Invoicera
DATA PROCESSING AGREEMENT

www.invoicera.com (collectively, “Invoicera” or “Service Provider”) and the undersigned entity (“ Customer”) have entered into a commercial engagement (“Agreement”), where the Service Provider is providing the Customer with services and/or products. Now hereby this data processing agreement (“DPA”) to the Agreement governs the parties’ data processing and related obligations. The parties further agree that this DPA is incorporated by reference into, and made a binding part of, the Agreement. References to the Agreement shall include the Agreement as modified by this DPA, and to attachments or other documents governed by it. This DPA shall govern and if the event of any conflict between the terms in the DPA and in the Agreement, this DPA shall take precedence and therefore control and govern the parties’ obligations with regard to the matters addressed herein. All other terms not governed by the DPA are governed by the Agreement.

1. SUBJECT OF THE AGREEMENT

1.1. Pursuant to the Agreement, the Service Provider provides certain services to the Customer (“Services”).

1.2. In the course of providing the Services by the Service Provider pursuant to the Agreement, the Service Provider may process Protected Data (as defined herein) on behalf of the Customer.

1.3. The parties agree to comply with the provisions of this DPA with respect to the processing of any and all Protected Data collected by the Service Provider on behalf by the Customer in relation to the provision or receipt of the Services, including Protected Data processed under the European Union General Data Protection Regulation (GDPR) (EU) 2016/679.

2. DEFINITIONS

2.1. “Appropriate Safeguard” means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time.

2.2. “Customer Users” means the data subjects set out in Annex 2 (as amended from time to time).
2.3. “Data Subject Request” means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws.
2.4. “Data Protection Laws” means any and all applicable laws, codes and regulations as applicable to, or enforceable against, the Service Provider and the Customer in respect of the Services from time to time including but not limited to: (i) the Regulation; (ii) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) the Swiss Federal Act on Data Protection.

2.5. “EEA” means the European Economic Area.

2.6. “Personal Data”, “process/processing”, “Data Controller”, “Data Processor”, “Data Subject” and “Sub-Processor” shall have the same meaning as in the Data Protection Laws.

2.7. “Personal Data Breach” means any actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Protected Data.

2.8. “Protected Data” means Personal Data relating to the Customer Users and which is disclosed at any time to the Service Provider or Sub-Processors by or on behalf of the Customer in connection with this DPA and/or the Agreement.

2.9. “Regulation” means the General Data Protection 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.

2.10. “Standard Contractual Clauses” means Annex 3 to this DPA 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 which do not ensure an adequate level of data protection.

2.11. “Supervisory Authority” means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws.

In this DPA:

2.12. references to any Data Protection Laws and to terms defined in such Data Protection Laws shall be replaced with or incorporate (as the case may be) references to any Data Protection Laws replacing, amending, extending, re-enacting or consolidating such Data Protection Laws from time to time and the equivalent terms defined therein.

3. ROLES OF THE PARTIES

3.1. Unless specifically agreed in writing by the parties, the parties acknowledge and agree that with regard to the processing of Personal Data, the Service Provider is the Data Processor, the Customer is a Data Controller and that any subcontractors engaged by the Service Provider pursuant to the requirements set forth herein will be Sub-Processors.

3.2. The Data Controller will determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by the Data Processor. The Data Processor will process the Personal Data only as set forth in Data Controller’s written instructions.

3.3. The Service Provider acknowledges and agrees that, under the terms of the Agreement, the Service Provider receives or has access to Protected Data. the Service Provider shall comply with the terms and conditions set forth in this DPA in its collection, receipt, transmission, storage, disposal, use and disclosure of such Protected Data and as required by the Data Protection Laws.

4. PURPOSE LIMITATION The processing of Protected Data by the Service Provider for the Customer is such as is required in the performance of the contracted Services under the Agreement. Further details of the Protected Data and Data Subjects required providing the contracted Services can be found in Annex 2.

5. OBLIGATIONS OF THE PROCESSOR FOR DATA PROTECTION

5.1. The Service Provider shall in relation to Protected Data processed by the Service Provider on behalf of the Customer as a Data Processor:

a) process the Protected Data only on documented instructions from the Customer. The Customer's instructions may be specific instructions or standing instructions of general application in relation to the performance of the Service Provider's obligations under the Agreement;

b) warrant that anyone authorized by the Service Provider to process Protected Data ("Authorized Persons") shall be subject to a duty of confidentiality by contract and by law, where applicable. 2 the Service Provider shall not permit any person not subject to confidentiality to process Protected Data. The Service Provider will ensure that only Authorized Persons will have access to and will process Protected Data. The Service Provider will ensure that such access and processing of Protected Data is limited to the extent necessary for the provision of the contracted Services. The Service Provider shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality;

c) take all measures required pursuant to Article 32 of the Regulation with respect to the security of processing;

d) respect the conditions of the Data Protection Laws for engaging a Sub-Processor;

e) taking into account the nature of the processing, assist the Customer by technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to

(i) any Data Subject Request, including but not limited to requests for access, rectification, erasure, opt-out and all similar requests, and will not respond to any such requests unless expressly authorized to do so by the Customer, or

(ii) any complaint relating to the processing of Protected Data by the Service Provider. The Service Provider will cooperate with the Customer with respect to any action taken relating to such request or complaint;

f) assist the Customer in ensuring compliance with the obligations under Data Protection Laws with respect to:
i) security of processing;
ii) notifications to the Supervisory Authority in case of any Personal Data Breach;
iii) communications to Data Subjects by the Customer in response to any Personal Data Breach;
iv) data protection impact assessments (as such term is defined in Data Protection Laws);
v) prior consultation with a Supervisory Authority regarding high-risk processing;

g) at the Customer's choice, delete or return all the Protected Data to the Customer, and ensure that all third parties supporting the Service Provider's processing of the Protected Data take the same action:
i) once processing by the Service Provider of any Protected Data is no longer required for the purpose of the Service Provider's performance of its relevant obligations under this DPA; or

ii) on request by the Customer;
iii) and delete existing copies unless Data Protection Laws require storage of the Protected Data and inform the Customer of such requirement;
iv) make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and assist in reasonable audits conducted by the Customer. 5.2. The Service Provider shall immediately notify the Customer if, in its opinion, an instruction infringes Data Protection Laws.

6. CONFIDENTIALITY

3 6.1. The Service Provider shall:
a) keep and maintain all Protected Data in confidence, using such degree of care as is appropriate to avoid unauthorized access, use or disclosure;

b) use and disclose Protected Data solely for the purposes for which the Protected Data, or access to it, is provided pursuant to the terms and conditions of the Agreement;

c) not use, sell, rent, transfer, distribute, or otherwise disclose or make available Protected Data for the Service Provider's own purposes or for the benefit of anyone other than the Service Provider, in each case, without the Customer's prior written consent;

d) not, directly or indirectly, disclose Protected Data to any person other than Authorized Persons, without prior written consent from the Customer, unless and to the extent expressly required by Data Protection Laws.

7. RECORDS, INFORMATION AND AUDIT

7.1. The Service Provider shall maintain, in accordance with Data Protection Laws binding on the Service Provider, written records of all categories of processing activities carried out on behalf of the Customer.

8. SUB-PROCESSORS

8.1. The Customer acknowledges that the provision of the Services by the Service Provider requires the use of Sub-Processors. The Customer hereby grants to the Service Provider general authorization for sub-processing in order to support the performance of the Services to third parties including data center operators, email service providers, providers of fraud detection/authenticity services and outsourced support providers, provided always that:

a) the Service Provider shall keep the Customer informed of all Sub-Processors engaged in the provision of the Services;

b) the Service Provider shall notify the Customer of any intended changes concerning the addition or replacement of Sub-Processors to the nominated contact, giving the Customer the opportunity to object to such changes on reasonable grounds based on non-compliance or a material risk of non-compliance by the Customer with Data Protection Laws;

c) obligations substantially no less protective of the Protected Data in question than those set out in this DPA shall be imposed on each Sub-Processor by way of a contract or other legally binding agreement. Where the Sub-Processor fails to fulfill its data protection obligations, the Service Provider shall remain liable to the Customer for the performance of the Sub-Processor's obligations, subject to the terms of the Agreement;

9. TECHNICAL/ORGANIZATIONAL MEASURES In relation to the processing of Protected Data, the Service Provider shall implement and maintain, at its cost and expense, a suitable written information security program taking into account the state of art, the costs of implementation and the nature, scope, context and purposes of processing the Protected Data. Such program shall include technical and organizational measures no less stringent than those set out in Annex 1.

10. AUDIT On an annual basis, the Service Provider grants the Customer permission to perform an on-site assessment, audit, examination and the right to review the Service Provider's data privacy and information security program 4 ("Customer Audit"). The Service Provider shall fully cooperate with each the Customer Audit by providing access to knowledgeable personnel, physical premises, documentation, infrastructure and application software that processes, stores or transports Protected Data. Any and all the Customer Audits shall be conducted at the Customer's own expense.

11. INTERNATIONAL DATA TRANSFERS

11.1. The Customer acknowledges that the provision of the Services under the Agreement may require the transfer or processing of Protected Data in countries outside the EEA from time to time.

11.2. The provisions of this DPA shall constitute the the Customer's instructions with respect to transfers.

11.3. The Service Provider commits to comply with the Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection and in its use of Protected Data pursuant to this DPA, including in respect of onward transfers.

11.4. If: a) the Standard Contractual Clauses (as applicable) should no longer be a data transfer mechanism recognized by a competent authority as an Appropriate Safeguard; and/or

b) the Service Provider, or a Sub-Processor appointed by Service Provider, processes Protected Data in or from a country outside the EEA the parties shall cooperate in good faith to put in place such alternative data export mechanisms as are required under Data Protection Laws to ensure an adequate level of protection for the Personal Data.

12. OBLIGATIONS OF THE CUSTOMER

12.1. The Customer will ensure that all Protected Data relating to the Customer Users disclosed or made available to the Service Provider will have been collected or made available in accordance with Data Protection Laws, including in respect of any required information, transparency and consents and that the collection, processing and use of such Protected Data by the Service Provider on behalf of the Customer in accordance with this DPA will not result in any contravention of Data Protection Laws.

12.2. The Customer warrants and represents that:

(a) all instructions given by it to the Service Provider in respect of Protected Data shall at all times be in accordance with Data Protection Laws;

(b) the Customer shall not unreasonably withhold, delay or condition its agreement to any change to this DPA requested by the Service Provider in order to ensure the Services and the Service Provider (and each Sub-Processor) can comply with Data Protection Laws.

12.3. The Customer warrants that it has all necessary rights to provide the Personal Data to the Service Provider for the Processing to be performed in relation to the Agreement. To the extent required by applicable Data Protection Law, the Customer is responsible for ensuring that any necessary data subject consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. Should such consent be revoked by the data subject, the Customer is responsible for communicating the fact of such revocation to the Service Provider,

and the Customer remains responsible for implementing any the Customer instruction with respect to the further processing of that Personal Data.

13. REPORTING PERSONAL DATA BREACHES

13.1. The Service Provider shall promptly notify the Customer of a Personal Data Breach impacting the Protected Data.

13.2. Any notifications made to the Customer pursuant to this section shall contain:

a) a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Protected Data records concerned;

b) the name and contact details of the Service Provider's data protection officer or another contact point where more information can be obtained;

c) a description of the likely consequences of the incident; and

d) a description of the measures taken or proposed to be taken by the Service Provider to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

14. INDEMNITY

Either party shall indemnify the other party and hold it harmless against all claims, actions, third party claims, losses, harm, costs, fines, liability, and expense incurred by and arising, directly or indirectly, out of or in connection with its breach of this DPA and/or applicable Data Protection Laws.

15. GENERAL PROVISIONS

15.1. Regarding the subject matter stated herein, this DPA, including the annexes attached hereto, constitutes the entire agreement between the parties, and supersedes all previous communications, representations, understandings, and agreements, either oral, electronic, or written.

15.2. In the event that the Standard Contractual Clauses apply to transfers, in case of any conflict between the general terms of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

15.3. Changes and amendments to this DPA and all of its components require written agreement and an explicit statement that they represent a change or amendment to these conditions. The same applies to a waiver of this formal requirement.

15.4. This governing law and jurisdiction applicable to this DPA shall be the law and jurisdiction of the Agreement. FOR THE SERVICE PROVIDER FOR THE CUSTOMER

_____ _____ Signature

Signature _____ _____

Date Date

ANNEX 1

SUMMARY OF TECHNICAL/ORGANIZATIONAL MEASURES

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, without prejudice to any other security standards agreed upon by the Service Provider shall implement appropriate technical and organizational measures to ensure a level of security of the processing of Protected Data appropriate to the risk. These measures shall include as appropriate:

1) measures to ensure that the Protected Data can be accessed only by authorized personnel for the purposes set forth in this DPA and the Agreement;

2) in assessing the appropriate level of security account shall be taken in particular of all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of Protected Data;

3) the pseudonymization and encryption of Protected Data;

4) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

5) the ability to restore the availability and access to Protected Data in a timely manner in the event of a physical or technical incident;

6) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Protected Data;

7) measures to identify vulnerabilities with regard to the processing of Protected Data in systems used to provide services to the Customer;

8) any additional measures agreed upon by the Parties and attached hereto.

ANNEX 2
FURTHER DETAILS ON THE NATURE OF THE DATA AND THE CATEGORIES OF DATA SUBJECTS

1) Types of Protected Data: The Protected Data comprises those categories that are determined and controlled by Customer in its sole discretion, including:

a) Identifiers: personal email address, work email address, IP address, GPS location, unique identifier, device fingerprint, first and last name, member, home address, work address, personal telephone number, or work telephone number.
b) Content data: ratings given, review content (text/photo/video), questions, answers, or nicknames;
c) Demographic information: location, age range, gender, and other the Customer-specified demographics;
d) Behavioral data: product interests, website browsing information, transaction data e.g. online purchases, website registrations.

2) Data Subjects
a) end users of the Customer's websites, mobile applications and other online properties, the Customer's interested parties and prospective end users and customers; and

b) visitors to the Customer's website(s), users of the Customer's mobile applications and/or other online properties.

3) Processing Required in Performance of the Services Invoicera will Process Protected Data as necessary to perform the Services pursuant to the Agreement, as further specified in the DPA, and as further instructed by Customer in its use of the Services.

4) Duration of Processing of Protected Data Subject to Section 5(g) of the DPA, Invoicera will Process Protected Data for the duration of the Agreement, unless otherwise agreed upon in writing.

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 Name of the data exporting organization: Invoicera (the data importer) AND The undersigned entity (the data exporter) 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 ; 1

(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 subprocessor' 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 1 which forms an integral part of the Clauses.

---

1 Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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

2 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;

(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 inquiries 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 subprocessing, 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter. 2 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. 11 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor 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 subprocessor, 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 subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, 12 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 Subprocessing 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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses . Where the subprocessor fails to 3 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 subprocessor's obligations under such agreement. 2. The prior written contract between the data importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses. 3. The provisions relating to data protection aspects for subprocessing 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 subprocessing 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 subprocessor 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. 3 This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision. 13 2. The data importer and the subprocessor 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.