HELIOS DATA PROCESSING and SECURITY AGREEMENT

Last Updated: 2021-Mar-09

This Helios Data Processing and Security Agreement, including its appendices (the "DPA"), supplements and forms part of the Helios Online Subscription Agreement ("Agreement"), which is available here: Helios Online Subscription Agreement. Terms used but not defined in this DPA have the meaning given in the Agreement.

1. Definitions

a. **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.

b. **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.

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

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

e. **EU** means the European Union.

f. **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.

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

h. **Information Security Incident** means a breach of Tx3's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Tx3'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 Software attacks, or other network attacks on firewalls or networked systems.

i. **Personal Data** means (a) the personal data (as defined in GDPR) that Customer provides to Tx3 for the provision of the Software and (b) any other information that Customer provides to Tx3 for the provision of the Software that constitutes "personal information" under and governed by the CCPA.

j. **Security Measures** has the meaning given in Section 1 (Tx3's Security Measures).

k. **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.

l. **Subprocessors** means third parties authorized under this DPA to process Personal Data in relation to the Software.

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

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

2. Duration and Scope of DPA

a. This DPA will, notwithstanding the expiration of the Agreement, remain in effect until, and automatically expire upon, Tx3's deletion of all Personal Data.

b. Annex 1 (EU Annex) to this DPA applies to Personal Data or the processing thereof subject to European Data Protection Laws. Annex 2 (California Annex) to this DPA, applies to Personal Data or the processing thereof subject to the CCPA.

3. **Customer Instructions**

Tx3 will process Personal Data only in accordance with Customer's instructions. By entering into this DPA, Customer instructs Tx3 to process Personal Data to provide the Software. Customer acknowledges and agrees that such instruction authorizes Tx3 to process Personal Data (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 written instructions given by Customer and acknowledged in writing by Tx3 as constituting instructions for purposes of this DPA; and (d) as reasonably necessary for the proper management and administration of Tx3's business.

4. **Security**

a. Tx3 Security Measures. Tx3 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 Annex 3 (the "Security Measures").

b. Information Security Incidents. If Tx3 becomes aware of an Information Security Incident, Tx3 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 Tx3 recommends Customer take to address the Information Security Incident. Tx3's notification of or response to an Information Security Incident under this Section 4.2 will not be construed as an acknowledgement by Tx3 of any fault or liability with respect to the Information Security Incident.

c. Customer's Security Responsibilities and Assessment

i. Customer's Security Responsibilities. Customer agrees that, without limitation of Tx3's obligations under Section 1 (Tx3 Security Measures) and Section 4.2 (Information Security Incidents), Customer is solely responsible for its use of the Software, including (a) making appropriate use of the Software 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 Software; (c) securing Customer's systems and devices that Tx3 uses to provide the Software; and (d) backing up Personal Data.

ii. Customer's Security Assessment. Customer is solely responsible for evaluating for itself whether the Software, the Security Measures and Tx3's commitments under this DPA 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 Tx3 provide a level of security appropriate to the risk in respect of the Personal Data.

5. **Data Subject Rights**

a. Customer's Responsibility for Requests. If Tx3 receives any request from a data subject in relation to the data subject's Personal Data, Tx3 will advise the data subject to submit the request to Customer and Customer will be responsible for responding to any such request.

b. Tx3's Data Subject Request Assistance. Tx3 will (taking into account the nature of the processing of Personal Data) provide Customer with self-service functionality through the Software 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 Tx3 for any such assistance, beyond providing self-service features included as part of the Software, at Tx3's then-current professional services rates, which shall be made available to Customer upon request.

6. **Customer Responsibilities**

Customer represents and warrants to Tx3 that (a) Customer has established or ensured that another party has established a legal basis for Tx3's processing of Personal Data contemplated by this DPA; and (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

7. **Analytics**

Customer acknowledges and agrees that Tx3 may create and derive from processing Personal Data 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 Tx3'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 Tx3 to Customer may be given (a) in accordance with any notice clause of the Agreement; (b) to Tx3's primary points of contact with Customer; or (c) to any email provided by Customer for the purpose of providing it with Software-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 DPA, the terms of the Agreement remain in full force and effect. To the extent of any conflict or inconsistency between this DPA and the other terms of the Agreement, this DPA will govern. This DPA replaces all other privacy, security or other data protection terms of the Agreement. Any liabilities arising in respect of this DPA are subject to the limitations of liability under the Agreement.

Annex 1

EU Annex

1. **Processing of Data**

a. Subject Matter and Details of Processing. The parties acknowledge and agree that (a) the subject matter of the processing under the Agreement is Tx3's provision of the Software; (b) the duration of processing is from Tx3's receipt of Personal Data until deletion of all Personal Data by Tx3 in accordance with the Agreement; (c) the nature and purpose of the processing is to provide the Software; (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.

b. Roles and Regulatory Compliance; Authorization. The parties acknowledge and agree that (a) Tx3 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.

c. Tx3's Compliance with Instructions. Tx3 will only process Personal Data in accordance with Customer's instructions described in this Section 3 (Customer Instructions) of the DPA unless European Data Protection Laws requires otherwise, in which case Tx3 will notify Customer (unless that law prohibits Tx3 from doing so on important grounds of public interest).

d. Data Deletion. Upon termination of Customer's access to the Software, Customer instructs Tx3 to delete all Personal Data from Tx3's systems as soon as reasonably practicable, unless European Data Protection Laws requires otherwise.

2. **Data Security**

a. Tx3 Security Measures, Controls and Assistance

i. Tx3 Security Assistance. Tx3 will (taking into account the nature of the processing of Personal Data and the information available to Tx3) 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 2 (Information Security Incidents) of the DPA; and (c) complying with this Annex 1.

ii. Security Compliance by Tx3 Staff. Tx3 will grant access to Personal Data only to Tx3 personnel who need such access for the scope of their job duties and are subject to appropriate confidentiality arrangements.

b. Reviews and Audits of Compliance

i. Customer may audit Tx3's compliance with its obligations under this DPA 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. Tx3 will contribute to such audits by providing Customer or Customer's supervisory authority with the information and assistance reasonably necessary to conduct the audit.

ii. If a third party is to conduct the audit, Tx3 may object to the auditor if the auditor is, in Tx3's reasonable opinion, not independent, a competitor of Tx3, or otherwise manifestly unsuitable. Such objection by Tx3 will require Customer to appoint another auditor or conduct the audit itself.

iii. To request an audit, Customer must submit a detailed proposed audit plan to Tx3 at least thirty (30) days 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. Tx3 will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Tx3 security, privacy, employment or other relevant policies). Tx3 will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 2 shall require Tx3 to breach any duties of confidentiality.

iv. The audit must be conducted during Tx3's regular business hours, subject to the agreed final audit plan and Tx3's safety, security or other relevant policies, and may not unreasonably interfere with Tx3 business activities.

v. Customer will promptly notify Tx3 of any non-compliance discovered during the course of an audit and provide Tx3 any audit reports generated in connection with any audit under this Section 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 DPA.

vi. Any audits are at Customer's expense. Customer shall reimburse Tx3 for any time expended by Tx3 or its Third Party Subprocessors in connection with any audits or inspections under this Section 2 at Tx3'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 DPA shall be construed to require Tx3 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**

Tx3 will (taking into account the nature of the processing and the information available to Tx3) 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 Tx3's information security program and the security measures applied in connection therewith; and (b) providing the other information contained in the Agreement including this DPA.

4. **Data Transfers**

a. Data Processing Facilities. Tx3 may, subject to Section 2 (Transfers out of the EEA), store and process Personal Data in the United States or anywhere Tx3 or its Subprocessors maintains facilities.

b. Transfers out of the EEA. If Customer transfers Personal Data out of the EEA to Tx3 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:

i. for purposes of the Standard Contractual Clauses, (a) Customer will act as the data exporter and (b) Tx3 will act as the data importer;

ii. 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 to this Annex 1 (Subject Matter and Details of Processing);

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

iv. 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, before providing the copy to data exporter;

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

vi. Customer's authorizations in Section 5 of this Annex 1 (Subprocessors) will constitute Customer's prior written consent to the subcontracting by Tx3 of the processing of Personal Data if such consent is required under Clause 5(h) of the Standard Contractual Clauses;

vii. 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

c. 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**

a. Consent to Subprocessor Engagement. Customer specifically authorizes the engagement of Tx3's Affiliates as Subprocessors. In addition, Customer generally authorizes the engagement of any other third parties as Subprocessors ("**Third Party Subprocessors**").

b. Information about Subprocessors. Information about Subprocessors, including their functions and locations, is available at https://tx3services.com/legal/helios-subprocessors (as may be updated by Tx3 from time to time in accordance with this Annex 1).

c. Requirements for Subprocessor Engagement. When engaging any Subprocessor, Tx3 will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in this DPA with respect to Personal Data to the extent applicable to the nature of the Softwares provided by such Subprocessor. Tx3 shall be liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

d. Opportunity to Object to Subprocessor Changes. When any new Third Party Subprocessor is engaged during the term of the Agreement, Tx3 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 0 (Information about Subprocessors). If Customer objects to such engagement in a written notice to Tx3 within 15 days of being informed thereof on reasonable grounds relating to the protection of Personal Data, Customer and Tx3 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, Customer may, as its sole and exclusive remedy, terminate the Agreement and cancel the Software by providing written notice to Tx3.

Annex 2

California Annex

1. Tx3 shall not retain, use, or disclose any Personal Data that constitutes "personal information" under the CCPA ("CA Personal Information") for any purpose other than for the specific purpose of providing the Softwares, or as otherwise permitted by CCPA, including retaining, using, or disclosing the CA Personal Information for a commercial purpose (as defined in CCPA) other than providing the Softwares.

2. Tx3 shall not (a) sell any CA Personal Information; (b) retain, use or disclose any CA Personal Information for any purpose other than for the specific purpose of providing the Softwares, including retaining, using, or disclosing the CA Personal Information for a commercial purpose (as defined in the CCPA) other than provision of the Software; or (c) retain, use or disclose the CA Personal Information outside of the direct business relationship between Tx3 and Customer. Tx3 hereby certifies that it understands its obligations under this Section 2 and will comply with them.

3. Provision of the Software encompasses the processing authorized by Customer's instructions described in Section 3 of the DPA (Customer Instructions).

4. Notwithstanding anything in the Agreement or any order form entered in connection therewith, the parties acknowledge and agree that Tx3's access to CA Personal Information or any other Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

Annex 3

Security Measures

As from the DPA Effective Date, Tx3 will implement and maintain the Security Measures set out in this Annex 3.

1. **Organizational management and dedicated staff** responsible for the development, implementation and maintenance of Tx3's information security program. A "zero trust" approach is used, following the latest IT industry guidelines.

2. **Audit and risk assessment** procedures for the purposes of periodic review and assessment of risks to Tx3's organization, monitoring and maintaining compliance with Tx3's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3. **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. Systems are "single-tenant", with each customer on their own network and infrastructure. Customers do not share systems, data, networks, or infrastructure.

    b. All data is encrypted at rest and in transit.

    c. SQL Transparent Data Encryption enabled

    d. Network perimeter is enforced by a gateway device providing WAF/OWASP protection.

    e. Published Backup/Restore SLA's and Disaster Recovery

4. **Operating System Security**

    a. Azure Defender is enabled to scan/assess vulnerabilities

    b. Antivirus/Antimalware is enabled

    c. Windows Firewall

    d. No Public IP on servers

    e. Monthly OS updates, with immediate critical security patching, if necessary

    f. Encryption

    g. ISO 27001 Compliance Monitoring

    h. Azure Security Center

5. **Network security** controls that provide for the use of enterprise firewalls, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

    a. Monitors

    b. Firewall & Network Security Group rules to close all ports, opening minimally, as required

    c. One public access point, with no application servers having public IP addresses.

6. A**ccess 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).

    a. All Tx3 employees are trained on Tx3 standard operating procedures, delivered and recorded via Tx3 Learning Management System.

    b. RBAC Controlled, logged access is provided to a select few employees to provide support or infrastructure activities

    c. Direct RDP/SSH over the internet is not available and disabled

    d. 2FA is enabled for access

7. **Password controls** designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that Tx3 passwords that are assigned to its employees: (i) be at least eight (8) characters in length, (ii) not be stored in readable format on Tx3'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.

8. **Monitoring & Assessment**

    a. All resources are automatically monitored upon creation via automation

    b. Assessment features monitor standards compliance (e.g. ISO 27001)

9. **Physical and environmental data center security** is delivered and managed by Tx3's infrastructure-as-a-service provider. Currently, that is Microsoft Azure. Azure complies to all Life Science relevant standards for security and control including SOC2, 21CFRPart11, GDPR, and multiple ISO standards. See Azure compliance documentation at https://aka.ms/AzureCompliance, and audit reports at https://servicetrust.microsoft.com.

10. **Change management** procedures and tracking mechanisms designed to test, approve and monitor all changes to Tx3's technology and information assets. Changes are documented, logged, and controlled via SOPs and change management systems. All changes are coordinated with customers to avoid disruption and assess potential impact.

11. **Incident / problem management** procedures design to allow Tx3 to investigate, respond to, mitigate and notify of events related to Tx3's technology and information assets.

    a. All resources are monitored. Potential problems are often addressed before impact on end users.

    b. Tx3's support site enables all customers to log high priority and business critical issues that immediately notify a response team.

12. **Business resiliency/continuity** and disaster recovery procedures designed to maintain Software and/or recovery from foreseeable emergency situations or disasters. Disaster Recovery procedures are tested annually.

Tx3 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 Software.