RADICL DATA PROCESSING ADDENDUM

Last Updated: 02/13/2024

This Data Processing Addendum ("**DPA**") is incorporated into and forms part of the Services Terms and Conditions (the "**Agreement**") between RADICL and Customer. RADICL and Customer are each referred to herein as a "**Party**" and together, the "**Parties**".

Capitalized terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms used but not otherwise defined herein shall have the meanings given to them in the Agreement. Except as expressly modified below, the terms of the Agreement shall remain in full force and effect. This DPA supersedes and replaces any privacy or data protection terms relating to the subject matter of this DPA that were previously entered into between RADICL and Customer from the Effective Date.

The following obligations shall only apply to the extent required by Data Protection Laws with regard to the relevant Customer Personal Data, if applicable.

1. DEFINITIONS.

1.1. "**Controller**" means an entity that determines the purposes and means of the Processing of Personal Data.

1.2. "**Customer**" means the entity identified on the Order Form that is receiving the Services from RADICL and has agreed to the terms of the Agreement with RADICL.

1.3. "**Customer Personal Data**" means Personal Data Processed by RADICL on behalf of Customer to perform the Services under the Agreement.

1.4. "**Data Protection Laws**" means the data privacy and security laws and regulations of any jurisdiction applicable to the Processing of Customer Personal Data, including, in each case to the extent applicable, European Data Protection Laws and the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and its implementing regulations (collectively, "**CCPA**").

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

1.6. "**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 FADP**"); 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 DPA.

1.7. "**Personal Data**" means information that constitutes "personal information," "personal data," "personally identifiable information," or similar term under Data Protection Laws.

1.8. "**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.

1.9. "**Processor**" means an entity that Processes Personal Data on behalf of a Controller.

1.10. "**RADICL**" means RADICL Defense, Inc.

1.11. "**Security Incident**" means a breach of RADICL's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data in RADICL's possession, custody, or control. "Security Incident" does 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.

1.12. "**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 Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (currently available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0914&qid=1688587744942), as supplemented or modified by **Appendix 3**.

1.13. "**Subprocessor**" means any Processor appointed by RADICL to Process Customer Personal Data on behalf of Customer under the Agreement.

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

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 RADICL is a Processor. In some circumstances, the Parties acknowledge that Customer may be acting as a Processor to a third-party Controller in respect of Customer Personal Data, in which case RADICL will remain a Processor with respect to the Customer in such event. 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**. RADICL will Process Customer Personal Data only in accordance with Customer's documented instructions unless otherwise required by applicable law, in which case RADICL will inform Customer of such Processing unless notification is prohibited by applicable law. Customer hereby instructs RADICL to Process Customer Personal Data: (a) to provide the Services to Customer; (b) to perform its obligations and exercise its rights under the Agreement and this DPA; and (c) as necessary to prevent or address technical problems with the Services. RADICL will notify Customer if, in its opinion, an instruction of Customer infringes upon Data Protection Laws. Customer's instructions for the Processing of Customer Personal Data shall comply with Data Protection Laws. Customer shall be responsible for: (i) giving adequate notice and making all appropriate disclosures to Data Subjects regarding Customer's use and disclosure and RADICL's Processing of Customer Personal Data; and (ii) obtaining all necessary rights, and, where applicable, all appropriate and valid consents to disclose such Customer Personal Data to RADICL to permit the Processing of such Customer Personal Data by RADICL for the purposes of performing RADICL's obligations under the Agreement or as may be required by Data Protection Laws. Customer shall notify RADICL of any changes in, or revocation of, the permission to use, disclose, or otherwise Process Customer Personal Data that would impact RADICL's ability to comply with the Agreement, this DPA, or Data Protection Laws.

2.3. **Details of Processing**. The Parties acknowledge and agree that the nature and purpose of the Processing of Customer Personal Data, the types of Customer Personal Data Processed, the categories of Data Subjects, and other details regarding the Processing of Customer Personal Data are as set forth in **Appendix 1**.

2.4. **Processing Subject to the CCPA**. As used in this Section 2.4, 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. RADICL 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 RADICL; 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 RADICL's own interaction with Data Subjects, except to perform any Business Purpose permitted by the CCPA. RADICL hereby certifies that it understands the foregoing restrictions under this Section 2.4 and will comply with them. The Parties acknowledge that the Personal Information disclosed by Customer to RADICL is provided to RADICL only for the limited and specified purposes set forth in **Appendix 1**. RADICL 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 RADICL uses the Personal Information transferred in a manner consistent with Customer's obligations under the CCPA by exercising Customer's audit rights in Section 8. RADICL will notify Customer if it makes a determination that RADICL can no longer meet its obligations under the CCPA. If RADICL 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 RADICL, terminating the portion of the Agreement relevant to such unauthorized use, or such other steps mutually agreed between the Parties in writing.

2.5. **De-identified Data.** With respect to any de-identified data created by RADICL from Customer Personal Data, RADICL will: (i) take any necessary measures to ensure that such de-identified data cannot be associated with a Data Subject; (ii) publicly commit to maintaining and using de-identified data without attempting to re-identify the data; (iii) comply with the requirements of Data Protection Laws with respect to the creation of such de-identified data; and (iv) contractually obligate any recipients of the de-identified data to comply with restrictions substantially similar to those set forth in this Section 2.5.

3. **CONFIDENTIALITY**. RADICL shall take reasonable steps to ensure that RADICL personnel who Process Customer Personal Data are subject to obligations of confidentiality or are under an appropriate statutory obligation of confidentiality with respect to such Customer Personal Data.

4. **SECURITY**.

4.1. **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, RADICL shall implement appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk, in accordance with the security standards in **Appendix 2** (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 RADICL's security obligations hereunder.

4.2. **Security Incidents**. Upon becoming aware of a confirmed Security Incident, RADICL 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. RADICL will take reasonable steps to provide Customer with information available to RADICL that Customer may reasonably require to comply with its obligations under Data Protection Laws. RADICL's notification of or response to a Security Incident under this Section 4.2 will not be construed as an acknowledgement by RADICL of any fault or liability with respect to the Security Incident.

4.3. **Customer Responsibilities**. Customer agrees that, without limitation of RADICL's obligations under this Section 4, Customer is solely responsible for its 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; and (b) securing any account authentication credentials, systems, and devices Customer uses to access or connect to the Services, where applicable. Without limiting RADICL's obligations hereunder, Customer is responsible for reviewing the information made available by RADICL 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.

5. **SUBPROCESSING**. Subject to the requirements of this Section 5, Customer generally authorizes RADICL to engage Subprocessors as RADICL considers reasonably appropriate for the Processing of Customer Personal Data. A list of RADICL's Subprocessors, including their functions and locations, is available upon Customer's request and may be updated by RADICL from time to time in accordance with this Section 5. RADICL will notify Customer of the addition or replacement of any Subprocessor at least ten (10) days prior to such engagement. Customer may object to such changes on reasonable data protection grounds by providing RADICL written notice of such objection within ten (10) days. Upon receiving such an objection, where practicable and at RADICL's sole discretion RADICL will use commercially reasonable efforts to: (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; or (b) take corrective steps requested by Customer in its objection and proceed to use the new Subprocessor. If RADICL informs Customer that such change or corrective steps cannot be made, Customer may, as its sole and exclusive remedy available under this Section 5, terminate the relevant portion of the Agreement involving the Services which require the use of the proposed Subprocessor by providing written

notice to RADICL. When engaging any Subprocessor, RADICL will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in this DPA. RADICL shall be liable for the acts and omissions of the Subprocessor to the extent RADICL would be liable under the Agreement and this DPA.

6. **DATA SUBJECT RIGHTS**. RADICL will, taking into account the nature of the Processing of Customer Personal Data and the functionality of the Services, provide reasonable assistance to Customer by appropriate technical and organizational measures, insofar as this is possible, as necessary for Customer to fulfill its obligations under Data Protection Laws to respond to requests by Data Subjects to exercise their rights under Data Protection Laws. RADICL reserves the right to charge Customer on a time and materials basis in the event that RADICL considers that such assistance is onerous, complex, frequent, or time consuming. If RADICL receives a request from a Data Subject under any Data Protection Laws with respect to Customer Personal Data, RADICL will advise the Data Subject to submit the request to Customer and Customer will be responsible for responding to any such request.

7. **ASSESSMENTS AND PRIOR CONSULTATIONS**. In the event that Data Protection Laws require Customer to conduct a data protection impact assessment, transfer impact assessment, or prior consultation with a Supervisory Authority in connection with RADICL's Processing of Customer Personal Data, following written request from Customer, RADICL shall use reasonable commercial efforts to provide relevant information and assistance to Customer to fulfil such request, taking into account the nature of RADICL's Processing of Customer Personal Data and the information available to RADICL. RADICL reserves the right to charge Customer on a time and materials basis in the event that RADICL considers that such assistance is onerous, complex, frequent, or time consuming.

8. **RELEVANT RECORDS AND AUDIT RIGHTS**.

8.1. **Review of Information and Records**. Upon Customer's reasonable written request, RADICL will make available to Customer all information in RADICL's possession reasonably necessary to demonstrate RADICL's compliance with Data Protection Laws and RADICL's obligations set out in this DPA. Such information will be made available to Customer no more than once per calendar year and subject to the confidentiality obligations of the Agreement or a mutually-agreed non-disclosure agreement.

8.2. **Audits**. If Customer requires information for its compliance with Data Protection Laws in addition to the information provided under Section 8.1, at Customer's sole expense and to the extent Customer is unable to access the additional information on its own, RADICL will allow for, cooperate with, and contribute to reasonable assessments and audits, including inspections, by Customer or an auditor mandated by Customer ("**Mandated Auditor**"), provided that (a) Customer provides RADICL with reasonable advance written notice including the anticipated date of the audit, the proposed scope of the audit, and the identity of any Mandated Auditor, which shall not be a competitor of RADICL; (b) RADICL approves the Mandated Auditor in writing, 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 RADICL's normal business operations; (d) Customer or any Mandated Auditor complies with RADICL's standard safety, confidentiality, and security policies or 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, or any results of any such audit, will be deemed to be the Confidential Information of RADICL and subject to a nondisclosure agreement to be provided by RADICL; and (f) Customer may initiate such audit not more than once per calendar year unless otherwise required by a Supervisory Authority or Data Protection Laws.

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

9. **DATA TRANSFERS**.

9.1. **Data Processing Facilities**. RADICL may, subject to Sections 9.2 and 9.3, Process Customer Personal Data in the United States or anywhere RADICL or its Subprocessors maintains facilities. Customer is responsible for ensuring that its use of the Services complies with any cross-border data transfer restrictions of Data Protection Laws.

9.2. European Transfers. If Customer transfers Customer Personal Data to RADICL 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 RADICL (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 DPA shall constitute execution of the applicable Standard Contractual Clauses as of the DPA 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.

9.3. Other Jurisdictions. If Customer transfers Customer Personal Data to RADICL that is subject to Data Protection Laws other than European Data Protection Laws which require the Parties to enter into standard contractual clauses to ensure the protection of the transferred Customer Personal Data, and the transfer is not subject to an alternative adequate transfer mechanism under Data Protection Laws or otherwise exempt from cross-border transfer restrictions, then the Parties agree that the applicable terms of any standard contractual clauses approved or adopted by the relevant Supervisory Authority pursuant to such Data Protection Laws shall automatically apply to such transfer and, where applicable, shall be completed on a *mutatis mutandis* basis to the completion of the Standard Contractual Clauses as described in Section 9.2.

10. DELETION OR RETURN OF CUSTOMER PERSONAL DATA. Following termination or expiration of the Agreement, RADICL will delete Personal Data in accordance with the Agreement except to the extent required by applicable law. If RADICL retains Customer Personal Data pursuant to applicable law, RADICL agrees that all such Customer Personal Data will continue to be protected in accordance with this DPA.

11. MODIFICATIONS. Notwithstanding anything to the contrary in the Agreement, RADICL may modify this DPA if changes are necessary: (a) for compliance with Data Protection Laws or guidance issued by a Supervisory Authority; or (2) to reflect RADICL's adoption of an alternative transfer mechanism under Section 9. RADICL will notify Customer at least 30 days (or such other period as may be required for compliance with Data Protection Law or guidance of a Supervisory Authority) before such amendment will take effect. If Customer objects to any such amendment, Customer may immediately terminate the Agreement by giving written notice to RADICL within 90 days of RADICL's notice.

12. GENERAL TERMS. This DPA will, notwithstanding the expiration or termination of the Agreement, remain in effect until, and automatically expire upon, RADICL's deletion or return 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 in relation to the Processing of Customer Personal Data, this DPA will govern. All notices to be provided under this DPA shall be provided in accordance with the Agreement, provided that any notices required to be provided by RADICL may be sent via email to Customer. 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 or the Standard Contractual Clauses.

APPENDIX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

1. Subject matter and duration of the Processing of Customer Personal Data

The subject matter and duration of the Processing are as described in the Agreement and the DPA.

2. Nature and purpose of the Processing of Customer Personal Data

The nature of the Processing involves those activities reasonably required to facilitate or support the provision of the Services as described in the Agreement and the DPA.

The purpose of the Processing of Customer Personal Data includes the following: (a) helping to ensure security and integrity, to the extent the use of Customer Personal Data is reasonably necessary and proportionate for these purposes; (b) debugging to identify and repair errors that impair existing intended functionality; (c) performing the Services as described in the Agreement and carrying out the instructions set forth in Section 2.2; (d) undertaking internal research for technological development and demonstration; and (e) undertaking activities to verify or maintain the quality or safety of the Services, and to improve, upgrade, or enhance the Services.

3. The categories of Data Subjects to whom Customer Personal Data relates

The categories of Data Subjects shall be as is contemplated or related to the Processing described in the Agreement, and may include employees, contractors, and other Customer infrastructure users.

4. The categories of Customer Personal Data

The categories of Customer Personal Data Processed are those categories contemplated in and permitted by Agreement, and may include IP address and related location data, device or user identifiers, related online activity data, audit trails, email addresses, first and last names, contents of potential phishing emails, and phone numbers.

5. The sensitive data included in Customer Personal Data

N/A

6. The frequency of Customer's transfer of Customer Personal Data to RADICL:

On a continuous basis for the term of the Agreement.

7. 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 or the Agreement.

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

For the same subject matter, nature, and duration set forth above.

APPENDIX 2: SECURITY MEASURES

1. **Information Security Program**. Implement, maintain, and comply with information security policies and procedures designed to protect the confidentiality, integrity, and availability 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., SOC 2 Type 2); (b) approved by executive management; (c) reviewed and updated at least annually; and (d) communicated to all personnel with access to Customer Personal Data.

2. **Risk Assessment**. Maintain 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.

3. **Personnel Training**. Train personnel to maintain the confidentiality, integrity, and availability of Customer Personal Data, consistent with the terms of the Agreement and Data Protection Laws.

4. **Vendor Management**. Prior to engaging Subprocessors and other subcontractors, conduct reasonable due diligence and monitoring to ensure subcontractors are capable of maintaining the confidentiality, integrity, and availability of Customer Personal Data.

5. **Access Controls**. Only authorized personnel and third parties are permitted to access Customer Personal Data. Maintain 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 or changing access when employment terminates or changes in job functions occur).

6. **Secure User Authentication**. Maintain 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 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.

7. **Incident Detection and Response**. Maintain policies and procedures to detect and respond to actual or reasonably suspected Security Incidents, and encourage the reporting of such incidents.

8. **Encryption**. Apply 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.

9. **Network Security**. Implement network security controls such as up-to-date firewalls, layered DMZs, updated intrusion detection and prevention systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

10. **Vulnerability Management**. Detect, assess, mitigate, remove, and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code, by implementing vulnerability management, threat protection technologies, and scheduled monitoring procedures.

11. **Change Control**. Follow change management procedures and implement tracking mechanisms designed to test, approve, and monitor all changes to the organization's technology and information assets.

12. **Physical Security**. Take steps to ensure the physical and environmental security of data centers, server room facilities and other areas containing Customer Personal Data, including by: (a) protecting information assets from unauthorized physical access; and (b) guarding against environmental hazards such as heat, fire, and water damage.

13. **Business Continuity and Disaster Recovery**. Maintain business continuity and disaster recovery policies and procedures designed to maintain service and recover from foreseeable emergency situations or disasters.

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, RADICL 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 of the Standard Contractual Clauses: (a) the Parties select Option 2 in Clause 9(a) and the specified time period shall be the notification time period set forth in Section 5 of the DPA; (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 DPA shall be used to complete Annex I.A. of the Standard Contractual Clauses. The information set forth in **Appendix 1** to the DPA 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 DPA.

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. RADICL and Customer therefore agree that the applicable terms of the Agreement and the DPA shall apply if, and to the extent that, they are permitted under the Standard Contractual Clauses, including without limitation the following:

   (a) Instructions. The instructions described in Clause 8.1 are set forth in Section 2.2 of the DPA.

   (b) Protection of Confidentiality. In the event a Data Subject requests a copy of the Standard Contractual Clauses or the DPA under Clause 8.3, Customer shall make all redactions reasonably necessary to protect business secrets or other confidential information of RADICL.

   (c) Deletion or Return. Deletion or return of Customer Personal Data by RADICL under the Standard Contractual Clauses shall be governed by Section 10 of the DPA. Certification of deletion of Customer Personal Data under Clause 8.5 or Clause 16(d) will be provided by RADICL upon the written request of Customer.

   (d) Audits and Certifications. Any information requests or audits provided for in Clause 8.9 shall be fulfilled in accordance with Section 8 of the DPA.

   (e) Liability. The relevant terms of the Agreement which govern indemnification or limitation of liability shall apply to RADICL's liability under Clauses 12(a), 12(d), and 12(f).

   (f) Termination. 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 RADICL 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 DPA**") shall be incorporated by reference herein; (b) the UK DPA 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 DPA shall be completed using the information provided in this **Appendix 3** and the DPA; and (d) either Party may end the UK DPA in accordance with section 19 thereof.

6. **Transfers from Switzerland.** If Customer transfers Customer Personal Data to RADICL that is subject to the Swiss FADP, the following modifications shall apply to the Standard Contractual Clauses to the extent that the Swiss FADP 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) the Standard Contractual Clauses shall also protect the data of legal entities until the entry into force of the revised Swiss FADP; (c) references to the GDPR or other governing law contained in the Standard Contractual Clauses shall also be interpreted to include the Swiss FADP; and (d) 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.