**Data Protection Policy Guidelines**

Contents

1. Introduction .......................................................................................................................2

2. Purpose ............................................................................................................................. 2

3. Definitions ..........................................................................................................................2

4. Summary of Conditions ......................................................................................................3

5. Principles of GDPR ............................................................................................................. 4

6. How and why we obtain and process information .............................................................5

7. Sharing information, consent & withdrawal of consent......................................................6

8. Data Subject Access Requests, rectification/erasure ..........................................................6-7

9. Profiling ................................................................................................................................7

10. Retention Periods ..............................................................................................................8

11. Data Breach .....................................................................................................................…9

12. Limitations ..........................................................................................................................9

13. Request for Data/Change/Deletion (sample) ........................................................………….10

**1. Introduction**

FTI Wellbeing and Training Ltd is committed to providing quality and transparent services to our clients and staff.

As an organisation we gather and store data that is crucial to the management and operation of our services.

We rely on information volunteered by clients and staff to provide safe and effective services and we place in high regard the trust that is bestowed on us in ensuring that privacy rights and dignity are protected and valued at all times.

We aim to be transparent and respectful when handling personal data and we work on the principle that it doesn’t belong to us we are merely temporary custodians. Questions we need to consider before we collect any data are: Is the information necessary to carry out our duties? Can we significantly safeguard the information from theft?

**2. Purpose**

The purpose of this document is to provide guidance on new data protection regulations coming into place from May 25th 2018.

**3. Definitions**

Data subject - A person/individual who can be identified byinformation such as name, online identity,photograph et al.

Personal Data - Any information relating to an identified or identifiable data subject, name address, date of birth

Sensitive Personal Data - Data relating to racial or ethnic origin, political, religious or philosophical beliefs, trade union membership, health information, mental health, sex life and sexual orientation, and genetic or biometric data.

Data Processing - An operation that is carried out on personal data. It includes transmission, back up, storage and destroying, even when encrypted.

Data Controller - An entity who ‘determines the purposes and means of processing of personal data’.

The organisation Data Processor - An entity that processes personal data on behalf of a controller. Example: Salesforce

Pseudonymous Data Personal data that cannot be tied to a specific data subject without additional information.

Anonymous Data Data that cannot ever be connected to an identified or identifiable person.

**4. Summary of Conditions**

Enforcement

• Maximum fine increased from €500,000 to €20,000,000 or 4% of annual turnover

• Easier for data subjects to make a claim

• Data subjects are entitled to compensation from a data controller or data processor

Accountability

• Need to demonstrate compliance – fine can apply even if there is no breach

• Must keep an audit trail of processing

• Systems must be privacy by design and privacy by default

Data subject rights

• No fees for data requests

• Right to restrict processing

• Right of portability

• Right of erasure

• Right to object to data processing for risk purposes if it amounts to profiling

Data protection officers

• An organisation with more than 250 employees will be required to have a data protection

officer, (DPO).

• DPO must be impartial and not instructed on how to carry out their role

• DPO must report directly to the highest level of management.

Conditions for processing

• Article 9, processing of special categories of personal data includes the provision of social care

Breach Notifications

• Data subjects must be informed of a breach that involves personal or sensitive data

• Data protection Commissioner must be notified within 72 hours of breaches that include personal or sensitive data

Data processors responsibilities

• Duty to act in accordance with controller instructions

• Processors become controllers if they act outside of the scope of the controller’s instructions.

• Extra requirements for data processing agreements

Fair processing procedures

• The information gathered does not exceed the limits of its purpose

• The information is in proportion to the task

• There is a fundamental understanding that data subject have the right to privacy and a private

life.

**5. Principles of GDPR**

**5.1**. Lawfulness, Fairness & Transparency: Processing personal data is based on the principle that the data subject is fully aware and understands their rights and freedoms around the scope of the data being processed, the purpose of the processing, how it is processed, who has access to the information and how to contact the data controller in the event of amelioration.

**5.2**. Purpose Limited: We collect and manage data to allow us to provide services to our clients and to carry out our day to day function as an employer. We collect and process various categories of data including personal and sometimes sensitive data, this can include personal details like name, address and date of birth and also sensitive information like mental & physical health, gender and criminal convictions. Processing personal data is limited to the purpose of collection. For example, data that is collected for the purpose of a staff file cannot automatically be used to target a newsletter. Further, data that is collected for the purpose of a processing certification cannot automatically be used to apply for any other reason. With consent of the customer we keep details on file such as exams, evaluation forms, candidate forms and any material relevant to processing certificates.

**5.3**. Data Minimisation: Processing personal data should be adequate, relevant and restricted to the purpose at hand. For example, where a customer accesses our centre is it necessary to start collecting data around mental and physical health and further, where a client is obviously an adult is it necessary to collect date of birth.

**5.4**. Accuracy: Data must be accurate and up to date. Information that is known to be incorrect or no longer relevant must be rectified or deleted.

**5.5**. Storage limitation: Personal data must be kept solely within the retention period specified by the organisation.

**5.6**. Integrity & Confidentiality: The organisation will ensure that appropriate security measures are undertaken to safeguard personal data. Information is held on a number of formats, for example; paper files, Microsoft office suite and third-party cloud services such as Salesforce. FTI Wellbeing and Training Ltd will ensure that appropriate measures will be put in place to safeguard the security of the information held. Measures will include securely locking paper files, password protecting files on computers and safeguarding hardware through passwords and in the case of laptops they will be encrypted. Where paper files are held appropriate security measures must be undertaken to prevent any keys from being misplaced or stolen. Access to files will solely be undertaken on a need to know basis. The more sensitive the data the more robust the security measures need to be.

**5.7**. Liability and accountability: We have a legal responsibility to demonstrate that we are compliant with the current legislation and we exercise reasonable care to ensure that we carry out processing fairly and accurately. There is equal responsibility for third parties who carry out processing on our behalf to ensure that they are also compliant with legislation.

**6. How and why we obtain and process information**

**6.1**. We obtain information through various means and primarily through customers attending the centre of our daily business.

**6.2**. To obtain data fairly the organisation needs to satisfy itself that it meets criteria from at least one of the following conditions.

• Consent: The data subject has clearly agreed to their data being processed for a specific and

unambiguous purpose.

• Contract: Processing data is necessary to satisfy the management of a contractual

arrangement between the organisation and the data subject, for example; recording of sick

leave, reference checking, garda vetting, health checks, et al.

• Vital Interests: Where it is necessary to protect the vital interests of the data subject, for

example risk of suicide, self-harm or harm to others, overdose, medical emergency et al. It is

critical in our daily professional practice that the vital interest clause does not give carte

blanche justification for gathering data. The principles of vital interest apply when a person is

‘physically or legally incapable of giving consent’. Where the vital interest clause is used for the

basis of carrying out a risk assessment the principles of a frequency and severity scale must

be considered. For example, a known risk that had occurred on one occasion, which may have

occurred three years previously potentially falls outside of the scope of a legitimate and vital

reason to process, the key principles are that information is ‘up to date’, relevant and can be

evidenced.

• Legitimate activities: Where individuals can be identified consent must be given. Word of

caution; it doesn’t automatically follow that anonymised data makes a person anonymous. An

association with the organisation and a specific set of anonymous data may identify a data

subject.

• Legal Obligation: Processing is necessary to comply with legislation and legal requirements, for

example; Health & safety reporting, protecting vulnerable adults from abuse and for the

administration of justice.

• Defence of a legal claim: The organisation has the right to process data for the purpose of

defence in a legal claim.

• Public Health / Official Authority: Processing is carried out when the organisation is providing a

service on behalf of a statutory agency.

**7. Sharing information, consent & withdrawal of consent**

**7.1**. Focused Training Ireland relies on a network of other services to successfully carry out its duties as an employer for processing.

**7.2**. To process information regarding children under the age of 16 we must get the explicit consent of the child’s legal guardian.

**8. Data Subject Access Requests, rectification/erasure**

**8.1** Data subjects have the right to access all personal data that is collected by the organisation regarding him or her.

**8.2**. We have 30 days to comply with the request.

**8.3**. There is no charge for the request however a reasonable administration charge can be applied for additional copies.

**8.4**. Any request must be in writing, including electronic requests, and should be coordinated by the manager of each individual service.

**8.5**. A data subject is entitled to a copy of all personal data that is held by the organisation. This includes, but is not limited to; paper files, electronic files, emails, text messages, word documents and also data that was processed by a third party contractor on behalf of the organisation.

**8.6**. In order to maximise the efficiency of a data request, and where it is deemed that the request is excessive, data subjects should narrow the parameters of the information required. Fostering a culture of transparency and honesty between the data subject and the controller is critical to providing a smooth and efficient process that benefits both the individual and the organisation.

**8.7**. On submitting a data request the data subject has the right to the following information:

• Who processed the information

• When it was processed

• Why it was processed

• How and where it was processed

• How long the processing has been taking place

• Who had access to the data, including third parties

**8.8**. A log should be kept of all data requests. Logs must include, name, date requested, date submitted, information requested, information handed over, information not handed over and reason why and any other problems or shortfalls in the process.

**8.9**. Data subjects have the right to have data rectified or corrected if they feel it is inaccurate or it was unfairly obtained.

**8.10**. In the event that the data subject and the controller are in disagreement around the accuracy of certain data, a supplementary statement must be included which reflects a common understanding of the data.

**8.11**. Rectification is not always feasible; however, we must demonstrate just cause in the event that we refuse.

**8.12**. Data subjects have the right to request deletion of personal data with undue effect. The organisation will comply if one of the following conditions are met:

• The personal data no longer has a purpose. For example, a staff member or client leave the

organisation and there is no legal basis to keeping the information.

• The processing of data was through consent which is withdrawn and subsequently there is no legal

basis to process the data.

• Data was obtained unlawfully.

• Compliance with a legal obligation or instruction.

**8.13**. The principles of justice and fairness will apply when a request for deletion or rectification are made and the organisation will endeavour to facilitate the request.

**8.14**. In the event that the data subject is unsatisfied with the outcome of the process it can be appealed to the FTI Wellbeing and Training Ltd data protection officer for review.

**8.15**. In the event that the data subject is still unsatisfied with the outcome of the process they should seek guidance or consider bringing a complaint to the Irish Data Protection Commissioner.

**8.16**. In the interest of best practice every effort must be made to facilitate such a request.

**9. Profiling**

**9.1**. Profiling is understood as; the use of personal data to analyse characteristics of the data subject in order to predict aspects of a person’s behaviour or capabilities. The principle can be applied to work performance, reliability, mental & physical health, personal interests or habits.

**9.2**. Profiling is not permitted without consent where the processing can significantly affect or have legal implications on the data subject.

**9.3**. Profiling has potential to influence circumstances that could potentially lead to discrimination.

**9.4**. The principles of client risk assessments have the potential to be considered profiling. We require to risk assess clients to ensure their safety and the safety of other people who live and work in their communities.

**9.5**. To reduce the risk of profiling, risk assessments must be specific and succinct. They should avoid being overly descriptive and excessively long, they should avoid assessing every aspect of the data subject’s life. The information must be up to date and focus solely on the identified and presenting need to mitigate the safety of the data subject or the community.

**9.6**. The data subject should be entitled to express their point of view and challenge the outcome that arises out of the process.

**10. Retention Periods**

**10.1**. Information is held for the duration of the person’s involvement with the organisation plus an additional archiving period, usually 4 years.

**10.2.** Individual services are responsible for retention and archiving of files unless there is a legal basis to retain them. All files that are held on the grounds of a legal basis will be archived in the centre.

**10.3**. It is the project manager’s responsibility to ensure robust security measures are in place to safeguard and protect all personal data that is retained within services.

**11. Data Breach**

11.1. A data breach is understood to be a confirmed incident where sensitive, confidential or protected data has been accessed, disclosed, altered or destroyed in an unauthorised way, whether through deliberate or accidental causes.

**11.2**. All data breaches need to be logged and the data protection officer must be notified.

**11.3**. A data breach can vary in degree from a misdirected email to a mass compromise of organisation systems.

**11.4**. In the event that, personal or sensitive personal data, that is likely to cause harm to the individual is compromised, no matter how many individuals, the Irish Data Protection Commissioner must be notified.

**11.5.** Where personal information is breached the data-subject has the right to be informed of scope and severity of the breach.

**11.6**. In the event that the data breached is encrypted or anonymised there is no need to inform the data protection commissioner.

**11.7**. The data protection officer of the organisation is responsible for notifying the Irish Data Protection Commissioner of any breaches.

11.8. Notification to individuals or the Data Protection Commissioner must be carried out within 72 hours of notification.

**11.9**. In the event that the data protection officer is unavailable to report within 72 hours the following hierarchy will apply:

1. Project Manager

2. Data Champion

3. Head of legal and HR

**11.10**. In the event of a data breach security systems will be reviewed.

**11.11**. Data breach notification table:

Low risk – Log and notify data protection officer

High Risk – Notify data protection officer, data protection commissioner & data subject

Anonymised Data Identity theft

Encrypted Data Breach of confidentiality

Loss or breach of personal information

Loss or breach of sensitive information

**12. Limitations**

**12.1**. Understanding the relationship as a co-controller for example PASS, and the potential implications and responsibilities

**12.2**. Child-friendly version needs to be drafted as per the regulations

**12.3**. Lack of data map

**13. Data Request form**

Name : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date of Request : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Service : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Manager : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

I would like to request the following, please tick

□ I wish to make an access request for a copy of information you keep about me

□ I wish to have inaccuracies corrected

□ I wish to have information deleted

on computer or in manual file in relation to: (try to be specific, is it in relation to a specific issue, is it in relation to

one project or more than one project etc.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

We will endeavour to comply with your request within 30 days. However, if the request is large we may extend this period but will notify you in writing.

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

David Gahan

Managing Director

Date: 18th of August 2022

Date of review: 18th of August 2023