GENERAL TERMS FOR EU DATA PROCESSING

Last Updated on November 9, 2018.

These terms and conditions ("**Terms**") for data processing are an integral part of the agreement between HEBS Digital, One Penn Plaza, 48th Fl, New York, NY 10119, USA ("**Processor**") and its Customer ("**Controller**") referring to these Terms (the „**Agreement**") which inter alia provides that Processor shall, in connection with the services under the Agreement ("**Services**") process personal data on behalf of the Controller or may have access to such data in connection with the Services (the "**Processor Relationship**") which personal data fall within the scope of Regulation (EU) 2016/679 (General Data Protection Regulation – „**GDPR**"). Terms used herein and not otherwise defined shall have the meaning attributed thereto in the GDPR.

If the Processor has entered, or enters, into an Agreement covering one or more separate legal entities (each a "**Site**"), the Processor Relationship and these Terms shall apply for each Site with respect to the data it controls as an agreement for the benefit of such Site. Based on this, each Site can in this respect independently and directly assert all rights of the Controller as defined in these Terms directly vis-á-vis the Processor.

The Processor shall be liable for breaches in connection with the Processor Relationship, including breaches of obligations under these Terms, only in accordance with the Agreement and subject to the limitations on warranty and liability set forth in the Agreement. The Controller shall hold the Processor harmless, irrespective of Controller's negligence, and without any limits as to scope or amount, from any claim asserted or alleged by a data subject or third party (including public authorities) whether or not such claim is substantiated, and any damages, liabilities, costs, fines, penalties and/or expenses payable in connection therewith such as legal and other professional fees, in connection with the Processor's hosting, processing and use of the Controller's Data, except if and to the extent that such claim was caused by a breach of obligations for which the Processor is liable in damages under the terms of the Agreement.

The Processing Operations are specified in Sec. A below. The Processing Relationship shall generally be governed by the General Processing Terms set forth in Sec. B below. Where the Services encompass an export of personal data which fall within the scope of the GDPR from the European Economic Area outside of the European Economic Area, the Standard Contractual Clauses (Processors) in Sec. C below shall apply and prevail over anything stated in Sec. B:

A.
Processing Operations

Except as otherwise specified in the Agreement, the hosting, processing and use of personal data in the context of the Services will in particular encompass the following:

Scope of Services	Digital marketing, website design and customer management services by the Processor to Controller
Data Subjects	End customers (guests, travellers), and prospective end customers of Controller, employees, suppliers, service providers or other partners of Controller
Categories of Data	Contact information of data subjects, correspondence and communications between the Controller and the data subjects, Information on Use of websites and newsletters: Identifiers: hashed email addresses, IP address, data that could be used for device fingerprinting, latitude and longitude, such as advertising IDs (such as Apple IDFA or Google Advertising ID) or Party specific IDs Demographic information: age range, gender, other client-specified demographics (tied to an identifier) Geographic Information: non-precise information from the IP address, precise information according to geolocation permissions granted (tied to an identifier) Behavioral data: inferences about a users' interests including product interests, website browsing information, content viewed on that website, referring/exit pages, events related to ad serving such as the number of ads displayed, date/time stamp, and/or the user's interactions with the ad (e.g. view time, action, clickstream), other transaction data (e.g. online purchases), website registrations, information related to the user device (tied to an identifier)

Special Categories of Data	None
Purposes	provision of digital marketing and website design services by the Processor to Controller
Recipients	Employees of the Processor, Controller and permitted subprocessors
Contacts	For HEBS Digital: dataprivacy@hebsdigital.com For Controller: as stated in the Agreement
Risk Assessment	Except where expressly otherwise agreed in the Agreement, the Parties mutually acknowledge and agree that, taking into account the likelihood and severity of risks for the rights and freedoms of natural persons, such data require a normal level of protection. The Parties will regularly update this risk assessment during the term of the Agreement.
Additional Processors	The Controller acknowledges and agrees that the Processor currently uses the Additional Processors disclosed here: https://www.hebsdigital.com/privacy-policy/subprocessors. The Controller consents that the Processor may in future retain additional service providers such as 3rd party advertisers, email service providers, customer relationship management tools, website optimization software, open source software, cloud hosting solutions, etc. as Additional Processors without requiring specific individual consent, subject only to the Controller's right to object thereto as set forth in Schedule 1.

B.
General Processing Terms

0. Scope, Definitions

The personal data processed are specified in the Agreement. Except where expressly otherwise agreed in the Agreement, the Controller and Processor mutually acknowledge and agree that, taking into account the likelihood and severity of risks for the rights and freedoms of natural persons, such data require a normal level of protection. The Controller and Processor will regularly update this risk assessment during the term of the Processor Relationship.

1. Subject Matter and Term

The Processor will process personal data on behalf of the Controller within the meaning of Art. 4 no. 2 and Art. 28 of the GDPR on the basis of the Agreement and these Terms. The Processor Relationship constitutes a material part of the Agreement. All cost and efforts for compliance with these Terms are included in the fees agreed in the Agreement and shall not otherwise be compensated. The scope and purposes of the Processor Relationship have been laid down in Sec. A and/or the Agreement. The Processor will process personal data only in accordance with the Processor Relationship, the Agreement, the Controller's instructions (clause 3) and applicable laws. The term of the Processor Relationship shall correspond with the term of the Agreement, unless otherwise agreed.

Breaches in connection with the Processor Relationship may constitute cause for termination of the Agreement. The Controller may in particular, without limitation, terminate the Agreement for cause where the Processor materially breaches terms of the Agreement, fails to duly carry out instructions of the Controller, or refuses to cooperate in giving full effect to the Controller's audit and information rights. Any non-compliance with any of the obligations expressly stated in this Agreement or in Art. 28 of the GDPR shall be considered a material breach.

Similarly, the Processor shall be entitled to terminate the Agreement for cause where instructions of the Controller in connection with the Processor Relationship or Controller's non-compliance with the GDPR prevent or unduly inhibit consummation of the Agreement. The same shall apply where additional investments or efforts of Processor may in future be required due to a revised assessment of the likelihood and severity of risks for the rights and freedoms of natural persons or where the Controller objects to any intended subcontracting, and the Parties fail to agree on a corresponding adjustment of the fees payable under the Agreement.

2. Scope, Nature, Purpose, Data Subjects and Place of Data Processing, Cost

The scope, nature and purpose of the collection, processing or use of personal data as well as the categories of personal data, the data subjects and place of data processing activities have been laid down in Sec. A and/or the Agreement. In the absence of any express provisions in the Agreement, the Agrement shall be construed to provide that the Processor will process personal data only for consummation of the Agreement. Unless expressly otherwise agreed, instructions hereunder will be given directly to the Processor's management.

The Processor agrees that the Controller may disclose the Processor as its processor and copy relevant provisions from the Processor's Privacy Statement in order to fulfill respective transparency obligations under the GDPR. However, this shall not limit the Controller's obligation to make an independent assessment of the scope of application of the GDPR and its transparency obligations in this respect and the Processor shall not have any liability whatsoever with respect to any wording copied from the Processor's Privacy Statement. The Controller acknowledges and agrees that the Processor will, and may, in the context of the Services, assume that the Controller has fulfilled all controller obligations under the GDPR and has obtained any data subject or third party consent required for the Services.

Cost and efforts in connection with these Terms which are unrelated to the Services, such as (a) cooperation under Sec. 4, or assistance under Sec. 10; (b) activities related to audits by Controller or third parties; and (c) production of any reports or documentation required by Controller over and above Processor's regular business reporting, are not included in the fees agreed in the Agreement and shall be compensated on a time and materials basis at the rates agreed in the Agreement or otherwise the Processor's standard rates.

3. Rights and Obligations of the Controller, Instructions

The Controller shall be solely responsible for ensuring compliance of all processing with Art. 6 par. 1 of the GDPR and for preserving the rights of the data subjects in accordance with Artt. 12 through 22 of the GDPR. Not limiting the foregoing, the Processor shall forward to the Controller without undue delay any data subject inquiries which refer (solely) to the Controller.

Any changes to the scope and/or the procedures of processing shall be coordinated between the Controller and the Processor and documented in writing or in a documented electronic format. The Controller shall generally issue all orders, call-offs and/or instructions in writing or a documented electronic format. Oral instructions shall be promptly confirmed in writing or in a documented electronic format. Instructions shall be archived for the term of their effectiveness and at least three years thereafter.

The Controller shall have the right, as agreed in clause 9, to reasonably audit, prior to commencement of the processing, and thereafter regularly, the compliance of the Processor's technical and organizational measures with these Terms and the Processor's compliance with the Agreement in accordance with in clauses 9 and 11.

The Controller shall promptly notify the Processor whenever it becomes aware of errors or incidents when reviewing the results of processing.

Where the agreed contacts for communications with respect to the Processor Relationship are unavailable permanently or for an extended period of time, the Party affected shall promptly appoint and communicate a new contact. Such communication shall take place in writing or electronically.

4. Obligations of the Processor

The Processor shall exclusively process personal data in compliance with the Agreement and the instructions of the Controller, unless required to do so by Union or Member State law to which the processor is subject (e.g. investigations of prosecution or investigation authorities); in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest (Art. 28 par 3 2nd sentence lit. a of the GDPR).

The Processor shall not process or use the personal data transferred or disclosed for its services for any other purpose, in particular not for its own purposes. The Processor may not create any copies or duplicates of personal data without the Controller's knowledge.

The Processor undertakes to ensure that all agreed measures with respect to the processing of personal data are implemented in compliance with the Agreement. The Processor undertakes to ensure that the data processed on behalf of the Controller are strictly separated from any other data in its possession.

All data and media which are provided by the Controller, or used for the Controller, shall be marked as such. Receipt and shipping, as well as any use thereof, shall be documented.

The Processor shall regularly conduct the agreed audits with respect to the processing services within its area of responsibility. The results of such audits shall be documented.

The Processor shall reasonably cooperate with the Controller, and support the Controller, as far as possible (Art. 28 par 3 2nd sentence lit. b and f of the GDPR), with respect to (a) the consummation of the rights of the data subjects according to Artt. 12 through 22 of the GDPR by the Controller, (b) drafting the records of processing activities, as well as (c) the implementation of data protection impact assessments. The Processor shall promptly provide all required information to the authorized representative of the Controller. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes applicable data protection provisions (Art. 28 par 3 3rd sentence of the GDPR). The Processor shall then be entitled to suspend implementation of any instruction pending the Controller's review and confirmation of such instruction. The Processor shall correct, erase, or restrict the processing of, personal data which fall within the scope of the Processor Relationship upon the Controller's instructions, provided that these do not conflict with a prevailing legitimate interest of the Processor. The Processor shall provide information to any third parties or data subjects with respect to personal data within the scope of the Processor Relationship only upon instruction of the Controller or with the Controller's prior consent.

The Processor acknowledges and agrees that the Controller may reasonably audit, or have audited by a third party retained by the Controller, the Processor's compliance with all applicable data protection and data security provisions and with the terms of the Agreement, in particular, without limitation, by requesting information, reviewing data files and/or hardware or software used for processing, and/or through on-site inspections – normally after having made an appointment (Art. 28 par. 3 2nd sentence lit. h of the GDPR). The Processor undertakes to reasonably cooperate, to the extent required, with such audits.

The Processor confirms that is fully aware of all provisions of the GDPR which are relevant to processing on behalf. The Processor undertakes to to maintain and preserve full confidentiality whenever it processes personal data own behalf of the Controller. This obligation shall survive expiry or termination of the Agreement. The Processor guarantees that it has instructed all employees involved in processing hereunder prior to such involvement on the provisions applicable to the protection of personal data and has ensured, in an appropriate manner, that they are, and remain even after the expiry or termination of employment, subject to an obligation of confidentiality (Art. 28 par. 3 2nd sentence lit. b and Art. 29 of the GDPR). The Processor shall ensure and supervise full compliance with all provisions applicable to the protection of personal data in all of its offices and facilities.

5. Additional Secrecy Obligations

The Processor further undertakes to observe all additional secrecy obligations which apply to the Controller and are referenced in the Agreement during and after the term of the Agreement.

6. Data Protection and Data Security Policy

The Processor shall implement appropriate technical and organisational measures for ensuring that, by default, all processing hereunder fulfills all data protection requirements. The Processor has enacted an IT Security and Data Protection Policy ("**Policy**") specifying the measures implemented in Agreement to comply with obligations under Art. 32 of the GDPR. Unless the Policy has been attached to the Agreement it will be made available to the Controller upon request at any time. Material changes to the Policy shall be documented. The amended Policy shall be made available to the Controller upon request any time.

To the extent that these Terms are explicitly agreed exclusively because Processor's access to personal data is not intended but cannot be excluded, the Processor is not required to enact a Policy of its own. In such case, the Processor shall be obligated, in lieu of obligations under clause 6 and 7, to comply with the Controller's policies and regulations with respect to confidentiality, the protection of personal data and data security, when conducting it services on the Controller's systems or premises. The same shall apply where processing of personal data within the scope of the Processor Relationship is conducted partly on systems of the Processor and partly on systems of the Controller. With respect to all works or services conducted on Controller's systems or premises, Controller's policies and regulations with respect to confidentiality, the protection of personal data and data security shall apply and shall prevail over any conflicting terms.

7. Technical and Organizational Measures under Art. 32 of the GDPR (Art. 28 par. 3 2nd sentence lit. c of the GDPR)

The Parties agree that all data must be subject to a level of protection which is adequate taking into account the likelihood and severity of risks for the rights and freedoms of natural persons. For this purpose adequate technical and organizational measures must be implemented which effectively and permanently exclude any risk with respect to attainment of the protection goals determined by Art. 32 par. 1 of the GDPR including, without limitation, the ongoing confidentiality, integrity, availability and resilience of processing systems and services in view of the nature, scope, context and purposes of processing.

By entering into the Agreement the Processor undertakes to ensure that all technical and organizational measures specified in the Policy on the effective date of the Agreement are, and will be implemented, and that such technical and organizational measures (a) are, in its professional view, sufficient to exclude risk with respect to the aforementioned goals of protection taking into account the state of the art and the particular IT systems and processes of the Processor; and (b) will comply with all requirements of the GDPR. Such measures shall be audited in the context of the Initial Audit in accordance with clause 9. Not limiting any of the foregoing, the Processor shall in any event always comply with any generally agreed processing principles and any other applicable general or customary standards or regulations.

The Processor will maintain the technical and organizational measures agreed herein during the entire term of the Agreement. The measures may be adapted to technical progress and further developments, provided that the standards agreed herein are adhered to.

Upon the Controller's request, the Processor must establish compliance with all requirements of this clause 7. For this purpose, the Controller may require the Processor to provide, at the Processor's option either a disclosure letter, or up to date reports of independent third parties (e.g. an accounting firm, the data protection officer, or an external data protection auditor or quality auditor), or an appropriate certificate issued by an IT security audit or a data protection audit firm (collectively „**Certificate**").

Compliance with the standards and requirements agreed herein shall be subject to regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. The complete audit documents for any certification specified in the Agreement shall be made available to the Controller at any time upon request.

8. Subcontractors

The Processor may only subcontract processing services to additional processors within the scope of Art. 28 par. 2 of the GDPR ("**Additional Processor(s)**") only with the Controller's prior specific or general written authorisation, Art. 28 par. 2 of the GDPR, which shall be granted through any of the agreed communication venues but not orally. Authorization will only be granted where the controller has been informed of the name and address of the Additional Processor and the scope of subcontracting. In addition the Processor must ensure that it has selected the Additional Processor with due diligence taking into account the effectiveness of the technical and organizational measures implemented by the Additional Processor within the scope of Art. 32 of the GDPR. Upon request the relevant audit documentation shall be provided to the Controller.

Subcontracting to Additional Processors located in third countries is admissible only if the additional requirements under Artt. 44 et seq. of the GDPR have been fulfilled (e.g. adequacy decision of the Commission, standard data protection clauses, approved code of conduct).

The Processor's agreement with the Additional Processor must give full effect to all provisions of the Agreement. The Additional Processor's services must be specified in sufficient detail to clearly demarcate the sphere of responsibility of the Processor on the one hand and of the Additional Processor on the other hand. Where the Processor retains more than one Additional Processor the same applies with respect to the respective spheres of responsibility of the individual Additional Processors.

In particular, without limitation, the Controller must be able to conduct, or have conducted, audits and inspections, including on-site inspections, with respect to all Additional Processors.

The subcontract must be made in writing, including electronic format (Art. 28 par. 4 and par. 9 of the GDPR). Data may not be disclosed or transferred to the Additional Processor before it has consummated all obligations under Art. 29 and Art. 32 par. 4 of the GDPR with respect to its employees.

The Processor shall regularly audit compliance of the Additional Processor with its obligations. The results of such audits shall be documented and such documents shall be made available to the Controller upon request.

The Processor shall be liable to the Controller for the Additional Processor's compliance with all obligations specified in this clause.

The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Additional Processors, thereby giving the Controller the opportunity to object to such changes (Art. 28 par. 2 2nd sentence of the GDPR) in which case such change may not be implemented.

The foregoing limitations shall not apply to services which the Processor may receive from third parties which are merely auxiliary to consummation of the Processor Relationship such as cleaning, surveillance or telecommunications services, provided that Processor shall, also with respect to such services, make, and reasonably enforce, contractual agreements with the service providers ensuring data protection and security.

9. Initial Audit, Controlling Rights of the Controller

Prior to the first data transfer, the Controller may audit or have audited the measures pursuant to clause 6 and 7 („**Initial Audit**") or request Processor to submit relevant Certificates.

Upon request, the Processor will provide the Controller, with any information or documentation necessary for processor compliance control. The Processor shall further enable the Controller to ascertain that the Processor has implemented the required technical and organizational measures pursuant to clause 6 and 7 by audits and information requests in accordance with clause 3 and 9. For this purpose, the Processor may, with respect to measures which are not limited to the Processor Relationship with the specific Controller, at its option submit a Certificate.

The Controller shall give the Processor reasonable advance notice of not less than 30 days of any audit. The start date, scope and duration of, and security and confidentiality controls applicable to, any audit will be discussed and agreed between the Parties. Audits shall not interfere with the Processor's buiness operations or compromise the security of its sytems or premises. The Processor may object to any third party auditor appointed by Controller if the auditor is, in its reasonable opinion, not suitably qualified or independent, a competitor or otherwise manifestly unsuitable. Any such objection will require Controller to appoint another auditor.

10. Notification in case of Incidents or Personal Data Breaches

The Processor will notify the Controller immediately in case there is reason to believe that a data security incident or a personal data breach may have occurred giving rise to notification obligations of the Controller under Artt. 33, 34 of the GDPR. The Processor shall reasonably assist the Controller in consummation of notification obligations of the Controller under Artt. 33, 34 of the GDPR (Art. 28 par. 3 2nd sentence lit. f of the GDPR). The Processor may only issue notifications under Artt. 33, 34 of the GDPR upon Controller's instructions in accordance with clause 3.

11. Confidentiality

Each party will maintain all information on business or trade secrets and/or data security measures of the respective other party which are disclosed in the context of the Processor Relationship as confidential for an unlimited period of time even after termination or expiry of the Agreement.

In order to protect its own business and trade secrets and other confidential information, the Processor may require that information, audits and the submission or review of documents under the Processor Relationship and these Terms are limited in scope to what is strictly necessary to establish compliance of the Processor with its obligations hereunder and/or only implemented through an independent third party to be retained by the Controller who is under an express obligation to disclose to the Controller only such information as is strictly necessary to establish compliance of the Processor with its obligations under the Processor Relationship.

12. Obligations of the Processor upon Termination (Art. 28 par. 3 2nd sentence lit. c of the GDPR)

Upon expiry or termination of the Agreement, the Processor will return or destroy/erase all documents, all results of the use and/or processing of data and all data as well as all testing and waste materials in connection with the Agreement which are in its possession or the possession of a subcontractor (collectively the „**Records**"). With the Controller´s prior consent, the Processor may erase or destroy such Records instead. Upon request, the Processor will provide the Controller with a protocol on the destruction process. The Procssor shall have no right of retention with respect to any Records. The Processor Relationship shall not be considered to have expired until and unless the Processor has fully consummated its obligation to return or destroy/erase. The Processor shall confirm the complete destruction and/or erasure and the date thereof in written or documented electronic form.

Documentation evidencing compliance with the Agreement, proper data processing rules or with statutory data retention duties, shall be preserved by the Processor after the termination of the Agreement in accordance with applicable statutory document retention provisions. The Processor may return such documentation to the Controller. In any event, such documenation must be barred for other uses.

C.
STANDARD
CONTRACTUAL CLAUSES
(PROCESSORS)[1]

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 Controller (in the Clauses hereinafter referred to as the '**data exporter'**) and the Processor (in the Clauses hereinafter referred to as 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

---

[1] Pursuant to Commission Decision of 5 February 2010 (2010/87/EU)

the data importer of the personal data specified in Appendix 1.

<div align="center">

Clause 1

Definitions

</div>

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

<div align="center">

Clause 2

Details of the transfer

</div>

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.

<div align="center">

Clause 3

Third-party beneficiary clause

</div>

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 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.

<div align="center">

Clause 4

Obligations of the data exporter

</div>

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 organizational 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, unauthorized 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 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

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 organizational 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 unauthorized access; and

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

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is the Controller.

Data importer

The data importer is the Processor.

Data subjects

The personal data transferred concern the following categories of data subjects: *Specified in Sec. A and/or the Agreement.*

Categories of data

The personal data transferred concern the following categories of data: *Specified in Sec. A and/or the Agreement.*

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data: *None, unless expressly identified in Sec. A and/or the Agreement.*

Processing operations

The personal data transferred will be subject to the following processing activities: *Specified in Sec. A and/or the Agreement.*

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

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