ARMOR DEFENSE
DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA) shall serve as Amendment to the Services Agreement between Armor Defense Limited and/or its affiliates ("Armor" or "Supplier") and the entity receiving Services listed on the signature pages hereto ("Customer") to reflect the parties' agreement with regard to the processing of personal data.

This DPA consists of three parts: the main body of the DPA, Schedule 1 (the Customer's written instructions), Schedule 2 (Armor's Technical and Organizational Security Measures) and Schedule 3 (Standard Contractual Clauses).

HOW TO EXECUTE THIS DPA:
To complete this DPA, Customer should:

(a) Sign the main body of this DPA in the signature section below.
(b) Complete and sign Schedule 1
(c) Complete and sign Schedule 3.
(d) Send the completed and signed DPA to Supplier to Privacy@armor.com for review and counter signature.

BACKGROUND:

WHEREAS, Customer and Armor are parties to a Services Agreement pursuant to which Armor provides certain secure hosting and other security-related services as ordered by Customer from time to time under the Services Agreement (the "Services") to Customer.

WHEREAS, the parties have agreed to supplement and amend the terms of the Services Agreement as set out in this Data Processing Addendum.

In consideration of the mutual obligations in this Data Processing Addendum and payment to the Supplier, the receipt of which is duly acknowledged by the Supplier, the parties agree as follows:

1. **EFFECTIVE DATE**

1.1. The Services Agreement shall be amended with effect from the date of Supplier's signature below (the **"Effective Date"**).

2. **DEFINITIONS AND INTERPRETATION**

2.1. All terms defined in the Services Agreement shall be deemed to have the same meaning in this Data Processing Addendum, other than as amended by this Data Processing Addendum.

2.2. In this Data Processing Addendum, the following terms have the following meanings:

(a) **"Personal Data"** shall mean all information relating to an identified or identifiable natural person ("**Data Subject**") that is Processed by the Supplier as a Data Processor for Customer under the Service Agreement. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her identity.

(b) **"Customer Personal Data"** shall mean Personal Data relating to an employee, contractor, or other natural person working for the Customer, that is processed by the Supplier for the purposes of providing Services to and communicating with the Customer.

(c) **"Data Controller"** shall mean the natural or legal person or entity which alone or jointly with others determines the purposes and means of the Processing for the purposes of this Agreement.

(d) **"Data Processor"** shall mean any natural or legal person or entity which processes Personal Data on behalf of and under the strict instructions of the Data Controller for the purposes of this Agreement.

(e) **"Data Protection Legislation"** means Regulation (EU) 2016/679 (the "GDPR"), in each case along with any national implementing laws, regulations and secondary or supplementary legislation, as amended or updated from time to time, in the UK and any successor legislation to the GDPR, and all other applicable laws and regulations relating to the processing of personal data and privacy applicable to a Data Controller in the Member State in which the Data Controller is established, and amendments and re-enactments of the same, including where applicable the guidance and codes of practice issued by the Data Protection Regulator, and any applicable similar or analogous laws and regulations made outside the United Kingdom;

(f) **"Data Protection Regulator"** means the Information Commissioner's Office in the UK; and

(g) **"Process," "Processed," or "Processing"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

(h) **"Term"** means the term of the Services Agreement.

(i) **"Third Party"** designates any company, other than an Armor affiliate, which is engaged by Armor for the provision of the Services.

3. CHANGES TO THE SERVICES AGREEMENT

3.1. From the Effective Date, the provisions of this Data Processing Addendum shall apply in respect of all Personal Data Processed by Supplier as a Data Processor for Customer, a Data Controller, under the Services Agreement.

3.2. Existing provisions of the Services Agreement which apply to Supplier's Processing of Personal Data shall be deleted and replaced with the provisions of the Data Processing Addendum.

3.3. Other than as set out in Section 3 of this Data Processing Addendum, all other provisions of the Services Agreement shall remain in full force and effect.

4. PROVISIONS RELATING TO PERSONAL DATA

4.1. **Customer's role and obligations**. The parties expressly agree that Customer is the Data Controller for the Personal Data (including Customer Personal Data) that is Processed for the purpose of the provision of the Services under this Addendum. Customer, as Data Controller, shall ensure that any Personal Data Processed by Armor on its behalf for the purposes of this Addendum is processed in accordance with the Data Protection Regulation and complies with the principles stated in the GDPR. Accordingly, Customer expressly guarantees:

(a) any Personal Data is processed on the basis of an adequate legal ground as permitted under the Data Protection Legislation.

(b) any Personal Data is processed for a defined, explicit and legitimate purpose.

(c) any Personal Data processed is relevant and non-excessive in consideration of the purpose of the processing.

(d) any Personal Data is and will be maintained accurate and up to date for the entire term of the provision of the Services under the Services Agreement.

(e) a term of retention has been defined for Personal Data, which is legitimate in consideration of the purpose of the processing and the nature of Personal Data processed.

(f) complete, clear and accurate information is provided to the Data Subjects whose Personal Data is processed under this Addendum, including, if relevant, information about the fact that Personal Data may be transferred outside the European Economic Area;

(g) Data Subjects whose Personal Data is processed under this Addendum are granted adequate and effective means to exercise their rights with regards to the processing of their Personal Data in accordance with applicable legislation (access, rectification, update, erasure, etc. as applicable). Supplier shall not be liable in cases where Customer fails to respond to the Data Subject's request in total, correctly or in a timely manner.

(h) all adequate and necessary formalities, if any, or internal documentation, as per applicable Data Protection Legislation, have been completed with all competent authorities, completed or otherwise retained internally by Customer.

(i) it has conducted all relevant verifications and obtained all relevant information which it deems necessary regarding Supplier and is satisfied that Supplier provides sufficient guarantees to process Customer Personal Data and Personal Data in accordance with the requirements of Data Protection Legislation.

(j) it shall maintain a register of data Processing activity.

4.2. Nothing in the Services Agreement shall relieve Supplier of its own direct responsibilities and liabilities under the Data Protection Legislation.

4.3. **Customer's Processing Instructions**. Schedule 1 sets out Customer's documented instructions related to the scope, nature and purpose of processing of Personal Data by the Supplier, the duration of the processing, the types of Personal Data and categories of Data Subject. Supplier shall not process Personal Data other than on Customer's documented instructions (including the Services Agreement) unless processing is required by applicable law to which Supplier is subject, in which case Supplier shall unless prohibited by applicable law inform Customer of that legal requirement before the relevant processing of that Personal Data. Should Customer wish to implement modifications to its instructions, it shall notify Supplier at least thirty (30) days in advance in order for both parties to evaluate Customer's proposed modification.

The parties expressly agree that Customer's modifications to its instructions may have a direct impact on the delivery of the Services which may require a review and modification of the terms of the Services Agreement and this Data Processing Addendum, including the financial terms. If Supplier cannot provide such compliance with Customer's written instructions for whatever reasons, it agrees to inform promptly the Customer of its inability to comply, in which case the Customer is entitled to review and amend its instructions to allow Supplier to remain in compliance with its obligation.

In any event, Customer hereby expressly acknowledges and accepts that Armor shall not be bound by any Customer Instructions breaching applicable law (including Data Protection Legislation). As such, Armor shall be entitled to suspend performance on such Instructions until Customer conforms or modifies such Instructions. In such cases, Armor shall provide a prior notice to the Customer of such intended suspension.

4.4. **Armor's roles and obligation.** The parties expressly agree that Armor is the Data Processor in the event Armor collects or otherwise Processes (including to store) Personal Data on behalf of Customer when performing the Services. Accordingly, Armor will:

(a) ensure that all persons authorised by Supplier to Process the Personal Data are under an enforceable obligation to keep Personal Data strictly confidential;

(b) adopt and maintain appropriate technical and organisational measures specified in Schedule 2 to ensure the Personal Data is kept secure, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, including but not limited to any specific measures agreed between Customer and Supplier elsewhere in the Services Agreement;

(c) subject to Section 4.3 (Customer Processing Instructions), only transfer the Personal Data in accordance with any reasonable written instructions set forth in Schedule 1 from Customer and take all further steps necessary to ensure that the transfer is and remains in accordance with the Data Protection Legislation;

(d) without limitation and notwithstanding any other obligation under the Services Agreement, Supplier shall, (and shall ensure that any sub-processor shall), on request, provide all information and assistance reasonably required by Customer to enable it to comply with the Data Protection Legislation in relation to Personal Data, including but not limited to the exercise of the rights of Data Subjects to the extent Supplier can reasonably have access to Data Subject Personal Information with regard to the Processing of Personal Data performed by Supplier. Notwithstanding the foregoing, Supplier shall not respond to any such Data Subject request, inquiry, complaint, or claim relating to Processing of Personal Data without Customer's prior written consent except to the extent required by the Data Protection Legislation or reasonably necessary to confirm that the request relates to Customer. Supplier shall not be liable in cases where Customer fails to respond to the Data Subject's request in total, correctly or in a timely manner;

(e) ensure that it has adequate processes and systems in place to comply with its obligations under Section 4.4(d) above;

(f) Armor shall not communicate any Personal Data or subcontract whole or part of the Processing for the purpose of the provision of the Services under this Agreement to any Third Party unless Armor has the specific prior written consent of Customer, which shall not be unreasonably withheld. Customer hereby authorizes Supplier or any such affiliate to engage third parties from time to time to process personal data in connection with the Services. Supplier shall make available to Customer a current list of subcontractors for the Services upon Customer's written request. Where Customer objects to Armor's use of such a Third Party subcontractor, Customer shall notify Armor in writing within 5 business days after receipt of Armor's written request to appoint a Third Party subcontractor. In the event Customer objects to a Third Party subcontractor, it shall justify its material or legal reasons for such objection.

(g) not modify, amend or alter the contents of the Personal Data or disclose or permit the disclosure of any of the Personal Data to any third party unless specifically approved in advance in writing by Customer;

(h) immediately notify Customer with full details if it:

(i) becomes aware of any breach of the Data Protection Legislation in relation to the Services Agreement;

(ii) except as prohibited by the Data Protection Legislation, believes that instructions provided by Customer in respect to the processing of Personal Data are contrary to or would require it to act in a way contrary to the Data Protection Legislation and/or applicable law.

Customer shall adapt its instructions in order to comply with such legislation. Such modifications may have a direct impact on the delivery of Services which may require a review and modification of the terms of this Agreement, including, notably, the scope of the Services and the financial terms, to the terms of this Agreement as necessary, including notably, the term of implementation of requested modifications. In any event, Customer hereby expressly acknowledges and accepts that Supplier shall not be bound by any Customer instructions breaching applicable law (including applicable Data Protection Legislation). As such, Supplier shall be entitled to suspend performance on such instructions until Customer conforms or modifies such instructions. In such a case, Supplier shall provide a prior notice to Customer of such intended suspension; or

(iii) subject to Section 4.4(d), receives any request (including from a Data Subject or the Data Protection Regulator) to disclose any Personal Data; provided Supplier shall not directly answer to such requests except as duly and expressly agreed between the parties as part of the Services under the Services Agreement;

(i) upon no less than thirty (30) days' written notice by Customer:

(i) make available to Customer all such information as is reasonably necessary to demonstrate Supplier's compliance with Data Protection Legislation;

(ii) shall allow Customer to carry out or have an independent duly appointed third party established on the market for its auditing functions and bound by a strict obligation of confidentiality, an audit of Supplier's processing facilities in order to ensure the compliance with the obligations set forth in this Addendum. Supplier shall be entitled to reject third party auditors which are competitors of Supplier. Such audit operations shall not exceed a period of twelve (12) hours per year, shall occur not more than once per year, shall not hinder or otherwise disrupt in any way Supplier's operations or business activities and shall only relate to that part of the relevant infrastructure which processes Customer's Personal Data. Supplier's assistance in relation to such activity shall be invoiced at Supplier's then applicable rates; and

(iii) provide, at Customer's cost and during normal business hours, all reasonable co-operation, access and assistance in the carrying out of such an audit, and allow Customer the right to take copies of the records or any information relevant to its audit;

(j) notwithstanding any agreed retention periods applicable to Personal Data in the Services Agreement, on termination of the Services Agreement, at Customer's sole election, Supplier will provide all Personal Data to Customer and/or permanently delete such Personal Data, save where applicable law requires Supplier to retain Personal Data, in which case Supplier shall provide Customer with written particulars of any Personal Data so retained. For the avoidance of doubt this sub-clause 4.4(j)shall survive termination of the Services Agreement.

4.5. **Transfers of Customer Personal Data to Third Party Countries.** By entering into this Addendum, Customer hereby expressly acknowledges and accepts that Customer Personal Data may be transferred and/or processed to Armor's affiliates, which are located outside the European Economic Area.

Armor and its affiliated entities (hereafter together "Armor Group") are bound by Model Clauses as approved by the European data protection authorities and as attached as Schedule 3 of this addendum.

Customer acknowledges that, in the event that Armor transfers Customer Personal Data to any entity of the Armor Group located outside the European Economic Area, the Model Clauses constitute a sufficient safeguard to establish that such entities provide an adequate protection to Personal Data as required under applicable Data Protection Legislation.

For purposes of this Agreement, Armor commits to comply with the terms of the Model Clauses. Accordingly, Customer hereby expressly consents that Customer Personal Data may be transferred to any of the Armor Group entities bound by the terms of the Model Clauses. Armor commits to provide adequate information to Data Subjects regarding use of Armor as processor (including Armor entities located outside the European Economic Area), which is available at https://www.armor.com/privacy-policy/.

In addition, Customer hereby expressly consents that Customer Personal Data may be transferred to a Third Party (approved pursuant to Section 4.4(f)) located in a Third-Party Country.

Upon express written request from the Customer, Armor shall provide Customer with a list of subcontractors used by Armor for the provision of the Services.

Armor shall ensure that Third Party subcontractors provide an adequate level of protection to Customer Personal Data. For that purpose, Armor will procure any duly authorized subcontractor brought to process Personal Data outside the European Economic Area shall enter into and comply with the obligations set out in appropriate standard contractual clauses for the transfer of Personal Data as set out by the European Commission (or any competent authority) with Customer or with Armor in accordance with the mandate granted above.

4.6. **Parties' compliance with Laws.** The Supplier warrants to Customer and Customer warrants to Supplier that it will fully comply with the provisions of the Data Protection Legislation in carrying out its obligations under the Services Agreement.

5. TERMINATION OF THIS ADDENDUM

5.1. Upon termination of this Addendum for whatever reason, Armor shall cease processing any Personal Data on behalf of Customer, and at Customer's option, shall either return to Customer all of the Customer Personal Data and any copies thereof which it is processing, has processed or have had processed on behalf of Customer, or destroy the Customer Personal Data within 15 calendar days of being requested to do so by Customer and provide written confirmation of such destruction, unless otherwise required by law.

6. MODIFICATION OF THIS ADDENDUM

6.1. No modification of this Addendum and/or any of its components shall be valid and binding unless made in writing. Such modification shall expressly state that it applies to the regulations of this Addendum and must be signed by the authorized representatives of the parties to be considered valid.

7. GOVERNING LAW AND JURISDICTION

7.1. This Data Processing Addendum shall be governed by and will be interpreted in accordance with the laws of England and Wales. The United Nations Convention on Contracts for the International Sale of Goods (1980) shall not apply. No modification of this Addendum and/or of its components shall be valid and binding unless made in writing. Furthermore, such modification shall expressly state that it applies to the regulations of this Addendum to be considered valid.

7.2. All disputes arising out of or relating to this Data Processing Addendum or any non-contractual obligations arising out of or relating to this Data Processing Addendum shall be subject to the exclusive jurisdiction of the courts of England Wales.

This Data Processing Addendum has been signed on behalf of each of the parties by a duly authorised signatory.

Signed for and on behalf of	**Signed for and on behalf of**

CUSTOMER:	**SUPPLIER: ARMOR DEFENSE LIMITED**
By ……..	**By** ……..
Name ……	**Name** ……
Title ……	**Title** ……
Date ……	**Date** ……

SCHEDULE 1
CUSTOMER'S WRITTEN INSTRUCTIONS FOR THE PROCESSING OF PERSONAL DATA

This Schedule 1 forms part of the Data Processing Addendum and is incorporated into the Data Processing Addendum.

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

Data Controller

For the purposes of the Data Processing Addendum, the Data Controller is _____.

Data Controller intends to transfer Personal Data of their customers and customers of their Customers to Armor Defense Ltd. and its affiliate Armor Defense Inc., whose servers are located in the United States, for data hosting and storage purposes and/or web portal hosting services.

Data Processor

The Data Processor is Armor Defense Limited, together with its affiliate, Armor Defense Inc. (collectively, "Armor").

The Data Processor, Armor, is a provider of secure cloud hosting and other security related services (the "Platform") which processes Personal Data in accordance with the terms of the Services Agreement. The core purpose of the Platform is to provide data hosting and storage processing services in order to allow Platform users authorized by the Data Controller to manage and administer its data and websites.

Data Subjects
The personal data transferred concern the following categories of data subjects (please specify):

- Current and former customers and customers of clients and business partners and vendors of data controller (who are natural persons)
- Employees, agents, advisors, freelancers of Data Controller (who are natural persons)
- Data controller's Users authorized by data controller to use the Armor Services
- _____
- _____
- _____

Categories of data
The personal data transferred concern the following categories of data. The following data categories are associated with Account Data (as defined in the Services Agreement):

- First and last name
- Contact details (e.g., email, phone, physical address)
- Salutation

The following data categories are associated with Services Data (as defined in the Services Agreement):

- _____
- _____
- _____
- _____

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

- _____
- _____

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

- The purpose of the data processing is to provide global data hosting and storage, as well web application hosting services.

- The Data Processor will, through authorized personnel perform the following processing Services:

    - provide the Services puruant to the the terms of the Services Agreement;
    - maintain storage for the Data Controller's personal data that is contained within Services Data;
    - enable the Data Controller to access, modify, enhance and/or delete its personal data maintained on the processor's servers;
    - prevent unauthorized access to or modification of the Data Controller's personal data by Data Processor's employees;
    - enable the Data Controller to generate standardized reports and analysis regarding its personal data;

- The Data Processor shall not make any copy of the personal data without informing the Data Controller, unless it is a security copy required to duly perform the data processing, or unless it is required to comply with applicable statutory retention periods.

- As soon as the parties agree that the Data Processor shall cease the provision of the data processing services, the Data Controller may extract the transferred Personal Data and the Data Processor shall delete such data.

SCHEDULE 2
ARMOR'S TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES
FOR THE PROCESSING OF PERSONAL DATA

This Schedule 2 forms part of the Data Processing Addendum and is incorporated into the Data Processing Addendum.

Description of the technical and organizational security measures implemented by the Data Processor in accordance with Section 4.4(b) of the Data Processing Addendum:

Data Processor will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Armor secure customer portal and stored on other Armor controlled systems including the secure virtual servers provided by Armor for Customer to store Customer's Services Data.

Armor maintains an information security program that has been certified against the ISO/IEC 27001:2013 standard. The program includes an information security policy, and other corporate policies and procedures that are designed to give Armor the capability to protect non-public personal information consistent with applicable federal, state, and international regulations. In addition to ISO 27001 certification, Armor also holds unqualified SSAE 16 SOC 2 Type II reports that further validate Armor's information security program.

Users of confidential and private information within Armor aim to keep the volume of such material to a reasonable level in proportion to the business responsibilities and services being delivered to customers, employees, and other parties.

Personnel security measures include employees undergoing a multi-component background check as part of the hiring process in accordance with applicable law. Employees are required to sign confidentiality and non-disclosure agreements as a condition of employment.

Vendor management procedures are in place to review contractors, business partners, and vendors that will have access to confidential information.

Armor's secure cloud hosting environments including all of the services Armor provides to customers have been validated against the Payment Card Industry Data Security Standard v3.2 and the HITRUST CSF. These validations require controls designed to help protect the confidentiality and integrity of Customer's Services Data. These controls include the following:

- IP Reputation Management
- DoS/DDoS mitigation
- Web Application Firewalls
- Network Intrusion Detection (NIDS)
- Hypervisor based network firewall resident on each Customer virtual server
- Managed anti-malware/anti-virus protection
- Operating system file integrity monitoring
- Operating system patching
- Operating system log management

Armor provides for only secure, encrypted remote access by Customer for administrative access to its servers and controls Armor support staff access to Customer servers for support purposes via secure, two factor authenticated jump servers and a privileged access management system that logs and fully records each Armor session.

Data Processor will not materially decrease the overall security of the Armor Services during the Term.

SCHEDULE 3

2010 EU Model clauses extracted from 2010/87/EU Annex EU Standard Contractual Clauses for the transfer of personal data to data processors established in third countries which do not ensure an adequate level of data protection

---

Name of the data exporting organisation:.....

Address:

Tel: .....; fax: ……; e-mail: ……

Other information needed to identify the organisation:

registered in …… Company Registration Number: ……..

(the data exporter)

And

Name of the data importing organisation: Armor Defense Inc. .....

Address: 2360 Campbell Creek Blvd., Suite 525, Richardson, Texas 75082, USA

Tel.:+1 877-262-3473.....; fax:..... ; e-mail:legal@armor.com.....

Other information needed to identify the organisation:

……
(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 Controller (referenced as a "data exporter" for the purposes of these Clauses) to the Data Processor (referenced as a "data importer" for the purposes of these Clauses) of the Personal Data specified in Schedule 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 Schedule 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the 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.

[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 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 Schedule 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 Schedule 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:

[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, defense, 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 recognized sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(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 Schedule 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 Schedule 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.

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, 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[3]. Where the subprocessor 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 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.

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.

[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.