GDPR Data Protection Policy

Turas Training

Approval date: January 2020

Revision date: January 2022

1. Policy Statement

1.1. Turas is committed to protecting the privacy and personal data of individuals with whom we interact. This Data Protection Policy outlines our approach to complying with the General Data Protection Regulation (GDPR) and ensuring the lawful and secure processing of personal data. We aim to be transparent in our data practices and to handle personal data responsibly to maintain the trust of our stakeholders and operate in a manner consistent with the guidelines of the General Data Protection Regulation and Data Protection Commissioner.

.

2. Purpose

2.1. To set out our processes and procedures in respect of data protection

2.2. To provide a framework within which data protection can be managed, such that Turas is compliant with its statutory obligations

3. Glossary of Terms and Definitions

3.1. *Data* means information in a form which can be processed. It includes both automated (computerised) and manual data

3.2. *Processing* means performing any operation or set of operations on data including:

- 3.2.1. Obtaining, recording or keeping data
- 3.2.2. Collecting, organising, storing, altering or adapting data
- 3.2.3. Retrieving, consulting or using the data
- 3.2.4. Disclosing the information or data by transmitting, disseminating or otherwise making it available
- 3.2.5. Aligning, combining, blocking, erasing or destroying the data

3.3. *Personal Data* means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. This can be a very wide definition depending on the circumstances.

3.4. *Sensitive Personal Data* relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

3.5. *Data Subject* is an individual who is the subject of personal data.

3.6. *Data Controllers* are those who, either alone or with others, control the contents and use of personal data. Data Controllers can be either legal entities such as companies, Government Departments or voluntary organisations, or they can be individuals such as GPs, pharmacists or sole traders.

3.7. *Service User* is an individual who uses the services of TURAS and on whom TURAS keeps personal data.

3.8. *Staff member* is an individual who works with the organisation and on whom TURAS keeps personal data. It should be construed broadly and includes employees, students, volunteers and locums.

3.9. *Line manager* is an individual with supervisory responsibilities for other staff members

4. Scope

4.1 This policy concerns the duties Turas as a data controller. It applies to all data in the organisation and to all staff members who have access to data.

5. Legislation and relevant documents

5.1. The Data Protection Act 1988

5.2. The Data Protection (Amendment) Act 2003

5.3. The Freedom of Information Act 1997

5.4. The Freedom of Information (Amendment) Act 2003

5.5. The Data Protection Act 2018

5.6. National Protocols and Common Assessment Guidelines to accompany the National Drugs Rehabilitation Framework

5.7. Turas Service User Confidentiality Policy
5.8. Turas Complaints Policy

6. Principles

6.1. TURAS undertakes to[1]:
- 6.1.1. obtain and process information fairly
- 6.1.2. keep it only for one or more specified, explicit and lawful purposes
- 6.1.3. use and disclose it only in ways compatible with these purposes
- 6.1.4. keep it safe and secure
- 6.1.5. keep it accurate, complete and up-to-date
- 6.1.6. ensure that it is adequate, relevant and not excessive
- 6.1.7. retain it for no longer than is necessary for the purpose or purposes
- 6.1.8. give a copy of his/her personal data to an individual, on request

6.2. Access to personal data should be strictly on a 'need to know' basis.

7. Roles and Responsibilities

7.1. The project coordinator is the person with responsibility for data protection issues in the organisation. This person is responsible for:
- 7.1.1. addressing all queries in relation to data protection
- 7.1.2. ensuring that this policy is kept up to date
- 7.1.3. overall implementation of this policy

7.2. Line managers are responsible for ensuring that staff members have read, understood and signed off on this policy, and other relevant policy documents, such as those on confidentiality. Record keeping and data protection requirements and responsibilities will form part of the induction process for new staff.

7.3. All staff members are responsible for ensuring that management of data in the organisation is consistent with the practices outlined in this policy. All staff members should report any data protection concerns to the project coordinator immediately.

7.4. The Board of Directors is ultimately responsible for ensuring the organisation's compliance with data protection laws and the implementation of this policy.

8. Storing Manual Data

8.1. Any manual data kept by the organisation should be kept in a manner consistent with good data retention:
- 8.1.1. All personal data should be kept in a locked file, with the key being held only by relevant staff members
- 8.1.2. All records should be written legibly and indelibly. Records should be clear, unambiguous and accurate including the date (Day/Month/Year), and the printed name and signature of the person completing the record.
- 8.1.3. Alterations are made by scoring out with a single line followed by the initialled and dated correct entry. The use of correction fluid such as 'Tipp-ex' is not permitted.
- 8.1.4. Records are not to include jargon, subjective statements or abbreviations other than those in common organisational use. All records should be written in a way that is easy to understand
- 8.1.5. Records must be objective and factual and describe what is observed. If for some reason a more subjective statement needs to be made, the recorder should acknowledge this as a subjective opinion.
- 8.1.6. Records should include only essential and relevant details.

9. Storing Automated Data

9.1. The principles for manual data also apply to automated data. In addition:

[1] Data Protection Commissioner, *Data Protection Acts 1998 and 2003. A Guide for Data Controllers*. P.5. Available from http://www.dataprotection.ie

9.1.1. Staff must ensure that computerised records are not left unattended and that all computerised systems are logged off or locked appropriately.

9.1.2 All computerised systems which hold personal data must be password protected. Passwords must be changed regularly, be specific to individuals and have at least 10 characters (including at least one letter, one symbol (e.g. &, *, @, €, $ etc.), and one number (0 - 9))

9.1.3 Passwords must not be written down

9.1.4 Passwords must not be shared among colleagues.

9.2. All computerised records must be backed up regularly on an appropriate data storage backup system.

9.3. Personal data must never be downloaded onto an external system. Where it is required to carry personal data outside the organisation, it must be secure and password protected.

10. Retention and Review of Data

10.1. Precautions should be taken to protect written copies from damages due to fire, and water.

10.2. Precautions should be taken to protect all electronic data from viruses or technical failure.

10.3. Data management systems need to be regularly monitored. The project coordinator and or administrator will do spot checks on quality of documentation and record keeping.

10.4. The project coordinator and administrator will do a review every year to ensure that data are not being kept for any longer than they need to be. The table below is a guideline only to retention periods for specified data. In the event of unspecified data, a blanket period of six years will apply in respect of retention. Data related to ongoing legal and investigative actions should not be destroyed.

10.5. Care should be taken to ensure that data are disposed of correctly and securely. Where possible, old records should be shredded.

Type of Data	Retention Period
Accident books, accident record / reports	6 years after the date of last entry
Accounting Records	6 years for private companies, 6 years for public limited companies
Tax records	Not less than three years after the financial year to which they relate
Statutory Maternity Pay Records	6 years after the end of the tax year in which the maternity period ends
Statutory Sick Leave records	6 years after the end of the tax year in which the sick leave period ends
Holidays, public holidays, and rest periods	3 years after the end of the tax year in which the holiday period ends
Wages/salary records (also overtime, bonuses, expenses)	6 years
Application forms and interview notes (for unsuccessful candidates)	1 year
Pension Records	12 years after benefits cease
Personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases
Service User Records	6 years after last recorded engagement with the organisation
Redundancy details	6 years after employment ceases
Time cards	6 years after audit
Trade Union Agreement	10 years after ceasing to be effective

11. Access Controls

11.1. Access to data containing personal information strictly limited to a "need to know" basis. However, for an effective team response to the needs of Service Users, all staff members involved in an individual's care will "need to know" relevant personal information. This should be explained clearly to Service Users at the outset of their relationship with the organisation.

11.2. Personal data will not be shared between separate teams, unless valid consent exists, or the data is shared in accordance with the Confidentiality policy.

12. Access for Data Subjects

12.1. Data subjects have the right to access the data Turas holds on them. In order to access this information, they should make a request in writing to the project coordinator or administrator. The project coordinator or administrator will then process the request such that, at a minimum, a description of the requested information to the Service User within 21 days of receiving a written request, and a copy of the

12.2. Documentation is provided within 40 days of receiving a written request. In meeting the request, the project coordinator or administrator should:

12.2.1. Find out why the person wants to see their records to identify if there is a specific piece of information they want to see rather than their entire file. If the person does not wish to disclose their reason for wishing to access their file they are still entitled to full access.

12.2.2. Make an appointment to meet the person with their records. Personal information should only be given to the individual concerned (or someone acting on his or her behalf and with their pre-arranged written authority).

12.2.3. Collate a copy of the records, removing all information relating to other people. When providing people with access to personal data, care must be taken to ensure the confidentiality of other individuals identified. If other names are mentioned on the documentation, these should be blacked out by a permanent pen.

12.2.4. Present the records to the person and offer to take them through it. When necessary, explain how the different records are used and be prepared to answer any questions the person may have.

12.2.5. Inform the person that they are entitled to receive copies of files, but that all original documentation will remain on their file in a secured location.

12.3. The project coordinator and administrator should ensure that they are familiar with the 'Data Protection and Freedom of Information Legislation. Guidance for Health Service Staff' document. This document is located at http://www.hse.ie.

12. Complaints

12.1 In the event that a data subject is unhappy with the way they have been treated in respect of the management of data relating to them, they should be supported to make a complaint, or institute a grievance in line with the Complaints policy.

12.2 Data subjects are also encouraged to contact the Data Protection Commissioner for further information on how to make a complaint to the Office of the Data Protection Commissioner:

http://www.dataprotection.ie
1890 252 231
Info@dataprotection.ie
Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois

12.3 In the event that TURAS holds a Service Level Agreement (SLA) with a state body such as the HSE, it may be necessary to follow their complaints procedure, for example the HSE's 'Your Service Your Say' available on http://www.hse.ie.