Data Protection Policy
Trasna (trading name of Oases Health Horizons Ltd.)

Introduction

1.1 Background to the General Data Protection Regulation (EU) 2016/679 ('GDPR')

The GDPR replaces the EU Data Protection Directive of 1995, 95/46/EC and supersedes the laws of individual Member States that were developed in compliance with Directive 95/46/EC. Its primary purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) particularly their right to protection of their personal data. A further purpose of the GDPR is to create a uniform and harmonised set of laws for the protection of personal data within the EU so that the free movement of personal data within the Union is not hindered.

1.2 Definitions used by the organisation (drawn from Article 4 GDPR)

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of
genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's

performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

2. Policy statement

2.1 Trasna is committed to complying with its obligations as a data controller pursuant to the GDPR and the Data Protection Acts 1988-2018 (collectively referred to as 'the DPA'). Compliance with the DPA is described by this policy and other relevant policies such as the Privacy Statement, the Data Protection Consent Form and our Terms of Use (available on www.trasna.com)

2.2 This policy applies to all of Trasna's personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

3. Responsibilities and roles under the General Data Protection Regulation

3.1 Trasna is primarily a data controller under the GDPR.

3.2 The Directors and all those in managerial or supervisory roles throughout Trasna are responsible for developing and encouraging good information handling practices within Trasna;

3.3 The Operations Director, Aonghus O'Rourke has been appointed to manage Trasna's compliance with this policy and, in particular, has direct responsibility for ensuring that Trasna complies with the DPA however, generally compliance is the responsibility of all employees of Trasna who process personal data.

4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Trasna's policies and procedures are designed to ensure compliance with those principles which are detailed below.

4.1 Personal data will be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent. Trasna sets out the

lawful basis for its processing activities in its Privacy Statement and Data Protection Consent Form (available on www.trasna.com).

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language. Trasna sets out this information in its Privacy Statement and Data Protection Consent Form (available on www.trasna.com).

4.2 Personal data can only be collected for specific, explicit and legitimate purposes. As set out in our Privacy Statement and Data Protection Consent Form (available on www.trasna.com), Trasna commits to only processing your personal data for the purpose for which it was collected.

4.3 Personal data must be adequate, relevant and limited to what is necessary for processing

4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify unrequired data without delay. Trasna shall ensure that all staff are trained in the importance of collecting accurate data and maintaining it however, it is also the responsibility of the data subject to ensure that data held by Trasna is accurate and up to date and if you are aware that any personal data which Trasna processes about you is not accurate or up to date, please let us know by emailing info@trasna.com. This includes personal data in relation to employees.

4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing. Where personal data is retained beyond the processing date, it will be securely deleted/encrypted/pseudonymised where possible in order to protect the identity of the data subject in the event of a data breach.

4.6 Personal data will be processed in a manner that ensures the appropriate security of the personal data and that maintains its integrity and confidentiality. In determining appropriateness, Trasna will consider the following:

- Password protection
- Automatic locking of idle terminals
- Removal of access rights for USB and other memory media
- Virus checking software and firewalls
- Role-based access rights including those assigned to temporary staff
- Encryption of devices that leave the organisations premises such as laptops
- Security of local and wide area networks
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to Trasna;
- The appropriate training levels throughout Trasna;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;

• Monitoring of staff for compliance with relevant security standards;
• Physical access controls to electronic and paper based records;
• Adoption of a clear desk policy;
• Storing of paper based data in lockable fire-proof cabinets;
• Restricting the use of portable electronic devices outside of the workplace;
• Restricting the use of employee's own personal devices being used in the workplace;
• Adopting clear rules about passwords;
• Making regular backups of personal data and storing the media off-site;
• The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

All employees are responsible for ensuring that any personal data that Trasna holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Trasna to receive that information and has entered into confidentiality obligations. In this regard all Trasna employees have signed an Employee Confidentiality Policy.

4.7 The controller must be able to demonstrate compliance with the GDPR's other principles i.e. accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the data protection principles and states explicitly that this is the controller's responsibility.

Trasna demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

5. Data subjects' rights

Data subjects have the following rights regarding data processing:

- Access– you have the right to request a copy of the personal data that we hold about you, together with other information about our processing of that personal data.
- Rectification- you have the right to request that any inaccurate data that is held about you is corrected, or if we have incomplete information you may request that we update the information such that it is complete.
- Erasure – you have the right to request us to delete personal data that we hold about you. This is sometimes referred to as the right to be forgotten.
- Restriction of processing or to object to processing – you have the right to request that we no longer process your personal data for particular purposes, or to object to our processing of your personal data for particular purposes for example to prevent processing that is likely to cause damage or distress or to prevent processing for the purposes of direct marketing.
- Data portability – you have the right to request us to provide you, or a third party, with a copy of your personal data in a structured, commonly used machine readable format.
- Right to be informed about the mechanics of automated decision-taking process that will significantly affect them and the right not to have significant decisions that will affect you taken solely by automated processes.
- Right of action before the courts for any contravention of the DPA.

- Right to request that the Data Protection Commission assess whether any provision of the DPA has been contravened.
- Right to make a complaint to the Data Protection Commission for any contravention of the DPA.
- Right to withdraw your consent to consent-based processing (see section 6 below).

To exercise any of these rights, please email info@trasna.com.

6. Consent

6.1 Trasna understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

6.2 Trasna also understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

6.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. Trasna must be able to demonstrate that consent was obtained for the processing operation.

6.4 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

As Trasna relies on consent for the purposes of providing healthcare services to customers/patients and obtains explicit consent to the processing of customer/patient personal data (which is likely to include special categories of personal data) by way of our Data Protection Consent Form (available on www.trasna.com).

7. Disclosure of data

Trasna will ensure that all personal data processed is not transferred to a third party save where an agreement is in place with that party which serves to maintain the integrity and confidentiality of the personal data as required pursuant to Article 26 and/or Article 28 GDPR.

8. Retention and disposal of data

8.1 Trasna shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected save where such retention is permitted by law or best industry practice.
8.2 Trasna may store data for longer periods than set out at 8.1 above if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.
8.3 The retention period for each category of personal data will be as set out in Trasna's privacy statements save where Trasna has a legitimate basis to retain the data for longer for

example to defend actual/threatened litigation or in order to comply with a statutory obligation.
8.4 Personal data no longer required to be processed by Trasna will be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects.

9. Data transfers

All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

Pursuant to the GDPR, the transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions set out in Chapter 5 of the GDPR apply.

Trasna generally does not transfer personal data outside of the EEA however, it uses Zendesk software to manage its client base. As Zendesk is a US registered company, this may result in the unintended transfer of personal data outside the EEA to the US. Such cross-border processing is legitimised by virtue of the fact that Zendesk Inc is a signatory to the Privacy Shield Framework at the U.S. Department of Commerce.

Furthermore, post-Brexit Trasna may continue to work with healthcare providers in the UK. In such circumstances Trasna shall enter into contracts comprising standard contractual clauses adopted by the European Commission for the purposes of ensuring the ongoing protection of the personal data of data subjects who are placed for healthcare in the UK.A

10. Providing information

This policy should be read in conjunction with the Privacy Statement, the Data Protection Consent Form and the Terms of Use each of which contain details on our data protection processes.

11. Review of Policy

Trasna will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required taking into account any changes to current data protection laws.

V2 reviewed May 2019