from FORUS website
6. FORUS Data Protection Form 6 Right to Object to Processing Download from FORUS website
7. FORUS Data Protection Form 7 Right to Object to Auto Decisions Download from FORUS website
8. FORUS Data Protection Form 8 Right to Withdraw Consent Download from FORUS website

SECTION 6: DATA BREACH NOTIFICATION

Data Breach Notification Policy

All personal data breaches must be reported immediately to Forus Training's Data Protection Officer.

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 Data Protection Regulator is informed of the breach without delay, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Art 3.2) 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.

Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of Forus Training's Data Protection Officer;
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by Forus Training to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Data Protection Policy – Roles and Responsibilities

Implementation

The management team of Forus Training must ensure that all Forus Training employees responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition, Forus Training will make sure all third parties engaged to process personal data on their behalf (i.e their data processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by Forus Training.

Support, Advice and Communication

For advice and support in relation to this policy, please contact the Data Protection Officer on +353 87 8386129 email certification@forustraining.ie

Data Protection Policy -review

This policy will be reviewed by the Data Protection Officer every three years, unless there are any changes to regulations or legislation that would enable a review earlier.

Records management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised Forus Training recordkeeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

RESPONSIBILITIES

Compliance, monitoring and review

The overall responsibility for ensuring compliance with the requirements of the related legislation atForus Training Head Office rests with the Data Protection Officer.

All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant Forus Training policies and procedures.

Reporting in case of a data breach

In the case of possible data breach, the staff member(s) who first identifies the breach or incident, must immediately report all details of the incident to the Data Protection Officer.

The Data Protection Officer is required to report a personal data breach to the competent Data Protection Authority not later than 72 hours after becoming aware of it. The notification must include at least:

- a description of the nature of the breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned;
- the name and contact details of the relevant Data Protection Officer or contact point;
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the Data Protection Officer must communicate the breach to the data subject(s) without undue delay. The communication must describe in clear and plain language, the nature of the breach and at least:

- the name and contact details of the relevant Data Protection Officer or contact point;
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

Records management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised Forus Training Group recordkeeping system.
All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

Feedback and Suggestions

Forus Training employees may provide feedback and suggestions about this document by emailing certification@forustraining.ie

Appendices

Appendix 1 - Data Protection Policy – Related Legislation and Documents

Appendix 2 - Data Protection Policy – Related Legislation and Documents

Appendix 3 – Subject Access Request Form

Appendix 4 – Subject Removal Request Form

Appendix 5 – Data Processing Agreement

Appendix 1 - Data Protection Policy – Related Legislation and Documents

Europe

The European Commission has published a plain English introduction to GDPR:

http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_en.htm.

Because European member states are permitted to legislate additional data protection requirements over and above GDPR's baseline, it is important that you check with your national data protection regulator for information on your country's GDPR compliance requirements. A list of regulators is available http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm.

Outside the EU

We recommend using ICO's English language guidance for basic compliance information.

Forinformationonspecificdataprotectionagreementsyourcountriesmayhavewiththe EuropeanUnion,andforalistofregulatorsandagencieswhichworkwiththeEUondata protection matters, visit this page: http://ec.europa.eu/justice/data- protection/bodies/authorities/third-countries/index_en.htm.

Other links

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- https://www.gov.uk/
- http://www.fieldfisher.com/publications/2017/07/the-clock-is-ticking-is-your-franchise-business-gdpr-ready#sthash.wxk4KYbF.dpbs
- https://www.globalfranchisemagazine.com/advice/are-you-preparing-for-gdpr
- https://www.eugdpr.org/gdpr-faqs.html
- https://ico.org.uk/fororganisations/
- guide-to-data-protection/privacy-notices-transparency-and-control/privacynotices-
- under-the-eu-general-data-protection-regulation/
- https://www.smashingmagazine.com/2017/07/privacy-by-design-framework/
- https://www.privacyshield.gov/welcome
- https://www.theregister.co.uk/2017/09/26/small_businesses_gdpr_affects_you_too/

Appendix 2 - Data Protection Policy – Related Legislation and Documents

USE LETTERHEAD

DATE

RECIPIENT NAME

ADDRESS

Dear Sir/Madam

Forus Training is currently contacting all suppliers of services to our company for the purposes of performing a due diligence check in regard to the new General Data Protection Regulation due to come into force on the on the 25th May 2018.

Please note that as per Article 28(1) of the GDPR we can only use a supplier (Data Processor) who is **"providing sufficient guarantees to implement appropriate technical or organisation measures, in such a manner that processing will meet the requirements of this regulation..."**. Therefore, we have compiled a supplier questionnaire (see attached) which we would like your organisation to complete and return to Forus Training. We will carefully review responses from suppliers and make decisions in the very near future so a reply as soon as possible would be appreciated.

If we are within an extended period contract, which extends beyond 25th May 2018, we will still require a response to the questions attached as well as confirmation that the terms and conditions, on the existing contract, will be amended to contain the specific data privacy wording required by the GDRP legislation, to clarify your organisations obligations and duties to Forus Training under the new legislation.

Thank you,

_____

Managing Director

Forus Training

Data Processor Checklist

Please complete and return to email address hello@forustraining.ie

Name of supplier:

Main supplier contact details for all data privacy matters:

Name:
Job Title:
E-mail:
Phone:
Address:

REQUIREMENT	YES/NO	COMMENT
Please confirm what sufficient guarantees you can give Forus Training that demonstrate your understanding and implementation of your obligation, as a processor, under the new GDPR legislation, including any certifications or externally audited processes.		
Do your standard contract terms include the new GDPR mandatory provisions?		
Do your standard contract terms propagate down, within a formal contract, to your sub contract providers involved in the service to Forus Training?		
Are you maintaining Data Processing Records? (as outlined in Article 30 of GDPR)		
Please detail all subcontractors, included in the provision of your service to Forus Training.		
Do you have a documented Breach Notification Process to ensure notification to Forus Training within 72hrs?		
Do you and your sub processors, providing the service to Forus Training, have a documented process for the deletion of subject's records, upon request, from both live or archived records and backups of your systems?		
Can you confirm our right to have personal data deleted or upon termination of contract at no extra cost?		
Does yours and your sub processor/s, involved in the delivery of services to Forus Training, website/software have a data privacy policy and fair processing notice which meet GDPR requirements?		
Do your contracts of employment contain confidentiality and gross misconduct clauses, in the context of customers data privacy?		
Further checks		
Have you received any data complaints? Please detail.		

Has the individual(s) expressed any other preferences – e.g. regarding marketing calls or mail?		
Has the list been screened against TPS or other relevant preference services? If so, when?		
When was consent obtained?		
Who obtained consent and in what context?		
What method of consent was used (e.g. opt in, opt out)?		
Was the information to the prospected provided clear and intelligible? How was it provided? E.g. behind a link, in a footnote, in a pop-up box, in a clear statement next to the opt in box?		
Did the opt in specifically mention texts, email or automated calls?		
Did the opt in specifically mention Forus Training in name, by description or was the consent for disclosure to any third party?		
Has the list been amended at all, and if so, when and why?		

Subject Access Request Form

If you want us to supply you with a copy of any personal data we hold about you, please complete this form and send it the address below. You are currently entitled to receive this information under the EU General Data Protection Regulation (GDPR).

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request.

Please send your completed form and proof of identity to:
Forus Training, Castle House, Castle Street, Mullingar, Co. Westmeath, N91Y896

Section 1: Details of the person requesting information

PLEASE USE BLOCK CAPITALS

First Name:		Surname:	
Address:			
Email:		Phone:	

Section 2: Are you the data subject?

☐ Yes: I am the data subject. I enclose proof of my identity (see below). Please proceed to Section 4.

☐ No: I am acting on behalf of the data subject's written authority and proof of the data subject's identity and my own identity (see below). Please proceed to Section 3.

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one of both of the following:

1) **Proof of Identity.** We need one of the following: passport, photo driving license, national identity card, birth certificate.
2) **Proof of Address.** We need one of the following: utility bill, bank statement, credit card statement (no more than 3 months old); current driving license; local authority tax bill.

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

Section 3: Details of the data subject (if different from Section 1)

First Name:		Surname:	
Address:			
Email:		Phone:	

Section 4: What information are you seeking?

Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require.

Please note that if the information you request reveals details directly or indirectly about another person we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision.

While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, in accordance with Article 12 of the GDPR to charge a fee or refuse the request if it is considered to be "manifestly unfounded or excessive". However, we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

Section 5: Information about the data collection and processing

- ☐ Why we are processing your personal data
- ☐ To whom your personal data are disclosed
- ☐ The source of your personal data

Section 6: Declaration

Please note that any attempt to mislead may result in legal action.

I confirm that I have read and understood the terms of this Data Subject Removal Request Form and certify that the information given in this application to Forus Training is true. I understand that it is necessary for Pitman Training to confirm my / the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Signature: Date:

Section 7: Attachments

I am enclosing the following as proof of identity.

Subject Removal Request Form

If you want us to remove any personal data we hold about you, please complete this form and send it the address below. You are currently entitled to receive this information under the EU General Data Protection Regulation (GDPR).

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request.

Please send your completed form and proof of identity to:
Forus Training, Castle House, Castle Street, Mullingar, Co. Westmeath, N91Y896

Section 1: Details of the person requesting information

PLEASE USE BLOCK CAPITALS

First Name:		Surname:	
Address:			
Email:		Phone:	

Section 2: Are you the data subject?

☐ Yes: I am the data subject. I enclose proof of my identity (see below). Please proceed to Section 4.

☐ No: I am acting on behalf of the data subject. I have enclosed the data subject's written authority and proof of the data subject's identity and my own identity (see below). Please proceed to Section 3.

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one of both of the following:

1) **Proof of Identity.** We need one of the following: passport, photo driving license, national identity card, birth certificate.
2) **Proof of Address.** We need one of the following: utility bill, bank statement, credit card statement (no more than 3 months old); current driving license; local authority tax bill.

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

Section 3: Details of the data subject (if different from Section 1)

First Name:		Surname:	
Address:			
Email:		Phone:	

Section 4: What information would you like removing?

Please describe the information you want us to remove.

Section 5: Information about the data collection and processing

- ☐ Why we are processing your personal data
- ☐ To whom your personal data are disclosed
- ☐ The source of your personal data

Section 6: Declaration

Please note that any attempt to mislead may result in legal action.

I confirm that I have read and understood the terms of this Data Subject Removal Request Form and certify that the information given in this application to Forus Training is true. I understand that it is necessary for Pitman Training to confirm my / the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Signature: Date:

Section 7: Attachments

I am enclosing the following as proof of identity.

Data Processing Agreement – External Authenticator

Data Processing Agreement

This Agreement (the "Agreement") is made and entered into this **DATE** (the "Effective Date") by and between **Forus Training** with its principal place of business located at **Castle House Castle Street** (the Controller – hereinafter referred to as the "Client") and **FIRST NAME LAST NAME** with its principal place of business located at **ADDRESS** (the Processor - hereinafter referred to as the "Supplier") (hereinafter referred to individually as a "Party" and collectively as "the Parties").

1. Subject matter and duration of the Order or Contract

(1) Subject matter - The Subject matter of the Order or Contract regarding the processing of data is the execution of External Authentication by the Supplier.

(2) Duration - The Order or Contract will be authorised for one-time execution only and entered into for each instance of the contract.

2. Specification of the Order or Contract Details

(1) Nature and Purpose of the intended Processing of Data

1. The External Authenticator shall:
   - Confirm fair and consistent assessment of learners;
   - Review internal verification reports;
   - Apply a sampling strategy and moderate assessment results;
   - Visit the centre and meet staff and learners as appropriate;
   - Participate in the results approval process;
   - Identify irregularities and make recommendations.

The data is processed on-site at Castle House, Castle Street, Mullingar, Co. Westmeath. Aggregate data is collated within a report and no individual's data is represented. Where data / an assessment event is referred to it should be anonymised.

The data that is viewed by the processor is not removed from the processing location nor photocopied / reproduced in any way.

(2) Type of Data

The type of personal data used:

ID, PPS, DOB, Gender, Contact Information, Proof of Identification

Correspondence	Attendance patterns Registers/Roll books	Scores, results, grade
Registration Forms		feedback
Name of Programme	Course completion	Plagiarism detection
Award type, Award Name, Award Code, Award Year of programme	Learner Evidence inc. video evidence	
Date of commencement,	Reaction sheets	
Number of Years completed	Current year credits	

** Processing in accordance with Article 28 General Data Protection Regulation (GDPR)*

Entry standard to programme Highest qualification	Accumulated credits	
Garda vetting form & outcome - Learners ❶ ₡		
Psychological assessments ?		
Special Education Needs' files, reviews, correspondence ?		
Individual Education Plans ?		
Sensitive Learner information - Accident reports ?		
Sensitive Learner information - Records of complaints Ω or ❼* ₡	Complaint correspondence Ω or ❼* ₡	Complaint outcome Ω or ❼* ₡
Sensitive Learner information - Appeal Applications ❼ ₡	Appeal correspondence ❼ ₡	Appeal Outcome ❼ ₡

3. Technical and Organisational Measures

REQUIREMENT	YES/NO	COMMENT
Please confirm what sufficient guarantees you can give Forus Training that demonstrate your understanding and implementation of your obligation, as a processor, under the new GDPR legislation, including any certifications or externally audited processes.		
Do your standard contract terms include the new GDPR mandatory provisions?		
Do your standard contract terms propagate down, within a formal contract, to your sub contract providers involved in the service to Forus Training?		
Are you maintaining Data Processing Records? (as outlined in Article 30 of GDPR)		
Please detail all subcontractors, included in the provision of your service to Forus Training.		
Do you have a documented Breach Notification Process to ensure notification to Forus Training within 72hrs?		
Do you and your sub processors, providing the service to Forus Training, have a documented process for the deletion of subject's records, upon request, from both live or archived records and backups of your systems?		
Can you confirm our right to have personal data deleted or upon termination of contract at no extra cost?		
Does yours and your sub processor/s, involved in the delivery of services to Forus Training, website/software have a data privacy policy and fair processing notice which meet GDPR requirements?		

4. Rectification, restriction and erasure of data

(1) The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client.

(2) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Client without undue delay.

5. Quality assurance and other duties of the Supplier

In addition to complying with the rules set out, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

Mr/Ms TRUDI BARNETT is designated as a Data Protection Officer / Contact Person on behalf of the Supplier.

6. Communication in the case of infringements by the Supplier

(1) The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

a) Ensuring an appropriate level of protection through Technical and Organisational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

b) The obligation to report a personal data breach immediately to the Client

c) The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.

d) Supporting the Client with its data protection impact assessment

e) Supporting the Client with regard to prior consultation of the supervisory authority

7. Authority of the Client to issue instructions

(1) The Client shall immediately confirm oral instructions (at the minimum in text form).

(2) The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

8. Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, the Supplier shall hand over to the Client documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner.

Signed for and on behalf of Forus Training :		Signed for and on behalf of EXTERNAL AUTHENTICATOR	
Name:		Name:	
Title:		Title :	
Signature:		Signature:	
Date:		Date	