Please date, sign and return this Data Processing Addendum to privacy@tsohost.com

DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**Addendum**") is executed by and between Tsohost Limited and you ("**Customer**") and is annexed to and supplements our General Terms of Service, Privacy Policy and any product specific terms (collectively, the "Terms of Service") that govern those hosted services for which we may be considered, under applicable laws, to be processors of data on your behalf. Unless otherwise defined this Addendum, all capitalised terms not defined in this Addendum will have the meanings given to them in the Terms of Service.

1. **Definitions.**

"**Covered Services**" or "**Services**" means any hosted services we offer you that could involve our Processing of Personal Data.

"**Customer Data**" means the Personal Data of any Data Subject Processed by Tsohost within the Tsohost Network on behalf of Customer pursuant to or in connection with the Terms of Service.

"**Data Controller**" means the Customer, as the entity which determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means Tsohost as the entity which Processes Personal Data on behalf of the Data Controller.

"**Data Protection Laws**" means all laws and regulations, including laws and regulations of the European Union, applicable to the Processing of Personal Data under the Agreement.

"**Data Subject**" means the individual to whom Personal Data relates.

"**EEA**" means the European Economic Area.

"**Tsohost Network**" means Tsohost's data centre facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within Tsohost's control and are used to provide the Services.

"**Personal Data**" means any information relating to an identified or identifiable person.

"**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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. "Process", "processes" and "processed" will be interpreted accordingly. Detail of Processing are set forth in Annex 1.

"**Security Incident**" either (a) a breach of security of Tsohost's Security Standards leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Customer Data; or (b) any unauthorised access to Tsohost's equipment or facilities, where in either case such access results in destruction, loss, unauthorised disclosure, or alteration of Customer Data.

"**Security Standards**" means the security standards attached to this Addendum as Annex 2.

"**Standard Contractual Clauses**" or "**SCCs**" means Annex 3, attached to and forming part of this Addendum pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the Directive. In

"**Sub-processor**" means any Data Processor engaged by Processor to Process data on behalf of Data Controller.

2. Data Processing.

2.1. **Scope and Roles.** This Addendum applies when Customer Data is processed by Tsohost. In this context, Tsohost will act as the Data Processor on behalf of the Customer and as the Data Controller with respect to Customer Data.

2.2. **Details of Data Processing.** The subject matter of processing of Customer Data by Tsohost is the performance of the Services pursuant to the Terms of Service. Customer Data will be used or otherwise Processed only to provide Customer the Covered Services, including purposes compatible with providing those services. Tsohost shall only Process Customer Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Terms of Service; (ii) Processing initiated by end users in their use of the Services; (iii) Processing to comply with other documented, reasonable instructions provided by Customers (ex. via email) where such instructions are consistent with the terms of the Agreement. Tsohost shall not be required to comply with or observe Customer's instructions if such instructions would violate the GDPR or any other applicable data privacy laws. The duration of the Processing, the nature and purpose of the Processing, the types of personal data and categories of Data Subjects Processed under this Addendum are further specified in Annex 1 ('Details of the Processing') to this Addendum.

3. **Confidentiality of Customer Data.** Tsohost will not disclose Customer Data to any government or any other third party, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends Tsohost a demand for Customer Data, Tsohost will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Tsohost may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then Tsohost will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Tsohost is legally prohibited from doing so.

4. Security

4.1. Tsohost has implemented and will maintain appropriate technical and organisational measures for the Tsohost Network as described herein this Section and which may include some or all of those measures set out in Annex 2 to this Addendum, Security Standards. In particular, Tsohost has implemented and will maintain the following technical and organisational measures that address the (i) security of the Tsohost Network; (ii) physical security of the facilities; (iii) controls around employee and contractor access to (i) and/or (ii); and (iv) processes for testing, assessing and evaluating the effectiveness of technical and organisational measures implemented by Tsohost.

4.2. Tsohost makes available a number of security features and functionalities that Customer may elect to use in relation to the Services. Customer is responsible for (a) properly configuring the Services, (b) using the controls available in connection with the Services (including the security controls) to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, (c) using the controls available in connection with the Services (including the security controls) to allow the Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident (e.g. backups and routine archiving of Customer Data), and (d) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorised access and measures to control access rights to Customer Data.

5. **Data Subject Rights.** Taking into account the nature of the Services, Tsohost offers Customer certain controls as described in the "Security" section of this Addendum that Customer may elect to use to retrieve, correct, delete or restrict use and sharing of Customer Data as described in the Services. Customer may use these controls as technical and organisational measures to assist it in connection with its obligations under applicable privacy laws, including its obligations relating to responding to requests from Data Subjects. As commercially reasonable, and to the extent lawfully required or permitted, Tsohost shall promptly notify Customer if Tsohost directly receives a request from a Data Subject to exercise such rights under any applicable data privacy laws ("Data Subject Request"). In addition, where Customer's use of the Services limits its ability to address a Data Subject Request, Tsohost may, where legally permitted and appropriate and upon Customer's specific request, provide commercially reasonable assistance in addressing the request, at Customer's cost (if any).

6. **Sub-processing.**

6.1. Authorised Sub-processors. Customer agrees that Tsohost may use Sub-processors to fulfil its contractual obligations under its Terms of Service and this Addendum or to provide certain services on its behalf, such as providing support services. Customer hereby consents to Tsohost's use of Sub-processors as described in this Section. Except as set forth in this Section or as otherwise explicitly authorised by you, Tsohost will not permit any other sub-processing activities.

6.2. Sub-processor Obligations.

(i) Where Tsohost authorises any Sub-processor as described in Section 6.1: Tsohost will restrict the Sub-processor's access to Customer Data only to what is necessary to maintain the Services or to provide the Services to Customer and any End Users in accordance with the Services. Tsohost will prohibit the Sub-processor from accessing Customer Data for any other purpose;

(ii) Tsohost will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor is performing the same data processing services that are being provided by Tsohost under this Addendum, Tsohost will impose on the Sub-processor the same contractual obligations that Tsohost has under this Addendum; and

(iii) Tsohost will remain responsible for its compliance with the obligations of this Addendum and for any acts or omissions of the Sub-processor that cause Tsohost to breach any of Tsohost's obligations under this Addendum.

6.3. **New Sub-Processors.** From time to time, we may engage new Sub-processors under and subject to the terms of this Addendum. In such case, we will provide 60 days advance notice (via our website and email) prior to any new Sub-processor obtaining any Customer Data. If you Customer does not approve of a new Sub-processor, then Customer may terminate the Services which are subject to this Addendum without penalty by providing, within 10 days or receipt of notice from us, written notice of termination that includes an explanation of the reasons for your non-approval. If the Services covered by this Addendum are part of a bundle or bundled purchase, then any termination will apply to its entirety.

7. **Security Breach Notification.**

7.1. **Security Incident.** If Tsohost becomes aware of a Security Incident, Tsohost will without undue delay: (a) notify Customer of the Security Incident; and (b) take reasonable steps to mitigate the effects and to minimise any damage resulting from the Security Incident.

7.2. **Tsohost's Assistance.** To assist Customer in relation to any personal data breach notifications Customer is required to make under any applicable privacy laws, Tsohost will include in the notification under section 8.1 such information about the Security Incident as Tsohost is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to Tsohost and any restrictions on disclosing the information, such as confidentiality.

7.3. **Failed Security Incidents.** Customer agrees that:

(i) A failed Security Incident will not be subject to the terms of this Addendum. A failed Security Incident is one that results in no unauthorised access to Customer Data or to any of Tsohost's Network, equipment, or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-

on attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers) or similar incidents; and

(ii) Tsohost's obligation to report or respond to a Security Incident under this Section is not and will not be construed as an acknowledgement by Tsohost of any fault or liability of Tsohost with respect to the Security Incident.

7.4. **Communication.** Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means Tsohost selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the Tsohost management console and secure transmission at all times.

8. Customer Rights.

8.1. Independent Determination. Customer is responsible for reviewing the information made available by Tsohost relating to data security and its Security Standards and making an independent determination as to whether the Services meets Customer's requirements and legal obligations as well as Customer's obligations under this Addendum. The information made available is intended to assist Customer in complying with Customer's obligations under applicable privacy laws, including the GDPR, in respect of data protection impact assessments and prior consultation.

8.2. **Customer Audit Rights.** Customer has the right to confirm Tsohost's compliance with this Addendum as applicable to the Services, including specifically Tsohost's compliance with its Security Standards, by exercising a reasonable right to conduct an audit or inspection, including under the Standard Contractual Clauses if they apply, by making a specific request to Tsohost in writing to the address set forth in its Terms of Service. If Tsohost declines to follow any instruction requested by Customer regarding a properly requested and scoped audit or inspection, Customer is entitled to terminate this Addendum and the Terms of Service. If the Standard Contractual Clauses apply, nothing in this Section varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses. This Section will also apply insofar as the supplier carries out the control of his Sub-processors on behalf of the client.

9. Transfers of Personal Data.

9.1. **U.S. Based Processing.** Customer Data will be transferred within and outside the EEA and processed in the United States.

9.2. **Application of Standard Contractual Clauses.** The Standard Contractual Clauses will apply to Customer Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognised by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR). The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses will not apply where the data is transferred in accordance with a recognised compliance standard for the lawful transfer of personal data (as defined in the GDPR) outside the EEA, such as the EU-US and Swiss-U.S. Privacy Shield Frameworks.

10. **Termination of the Addendum.** This Addendum will continue in force until the termination of the Terms of Service (the "**Termination Date**"), though obligations with regard to its provisions will survive and continue for such time as we continue to process data on your behalf.

11. **Return or Deletion of Customer Data**. The Services provide Customer with controls that Customer may use to retrieve or delete Customer Data as described in the Services. Any deletion of Customer Data shall be governed by the terms of the particular Services.

12. **Limitations of Liability**. The liability of each party under this Addendum will be subject to the exclusions and limitations of liability set out in the Terms of Service. Customer agrees that any regulatory penalties incurred by Tsohost in relation to the Customer Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this Addendum and any applicable privacy laws will count towards and reduce Tsohost's liability under the Terms of Service as if it were liability to the Customer under the Terms of Service.

13. **Entire Terms of Service; Conflict**. This Addendum supersedes and replaces all prior or contemporaneous representations, understandings, agreements, or communications between Customer and Tsohost, whether written or verbal, regarding the subject matter of this Addendum, including any data processing addenda entered into between Tsohost and Customer with regard to the processing of personal data and on the free movement of such data. Except as amended by this Addendum, the Terms of Service will remain in full force and effect. If there is a conflict between any other agreement between the parties including the Terms of Service and this Addendum, the terms of this Addendum will control.

Executed on _____ by:

Customer Name: _____

Signed: _____

Customer Representative Name: _____

Position: _____

Tsohost Limited

Signed: 

Sara Rego

Brand Director

Please date, sign and return this Data Processing Addendum to privacy@tsohost.com

Annex 1

DETAILS OF THE PROCESSING

1. **Nature and Purpose of Processing.** Tsohost will Process Personal Data as necessary to perform the Services pursuant to the Terms of Service, product-specific agreements, and as further instructed by Customer throughout its use of the Services.

2. **Duration of Processing.** Subject to Section 12 of this Addendum, Tsohost will Process Personal Data during the effective date of the Terms of Service, but will abide by the terms of this Addendum for the duration of the Processing if in excess of that term, and unless otherwise agreed upon in writing.

3. **Categories of Data Subjects.** Customer may upload Personal Data in the course of its use of the Services, the extent to which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:
   - Prospects, customers, business partners and vendors of Customer (who are natural persons)
   - Employees or contact persons of Customer's prospects, customers, business partners and vendors
   - Employees, agents, advisors, freelancers of Customer (who are natural persons)
   - Customer's Users authorised by Customer to use the Services

4. **Type of Personal Data.** Customer may upload Personal Data in the course of its use of the Services, the type of and extent to which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data of Data Subjects:
   - Name
   - Address
   - Telephone number
   - Date of birth
   - Email address
   - Other data collected that could directly or indirectly identify you.

Annex 2

Security Standards

Technical and Organisational Measures

We are committed to protect our customers' information. Taking into account the best practices, the costs of implementation and the nature, scope, circumstances and purposes of processing as well as the different likelihood of occurrence and severity of the risk to the rights and freedoms of natural persons we take the following technical and organisational measures (TOM). When selecting the measures the confidentiality, integrity, availability and resilience of the systems are considered. A quick recovery after a physical or technical incident is guaranteed.

Data Privacy Program

Our Data Privacy Program is established to maintain a global data governance structure and secure information throughout its lifecycle. This program is driven by the office of the data protection officer, which oversees the implementation of privacy practices and security measures. We regularly test, assess and evaluate the effectiveness of our Data Privacy Program and Security Standards.

1. Confidentiality

"Confidentiality means that personal data is protected against unauthorised disclosure."

We use a variety of physical and logical measures to protect the confidentiality of its customers' personal data. Those measures include:

Physical Security

- Physical access control systems in place (Badge access control, Security event monitoring etc.)
- Surveillance systems including alarms and, as appropriate, CCTV monitoring
- Clean desk policies and controls in place (Locking of unattended computers, locked cabinets etc.)
- Visitor Access Management
- Destruction of data on physical media and documents (shredding, degaussing etc.)

Access Control & Prevention of Unauthorised Access

- User access restrictions applied, and role-based access permissions provided/reviewed based on segregation of duties principle
- Strong authentication and authorisation methods (Multi-factor authentication, certificate based authorisation, automatic deactivation/log-off etc.)
- Centralised password management and strong/complex password policies (minimum length, complexity of characters, expiration of passwords etc.)
- Controlled access to e-mails and the Internet
- Anti-virus management
- Intrusion Prevention System management

Encryption

- Encryption of external and internal communication via strong cryptographic protocols
- Encrypting PII/SPII data at rest (databases, shared directories etc.)
- Full disk encryption for company PCs and laptops
- Encryption of storage media
- Remote connections to the company networks are encrypted via VPN
- Securing the lifecycle of encryption keys

Data Minimisation

- PII/SPI minimisation in application, debugging and security logs

- Pseudonymisation of personal data to prevent directly identification of an individual
- Segregation of data stored by function (test, staging, live)
- Logical segregation of data by role based access rights
- Defined data retention periods for personal data

Security Testing

- Penetration Testing for critical company networks and platforms hosting personal data
- Regular network and vulnerability scans

2. **Integrity**

"Integrity refers to ensuring the correctness (intactness) of data and the correct functioning of systems. When the term integrity is used in connection with the term "data", it expresses that the data is complete and unchanged."

Appropriate change and log management controls are in place, in addition to access controls to be able to maintain the integrity of personal data such as:

Change & Release Management

- Change and release management process including (impact analysis, approvals, testing, security reviews, staging, monitoring etc.)
- Role & Function based (Segregation of Duties) access provisioning on production environments

Logging & Monitoring

- Logging of access and changes on data
- Centralised audit & security logs
- Monitoring of the completeness and correctness of the transfer of data (end-to-end check)

3. **Availability**

"The availability of services and IT systems, IT applications, and IT network functions or of information is guaranteed, if the users are able to use them at all times as intended."

We implement appropriate continuity and security measures to maintain the availability of its services and the data residing within those services:

- Regular fail-over tests applied for critical services
- Extensive performance/availability monitoring and reporting for critical systems
- Incident response programme
- Critical data either replicated or backed up (Cloud Backups/Hard Disks/Database replication etc.)
- Planned software, infrastructure and security maintenance in place (Software updates, security patches etc.)
- Redundant and resilient systems (server clusters, mirrored DBs, high availability setups etc.) located on off-site and/or geographically separated locations
- Use of uninterruptible power supplies, fail redundant hardware and network systems
- Alarm, security systems in place
- Physical Protection measures in place for critical sites (surge protection, raised floors, cooling systems, fire and/or smoke detectors, fire suppression systems etc.)
- DDOS protection to maintain availability
- Load & Stress Testing

4. **Data Processing Instructions**

"Data Processing Instructions refers to ensuring that personal data will only be processed in accordance with the instructions of the data controller and the related company measures"

We have established internal privacy policies, agreements and conduct regular privacy trainings for employees to ensure personal data is processed in accordance with customers' preferences and instructions.

- Privacy and confidentiality terms in place within employee contracts
- Regular data privacy and security trainings for employees
- Appropriate contractual provisions to the agreements with sub-contractors to maintain instructional control rights
- Regular privacy checks for external service providers
- Providing customers full control over their data processing preferences

Regular security audits

[See Section 9.2 of the Addendum for applicability of these SCCs]

Annex 3

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity identified as "Customer" in the Addendum
(the "**data exporter**")

and

<third party address>
<third party address>.
(the "**data importer"**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the sub-processor'* means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[1]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

---

1 Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/ EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all enquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data

subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/ or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data

importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter

The data exporter is the entity identified as “Customer” in the Addendum

Data importer

The data importer is Tsohost, a provider of hosted services.

Data subjects

The processing operations are defined in Section 1.3 and Annex 1 of the Addendum.

Categories of data

The processing operations are defined in Section 1.3 and Annex 1 of the Addendum.

Processing operations

The processing operations are defined in Section 1.3 and Annex 1 of the Addendum.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses. By purchasing Services from Tsohost, the Addendum and this Appendix 2 are deemed accepted and executed by and between the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The technical and organisational security measures implemented by the data importer are as described in the Addendum, specifically in Annex 2, which is incorporated and attached to it.