EXPERLOGIX
DATA PROCESSING ADDENDUM

Updated: January 9, 2023

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, European Data Protection Laws and United States 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, in each case to the extent applicable: (a) the EU General Data Protection Regulation 2016/679 ("**GDPR**"); (b) the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"), the Data Protection Act of 2018, and all other laws relating to data protection, the processing of personal data, privacy, or electronic communications in force from time to time in the United Kingdom (collectively, "**UK Data Protection Laws**"); (c) the Swiss Federal Act on Data Protection ("**Swiss FDPA**"); and (d) any other applicable law, rule, or regulation related to the protection of Customer Personal Data in the European Economic Area, United Kingdom, or Switzerland that is already in force or that will come into force during the term of this Addendum.

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, as applicable, Module Two (Transfer controller to processor) or Module Three (Transfer processor to processor) of the standard contractual clauses approved by the European Commission's implementing decision (C(2021)3972) of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/678 or the European Parliament and of the Council (available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en), as supplemented or modified by Appendix 3.

1.17 "**Subprocessor**" means any Processor 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 "**United States Data Protection Laws**" means, in each case to the extent applicable: (a) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and its implementing regulations (collectively, "**CCPA**"); (b) the Virginia Consumer Data Protection Act ("**VCPDA**"), when effective; (c) the Colorado Privacy Act and its implementing regulations ("**CPA**"), when effective; (d) the Utah Consumer Privacy Act ("**UCPA**"), when effective; (e) Connecticut SB6, An Act Concerning Personal Data Privacy and Online Monitoring ("**CTDPA**"); and (f) any other applicable law or regulation related to the protection of Customer Personal Data in the United States that is already in force or that will come into force during the term of this Addendum.

1.20 "**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. As used in this Section 2.3, the terms "Sell," "Share," "Business Purpose," and "Commercial Purpose" shall have the meanings given in the CCPA and "Personal Information" shall mean any personal information (as defined in the CCPA) contained in Customer Personal Data. Experlogix will not: (a) Sell or Share any Personal Information; (b) retain, use, or disclose any Personal Information (i) for any purpose other than for the Business Purposes specified in the Agreement, including for any Commercial Purpose other than the Business Purposes specified in the Agreement, or as otherwise permitted by the CCPA, or (ii) outside of the direct business relationship between Customer and Experlogix; or (c) combine Personal Information received from, or on behalf of, Customer with Personal Data received from or on behalf of any third party, or collected from Experlogix's own interaction with Data Subjects, except to perform any Business Purpose permitted by the CCPA. Experlogix hereby certifies that it understands the foregoing restrictions under this Section 2.3 and will comply with them. The parties acknowledge that the Personal Information disclosed by Customer to Experlogix is provided to Experlogix only for the limited and specified purposes set forth in the Agreement and this Addendum. Experlogix will comply with applicable obligations under the CCPA and provide the same level of privacy protection to Personal Information as is required by the CCPA. Customer has the right to take reasonable and appropriate steps to help ensure that Experlogix uses the Personal Information transferred in a manner consistent with Customer's obligations under the CCPA by exercising Customer's audit rights in Section 7. Experlogix will notify Customer if it makes a determination that Experlogix can no longer meet its obligations under the CCPA. If Experlogix notifies Customer of unauthorized use of Personal Information, including under the foregoing sentence, Customer will have the right to take reasonable and appropriate steps to

stop and remediate such unauthorized use by limiting the Personal Information shared with Experlogix, terminating the portion of the Agreement relevant to such unauthorized use, or such other steps mutually agreed between the parties in writing.

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 ten (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 Sections 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 Customer transfers Customer Personal Data to Experlogix that is subject to European Data Protection Laws, and such transfer is not subject to an alternative adequate transfer mechanism under European Data Protection Laws or otherwise exempt from cross-border transfer restrictions, then Customer (as "data exporter") and Experlogix (as "data importer") agree that the applicable terms of the Standard Contractual Clauses shall apply to and govern such transfer and are hereby incorporated herein by reference. In furtherance of the foregoing, the parties agree that: (a) the execution of this Addendum shall constitute execution of the applicable Standard Contractual Clauses as of the Addendum Effective Date; (b) the relevant selections, terms, and modifications set forth in Appendix 3 shall apply, as applicable; and (c) 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.

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.

Previous Versions:

- June 10, 2022
- May 20, 2021

APPENDIX 1
SUBJECT MATTER AND DETAILS OF PROCESSING

This Appendix 1 includes certain details of the Processing of Customer Personal Data as may be required by Data Protection Laws 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.

Categories 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.

Special/Sensitive Categories of Customer Personal Data:

N/A

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.

Frequency of Customer's transfer of Customer Personal Data:

On a continuous basis for the term of the Agreement.

The period for which Customer Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:

As set forth in the DPA and the Agreement.

For transfers to Subprocessors, the subject matter, nature and duration of the Processing of Customer Personal Data:

As set forth in the DPA and the Agreement.

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 industry-standard control frameworks; (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 I.

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

1. **Application of Modules**. If Customer is acting as a Controller with respect to Customer Personal Data, "Module Two: Transfer controller to processor" of the Standard Contractual Clauses shall apply. If Customer is acting as a Processor to a third-party Controller with respect to Customer Personal Data, Experlogix is a sub-Processor and "Module Three: Transfer processor to processor" of the Standard Contractual Clauses shall apply.

2. **Sections I-V.** The parties agree to the following selections in Sections I-IV the Standard Contractual Clauses: (a) the parties select Option 2 in Clause 9(a) and the specified time period shall be ten (10) days; (b) the optional language in Clause 11(a) is omitted; (c) the parties select Option 1 in Clause 17 and the governing law of the Republic of Ireland will apply; and (d) in Clause 18(b), the parties select the courts of the Republic of Ireland.

3. **Annexes.** The name, address, contact details, activities relevant to the transfer, and role of the parties set forth in the Agreement and the Addendum shall be used to complete Annex I.A. of the Standard Contractual Clauses. The information set forth in Appendix 1 to the Addendum shall be used to complete Annex I.B. of the Standard Contractual Clauses. The competent supervisory authority in Annex I.C. of the Standard Contractual Clauses shall be the relevant supervisory authority determined by Clause 13 and the GDPR, unless otherwise set forth in Sections 5 or 6 of this Appendix 3. If such determination is not clear, then the competent supervisory authority shall be the Irish Data Protection Authority. The technical and organizational measures in Annex II of the Standard Contractual Clauses shall be the measures set forth in Appendix 2 to the Addendum.

4. **Supplemental Business-Related Clauses.** In accordance with Clause 2 of the Standard Contractual Clauses, the parties wish to supplement the Standard Contractual Clauses with business-related clauses, which shall neither be interpreted nor applied in such a way as to contradict the Standard Contractual Clauses (whether directly or indirectly) or to prejudice the fundamental rights and freedoms of Data Subjects. Experlogix and Customer therefore agree that the applicable terms of the Agreement and the Addendum shall apply if, and to the extent that, they are permitted under the Standard Contractual Clauses, including without limitation the following: (a) the instructions described in Clause 8.1 are set forth in Section 2.2 of the Addendum; (b) in the event a Data Subject requests a copy of the Standard Contractual Clauses or the Addendum under Clause 8.3, Customer shall make all redactions reasonably necessary to protect business secrets or other confidential information of Experlogix; (c) deletion or return of Customer Personal Data by Experlogix under the Standard Contractual Clauses shall be governed by Section 9 of the Addendum; (d) certification of deletion of Customer Personal Data under Clause 8.5 or Clause 16(d) will be provided by Experlogix upon the written request of Customer; (e) Experlogix shall be deemed in compliance with Clause 8.8 to the extent such onward transfers occur in accordance with Article 4 of the Commission Implementing Decision (EU) 2021/914 of 4 June 2021; (f) any information requests or audits provided for in Clause 8.9 shall be fulfilled in accordance with Section 7 of the Addendum; (g) the relevant terms of the Agreement which govern indemnification or limitation of liability shall apply to Experlogix's liability under Clauses 12(a), 12(d), and 12(f); and (h) the relevant terms of the Agreement which govern termination shall apply to a termination pursuant to Clauses 14(f) or 16.

5. **Transfers from the United Kingdom**. If Customer transfers Customer Personal Data to Experlogix that is subject to UK Data Protection Laws, the parties acknowledge and agree that: (a) the template addendum issued by the Information Commissioner's Office of the United Kingdom and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 (available at: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf), as it may be revised from time to time by the Information Commissioner's Office (the "**UK Addendum**") shall be incorporated by reference herein; (b) the UK Addendum shall apply to and modify the Standard Contractual Clauses solely to the extent that UK Data Protection Laws apply to Customer's Processing when making the transfer; (c) the information required to be set forth in "Part 1: Tables" of the UK Addendum shall be completed using the information provided in this Appendix 3 and the Addendum; and (d) either party may end the UK Addendum in accordance with section 19 thereof.

6. **Transfers from Switzerland.** If Customer transfers Customer Personal Data to Experlogix that is subject to the Swiss FDPA, the following modifications shall apply to the Standard Contractual Clauses to the extent that the Swiss FDPA applies to Customer's Processing when making that transfer: (a) the term "member state" as used in the Standard Contractual Clauses shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from suing for their rights in their place of habitual residence in accordance with Clause 18(c) of the Standard Contractual Clauses; (b) references to the GDPR or other governing law contained in the Standard Contractual Clauses shall also be interpreted to include the Swiss FDPA; and (c) the parties agree that the supervisory authority as indicated in Annex I.C of the Standard Contractual Clauses shall be the Swiss Federal Data Protection and Information Commissioner.