DATA PROCESSING AGREEMENT

Embrace-IT ApS, CVR.no. 36942320

Date: 07 February 2021

1 PARTIES

This agreement on collection, storage and use of documents and information (hereinafter the ”Data Processing Agreement”) has been agreed to by and between

Embrace-IT ApS
CVR.no. 36942320
Kildehøjvej 12
DK-3460 Birkerød
Denmark
(hereinafter referred to as ”Data Processor”)

and

The Customer
(as defined in the Sales and Delivery Terms and in this Data Processing Agreement referred to as the “Data Controller”)

(hereinafter jointly referred to as the ”Parties” and each a ”Party”)

2 DEFINITIONS

2.1 Terms and expressions with capital first letters used in this Data Processing Agreement shall have the meanings set out in the General Data Protection Regulation (EU Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, hereinafter the "GDPR") or the meanings otherwise defined in this Data Processing Agreement.

2.2 “Data Subject” shall mean the identified or identifiable natural person to whom Personal Data refers.

2.3 “Personal Data” shall mean the categories of personal data specified in the Sales and Delivery Terms and Appendix 1 to this Data Processing Agreement.

2.4 “Pre-approved Sub-processors” shall be the sub-processors of Data Processor, stated in Appendix 2.

2.5 "Third party" shall mean a natural or legal person, public authority, agency or body other than the Data Subject, the Data Processor, the Data Controller and persons who, under the direct authority of the Data Processor or Data Controller, are authorized to process Personal Data.

2.6 "Sales and Delivery Terms" shall mean the agreement on supply of services provided by the Data Controller to the Data Processor, entered into by and between the Parties, including the Data Controller's Sales and Delivery Terms.

3 SCOPE

3.1 This Data Processing Agreement regulates the Parties' obligations related to Data Processor's processing of Personal Data on behalf of the Data Controller.

3.2 This Data processing Agreement has been designed to ensure the parties' compliance with GDPR, Article 28(3).

3.3 This Data Processing Agreement shall apply to all the Data Processor's current and future deliveries under the Sales and Delivery Terms to all companies within Data Controller's group of companies, for whom the Data Processor processes Personal Data.

3.4 This Data Processing Agreement shall supplement and form part of the Sales and Delivery Terms. In case of any inconsistencies between this Data Processing Agreement and the Sales and Delivery Terms, this Data Processing Agreement shall prevail.

3.5 The Data Processor shall comply with the GDPR, including other applicable national Danish legislation issued according to the GDPR or as a supplement hereto.

3.6 Any Personal Data processed pursuant to this Data Processing Agreement is proprietary to the Data Controller.

3.7 The specific categories of Personal Data processed by the Data Processor under this Data Processing Agreement is set out in Appendix 1 to this Data Processing Agreement and in the Sales and Delivery Terms.

3.8 This Data Processing Agreement shall take priority over any similar provisions contained in other agreements between the Parties.

4 PRIOR SPECIFIC OR GENERAL WRITTEN AUTHORISATION

4.1 Data Processor shall process Personal Data on behalf of Data Controller and only on documented instructions from the Data Controller, unless required to do so by Union or Member State law to which the Data Processor is subject. Such instructions shall be specified in Appendix 1. The Data Controller has the right and the obligation to make decisions about the purposes and means of the processing of Personal Data.

4.2 If the Data Processor considers that any instructions from the Data Controller contravene or infringe statutory regulations, including the GDPR or other EU or applicable member state data protection provisions, the Data Processor must notify the Data Controller hereof immediately.

4.3 The Data Controller shall be responsible, among other, for ensuring that the processing of Personal Data, which the Data Processor is instructed to process, has a legal basis.

4.4 The Data Processor is not entitled to make use of Personal Data, information or otherwise provided by Data Controller, for purposes other than fulfilment of this Data Processing Agreement. The Data Processor may not use such Personal Data for historical, statistical, scientific or similar purposes, unless the data has been anonymized (and can therefore no longer be considered "Personal Data").

5 GEOGRAPHICAL LIMITATIONS

5.1 The Data Processor is not allowed to transfer, access, process or otherwise make available Personal Data in countries outside the EU/EEA, US, Pakistan or Vietnam, without prior, written approval from the Data Controller.

5.2 Any approved transfer outside of the EU/EEA shall always comply with the GDPR, chapter V.

5.3 The Data Processor is instructed and allowed to transfer, access, process or otherwise make personal data available to Pre-Approved Sub-

processorslisted in Appendix 2. Any such agreements with Pre-Approved Sub-processors outside the EU or EEA shall – prior to any transfer of data - be entered into pursuant to the EU Commission's decision of 2010/87/EU regarding the standard contractual clauses for transfer of personal data to countries outside the EU or EEA or subject to other appropriate safeguards pursuant to GDPR, Article 46, including permission from local supervisory authorities if legally required.

6 CONFIDENTIALITY

6.1 The Parties accept, both for the duration of this Data Processing Agreement and subsequently, not to disclose any Confidential Information to a Third Party. This non-disclosure obligation shall not apply to information which (a) a Party is obliged to disclose under applicable law, regulations or stock exchange rules (b) information provided to the client of the Data Controller if such information originates from or regards such client of the Data Controller or (c) information which a Party document has been created by the Party itself.

6.2 "Confidential Information" means all information of a technical, business, infra structural or similar nature, irrespective of whether this information has been documented, except for information which is or will be made available in another way than through breach of this Data Processing Agreement and all Personal Data.

6.3 The Parties shall ensure that employees and consultants who receive Confidential Information are obliged to accept a similar obligation regarding Confidential Information from the other Party and the cooperation in general in accordance with this Data Processing Agreement.

6.4 The Data Processor must further ensure that all people with access to Personal Data being processed on behalf of Data Controller are familiar with this Data Processing Agreement and are subject to the provisions of this Data Processing Agreement.

7 SECURITY MEASURES

7.1 GDPR, Article 32 stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the

rights and freedoms of natural persons, the Data Controller and Data Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

7.2 The Data Controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, including reasonably ensuring: a) Pseudonymisation and encryption of Personal Data; b) continuous confidentiality, integrity, availability and robustness of the processing systems and services for which the Data Processor is responsible; c) timely recovery of the availability of and access to Personal Data in case of a physical or technical incident; d) a procedure for regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure processing security; e) that Personal Data is not accidentally or unlawfully destroyed, lost or impaired and against any unauthorized disclosure, abuse or in any other way is processed in violation of any applicable law on Personal Data.

7.3 According to the GDPR, Article 32, the Data Processor shall also – independently from the Data Controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Data Controller shall provide the Data Processor with all information necessary to identify and evaluate such risks.

7.4 Furthermore, the Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller's obligations pursuant to the GDPR, Article 32, by inter alia providing the Data Controller with information concerning the technical and organisational measures already implemented by the Data Processor pursuant to the GDPR, Article 32 along with all other information necessary for the Data Controller to comply with the Data Controller's obligation under the GDPR, Article 32.

7.5 If subsequently – in the assessment of the Data Controller – mitigation of the identified risks require further measures to be implemented by the Data Processor, than those already implemented by the Data Processor pursuant to the GDPR, Article 32, the Data Controller shall specify these additional measures to be implemented in Appendix 3.

7.6 The Data Processor must always provide supervisory authorities and Data Controller with the necessary access to and insight into the Personal Data which is being processed and the systems used.

8 TRANSPARENT INFORMATION AND COMMUNICATION

8.1 The Data Processor must continuously report to Data Controller with the agreed contents, quality and frequency. The Data Processor must immediately inform Data Controller of any development which may significantly impair the Data Processor's current or future ability or possibility to comply with the Data Processing Agreement.

8.2 The Data Processor is obliged to inform Data Controller immediately, if the Data Processor is not able to ensure the correct processing of Data Controllers Personal Data in accordance with this Data Processing Agreement.

9 DATA SUBJECTS' RIGHTS

9.1 Data Processor shall upon request from the Data Controller, at the cost of the Data Controller and without undue delay provide all reasonable requested information and assistance to the Data Controller in regards to the Data Subject's rights on the following items: (1) processing security known to the Data Processor for any processing of Personal Data which is not provided directly by Data Processor or a Pre-Approved Sub-processors, (2) notification to the supervisory authority of any Data Security Breach, (3) notification to the Data Subject of any Data Security Breach, (4) consequential analysis of data protection and (5) preliminary hearing.

9.2 Data Processor shall also upon request from the Data Controller and at the cost of the Data Controller provide all reasonable requested information and assistance to the Data Controller in regards to the Data Subject's rights without undue delay on the following items: (1) the duty to inform when collecting Personal Data from the Data Subject, (2) the duty to inform if the Personal Data has not been collected from the Data Subject, (3) the Data Subject's right to access Personal Data, (4) the right to correct Personal Data, (5) the right to be deleted (»the right to be forgotten«), (6) the right to limitation of processing; (7) the duty to notify in connection with corrections or deletions of Personal Data or limitations in the processing activity, (8) the right to data portability and (9) the right to object for processing of Personal Data.

10 DATA SECURITY BREACH

10.1 In case of a Data Security Breach for which the Data Processor (or any Pre-Approved Sub-processor) is responsible, the Data Processor shall as soon as practical possible, inform Data Controller hereof, to enable the Data Controller to comply with the Data Controller's obligation to notify the personal data breach to the competent supervisory authority, cf. GDPR, Article 33.

10.2 This notification must at least:

a) include a description of the nature of the Data Security Breach including, if possible, the categories and the estimated number of affected Data Subjects as well as the categories and estimated number of affected registrations of Personal Data,

b) include the name of and contact information for the data protection officer (DPO) or another point of contact where further information may be obtained,

c) describe the probable consequences of the Data Security Breach,

d) describe the measures taken by the Data Processor or which the Data Processor proposes are taken in order to handle the Data Security Breach including, if relevant, measures to limit the possible consequential damages.

10.3 The Data Processor must document all Data Security Breaches, including the actual circumstances surrounding the Data Security Breach, its consequences and the remedial measures that have been taken.

10.4 This documentation must enable the regulatory authority to check that Data Processor complies with its duty to inform of any Data Security Breach.

11 USE OF SUB-PROCESSORS

11.1 The Data Processor shall meet the requirements specified in the GDPR, Articles 28(2) and 28 (4) in order to engage another processor (a sub-processor).

11.2 The Data Processor shall therefore not engage another sub-processor for the fulfilment of this Data Processing Agreement without the prior general written authorisation of the Data Controller.

11.3 The Data Processor has the Data Controller's general authorisation for the engagement of sub-processors. The Data Processor shall inform in writing the Data Controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the Data Controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix 2. The list of sub-processors already authorised by the Data Controller can be found in Appendix 2.

11.4 Where the Data Processor engages a sub-processor for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in this Data Processing Agreement shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Data Processing Agreement and the GDPR.

11.5 The Data Processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the Data Processor is subject pursuant to the Clauses and the GDPR.

11.6 A copy of such a sub-processor agreement and subsequent amendments shall – at the Data Controller's request – be submitted to the Data Controller, thereby giving the Data Controller the opportunity to ensure that the same data protection obligations as set out in this Data Processing Agreement are imposed on the sub-processor. Terms and conditions regarding business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the Data Controller.

11.7 If the sub-processor does not fulfil his data protection obligations, the Data Processor shall remain fully liable to the Data Controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in the GDPR, Articles 79 and 82 – against the Data Controller and the Data Processor, including the sub-processor.

12 DELIVERY OF PERSONAL DATA

12.1 During the term of this Data Processing Agreement, Data Controller has full access to any Personal Data being processed by the Data Processor.

12.2 If Data Controller so requests, the Data Processor is obliged to keep a back-up copy of Personal Data and additional information available in the Data Processor's systems for up to 3 months after the expiry or termination of the Data Processing Agreement. Provided such request has been made, the Data Controller may, until the expiration of such 3-month period and irrespective of the reason for the expiry of the Data Processing Agreement, request for an access to any Personal Data and additional information recorded in such back-up copy.

12.3 Data Processor may only disclose Personal Data and information to Data Controller and/or to a third party appointed by Data Controller.

12.4 The Data Processor must upon Data Controller's written instructions delete Personal Data or any information which has come to the Data Processor's possession under this Data Processing Agreement.

13 AUDIT AND INSPECTION

13.1 The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in the GDPR, Article 28, and this Data Processing Agreement and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

13.2 The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor's physical facilities on presentation of appropriate identification.

14 COOPERATION WITH THE SUPERVISORY AUTHORITY

14.1 The Data Controller and the Data Processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

15 COSTS

15.1 All costs, including costs related to revision, audit, inspection and regular implementation of measures under applicable law and to fulfil the Data Processor's obligations under this Data Processing Agreement is not included in any fees paid by to be paid by the Data Controller under the Sales and Delivery Terms and shall be paid by the Data Controller, respectively.

16 EFFECTIVE DATE AND TERMINATION

16.1 The Data Processing Agreement will enter into force on the data of the Parties' signature, i.e. the date on which both Parties have signed the Data Processing Agreement.

16.2 The Data Processing Agreement shall be effective and remain in force until the Sales and Delivery Terms are effectively terminated or expires.

16.3 Data Controller is always entitled to suspend the data processing by the Data Processor under this Data Processing Agreement.

17 CHANGES IN THE APPLICABLE DATA PROTECTION LEGISLATION

17.1 If a change in mandatory applicable data protection legislation applicable to Data Controller or to Data Processor requires Data Processor to (i) sign on to any additional documentation for mandatory data protection compliance purposes, or (ii) implement additional technical and organizational measures to the ones listed herein, or (iii) accept additional obligations to those set out herein, and such requirement mentioned in (i) - (iii) above cause additional costs or risks for Data Processor, then the Parties agree to negotiate in good faith a fair adjustment of any applicable fees.

17.2 Section 17.1 shall apply accordingly, in case (i) the Data Controller instructs Data Processor to undertake services not foreseen in this Data Processing Agreement or (ii) where mandatory applicable data protection legislation applicable to Data Controller or to Data Processor or the relevant supervisory authority imposes obligations on Data Processor in addition to those set out herein.

18 LIMITATION OF LIABILITY

18.1 The liability of the parties is regulated in accordance with the provisions of GDPR, Article 82 and, among other things, the general rules of liability and compensation under Danish law.

18.2 The Parties are each responsible for any administrative fines issued to a Party by the regulators, the purpose of which is to punish that Party for the party's breaches of the GDPR and Danish data protection legislation.

18.3 To the extent not prohibited by law, Data Processor shall in no event be liable for personal injury, or any incidental, special, indirect or consequential damages whatsoever, including, without limitation, damages for loss of profits, loss or reconstruction of data, business interruption or any other commercial damages or losses, arising out of or related to Data Controllers use or inability to use the licensed application, however caused, regardless of the theory of liability (contract, tort or otherwise) and even if Data Processor has been advised of the possibility of such damages.

18.4 In no event shall our total liability to Data Controller for all damages (including personal injury and fines) exceed the amount invoiced for each specific order under the Sales and Delivery Terms.

19 GENERAL TERMS

19.1 **Governing law and legal venue.** This Data Processing Agreement is governed by Danish law with the City Court of Copenhagen as its legal venue. United Nations Convention on Contracts for the International Sale of Goods (CISG) shall not apply to the Data Processing Agreement.

19.2 **Complete Agreement.** This Data Processing Agreement and the Sales and Delivery Terms constitute the complete and entire agreement on all terms and conditions between Data Processor and the Data Controller related to the Data Processor’s processing of Personal Data on behalf of the Data Controller.

19.3 **Amendments.** The terms of this Data Processing Agreement can only be amended by written agreement between the Parties.

Appendix 1 – Categories of Personal Data / Instruction

The purpose of the Data Processors processing of Personal Data on behalf of the Data Controller is:

Data Controller instructs the Data Processor to process the Personal Data in order for the Data Processor to provide its services to the Data Controller under the Sales and Delivery Terms.

The nature of the Data Processors processing of Personal Data on behalf of the Data Controller is:

The Data Processor's processing of Personal Data on behalf of the Data Controller shall mainly pertain to (the nature of the processing) prove SaaS services in accordance with the Sales and Delivery Terms.

The Data Processor processes the following categories of Personal Data under this Data Processing Agreement:

The Data Processor shall on behalf of the Data Controller process the following categories of personal data:

Type of personal data
Name
Address
Username
E-mail
Phone number

The Data Processor shall on behalf of the Data Controller process the following Special categories of personal data:

Type of personal data	**Yes**	**No**
Race		X
Ethnicity		X
Political orientation		X
Philosophical beliefs		X
A person who is suspected of a crime.		X
A person who is indicted for a crime		X
A person who is convicted of a crime		X
Information about a person's health, including and not limit to abuse of medicine, drugs, alcohol, etc.		X
Sexual orientation		X
Trade union membership		X
Biometric data		X
Genetical data		X

The Data Processor's processing on behalf of the Data Controller includes the following data subjects:

Customer of the Data Processor's SaaS services provided under the Sales and Delivery Terms.

The Data Processor's processing on behalf of the Data Controller has the following duration:

Personal data is stored until deleted by the Data Controller.

During the term of this Data Processing Agreement, Data Controller has full access to any Personal Data being processed by the Data Processor.

If Data Controller so requests, the Data Processor is obliged to keep a back-up copy of Personal Data and additional information available in the Data Processor's systems for up to 3 months after the expiry or termination of the Data Processing Agreement. Provided such re-quest has been made, the Data Controller may, until the expiration of such 3-month period and irrespective of the reason for the expiry of the Data Processing Agreement, request for an access to any Person-al Data and additional information recorded in such back-up copy.

Data Processor may only disclose Personal Data and information to Data Controller and/or to a third party appointed by Data Controller.

The Data Processor must upon Data Controller's written instructions delete Personal Data or any information which has come to the Data Processor's possession under this Data Processing Agreement.

Security of processing

The Data Processor shall be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The Data Processor shall however – in any event and at a minimum – implement the measures that have been agreed with the Data Controller and is further described in Appendix 3.

Assistance to the Data Controller

The Data Processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the Data Controller in accordance with Clause 8 of this Data Processing Agreement.

Instruction on the transfer of personal data to third countries

The Data Processor may transfer Personal Data to the countries stated in Appendix 2.

If the Data Controller does not subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the Data Processor shall not be

entitled within the framework of this Data Processing Agreement to perform such transfer.

Procedures for the Data Controller's audits, including inspections, of the processing of personal data being performed by the Data Processor

The Data Processor shall at the Data Controllers prior written request, and then only once a year, at the Data Controllers expense obtain an inspection report from an independent third party concerning the Data Processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of inspection report may be used in compliance with this Data Processing Agreement: ISAE 3000, type I.

The inspection report shall without undue delay be submitted to the Data Controller for information. The Data Controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the Data Controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and this Data processing Agreement.

The Data Controller or the Data Controller's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the Data Processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the Data Controller deems it required.

Appendix 2 - Pre-approved Sub-processors:

N/A

Data Processor has not been instructed to transfer data outside of the EU.

Appendix 3 – Security of Processing

1 Access to Personal Data is restricted to persons who have a material need for access to Personal Data. Personal Data will only be accessed on a "need to know" basis.

2 Employees, who handle Personal Data, are instructed and trained in what they must do with Personal Data and how to protect Personal Data.

3 There must be as few people as possible with access to Personal Data, with due regard for the operation. However, there must be a sufficient number of employees to ensure the operation of the tasks concerned in case of sickness, holidays, staff replacement, etc. Personal Data will only be accessed on a "need to know" basis.

4 Personal data on paper - for example in cartons and binders- are kept closed and locked when not in use.

5 When documents (papers, charts, etc.) are discarded, shredding and other measures are used to prevent unauthorized access to Personal Data.

6 Access codes are used to access PCs and other electronic equipment with Personal Data. Only those who need to have access will receive an access code and then only for the systems that they need to use. Those who have a password may not leave the code to others or leave it so others can see it. Checking of assigned codes must be done at least once every six months.

7 Unsuccessful attempts to access IT systems with Personal Data are detected and logged. If a specified number of consecutive rejected access attempts is detected, further tests must be blocked.

8 A responsible person to monitor such inaccessible access attempts is appointed. Taking into account the technological development, software is available that can clarify who has attempted to gain access to personal data.

9 If Personal Data is stored on a USB key, Personal data must be protected, e.g. by use of a password and encryption key. Otherwise, the USB key must be stored in a locked drawer or cabinet. Similar requirements apply to the storage of personal data on other portable data media.

10 PCs connected to the Internet shall have an updated firewall and virus control installed. When connecting to Wi-Fi, for free access, we ensure appropriate security measures taking into account the current state of technology development in the IT-area.

11 If sensitive personal data or social security numbers are sent by e-mail via the Internet, such e-mails must be encrypted. If you send Personal Data to us via email, please note that sending to us is not secure if your emails are not encrypted.

12 In connection with the repair and service of data equipment containing Personal Data and when data media are to be sold or discarded, we take the necessary measures to prevent information from being disclosed to a third party.

13 In the situations where a computer is submitted for repair and where Personal Data is stored on such computer, we establish several access codes for different sections of the personal data. For example, a repairer will not need to be able to access Personal Data that may be on the computer. Such a multi-code scheme may help - but not eliminate - the risk of misuse of Personal Data. In addition, agreement and verification should ensure that repairers do not unduly access Personal Data, for example, by using confidentiality statements.

14 When external data processing agent is used to handle Personal Data, a written data processing agreement is signed between us and the Data Processor. This applies, for example, when an external document archive is used or if cloud systems are used in the processing of personal data - including communication with the customer. In the same way, a written agreement between us and our customer is always entered into if we act as Data Processor. Data processing agreements are also available electronically.

15 Internal rules on information security exists. Internal rules on information security are adopted, that contain instructions and measures which protect Personal Data from being destroyed, lost or modified, from unauthorized disclosure, and against unauthorized access or knowledge of them. It is ensured that collected Personal Data are treated with care and protected according to applicable safety standards. There are strict security procedures for collecting, storing and transferring Personal Data in placed to prevent unauthorized access and compliance with applicable laws.

16 Necessary technical and organizational safeguards are taken to protect your Personal Data from accidental or illegal destruction, loss or change, and against unauthorized disclosure, abuse or other actions contrary to applicable law.

17 The systems are located on servers in secured premises.

18 Industry standards such as firewalls and authentication protection are used to protect your Personal Data.

19 All data transferred between client (browser and web app) and server(s) are encrypted according to the HTTPS protocol.

20 All production facilities are locked and only staff members who have signed a declaration of confidentiality have access to the production facilities. After the end of normal working hours, the production facilities are locked. Access to the production facilities is always carried out under the supervision of an employee.

21 All access to our premises is logged by electronic key or entered in the guestbook.

22 Backup of all databases and files on shared drives are taken every night. The backup is stored on an internal server, partly on an external data centre.

23 The following types of backup are taken:
a) Rolling backup. This method takes daily backup of all file and data updates and creates a backup of all new data. This creates a history of changes so that the ability to recover lost data is increased.
b) backup clone. This backup strategy creates a perfect copy of each device on the network
c) backup offsite. This backup ensures against data loss if backup is stored on site. All data and files are backed up and backup stored offsite.

24 All backup data and files are overwritten at 30-day intervals. It is not technically possible to complete deletion of individual files on a backup before such overwriting occurs. Thus, if you have request that we delete Personal Data, such Personal Data will be deleted in live environment, but will remain on backup until the specific backup is overwritten after 30 days. However, we have introduced internal processes and procedures to ensure that Personal Data is not reintroduced as live data by reloading data and files from a backup as Personal data has been deleted according to the "right to be forgotten."