GDPR Policy HealthBridge Technology Limited

Processing of Personal Data under Data Protection Legislation.

In this policy Data Protection Legislation means, as applicable, the Irish Data Protection Acts 1988 to 2003, the UK Data Protection Act 1998, the EU e-Privacy Directive 2002/58/EC, and from the 25 May 2018 the General Data Protection Regulation (EU 2016/679) and any relevant transposition, successor or replacement of those laws and any applicable guidelines or codes of practice, and the terms defined in the Data Protection Legislation shall apply to this policy.

HealthBridge Technology Limited undertakes to follow the procedures below and shall

- only process the personal data in accordance with the Data Protection Legislation as necessary for the performance of the Services of the Company or as required by law;
- implement appropriate organisational and technical security measures to guard against the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data in accordance with the Data Protection Legislation including those set out in the Annex attached;
- ensure that personnel having access to the personal data are bound by a duty of confidentiality and are aware of and comply with the provisions of this Letter;
- not engage another processer (a sub processor) without the prior written consent of the clients, any subcontractor must adhere to all Data Protection Legislation;
- inform the client, prior to processing the personal data, in the event that the Company is required by law in force in the EU to transfer the personal data outside the European Economic Area, of that legal requirement;
- not transfer the personal data outside the European Economic Area without the prior written consent of the client , such consent shall be subject to such requirements as are necessary to comply with the Data Protection Legislation; taking into account the nature of the processing and the information available to the Company,
- where requested, respond to the exercise by data subjects of their rights under the Data Protection Legislation (including access to personal data, rectification of inaccurate personal data, erasure of personal data, restriction of processing of personal data, data portability and to object to the processing of personal data or automated decision making);
- taking into account the nature of the processing, where requested, assist the client in respect of their obligations under the Data Protection Legislation (including in respect of the security of processing, notifications of personal data breaches, communication of personal data breaches and data protection impact assessments);
- inform the client immediately upon becoming aware of a personal data breach and unless required by law the Associate agrees that it will not communicate with any third party (including media, vendors, consumers and data subjects) without the consent and direction of the client ;

- promptly refer to the client any requests, notices or other communications in respect of processing of the personal data from data subjects or from anybody responsible for the enforcement of the Data Protection Legislation and cooperate with the client as reasonably required;
- not use any personal data which it processes on behalf of the client for direct marketing purposes without the client's prior written consent; and
- make available to the client reasonable information necessary to demonstrate compliance with this Letter and shall provide the client the right to conduct a reasonable audit and/or inspection of the Associate's processing operations to satisfy the client that the Company is in compliance with this policy.

The processing obligations in this policy shall apply for the duration of the Company's engagement as a service provider in connection with the Services. From the termination or cessation of the Services the Company shall stop processing personal data and shall at the client's request either return or delete from its systems all personal data (excepting any personal data it is required by applicable legislation to retain, in which case the provisions of this policy shall continue to apply to the retained personal data) and confirm to the client in writing that this has been complied with, or where relevant the reasons why any personal data must be retained.

The categories of personal data that shall be subject to this policy shall consist of such personal data in connection with participants, customers, employees and contractors or any other personal data which is necessary to be processed as part of the Services or received by the Company in the course of providing the Services. The personal data may include e.g. names, job titles, assignment grades, psychometric results, notes of coaching conversations, addresses, telephone numbers, national insurance numbers, employee numbers, trade union membership, pension information, health information or other personal data to be processed as part of the Services or received by the Company in the course of providing the Services.

No terms and conditions or other provisions relating to data processing ("Data Processing Clauses") that are delivered with, contained or referred to in any document supplied by the Associate shall be binding on the client to the extent that such Data Processing Clauses are inconsistent with those contained in this policy.

Signed: 

Printed Name: Dervilla O'Brien

GDPR Policy HealthBridge Technology Limited

Date: 21/5/19

Annex

The Company shall ensure that they have the appropriate technical and organisational security measures in place taking into account the nature, scope, context and purposes of processing. The Company implements technical and organisational measures pursuant to the appropriate Data Protection and Information Security safeguards to the extent reasonably required to achieve the intended protection purpose.

The Company shall ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; have the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident; and have a process in place for regularly testing, assessing and evaluating the effectiveness of the technical and organisational security measures for ensuring the security of processing.

The Company shall consider measures to prevent unauthorised persons from gaining access to data processing systems; measures to prevent data processing systems from being used without authorisation; measures to ensure that only data for which authorisation has been provided is accessed; the confidentiality of data is maintained; and that the data cannot be read, copied, modified, or removed without authorisation in the course of processing, in storage or transmission.

Associates should ensure:

IT Systems:

- are adequately protected by firewalls to prevent unauthorised intrusion;
- have hardware and software configured to provide the most effective protection, e.g. default passwords are changed;
- have access restricted to users and sources it trusts, each user being allocated an individual user name and password and permissions appropriate to the task the user is carrying out;
- have encryption methods in place as required;
- have detailed description of transmission protocols;
- passwords and other access to its IT Systems are removed immediately if a staff member leaves the organisation or is absent for long periods of time;
- are adequately protected with ant-virus products that are kept up to date;
- software in respect of its IT Systems is kept up to date, supported and regular patch management is under taken to address known security vulnerabilities;

- are adequately backed up at separate premises, with appropriate business continuity and disaster recovery plans in place.

Physical Security:

- The location of the processing activities should be physically secure, with appropriate access controls.
- Portable devices, and storage devices (such as mobile phones, lap tops, usb storage devise) should be encrypted

Staff:

- Staff should be trained so that they are aware of their responsibilities in relation to good data handling practices and data protection.
- Staff should be aware of their responsibilities to maintain confidentiality and non-disclosure agreements should be used as required.