PRIVACY POLICY

This data processing agreement (hereinafter referred to as "**Agreement**") forms part of the Contract for Cloud Services ("**Principal Agreement**") between

You (hereinafter referred to as the "**Customer**" or "**Controller**"),

And,

OneSource Cloud Corporation, registered at 900 N Dorothy Dr Richardson, TX 75081 (hereinafter referred to as "**OneSource Cloud**" or "**Processor**"),

(respectively referred to as "**Party**" , jointly referred to as "**Parties**").

Whereas,

(1) In accordance with Principal Agreement signed between Customer and OneSource Cloud, Parties agree to cooperate on Principal Agreement and the products and services further agreed in this Agreement;

(2) In the course of the relevant cooperation, Parties agreed to access to, process and protect personal data in compliance with REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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 referred to as "**the GDPR**") and other applicable laws and regulations on data protection (hereinafter collectively referred to as "**Data Protection Rules**"); and

(3) The terms and definitions in this Agreement have the same meaning as under the **GDPR.**

It is agreed by Parties as follows:

1. Scope, Duration and content of this Agreement

1.1. Scope

Processor processes the personal data on behalf of Controller. This Agreement covers all data protection related matters between Controller and Processor.

1.2. Duration

The duration of this Agreement corresponds to the duration of Principal Agreement.

1.3. Scope, nature and purpose of the intended data processing

Detailed description of the subject of the Agreement with regard to scope, nature and purpose of processor tasks:

- Provision of Cloud Related service;
- Provision of remote operation and maintenance services and technical support.

1.4. Location of data processing

The provision of the contractually agreed data processing can take only in European.
Any relocation to a third country is subject to the clauses in Appendix II and Appendix III STANDARD CONTRACTUAL CLAUSES (PROCESSORS) pursuant to Commission Decision of 5 February 2010 (2010/87/EU) (hereinafter referred to as "**the Clauses**") and requires the prior notification to Controller and may only take place if the special requirements set forth in art. 44 GDPR are met.

1.5. Type of personal data

The following data types are subject of the processing of personal data:
Customer determines the categories of data per Cloud Service subscribed. Customer can configure the data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. The personal data to be processed typically include the following categories of data: name, phone numbers, email address, time zone, address data, system access / usage / authorization data, company name, contract data, billing data, plus

any application-specific data that authorized users enter into the Cloud Service and may include bank account data, credit or debit card data.

1.6. Categories of data subjects

The categories of persons affected by processing include: employees, contractors, business partners or ot her individuals having personal data stored in the Cloud Service.

2. Rights and obligations of Parties

2.1 Controller's obligations / right to control

2.1.1. In the context of the contractual relationship between Customer, acting as Controller, and Processor, Customer is solely responsible for assessing the legal admissibility of the processing to be performed by Processor with regard to GDPR provisions and other rules on data protection.

2.1.2. Customer has the right to carry out inspections in consultation with Processor or to have them carried out by an examiner to be named on a case-by-case basis. Customer moreover has the right to verify that Processor complies with this Agreement in his business. The execution of such random checks shall be announced on reasonable notice. Processor shall ensure that Customer can convince himself of Processor´s compliance with regard to all of the latter´s obligations in accordance with art. 28 GDPR.

Upon request, Processor undertakes to provide Customer with all necessary information, what particularly applies to evidence on the implementation of appropriate technical and organizational measures and obligations agreed upon in this Agreement by suitable means.

The demonstration of such measures, which do not only concern the concrete order/agreement, is feasible in any of the following ways:

- Compliance with a code of conduct in accordance with art. 40 GDPR;
- Certification according to an approved certification procedure in accordance with art. 42 GDPR;
- Current certificates, reports or statements issued by independent bodies (e.g. privacy or auditors, accountants, data protection
- officers, IT security department);
  Appropriate certification through IT-security or privacy audits such as e.g.ISO 27001.

Processor shall be entitled to seek compensation for providing Controller with the opportunity to execute his controls.

2.1.3. Processor is obliged to inform Controller in a timely manner, once Processor finds any errors or irregularities regarding Data Protection Rules in the context of Principal Agreement.

2.2. Processor's obligations

In addition to compliance with the provisions of this Agreement, each Party has to comply with statutory obligations set forth in the GDPR. In particular, Processor has to make sure his compliance with the following issues:

2.2.1. Written appointment of a data protection officer, if required by law. The following person has been appointed as Processor's data protection officer:
Han Xuguang,with email address sales@onesourcecloud.net.
Any changes with regard to the appointment of a data protection officer and the latter's contact details must be communicated to Controller in a timely manner.

2.2.2. Confidentiality pursuant to the GDPR is guaranteed. Processor confirms that any staff has been obliged to maintain confidentiality in written. Such obligation shall be designed to outlast the termination of this Agreement.

2.2.3. Processor undertakes to implement and comply with all technical and organizational measures required for the Order in accordance with the GDPR [see Appendix I for details].

2.2.4. Concerning the performance of their duties under applicable data protection regulations, Controller and Processor will cooperate

upon request of the supervisory authority.

2.2.5. Processor undertakes to control his internal processes as well as the technical and organizational measures on a regular basis in order to ensure that any processing within his responsibility is performed according to the requirements of the applicable rules on data protection and ensure that the protection of the rights of data subjects is guaranteed at any time.

2.2.6. Unless Processor is obliged to data processing by European Union law or by local laws to which Processor is subject (e.g. investigations by law enforcement units or authorities), Processor will only process Controller's personal data in accordance with contractually specified conditions and Controller's specific individual instructions.
In such a case, Processor shall inform Controller of these legal requirements prior to processing, unless the law prohibits such communication because of an important public interest or further legal reason Processor is obliged to comply with.
Processor shall not process data for any other purposes and is not entitled to forward them to third parties.
Processor shall inform Controller if he considers an instruction as violating applicable law in a timely manner. Processor may suspend the execution of the instruction only until it has been confirmed or changed by Controller's authorized personnel/representative where Controller shall bear any risk and cost from the execution of any such instruction turning out to be illegal.

2.2.7. Processor is obliged to provide Controller with information upon Controller's written request as far as Controller's data and documents are concerned.

2.2.8. Processor shall keep records of processing activities in accordance with art. 30 para.2 of the GDPR and makes them available upon Controller's request. Controller provides Processor with necessary information required for this purpose. Processor moreover supports Controller in preparing the necessary data processing record required under art. 30 para. 1 of the GDPR.

2.2.9. Processor shall assist Controller in complying with any obligation set forth in art. 32 to 36 of the GDPR.

2.2.10. Processor may seek compensation for any supportive action he performs in favor of Controller if such action is not part of the contractual duties of Processor and when such action does not have to be performed as consequence of any misbehavior of Processor in regard of this Agreement.

2.2.11. Processor must inform Controller of any actions and measures of supervisory authorities in a timely manner, as far as such relate to orders subject to this Agreement. This also applies in case that a competent authority initiates any administrative or criminal proceedings against Processor in regard of any dataprocessing activities carried out by Processor.
Any additional costs arising at Processor's as consequence of the aforementioned actions shall be borne by Controller.

3. Return and deletion

3.1. For the data involved under this Agreement, Parties are legally able to claim relevant interests in the use of the data. Neither Party may create a copy of the data without the knowledge of the other Party, except in the following cases: 1) a backup copy necessary to ensure accuracy of data processing, and 2) a copy required to comply with the legal retention period.

3.2. At the termination of this Agreement, either Party is required to: 1) return the file and data processing (data usage) results (including data held or processed by its own appointed processor) of which it does not but the other Party has data usage rights; or, 2) After obtaining the consent from the other Party, delete the relevant data of which it does not but the other Party has the data usage rights. This paragraph also applies to all data and related materials used in the testing phase, as well as those that are discarded after processing.

3.3. Within **Fifteen (15) Days** of the termination of this Agreement, one Party shall providethe other Party with a written statement that he has deleted, anonymized or returned and retained no copies of the personal data that one Party has the right to claim, except for the retention period required by law. In this case, one Party is committed to ensuring the confidentiality of the transmitted personal data and only processing such personal data in compliance with legal obligations.

3.4. Parties shall keep documentation that provides relevant evidence of orderly and proper data processing in accordance with respective retention periods even beyond the end of this Agreement.

4. Sub-contractual relations

4.1. Processor may employ following other processors (hereinafter referred to as "**Subprocessor**")for the purpose of providing certain services respectively:

- Equinix, providing providing physical devices in the data center located in Germany and related services; and

- Globalswitch, providing physical devices in the data center located in the Netherlandsand related services.

4.2. Prior to employing further or replacing existing Sub-processors listed above, Processor shall inform Controller in due time, in writing.

4.3. Controller may – for important data protection reasons – object to such changes within a reasonable period of time (no longer than **Two (2) Weeks**) and appeal to the body Processor specified. If there is no objection within the deadline, acceptance of change is considered given.

In exceptional cases an agreement in the aftermath shall be possible. Processor then shall inform Controller about the exchange of a Sub-processor in a timely manner.

4.4. If Sub-processor provides agreed service(s) outside the EU/EEA, Controller and Processor shall ensure compliance in terms of data protection by taking appropriate measures.

4.5. Any further outsourcing by Sub-processor requires Controller's written explicit consent;any contractual provisions with regard to data protection within the contractual chain must also be imposed on the further Sub-processor to ensure data protection requirements are met.

4.6. Subcontracting in the sense of Agreement always refers to services that directly relate to the provision of the main service. This does not include other services provided by Processor, such as the disposal of data carriers and other measures with the aim to ensure confidentiality, availability, integrity and resilience of hard- and soft- ware of data processing systems. **However, Processor shall be obliged to hold appropriate and legally compliant contractual agreements and control measures for outsourced ancillary services in order to guaranteeing data protection and data security of Controller's data.**

5. Instructions

Data processing conducted by Processor is carried out exclusively within the framework of the agreements made and according to Controller instructions. Controller shall generally issue all instructions and orders in writing. Within the framework of this Agreement, Controller shall make explicit instructions regarding type, scope and procedure of data processing, and provide for individual/detailed instructions as appropriate. Changes to the scope of processing of this Agreement must be jointly agreed and documented in writing. Without a written confirmation, Processor shall not be deemed to have received any verbal instructions and shall not be liable for failure to comply with such instructions.

6. Data subject rights

6.1. Processor may not correct, delete or restrict the processing of the data processed on behalf of Controller unless a corresponding and written instruction has been issued by Controller. In the event that a data subject directly addresses Processor in this regard, Processor must forward such request to Controller in a timely manner.

6.2. Controller shall compensate for any additional cost arising from Processor's contribution to measures as under section 6.1.

7. Technical and organizational measures

7.1. Processor must ensure security according to art. 28 para. 3 of the GDPR. The actions to be taken consist of data security measures and measures that shall guarantee a level of protection commensurate with the risk as regards confidentiality, integrity, availability and resilience of systems.

7.2. Processor shall implement technical and organizational measures, or alternative adequate measures of which safety level shall be equivalent to specified measures provided in this Agreement. Significant changes to technical and organization measures taken by Processor shall be documented.

7.3. As far as the security measures taken by Processor do not meet Controller's requirements, he shall inform Controller in a timely manner.

7.4. In the event of a security breach, Processor should provide Controller with the following details within **Seventy-two (72) Hours** of the discovery of the security breach: type of violation; nature of the affected personal data, sensitivity and quantity; personal recognition; the severity of the consequences for an individual (e.g. physical injury, psychological distress, humiliation or reputation damage); a list of data subjects affected by security breaches (provided when available), including contact information; the type and approximate number of relevant data subjects and the categories and approximate quantities of relevant personal data records; the consequences that Controller may face due to personal data breaches suffered by Processors and/or cooperating third parties; Measures taken or proposed to mitigate impacts and minimize any damage caused by security breaches.

8. Liability

Violation of the applicable data protection laws and regulations or the obligations stipulated in this Agreement shall be subject to the corresponding liabilities in accordance with Principal Agreement and this Agreement; if there is no corresponding provisions under Principal Agreement and this Agreement, the applicable data protection laws and regulations shall apply.

9. Miscellaneous

9.1. Changes and amendments to this Agreement and all of its components shall be made in writing.

9.2. In the event of any disagreement or inconsistency between this Agreement and Principal Agreement and/or the provisions of other agreements between the Parties, the data protection obligations of the Parties shall be governed by the provisions of this Agreement. Meanwhile, if there is any doubt as to whether the terms of these other agreements involve data protection obligations of both Parties, this Agreement shall prevail.

9.3. Any liability arising out of or in connection with a breach of this Agreement shall be governed by the terms on liability contained in Principal Agreement, except as otherwise provided in this Agreement.

9.4. Any ineffectiveness of individual parts of Agreement does not affect the validity of Agreement as such. Parties shall replace the ineffective provision by a valid provision of the content closest possible to the initial intent of Parties.

9.5. Representative in European Union：sales@onesourcecloud.net

Appendix I to the Agreement, if applicable, the STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

– Security Measures Implemented by Processor

Description of technical and organizational security measures implemented by Processor (andhis cooperating third parties):

Taking into account the technical development, the cost of implementation, nature, scope, background and purpose, as well as the likelihood and severity of the rights and freedoms of natural persons, especially in view of the risks arising from data processing operations (these operations may result in transmission, storage, or accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data) The data processor shall perform the following technical and organizational measures for assessing the appropriate level of security of data processed in accordance with the definitions of this Agreement.

1. Pseudonymisation and Encryption

The following measures should be implemented to perform pseudonymisation of personal data:

- Data are stored on the back-end virtualized platform under the name of the cloud host.
- All the files corresponding to the Cloud host are stored in the form of block storage on the back-end. In extreme cases, even if the data are stolen, the customer data cannot be inverted to obtain Customer’s data.
- Other.

2. Confidentiality of processing system and corresponding service

The following measures should be implemented to address the confidentiality of the processing system and related services:

- No one but personnel from OneSource Cloud may login to the management platform which is built and managed purely on intranet.
- All of the computer room are locked and the key is kept by certain room manager.
- Anyone who aims to enter the computer room has to apply for authorization from OneSource Cloud prior to entering the computer room.
- All equipment in the computer room are protected against illegal access. Without operation by backstage personnel, data stored in the online equipment cannot be accessed.
- Other.

3. Integrity of processing system and corresponding service

The following measures should be implemented to address the integrity of the processing system and related services:

- For the OneSource Cloud platform system, the operation and maintenance personnel must be authorized by multiple parties to operate the customer cloud host.
- OneSource Cloud has a monitoring system for all configurations, which documents every step of the background operator's operations in details.
- Other.

4. Availability of processing system and corresponding service

The following measures should be implemented to address the integrity of the processing system and related services:

- All hardware devices of the OneSource Cloud platform system are of the hot standby structure, which will not affect the Customer cloud host when hardware and software problems occur.
- For the OneSource Cloud platform system, the operation and maintenance personnel must beauthorized by multiple parties to operate the customer cloud host.
- Other.

5. Resilience of processing systems and related services

The following measures should be implemented to address the resiliency of the processing system and related services:

- OneSource Cloud platform computing adopts cluster mode, which can expand the planningunit at any time.
- The OneSource Cloud storage platform is built on bank security storage devices with sufficient capabilities in data processing and data storage.
- Other.

6. Ability to restore the provision and access of personal data in a timely manner in the event

The following measures should be implemented to enable timely recovery of the provision and access of personal data in the event of physical or technical events:

- Multi-group RAID group mode, which has spare disks in the group
- Backup of RAID group.

- Other.

7. Regularly testing, evaluating and assessing the effectiveness of technical and organizational measures

The following measures should be implemented to achieve the effectiveness of periodic testing, evaluation and assessment of technical and organizational measures:

- Assessment conducted by Data Protection Officer
- External evaluation, review, certification
- Other

Appendix II to the Agreement, if applicable, the STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

Data Exporter

The Data Exporter is the Customer who subscribed to a Cloud Service that allows authorized users to enter, amend, use, delete or otherwise process Personal Data. Where Customer allows other controllers to also use the Cloud Service, these other controllers are also Data Exporters.

Data Importer

OneSource Cloud and its Sub-processors provide Cloud Service that includes types of services provided under Principal Agreement.

Data Subjects

Unless provided otherwise by Data Exporter, transferred personal data relates to the following categories of data subjects: employees, contractors, business partners or other individuals having personal data stored in Cloud Service.

Data Categories

The transferred personal data concerns the categories of data stated in section 1.5 of the Agreement.

Special Data Categories (if appropriate)

The transferred personal data concerns the following special categories of data: As set out in the Agreement if any.

Processing Operations / Purposes

The transferred personal data is subject to the following basic processing activities:

- ☐ use of Personal Data to set up, operate, monitor and provide Cloud Service (including

operational and technical support);

- ▢ storage of personal data in dedicated data centers (multi-tenant architecture); upload any fixes or upgrades to Cloud Service;
- ▢ back up of personal data;
- ▢ computer processing of personal data, including data transmission, data retrieval, data access;
- ▢ network access to allow personal data transfer;

execution of instructions of Customer in accordance with the Agreement.

Appendix III STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of art. 46 (2) the GDPR for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Customer

(in the Clauses hereinafter referred to as "**Data Exporter**"),

And,

OneSource Cloud

(in the Clauses hereinafter referred to as "Data Importer"),

(each a "**Party**", together "**Parties**"),

HAVE AGREED on 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 Data Exporter to Data Importer of the personal data specified in Appendix II.

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 the GDPR;

(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 art. 44 GDPR;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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 II which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against 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 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 Data Exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of 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 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

Data Exporter and 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 Data Exporter by contract or by operation of law s a result of which it takes on the rights and obligations of 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 Data Exporter

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 Data Importer to process the personal data transferred only on Data Exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that Data Importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix I 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

(a) informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted toa third country not providing adequate protection within the meaning of the GDPR;

(g) to forward any notification received from Data Importer or any Sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if 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 I, 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 Data Importer under the Clauses; and

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

Clause 5

Obligations of Data Importer

Data Importer agrees and warrants:

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

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from 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 Data Exporter as soon as it is aware, in which case 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 I before processing the personal data transferred;

(d) that it will promptly notify 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 inquiries from 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 Data Exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by 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 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 I 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 Data Exporter;

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

(i) that the processing services by 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 Data Exporter.

Clause 6

Liability

1. Parties agree that any data subject, who has suffered damage as a result of any breach of theobligations referred to in Clause 3 or in Clause 11 by any Party or

or Sub-processor is entitled to receive compensation from 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 Data Exporter, arising out of a breach by Data Importer or his Sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because Data Exporter has factually disappeared or ceased to exist in law or has become insolvent, Data Importer agrees that the data subject may issue a claim against Data Importer as if it were Data Exporter, unless any successor entity has assumed the entire legal obligations of Data Exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. 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 Data Exporter or Data Importer referred to in paragraphs 1 and 2, arising out of a breach by Sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both Data Exporter and 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 Sub-processor with regard to its own processing operations under the Clauses as if it were Data Exporter or Data Importer, unless any successor entity has assumed the entire legal obligations of 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. Data Importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, 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 thesupervisory authority;

   (b) to refer the dispute to the courts in the Member State in which Data Exporter is established.

2. he 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. 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 Data Exporter under the applicable data protection law.

3. Data Importer shall promptly inform Data Exporter about the existence of legislation applicable to it or any Sub-processor preventing the conduct of an audit of Data Importer, or any Subprocessor, pursuant to paragraph 2. In such a case 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 Data Exporter is established.

Clause 10

Variation of the contract

Variation of the contract Parties undertake not to vary or modify the Clauses. This does not preclude Parties from adding clauses on business related issues where required as

long as they do not contradict the Clause.

Clause 11

Sub-processing

1. Data Importer shall not subcontract any of its processing operations performed on behalf of Data Exporter under the Clauses without the prior written consent of Data Exporter. Where Data Importer subcontracts its obligations under the Clauses, with the consent of Data Exporter, itshall 17 / 17 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 Data Importer under the Clauses. Where the Sub-processor fails to fulfill its data protection obligations under such written agreement Data Importer shall remain fully liable to Data Exporter for the performance of the Sub-processor's obligations under such agreement.
2. The prior written contract between 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 Data Exporter or 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 Data Exporter or Data Importer by contract or by operation of law. Such third-party liability of the Sub-processorshall 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 Data Exporter is established.
4. Data Exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by Data Importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to Data Exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing

1. The parties agree that on the termination of the provision of data-processing services, Data Importer and the Sub-processor shall, at the choice of Data Exporter, return all the personal data transferred and the copies thereof to Data Exporter or shall destroy all the personal data and certify to Data Exporter that it has done so, unless legislation imposed upon Data Importer prevents it from returning or destroying all or part of the personal data transferred. In that case, 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. Data Importer and the Sub-processor warrant that upon request of Data Exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in para. 1.