VIRSAE DATA PROTECTION ADDENDUM

This Data Protection Addendum (the "**Addendum**") is incorporated into and forms a part of the Terms of Use Agreement (the "**Agreement**") between Virsae, Inc. and the party identified as the Customer in the Agreement ("***Customer***") under which Virsae has agreed to provide the Virsae Solution to Customer. This Addendum governs the parties' responsibilities regarding the use and protection of Personal Information. All capitalized terms used in this Addendum have the meaning given to them in this Addendum or the Agreement.

1. Definitions

For purposes of this Addendum, the terms below have the meanings set forth below. Capitalized terms that are used but not defined in this Addendum have the meanings given in the Agreement.

1.1 **Affiliate** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

1.2 **Applicable Data Protection Laws** means European Data Protection Laws and the CCPA, in each case, to the extent applicable to the relevant Personal Data or processing thereof under the Agreement.

1.3 **CCPA** means the California Consumer Privacy Act of 2018 and any regulations promulgated thereunder, in each case, as amended from time to time.

1.4 **EEA** means the European Economic Area.

1.5 **EU** means the European Union.

1.6 **European Data Protection Laws** means the GDPR and other data protection laws of the EU, its Member States, Switzerland, Iceland, Liechtenstein, Norway and the United Kingdom, in each case, to the extent it applies to the relevant Personal Data or processing thereof under the Agreement.

1.7 **GDPR** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as amended from time to time.

1.8 **Information Security Incident** means a breach of Virsae's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Virsae's possession, custody or control. Information Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

1.9 **Personal Data** means (a) the personal data (as defined in GDPR) contained within the Collected Data and (b) any other Collected Data that constitutes "personal information" under and governed by the CCPA. For purposes of this Addendum, Personal Data does not include personal data of representatives of Customer with whom Virsae has business relationships independent of the Virsae Solution.

1.10 **Security Measures** has the meaning given in Section 4.1 (Virsae's Security Measures).

1.11 **Standard Contractual Clauses** means the mandatory provisions of the standard contractual clauses for the transfer of personal data to processors established in third countries in the form set out by European Commission Decision 2010/87/EU.

1.12 **Subprocessors** means third parties authorized under this Addendum to process Personal Data in relation to the Virsae Solution.

1.13 **Third Party Subprocessors** has the meaning given in Section 5 (Subprocessors) of Annex 1.

1.14 The terms **controller**, **data subject**, **processing**, **processor** and **supervisory authority** as used in this Addendum have the meanings given in the GDPR.

2. Duration and Scope of Addendum

2.1 This Addendum will, notwithstanding the expiration of the Agreement, remain in effect until, and automatically expire upon, Virsae's deletion of all Personal Data.

2.2 Annex 1 (EU Annex) to this Addendum applies to Personal Data or the processing thereof subject to European Data Protection Laws.

3. Customer Instructions

Virsae will process Personal Data only in accordance with Customer's instructions, which instructions are set forth herein. By entering into this Addendum, Customer instructs Virsae to process Personal Data to provide the Virsae Solution. Customer acknowledges and agrees that such instruction authorizes Virsae to process Personal Data as permitted as a Service Provider under the CCPA including: (a) to perform its obligations and exercise its rights under the Agreement; (b) perform its legal obligations and to establish, exercise or defend legal claims in respect of the Agreement; (c) pursuant to any other reasonable, written instructions given by Client and acknowledged in writing by Virsae as constituting instructions for purposes of this Addendum; and (d) as reasonably necessary for the proper management and administration of Virsae's business. Virsae will not (a) "sell" (as defined in the CCPA) or (b) retain, use, or otherwise disclose Personal Data for any purpose other than the specific purpose of providing the Virsae Solution or as otherwise contemplated under the Agreement.

4. Security

4.1 Virsae Security Measures. Virsae will implement and maintain technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data as described in Appendix 2 (the "***Security Measures***").

4.2 Information Security Incidents. If Virsae becomes aware of an Information Security Incident, Virsae will (a) notify Customer of the Information Security Incident without undue delay after becoming aware of the Information Security Incident and (b) take reasonable steps to identify the cause of such Information Security Incident, minimize harm and prevent a recurrence. Notifications made pursuant to this Section 4.2 will describe, to the extent possible, details of the Information Security Incident, including steps taken to mitigate the potential risks and steps Virsae recommends Customer take to address the Information Security Incident. Virsae's notification of or response to an Information Security Incident under this Section 4.2 will not be construed as an acknowledgement by Virsae of any fault or liability with respect to the Information Security Incident.

4.3 Customer's Security Responsibilities and Assessment

4.3.1 Customer's Security Responsibilities. Customer agrees that, without limitation of Virsae's obligations under Section 4.1 (Virsae Security Measures) and Section 4.2 (Information Security Incidents), Customer is solely responsible for its use of the Virsae Solution, including (a) making appropriate use of the Virsae Solution to ensure a level of security appropriate to the risk in respect of the Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Virsae Solution; (c) securing Customer's systems and devices that Virsae uses to provide the Virsae Solution; and (d) backing up Personal Data.

4.3.2 Customer's Security Assessment. Customer is solely responsible for evaluating for itself whether the Virsae Solution, the Security Measures and Virsae's commitments under this Addendum will meet Customer's needs, including with respect to any security obligations of Customer under Applicable Data Protection Laws or other laws. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Virsae provide a level of security appropriate to the risk in respect of the Personal Data.

5. Data Subject Rights

5.1 Customer's Responsibility for Requests. If Virsae receives any request from a data subject in relation to the data subject's Personal Data, Virsae will advise the data subject to submit the request to Customer and Customer will be responsible for responding to any such request.

5.2 Virsae's Data Subject Request Assistance. Virsae will (taking into account the nature of the processing of Personal Data) provide Customer with self-service functionality through the Virsae Solution or other reasonable assistance as necessary for Customer to perform its obligation under Applicable Data Protection Laws to fulfill requests by data subjects to exercise their rights under Applicable Data Protection Laws, including if applicable, Customer's obligation to respond to requests for exercising the data subject's rights set out in Chapter III of the GDPR. Customer shall reimburse Virsae for any such assistance, beyond providing self-service features included as part of the Virsae Solution, at Virsae's then-current professional services rates, which shall be made available to Customer upon request.

6. Customer Responsibilities

Customer represents and warrants to Virsae that (a) Customer has established or ensured that another party has established a legal basis for Virsae's processing of Personal Data contemplated by this Addendum; (b) all notices have been given to, and consents and rights have been obtained from, the relevant data subjects and any other party as may be required by Applicable Data Protection Laws and any other laws for such processing; and (c) Personal Data does not and will not contain any protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA), any biometric information, or any payment card information subject to the Payment Card Industry Data Security Standard.

7. Analytics

Customer acknowledges and agrees that Virsae may create and derive from processing under the Agreement anonymized and/or aggregated data that does not identify Customer or any natural person, and use, publicize or share with third parties such data to improve Virsae's products and services and for its other lawful business purposes.

8. Notices

Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Virsae to Customer may be given (a) in accordance with any notice clause of the Agreement; (b) to Virsae's primary points of contact with Customer; or (c) to any email provided by Customer for the purpose of providing it with Virsae Solution-related communications or alerts. Customer is solely responsible for ensuring that such email addresses are valid.

9. Effect of These Terms

Except as expressly modified by the Addendum, the terms of the Agreement remain in full force and effect. To the extent of any conflict or inconsistency between this Addendum and the other terms of the Agreement, this Addendum will govern. This Addendum replaces all other privacy, security or other data protection terms of the Agreement. Any liabilities arising in respect of this Addendum are subject to the limitations of liability under the Agreement.

Annex 1

EU Annex

1. Processing of Data

1.1 Subject Matter and Details of Processing. The parties acknowledge and agree that (a) the subject matter of the processing under the Agreement is Virsae's provision of the Virsae Solution; (b) the duration of the processing is from Virsae's receipt of Personal Data until deletion of all Personal Data by Virsae in accordance with the Agreement; (c) the nature and purpose of the processing is to provide the Virsae Solution; (d) the data subjects to whom the processing pertains are Customer's employees and other personnel; and (e) the categories of Personal Data are contact details, workplace communications and other information processed by workplace information systems about such data subjects.

1.2 Roles and Regulatory Compliance; Authorization. The parties acknowledge and agree that (a) Virsae is a processor of that Personal Data under European Data Protection Laws; (b) Customer is a controller of that Personal Data under European Data Protection Laws; and (c) each party will comply with the obligations applicable to it in such role under the European Data Protection Laws with respect to the processing of that Personal Data.

1.3 Virsae's Compliance with Instructions. Virsae will only process Personal Data in accordance with Customer's instructions described in this Section 3 (Customer Instructions) of the Addendum unless European Data Protection Laws requires otherwise, in which case Virsae will notify Customer (unless that law prohibits Virsae from doing so on important grounds of public interest).

1.4 Data Deletion. Upon termination of Customer's access to the Virsae Solution, Customer instructs Virsae to delete all Personal Data from Virsae's systems as soon as reasonably practicable, unless European Data Protection Laws requires otherwise.

2. Data Security

2.1 Virsae Security Measures, Controls and Assistance

2.1.1 Virsae Security Assistance. Virsae will (taking into account the nature of the processing of Personal Data and the information available to Virsae) provide Customer with reasonable assistance necessary for Customer to comply with its obligations in respect of Personal Data under European Data Protection Laws, including Articles 32 to 34 (inclusive) of the GDPR, by (a) implementing and maintaining the Security Measures; (b) complying with the terms of Section 4.2 (Information Security Incidents) of the Addendum; and (c) complying with this Annex 1.

2.1.2 Security Compliance by Virsae Staff. Virsae will grant access to Personal Data only to personnel who need such access for the scope of their job duties, and are subject to appropriate confidentiality arrangements.

2.2 Reviews and Audits of Compliance

2.2.1 Customer may audit Virsae's compliance with its obligations under this Addendum up to once per year and on such other occasions as may be required by European Data Protection Laws, including where mandated by Customer's supervisory authority. Virsae will contribute to such audits by providing Customer or Customer's supervisory authority with the information and assistance reasonably necessary to conduct the audit.

2.2.2 If a third party is to conduct the audit, Virsae may object to the auditor if the auditor is, in Virsae's reasonable opinion, not independent, a competitor of Virsae, or otherwise manifestly unsuitable. Such objection by Virsae will require Customer to appoint another auditor or conduct the audit itself.

2.2.3 To request an audit, Customer must submit a detailed proposed audit plan to Virsae at least two weeks in advance of the proposed audit date and any third party auditor must

sign a customary non-disclosure agreement mutually acceptable to the parties (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Virsae will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Virsae security, privacy, employment or other relevant policies). Virsae will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 2.2 shall require Virsae to breach any duties of confidentiality.

2.2.4 If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor within twelve (12) months of Customer's audit request and Virsae has confirmed there are no known material changes in the controls audited, Customer agrees to accept such report lieu of requesting an audit of such controls or measures.

2.2.5 The audit must be conducted during regular business hours, subject to the agreed final audit plan and Virsae's safety, security or other relevant policies, and may not unreasonably interfere with Virsae business activities.

2.2.6 Customer will promptly notify Virsae of any non-compliance discovered during the course of an audit and provide Virsae any audit reports generated in connection with any audit under this Section 2.2, unless prohibited by European 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/or confirming compliance with the requirements of this Addendum.

2.2.7 Any audits are at Customer's expense. Customer shall reimburse Virsae for any time expended by Virsae or its Third Party Subprocessors in connection with any audits or inspections under this Section 2.2 at Virsae's then-current professional services rates, which shall be made available to Customer upon request. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit. Nothing in this Addendum shall be construed to require Virsae to furnish more information about its Third Party Subprocessors in a connection with such audits than such Third Party Subprocessors make generally available to their customers.

3. Impact Assessments and Consultations

Virsae will (taking into account the nature of the processing and the information available to Virsae) reasonably assist Customer in complying with its obligations under Articles 35 and 36 of the GDPR, by (a) making available documentation describing relevant aspects of Virsae's information security program and the security measures applied in connection therewith; and (b) providing the other information contained in the Agreement including this Addendum.

4. Data Transfers

4.1 Data Processing Facilities. Virsae may, subject to Section 4.2 (Transfers out of the EEA), store and process Personal Data in the United States or anywhere Virsae or its Subprocessors maintains facilities.

4.2 Transfers out of the EEA. If Customer transfers Personal Data out of the EEA to Virsae in a country not deemed by the European Commission to have adequate data protection, 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, the parties agree that:

4.2.1 for purposes of the Standard Contractual Clauses, (a) Customer will act as the data exporter and (b) Virsae will act as the data importer;

4.2.2 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 Section 1.1 to this Annex 1 (Subject Matter and Details of Processing);

4.2.3 for purposes of Appendix 2 to the Standard Contractual Clauses, the technical and organizational measures shall be the Security Measures;

4.2.4 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;

4.2.5 the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be performed in accordance with Section 2.2 of this Annex 1 (Reviews and Audits of Compliance);

4.2.6 Customer's authorizations in Section 5 of this Annex 1 (Subprocessors) will constitute Customer's prior written consent to the subcontracting by Virsae of the processing of Personal Data if such consent is required under Clause 5(h) of the Standard Contractual Clauses;

4.2.7 certification of deletion of Personal Data as described in Clause 12(1) of the Standard Contractual Clauses shall be provided only upon Customer's request; and

4.3 notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply to the extent an alternative recognized compliance standard for the lawful transfer of Personal Data outside the EEA (e.g., US-E.U. Privacy Shield, binding corporate rules) applies to the transfer.

5. Subprocessors

5.1 Consent to Subprocessor Engagement. Customer specifically authorizes the engagement of Virsae's Affiliates as Subprocessors. In addition, Customer generally authorizes the engagement of any other third parties as Subprocessors ("**Third Party Subprocessors**").

5.2 Information about Subprocessors. Information about Subprocessors, including their functions and locations, is available at https://www.virsae.com/virsae-subprocessors (as may be updated by Virsae from time to time in accordance with this Annex 1).

5.3 Requirements for Subprocessor Engagement. When engaging any Subprocessor, Virsae will enter into a written contract with such Subprocessor containing data protection obligations materially consistent with those in this Addendum with respect to Personal Data to the extent applicable to the nature of the services provided by such Subprocessor. Virsae shall be liable for all obligations subcontracted to, and any Subprocessor of such obligations.

5.4 Opportunity to Object to Subprocessor Changes. To the extent required by law, when any new Third Party Subprocessor is engaged during the term of the Agreement, Virsae will notify Customer of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform) by updating the website listed in Section 5.2 (Information about Subprocessors). If Customer objects to such engagement in a written notice to Virsae within 15 days of being informed thereof on reasonable grounds relating to the protection of Personal Data, Customer and Virsae will work together in good faith to find a mutually acceptable resolution to address such objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe using reasonable and good faith efforts, Customer may, as its sole and exclusive remedy, terminate the Agreement and cancel the Virsae Solution by providing written notice to Virsae.

Annex 2

Security Measures

As from the Addendum Effective Date, Virsae will implement and maintain the Security Measures set out in this Annex 2.

1. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Virsae's organization, monitoring and maintaining compliance with Virsae's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.
2. Data security controls which include at a minimum, but may not be limited to, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilization of commercially available and industry standard encryption technologies for Personal Data that is:
    a. transmitted over public networks (i.e. the Internet) or when transmitted wirelessly; or
    b. at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes).
3. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (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).
4. Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that Virsae passwords that are assigned to its employees: (i) be at least eight (8) characters in length, (ii) not be stored in readable format on Virsae's computer systems; (iii) must be changed every ninety (90) days; must have defined complexity; (iv) must have a history threshold to prevent reuse of recent passwords; and (v) newly issued passwords must be changed after first use.
5. Physical and environmental security of data center, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of Virsae facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.
6. Change management procedures and tracking mechanisms designed to test, approve and monitor all changes to Virsae's technology and information assets.
7. Incident / problem management procedures design to allow Virsae to investigate, respond to, mitigate and notify of events related to Virsae's technology and information assets.
8. Network security controls that provide for the use of enterprise firewalls and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.
9. Vulnerability assessment and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.
10. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

Virsae may update or modify such Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Virsae Solutions.