DTA
DATA PROCESSING ADDENDUM

Updated: May 20, 2021

This Data Processing Addendum ("**DPA**") is incorporated into and forms part of the agreement under which Experlogix has agreed to provide certain products and services to Customer (together with any Order(s), the "**Agreement**"). Capitalized terms used but not otherwise defined herein shall have the meaning given to them in the Agreement. Except as expressly modified below, the terms of the Agreement shall remain in full force and effect.

Experlogix and Customer agree as follows:

1. DEFINITIONS.

1.1 "**Affiliate**" means an entity that owns or controls, is owned or controlled by, or is or under common control or ownership with either Customer or Experlogix respectively, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 "**Controller**" means the individual or entity that determines the purposes and means of the Processing of Personal Data.

1.3 "**Customer**" means the individual or entity that has entered into the Agreement and agreed to the incorporation of this DPA into the Agreement.

1.4 "**Customer Personal Data**" means Personal Data received by Experlogix from or on behalf of Customer that is covered by Data Protection Laws. Customer Personal Data does not include Usage Data (as defined in the Agreement).

1.5 "**Data Protection Laws**" means, to the extent applicable to a party, the data protection or privacy laws of any country regarding the Processing of Customer Personal Data including, to the extent applicable, the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq. ("**CCPA**") and European Data Protection Laws.

1.6 "**Data Subject**" means the identified or identifiable natural person who is the subject of Personal Data.

1.7 "**European Data Protection Laws**" means, to the extent applicable to a party, the EU General Data Protection Regulation 2016/679 ("**GDPR**"), any data protection laws substantially amending, replacing or superseding the GDPR following any exit by the United Kingdom from the European Union ("**UK GDPR**"), and any other applicable national rule and legislation on the protection of Personal Data in the European Economic Area that is already in force or that will come into force during the term of this DPA.

1.8 "**Experlogix**" means Experlogix LLC, Experlogix B.V., Xpertdoc Technologies, Inc., or any other Affiliate of Experlogix, LLC that has entered into the Agreement with Customer and agreed to the incorporation of this DPA into the Agreement.

1.9 "**Order**" means any proposal, order, statement of work, or similar document entered into between Experlogix and Customer pursuant to the Agreement.

1.10 "**Personal Data**" means "personal data", "personal information", "personally identifiable information" or similar information defined in and governed by Data Protection Laws.

1.11 "**Process**" means any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, alignment, combination, restriction, erasure, destruction or disclosure by transmission, dissemination or otherwise making available.

1.12 "**Processor**" means the individual or entity that Processes Personal Data on behalf of a Controller.

1.13 "**Security Incident**" means any confirmed unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data Processed by Experlogix. Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

1.14 "**Sensitive Personal Data**" means any of the following: (i) credit, debit or other payment card data subject to the Payment Card Industry Data Security Standards or other financial account numbers or credentials; (ii) patient, medical or other protected health information regulated by the Health Insurance Portability and Accountability Act; (iii) social security numbers, driver's license numbers, passport numbers, or other government ID numbers; (iv) any information deemed to be "special categories of data" as defined under European Data Protection Laws; or (v) other Personal Data deemed "sensitive"

and subject to regulation or protection under the Gramm-Leach-Bliley Act, Children's Online Privacy Protection Act, or other Data Protection Laws.

1.15 "**Services**" means the products and services that Experlogix has agreed to provide to Customer under the Agreement.

1.16 "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of Personal Data to Processors established in third countries which do not ensure an adequate level of data protection pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 attached to this DPA as Appendix 3.

1.17 "**Subprocessor**" means any Processor (including any third party and any Experlogix Affiliate) appointed by Experlogix to Process Customer Personal Data on behalf of Customer under the Agreement.

1.18 "**Supervisory Authority**" means an independent competent public authority established or recognized under Data Protection Laws.

1.19 "**User**" has the meaning given in the Agreement or, if not defined in the Agreement, means any person authorized by Customer to access or use the Services.

2. PROCESSING OF CUSTOMER PERSONAL DATA.

2.1 Roles of the Parties; Compliance. The parties acknowledge and agree that, as between the parties, with regard to the Processing of Customer Personal Data under the Agreement Customer is a Controller and Experlogix is a Processor of Customer Personal Data. Each party will comply with the obligations applicable to it in such role under Data Protection Laws with respect to the Processing of Customer Personal Data.

2.2 Customer Instructions. Experlogix will Process Customer Personal Data only (a) in accordance with Customer's documented instructions, including the instructions set forth in the Agreement and this DPA and any instructions initiated by Users via the Services; (b) as necessary to provide the Services and prevent or address technical problems with the Services or violations of the Agreement or this DPA; or (c) as required by applicable law. Customer's instructions shall comply with Data Protection Laws and be duly authorized, with all necessary rights, permissions, and consents secured. Appendix 1 sets out a description of Experlogix's Processing of Customer Personal Data.

2.3 Processing Subject to the CCPA. Experlogix shall not (a) sell (as defined in the CCPA) any Customer Personal Data; (b) retain, use, or disclose any Customer Personal Data for any purpose other than for the specific purpose of providing the Services as described in Section 2.2 or as otherwise permitted by the CCPA, including retaining, using, or disclosing Customer Personal Data for a commercial purpose (as defined in the CCPA) other than provision of the Services; or (c) retain, use, or disclose the Customer Personal Data outside of the direct business relationship between Experlogix and Customer. Experlogix hereby certifies that it understands its obligations under this Section 2.3 and will comply with them. Notwithstanding anything in the Agreement, the parties acknowledge and agree that Experlogix's access to Customer Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

2.4 No Sensitive Personal Data. Customer specifically agrees not to use the Services to collect, store, transmit, or otherwise Process any Sensitive Personal Data. Experlogix shall have no liability under the Agreement (including this DPA) for Sensitive Personal Data, notwithstanding anything to the contrary herein.

3. SECURITY.

3.1 Experlogix Personnel. Experlogix shall take reasonable steps to ensure that Experlogix personnel that Process Customer Personal Data (a) access Customer Personal Data only to the extent necessary to perform Experlogix's Processing obligations under this DPA and the Agreement; (b) are bound by appropriate confidentiality obligations with respect to Customer Personal Data; and (c) are subject to appropriate training relating to the Processing of Customer Personal Data.

3.2 Security Measures. Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Experlogix shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, in accordance with the security standards in Appendix B (the "**Security Measures**"). Customer acknowledges that the Security Measures may be updated from time to time upon reasonable notice to Customer to reflect process improvements or changing practices, provided that the modifications will not materially decrease Experlogix's security obligations hereunder.

3.3 Security Incidents. Upon becoming aware of a confirmed Security Incident, Experlogix will (a) notify Customer of the Security Incident without undue delay after becoming aware of the Security Incident and (b) take reasonable steps to identify the cause of such Security Incident, minimize harm, and prevent a recurrence. Notifications made pursuant to this Section 3.3 will describe, to the extent possible, details of the Security Incident, steps taken to mitigate the potential risks, and steps Experlogix recommends Customer take to address the Security Incident. Experlogix's notification of or response to

a Security Incident under this Section 3.3 will not be construed as an acknowledgement by Experlogix of any fault or liability with respect to the Security Incident.

3.4 Customer Responsibilities. Customer agrees that, without limitation of Experlogix's obligations under this Section 3, Customer is solely responsible for its and its Users' use of the Services, including (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data; (b) securing the account authentication credentials, systems, and devices Customer uses to access the Services; and (c) determining the type and substance of Customer Personal Data. Customer is responsible for reviewing the information made available by Experlogix relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws.

4. SUBPROCESSORS.

4.1 Authorization. Customer (a) specifically authorizes Experlogix to engage its Affiliates as Subprocessors, and (b) generally authorizes Experlogix to engage third parties as Subprocessors as Experlogix considers reasonably appropriate for the Processing of Customer Personal Data.

4.2 Subprocessor List. A list of Experlogix's Subprocessors, including their functions and locations, is available upon written request of Customer and may be updated by Experlogix from time to time in accordance with this DPA.

4.3 New Subprocessors; Right to Object. Experlogix shall notify Customer of the addition or replacement of any Subprocessor and Customer may, on reasonable grounds, object to a Subprocessor by notifying Experlogix in writing within ten (10) days of receipt of Experlogix's notification, giving reasons for Customer's objection. Upon receiving such objection, Experlogix shall: (a) work with Customer in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; and (b) where such change cannot be made within 10 days of Experlogix's receipt of Customer's notice, Customer may by written notice to Experlogix with immediate effect terminate the portion of the Agreement or relevant Order to the extent that it relates to the Services which require the use of the proposed Subprocessor. This termination right is Customer's sole and exclusive remedy to Customer's objection of any Subprocessor appointed by Experlogix.

4.4 Subprocessor Engagement. Experlogix shall require all Subprocessors to enter into an agreement with equivalent effect to the Processing terms contained in this DPA. Experlogix shall remain responsible for the acts and omissions of each Subprocessor.

5. DATA SUBJECT RIGHTS.

Experlogix will (taking into account the nature of the Processing of Customer Personal Data) provide Customer with self-service functionality through the Services or other reasonable assistance as necessary for Customer to perform its obligations under Data Protection Laws to fulfill requests by Data Subjects to exercise their rights under Data Protection Laws, provided that Experlogix may charge Customer on a time and materials basis in the event that Experlogix considers, in its reasonable discretion, that such assistance is onerous, complex, frequent, or time consuming. If Experlogix receives a request from a Data Subject under any Data Protection Laws in respect to Customer Personal Data, Experlogix will advise the Data Subject to submit the request to Customer and Customer will be responsible for responding to any such request.

6. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION.

In the event that Customer considers that the Processing of Customer Personal Data requires a privacy impact assessment to be undertaken or requires assistance with any prior consultations to any Supervisory Authority, following written request from Customer, Experlogix shall use reasonable commercial efforts to provide relevant information and assistance to Customer to fulfil such request, taking into account the nature of Experlogix's Processing of Customer Personal Data and the information available to Experlogix.

7. RELEVANT RECORDS AND AUDIT RIGHTS.

7.1 Review of Reports. Experlogix will make available to Customer all information reasonably necessary to demonstrate compliance with the obligations set out in this DPA and allow for and contribute to reviews of relevant records by making available to Customer Experlogix's most recent SOC 2 or similar audit report or certification ("**Reports**"). The Reports will be made available to Customer upon written request no more than annually subject to the confidentiality obligations of the Agreement or a mutually-agreed non-disclosure agreement.

7.2 Audits. If Customer requires information for its compliance with Data Protection Laws in addition to the Reports, at Customer's sole expense and to the extent Customer is unable to access the additional information on its own, Experlogix will allow for and cooperate with Customer or an auditor mandated by Customer ("**Mandated Auditor**"), provided that: (a) Customer provides Experlogix with reasonable advance written notice including the identity of any Mandated Auditor, which shall not be a competitor of Experlogix, and the anticipated date and scope of the audit; (b) Experlogix approves the

Mandated Auditor by notice to Customer, with such approval not to be unreasonably withheld; (c) the audit is conducted during normal business hours and in a manner that does not have any adverse impact on Experlogix's normal business operations; (d) Customer or any Mandated Auditor complies with Experlogix's standard safety, confidentiality, and security procedures in conducting any such audits; (e) any records, data, or information accessed by Customer or any Mandated Auditor in the performance of any such audit will be deemed to be the Confidential Information of Experlogix; and (f) Customer may initiate such audit not more than once per calendar year unless otherwise required by a Supervisory Authority.

7.3 Results of Audits. Customer will promptly notify Experlogix of any non-compliance discovered during the course of an audit and provide Experlogix any audit reports generated in connection with any audit under this Section 6, unless prohibited by Data Protection Laws or otherwise instructed by a Supervisory Authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and confirming that Experlogix's Processing of Customer Personal Data complies with this DPA.

8. DATA TRANSFERS.

8.1 Data Processing Facilities. Experlogix may, subject to Section 8.2, Process Customer Personal Data in the United States or anywhere Experlogix or its Subprocessors maintains facilities. Subject to Experlogix's obligations in this Section 8, Customer is responsible for ensuring that its use of the Services comply with any cross-border data transfer restrictions of Data Protection Laws.

8.2 Standard Contractual Clauses. If the Services involve the transfer of Customer Personal Data under this DPA from the European Union, the European Economic Area, Switzerland, or the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of European Data Protection Laws, to the extent such transfers are subject to such European Data Protection Laws and no lawful alternative basis for such transfer applies, such transfer will be governed by the Standard Contractual Clauses, the terms of which are hereby incorporated into this DPA. In furtherance of the foregoing, Experlogix and Customer agree that:

(a) Customer (as data exporter) will be deemed to have entered into the Standard Contractual Clauses with Experlogix LLC (as data importer) and Experlogix will ensure that Experlogix LLC complies with its obligations under the Standard Contractual Clauses;
(b) for purposes of Appendix 1 to the Standard Contractual Clauses, the categories of data subjects, data, special categories of data (if appropriate), and the processing operations shall be as set out in Appendix 1;
(c) for purposes of Appendix 2 to the Standard Contractual Clauses, the technical and organizational measures shall be the Security Measures as set out in Appendix 2;
(d) upon data exporter's request under the Standard Contractual Clauses, data importer will provide the copies of the subprocessor agreements that must be sent by the data importer to the data exporter pursuant to Clause 5(j) of the Standard Contractual Clauses, and that data importer may remove or redact all commercial information or clauses unrelated the Standard Contractual Clauses or their equivalent beforehand;
(e) the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be performed in accordance with Section 7 of this DPA;
(f) Customer's authorizations in Section 4 of this DPA will constitute Customer's prior written consent to the subcontracting by Experlogix of the Processing of Customer Personal Data if such consent is required under Clause 5(h) of the Standard Contractual Clauses;
(g) certification of deletion of Customer Personal Data as described in Clause 12(1) of the Standard Contractual Clauses shall be provided only upon Customer's request;
(h) the Standard Contractual Clauses shall automatically terminate once the Customer Personal Data transfer governed thereby becomes lawful under European Data Protection Laws in the absence of such Standard Contractual Clauses on any other basis; and
(i) in the event that the Standard Contractual Clauses cease to be recognized as a legitimate basis for the transfer of Personal Data to an entity located outside the European Economic Area, the parties shall reasonably cooperate to identify and implement an alternative legitimate basis for such transfer to the extent that one is required by European Data Protection Laws.

9. DELETION OR RETURN OF CUSTOMER PERSONAL DATA.

Unless otherwise required by Data Protection Laws, following termination or expiration of the Agreement Experlogix shall, at Customer's option, delete or return Customer Personal Data and all copies to Customer.

10. GENERAL TERMS.

This DPA will, notwithstanding the expiration or termination of the Agreement, remain in effect until, and automatically expire upon, Experlogix's deletion of all Customer Personal Data. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (a)

amended as necessary to ensure its validity and enforceability, while preserving the intent of the provision as closely as possible or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein. To the extent of any conflict or inconsistency between this DPA and the other terms of the Agreement, this DPA will govern. Unless otherwise expressly stated herein, the parties will provide notices under this DPA in accordance with the Agreement, provided that all such notices may be sent via email. Any liabilities arising in respect of this DPA are subject to the limitations of liability under the Agreement. This DPA will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

APPENDIX 1
SUBJECT MATTER AND DETAILS OF PROCESSING

This Appendix 1 includes certain details of the Processing of Customer Personal Data as required by Article 28(3) of the GDPR or similar provisions of the UK GDPR or the Standard Contractual Clauses, as applicable.

Subject matter and duration of the Processing of Customer Personal Data:

The subject matter and duration of the Processing of Personal Data are set out in the Agreement and this DPA.

The nature and purpose of the Processing of Customer Personal Data

Processing of Customer Personal Data by Experlogix is reasonably required to facilitate or support the provision of the Services as described under the Agreement and this DPA.

Type of Customer Personal Data:

The types of Customer Personal Data Processed are determined and controlled by Customer in its sole discretion, and may include name and contact details.

Categories of Data Subjects:

The categories of Data Subject about whom the Customer Personal Data relates are determined and controlled by Customer in its sole discretion, and may include Customer's clients, potential clients, and other business contacts.

APPENDIX 2
SECURITY MEASURES

A. Experlogix Information Security Program.

Experlogix has implemented, maintains and complies with information security policies and procedures designed to protect the confidentiality, availability, and integrity of Customer Personal Data and any systems that store or otherwise Process it, which are: (a) aligned with an industry-standard control framework (e.g., NIST SP 800-53, ISO 27001, CIS Critical Security Controls); (b) approved by executive management; (c) reviewed and updated at least annually; and (d) communicated to all personnel with access to Customer Personal Data.

Experlogix is currently undergoing a SOC 2 audit to verify that the organization's information security program meets or exceeds the rigorous SOC 2 standards for security and availability and complies with SSAE-16 SOC 2 Type II.

B. Risk Assessment.

Experlogix maintains risk assessment procedures for the purposes of periodic review and assessment of risks to the organization, monitoring and maintaining compliance with the organization's policies and procedures, and reporting the condition of the organization's information security and compliance to internal senior management.

C. Personnel Training.

Experlogix trains personnel to maintain the confidentiality, integrity, availability and security of Customer Personal Data, consistent with the terms of the Agreement and Data Protection Laws.

D. Vendor Management.

Prior to engaging Subprocessors and other subcontractors, Experlogix conducts reasonable due diligence and monitoring to ensure subcontractors are capable of maintaining the privacy, confidentiality, security, integrity and availability of Customer Personal Data.

E. Access Controls.

Only authorized personnel and third parties are permitted to access Customer Personal Data. Experlogix maintains logical access controls designed to limit access to Customer Personal Data and relevant information systems (e.g. granting access on a need-to-know basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access when employment terminates or changes in job functions occur).

F. Secure User Authentication.

Experlogix maintains password controls designed to manage and control password strength, expiration, and usage. These controls include prohibiting users from sharing passwords and requiring that passwords controlling access to Customer Personal Data must: (a) be at least eight (8) characters in length and meet minimum complexity requirements; (b) not be stored in readable format on the organization's computer systems; (c) have a history threshold to prevent reuse of recent passwords; and (d) if newly issued, be changed after first use.

G. Incident Detection and Response.

Experlogix maintains policies and procedures to detect and respond to actual or reasonably suspected Security Incidents, and encourages the reporting of such incidents.

H. Encryption.

Experlogix applies industry standard encryption to Customer Personal Data: (a) stored on any medium (i.e., laptops, mobile devices, portable storage devices, file servers and application databases); and (b) transmitted across any public network (such as the Internet) or wirelessly.

I. Network Security.

Experlogix has implement network security controls such as up-to-date firewalls, layered DMZs, updated intrusion detection/prevention systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

J. Vulnerability Management.

To detect, assess, mitigate, remove, and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code, Experlogix has implemented vulnerability management, threat protection technologies, and scheduled monitoring procedures.

K. Change Control.

Experlogix follows change management procedures and has implemented tracking mechanisms designed to test, approve and monitor all changes to the organization's technology and information assets.

L. Physical Security.

The physical and environmental security of data centers, server room facilities and other areas containing Customer Personal Data is designed to: (a) protect information assets from unauthorized physical access; (b) manage, monitor and log movement of persons into and out of the organization's facilities; and (c) guard against environmental hazards such as heat, fire and water damage.

M. Business Continuity and Disaster Recovery.

Experlogix maintains business continuity and disaster recovery policies and procedures designed to maintain service and recover from foreseeable emergency situations or disasters. This includes the use of commercially reasonable efforts to maintain 99.5% service uptime except for (a) planned downtime or (b) any unavailability caused by circumstances beyond Experlogix's reasonable control (e.g., acts of God, acts of government, acts of terror, Internet service provider failures or delays).

APPENDIX 3

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Customer (the data exporter) and Experlogix LLC, 10808 S Riverfront Pkwy Suite 650, South Jordan, Utah 84095, United States of America (the data importer), each a "party"; together "the parties", HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
(b) 'the data exporter' means the controller who transfers the personal data;
(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
(e) that it will ensure compliance with the security measures;
(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
(d) that it will promptly notify the data exporter about:
    (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
    (ii) any accidental or unauthorised access; and
    (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for 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 or by operation of law, in which case the data subject can enforce its rights against such entity.
3. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
4. 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.