General Data Protection Regulation (GDPR)

On 25th May 2018 one of the biggest changes to data protection for a generation will come into force. It will have a profound impact on many organisations across the country. TurnKey I.T Solutions have been working hard to ensure that we remain compliant with the changes and we will be helping our customers to do the same.

What is GDPR?

The EU's General Data Protection Regulation (GDPR) will supersede the Data Protection Act (1998) and its principal aim is to give people more control over how their personal data is used. GDPR will have significance for commissioners, service providers and systems suppliers.

How does it affect the Substance Misuse Sector?

Any service that is required to hold and process personal data will be impacted by GDPR. This is particularly true of the substance misuse sector. Here are just some of the key changes that come into effect from the 25th May which will have a direct impact on the substance misuse sector:

- **Consent** – Service providers must request explicit consent to hold a client's personal information in a simple, accessible way and the purpose for which this data will be processed must be stated clearly in this request. *You must also check that data sharing agreements your organisation has with other parties too.*

- **Right to access** – Clients will have the right to know if their personal data is being processed and for what purpose. The data controller will need to be able to provide a free copy of this data in an electronic format.

- **Right to be forgotten** – Clients will be able to get the service provider to erase their data if they wish to withdraw consent.

- **Data Protection Officers (DPO) –** Where organisations are handling large volumes of personal client data, a DPO will need to be appointed.

- **Stricter penalties** – Breaching GDPR can result in a fine of up to 4% of annual global turnover or €20 Million (whichever amount is greater). These penalties will apply to both data controllers and data processors.

- **Data retention period** – Client GreenShoots records should be kept for 8 years after treatment completion, after which they must be destroyed.

What do you need to do?

All services already obtain client consent in line with PHE guidance as part their access to treatment, however there is more that services should be considering – this includes how information and data is shared and processed as part of the continuity of client care, in particular the client's 'right to be forgotten'.

Careful consideration needs to be given to core information about the client's medical, risk and mental health histories which form the basis of their long term treatment and recovery.

How can GreenShoots help?

Client data and information is key to our customers operations and GreenShoots functionality.

- **Data Processing Agreement –** We have created a Data Processing Agreement, which explicitly states TurnKey I.T Solutions role as your Data Processor in relation to the data we hold in GreenShoots. This is counter-signed by your named Data Controller to ensure compliance with GDPR.

- **Secure Data –** This is at the core of our development and delivery strategy. 2-factor authentication is already available for GreenShoots but from 25th May 2018, we will be advising and recommending all implement this as standard. Please contact us for more information.

- **Consents** – Easily manage data protection and third party consents within the client profile.

- **Right to be forgotten** – GreenShoots has been extended to allow authorised staff to delete client records.

- **Historic Client Removal Tool** – We have developed a tool that will enable customers to remove customer data 8 years after the client has been discharged from your treatment centre.

GreenShoots – EU DATA PROCESSING ADDENDUM

This Data Processing Addendum (the **Addendum**) forms part of the TurnKey I.T Solutions Ltd ('Turnkey') Terms & Conditions (and any ancillary or related documentation), as updated or amended from time to time (the

Agreement), between the Customer (as identified on page 4 below) and TurnKey. All capitalised terms not defined in this Addendum shall have the meaning set out in the Agreement.

HOW TO EXECUTE THIS ADDENDUM:

1. This Addendum has been pre-signed by TurnKey.
2. If Turnkey processes personal data on behalf of a TurnKey customer that qualifies as a controller with respect to that personal data under the EU General Data Protection Regulation (Regulation 2016/679) (an **Eligible Customer**), such Eligible Customer may execute this Addendum. Eligible Customers can complete this Addendum by:
    1. (a) Completing the information in the signature box and counter-signing on page 4; and
    2. (b) Submitting the completed and signed Addendum to TurnKey at support@turnkeyit.co.uk. Any

       questions regarding this Addendum should be sent to mike@turnkeyit.co.uk

3. Upon receipt of the validly completed and signed Addendum in accordance with the instructions

   above, this Addendum will become legally binding.

APPLICATION OF THIS ADDENDUM:

If the entity signing this Addendum is an Eligible Customer at the date of counter-signature, this Addendum will form part of the Agreement. In such case, the TurnKey entity that is a party to the Agreement will be a party to this Addendum, as identified in the Eligible Customer TurnKey Invoice.

If the entity signing this Agreement is not an Eligible Customer at the date of counter-signature, this Agreement will not be valid or legally binding.

The parties agree that the obligations under this Addendum that are specific to the EU General Data Protection Regulation (Regulation 2016/679) shall not apply until the later of the Eligible Customer counter-signature or the date the EU General Data Protection Regulation (Regulation 2016/679) has come into full force and effect.

1. Data Protection

1. 1.1. *Definitions:* In this Addendum, the following terms shall have the following meanings:
    1. (a) "**controller**", "**processor**", "**data subject**", "**personal data**", "**processing**" (and "**process**") and "**special categories of personal data**" shall have the meanings given in Applicable Data Protection Law;
    2. (b) "**Applicable Data Protection Law**" shall mean: (i) prior to 25 May 2018, the EU Data Protection Directive (Directive 95/46/EC); and (ii) on and after 25 May 2018, the EU General Data Protection Regulation (Regulation 2016/679); and
    3. (c) "**TurnKey**" means the TurnKey entity that is a party to this Addendum, as specified in paragraph 1 of the section “APPLICATION OF THIS ADDENDUM” above.
2. 1.2. *Relationship of the parties:* Customer (the controller) appoints TurnKey as a processor to process the personal data described in the Agreement (the "**Data**") for the purposes described, and the terms set out, in the Agreement, including, for the avoidance of doubt, to provide you with, and update and improve, our services (or as otherwise agreed in writing by the parties) (the "**Permitted Purpose**"). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

3. 1.3. *Prohibited data:* Unless explicitly requested by TurnKey to do so, Customer shall not disclose (and shall not permit any data subject to disclose) any special categories of personal data to TurnKey for processing.
4. 1.4. *International transfers:* TurnKey shall not transfer the Data outside of the European Economic Area ("**EEA**") unless it has taken such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) transferring the Data to a recipient in a country that the European Commission has decided provides adequate protection for personal data (e.g., New Zealand), to a recipient in the United States that has certified its compliance with the EU-US Privacy Shield, or to a recipient that has executed standard contractual clauses adopted or approved by the European Commission.
5. 1.5. *Confidentiality of processing:* TurnKey shall ensure that any person it authorises to process the Data (an "**Authorised Person**") shall protect the Data in accordance with TurnKey's confidentiality obligations under the Agreement.
6. 1.6. *Security:* TurnKey shall implement technical and organisational measures, as set out in Annex A, which may be amended and updated from time to time, to protect the Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Data (a "**Security Incident**").
7. 1.7. *Subcontracting:* Customer consents to TurnKey engaging third party subprocessors to process the Data for the Permitted Purpose provided that: (i) TurnKey maintains an up-to-date list of its subprocessors, which shall be available on its website on or before 25 May 2018, which it shall update with details of any change in subprocessors at least 30 days prior to the change; (ii) TurnKey imposes data protection terms on any subprocessor it appoints that require it to protect the Data to the standard required by Applicable Data Protection Law; and (iii) TurnKey remains liable for any breach of this Addendum that is caused by an act, error or omission of its subprocessor. Customer may object to TurnKey's appointment or replacement of a subprocessor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, TurnKey will either not appoint or replace the subprocessor or, if this is not reasonably possible, in TurnKey's sole discretion, Customer may suspend or terminate the Agreement without penalty (without prejudice to any fees incurred by Customer up to and including the date of suspension or termination).
8. 1.8. *Cooperation and data subjects' rights:* Turnkey shall provide reasonable and timely assistance to Customer (at Customer's expense) to enable Customer to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law; and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to TurnKey, TurnKey shall promptly inform Customer providing full details of the same.
9. 1.9. *Data Protection Impact Assessment:* If TurnKey believes or becomes aware that its processing of the Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall inform Customer and provide reasonable cooperation to Customer in connection with any data protection impact assessment that may be required under Applicable Data Protection Law.
10. 1.10. *Security incidents:* If it becomes aware of a confirmed Security Incident, TurnKey shall inform Customer without undue delay and shall provide reasonable information and cooperation to Customer so that Customer can fulfil any data breach reporting obligations it may have under (and in accordance with the timescales required by) Applicable Data Protection Law. TurnKey shall further take reasonably necessary measures and actions to remedy or mitigate the effects of the Security Incident and keep Customer informed of all material developments in connection with the Security Incident.

11. 1.11. *Deletion or return of Data:* Upon termination or expiry of the Agreement, TurnKey will, on Customer's explicit request, delete or return the Data in its possession or control (in a manner and form decided by TurnKey, acting reasonably). This requirement shall not apply to the extent that

TurnKey is required by applicable law to retain some or all of the Data, or to Data it has archived on back-up systems, which Data TurnKey shall securely isolate and protect from any further processing.

TurnKey I.T Solutions Ltd

Signature:

Name: Michael Turner

Position: Managing Director

Date: 24/5/18

Customer:_____

Signature:

Name:

Position:

Date: