

EHS INSIGHT GDPR DATA PROCESSING AGREEMENT

Updated March 27, 2026

Table of Contents

- EHS Insight Data Processing Agreement
- Annex 1 – StarTex Security Standards
- Annex 2 – California Consumer Privacy Act

This Data Processing Agreement (“**DPA**”) is an agreement between StarTex Software LLC, a Texas limited liability company (d/b/a EHS Insight) (“StarTex”) and the entity indicated on the applicable Order Form (defined below as “Customer”).

In the course of providing the Services under the Agreement, StarTex may Process certain Personal Data (such terms defined below) on behalf of Customer and where StarTex Processes such Personal Data on behalf of Customer the Parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

This DPA supplements the EHS Insight Terms of Service Agreement available at <https://www.ehsinsight.com/tos>, as updated from time to time between Customer and StarTex Software, or other agreement between Customer and StarTex governing Customer’s use of the Service (the “**Agreement**”) when the GDPR applies to your use of the EHS Insight Services to process Customer Data. Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 19 of this DPA. Except as modified below, the terms of the Agreement shall remain in full force and effect.

1. Data Processing.

- 1.1 **Scope and Roles.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, StarTex is the Processor and that StarTex may engage Sub-processors pursuant to the requirements set forth in Section 7 below.
- 1.2 **Customer Controls.** Customer can use the Service Controls to assist it with its obligations related to Data Protection Requirements, including its obligations to respond to requests from data subjects. Taking into account the nature of the Processing, Customer agrees that it is unlikely that StarTex would become aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if StarTex becomes aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. StarTex will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Standard Contractual Clauses by providing the Service Controls that Customer can use to erase or rectify Customer Data.
- 1.3 **Details of Data Processing.**
 - (a) **Subject matter.** The EHS Software provides a data management system that captures, stores, and analyzes quality events, quality assurance and compliance actions, workplace health and safety information.
 - (b) **Duration.** As between StarTex and Customer, the duration of the data Processing under this DPA is determined by Customer.

(c) **Purpose.** The purpose of the data Processing under this DPA is the provision of the Services initiated by Customer from time to time.

(d) **Nature of the Processing.** Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

(e) **Type of Personal Data.** First name, Last name, Employee ID, Email address, Position name, Hire Date, Date of Birth, Gender, Home Address, Phone Number

(f) **Categories of data subjects.** Customer Data may relate to the following categories of data subjects: (a) Customer's employees and prospective employees; (b) Customer's contractors and temporary workers; (c) Customer's agents and authorized representatives; and (d) such other individuals whose Personal Data Customer submits to the Services. Access to Customer Data is restricted to authorized users as determined by Customer through the Service Controls.

1.4 **Compliance with Laws.** Each party will comply with all laws, rules, and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR.

2. **Customer Instructions.** The parties agree that this DPA and the Agreement (including Customer providing instructions via configuration tools such as the EHS Insight application and API made available by StarTex for the Services) constitute Customer's documented instructions regarding StarTex's Processing of Customer Data ("**Documented Instructions**"). StarTex will process Customer Data only in accordance with Documented Instructions. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between StarTex and Customer, including agreement on any additional fees payable by Customer to StarTex for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if StarTex declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA. Taking into account the nature of the Processing, Customer agrees that it is unlikely StarTex can form an opinion on whether Documented Instructions infringe the GDPR. If StarTex forms such an opinion, it will immediately notify Customer, in which case, Customer is entitled to withdraw or modify its Documented Instructions. StarTex shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to process Customer Data, provided that all such discretion is compatible with the requirements of the DPA, in particular the Documented Instructions.

3. **Confidentiality of Customer Data.** StarTex will not sell, provide access, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain, provide, or improve the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends StarTex a demand for Customer Data, StarTex will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, StarTex may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then StarTex will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless StarTex is legally prohibited from doing so.

4. **Confidentiality Obligations of StarTex Personnel.** StarTex restricts its personnel from Processing Customer Data without authorization by StarTex as described in the StarTex Security Standards. StarTex imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

5. Security of Data Processing

5.1 StarTex has implemented and will maintain the technical and organizational measures for the StarTex Network as described in the StarTex Security Standards and this Section. In particular, StarTex has implemented and will maintain the following technical and organizational measures:

- (a) security of the StarTex Network as set out in Section 1.1 of the StarTex Security Standards;
- (b) physical security of the facilities as set out in Section 1.2 of the StarTex Security Standards;
- (c) measures to control access rights for StarTex employees and contractors to the StarTex Network as set out in Section 1.1 of the StarTex Security Standards; and
- (d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by StarTex as described in Section 2 of the StarTex Security Standards.

5.2 StarTex strongly recommends that Customer implement the Customer Security Measures to protect Customer Data. The Customer Security Measures represent industry best practices for securing access to and use of the Services and are described in the Documentation. Customer is solely responsible for determining whether the Customer Security Measures are appropriate for its environment and for any consequences arising from its decision not to implement them. The Customer Security Measures include:

- (a) measures to ensure the ongoing confidentiality, integrity, availability and resilience of the Processing systems and services that are operated by Customer;
- (b) measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and
- (c) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

6. Sub-processing.

6.1 **Authorized Sub-processors.** StarTex gets prior general written authorization from the Customer to use Sub-processors provided that StarTex informs the Customer of intended addition or replacement of Sub-processors, thereby giving Customer the opportunity to object to such changes ("Sub-processors"). The EHS Insight website (currently posted at <https://www.ehsinsight.com/subprocessors/>) lists Sub-processors that are currently engaged by StarTex, including the country in which each Sub-processor processes data and the general purpose for which each Sub-processor is engaged. At least 30 days before StarTex engages a new or replacement Sub-processor, StarTex will update the applicable website and provide Customer with a mechanism to obtain notice of that update. To object to a Sub-processor, Customer can: (i) terminate the Agreement pursuant to its terms; or (ii) cease using the Service for which StarTex has engaged the Sub-processor.

6.2 **Sub-processor Obligations.** Where StarTex authorizes a Sub-processor as described in Section 6.1:

- (a) StarTex will restrict the Sub-processor's access to Customer Data only to what is necessary to provide or maintain the Services in accordance with the

Documentation, and StarTex will prohibit the Sub-processor from accessing Customer Data for any other purpose;

- (b) StarTex will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data Processing services provided by StarTex under this DPA, StarTex will impose on the Sub-processor the same contractual obligations that StarTex has under this DPA; and
- (c) StarTex will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause StarTex to breach any of StarTex's obligations under this DPA.

7. **StarTex Assistance with Data Subject Requests.** Taking into account the nature of the Processing, the Service Controls are the technical and organizational measures by which StarTex will assist Customer in fulfilling Customer's obligations to respond to data subjects' requests under the GDPR. If a data subject makes a request to StarTex, StarTex will promptly forward such request to Customer once StarTex has identified that the request is from a data subject for whom Customer is responsible. The parties agree that Customer's use of the Service Controls and StarTex forwarding data subjects' requests to Customer in accordance with this Section, represent the scope and extent of Customer's required assistance.

8. **Security Measures.** StarTex makes available a range of Service Controls that Customer is strongly recommended to implement as part of the Customer Security Measures. These controls represent industry best practices for securing Customer Data within the Services. Customer is responsible for: (a) evaluating and implementing the Customer Security Measures appropriate to its environment, as described in the Documentation; (b) properly configuring the Services; (c) using available Service Controls to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident, including through backups and routine archiving; (d) using encryption technology to protect Customer Data from unauthorized access; (e) managing and controlling access rights to Customer Data; and (f) maintaining accurate administrator contact information in the EHS Insight Services and the helpdesk site at all times, to ensure Security Incident notifications and other critical communications are received without delay. StarTex bears no liability for losses or damages arising from Customer's failure to implement any of the Customer Security Measures.

9. **Security Incident Notification.**

9.1 **Security Incident.** StarTex will (a) notify Customer of a confirmed Security Incident without undue delay, and in any event not later than seventy-two (72) hours after becoming aware that a Security Incident has occurred, and (b) take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident. If StarTex is unable to notify Customer within seventy-two (72) hours, StarTex will provide the notification together with a written explanation of the reasons for the delay. The notification obligation under this Section applies only to confirmed Security Incidents and does not require notification of security events that have not been confirmed as Security Incidents.

9.2 **StarTex Assistance.** To enable Customer to notify a Security Incident to supervisory authorities or data subjects (as applicable), StarTex will cooperate with and assist Customer by including in the notification under Section 9.1(a) such information about the Security Incident as StarTex is able to disclose to Customer, taking into account the nature of the Processing, the information available to StarTex, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the Processing,

Customer agrees that it is best able to determine the likely consequences of a Security Incident.

9.3 **Unsuccessful Security Incidents.** Customer agrees that:

- (a) an unsuccessful Security Incident will not be subject to this Section 9. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of the equipment or facilities utilized by StarTex for storing Customer Data, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and
- (b) StarTex's obligation to report or respond to a Security Incident under this Section 9 is not and will not be construed as an acknowledgement by StarTex of any fault or liability of StarTex with respect to the Security Incident.

9.4 **Communication.** Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means StarTex selects, including via email. As part of the Customer Security Measures, Customer is strongly recommended to ensure its administrators maintain accurate and current contact information in the EHS Insight Services and the helpdesk site at all times. StarTex will have no liability for any failure or delay in Customer's receipt of a Security Incident notification resulting from inaccurate or outdated contact information maintained by Customer.

10. StarTex Certifications and Audits.

10.1 **StarTex ISO-Certification and SOC Reports.** In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, StarTex will make available the certificates issued for the ISO 27001 certification, and the ISO 27017 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001 and ISO 27017).

10.2 **SOC Reports and Data Hosting.** StarTex uses Amazon Web Services ("AWS") for hosting the Services, and annually verifies AWS continues to maintain and provide the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3). StarTex reserves the right to switch to another hosting vendor so long as the replacement vendor maintains similar controls and reports.

10.3 **StarTex Audits.** StarTex uses external auditors to verify the adequacy of its security measures. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at StarTex's selection and expense; and (d) will result in the generation of an audit report ("Report"), which will be StarTex's Confidential Information

10.4 **Audit Reports.** At Customer's written request, and provided that the parties have an applicable NDA in place, StarTex will provide Customer with a copy of the Report so that Customer can reasonably verify StarTex's compliance with its obligations under this DPA.

10.5 **Privacy Impact Assessment and Prior Consultation.** Taking into account the nature of the Processing and the information available to StarTex, StarTex will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation, by providing the information StarTex makes available under this Section 10.

11. **Customer Audits.** If Customer chooses to conduct any audit, including any inspection, it has the right to do so by instructing StarTex to carry out the audit described in Section 10.3, subject to the following conditions:

(a) **Frequency.** Customer may request no more than one (1) audit per calendar year, except where a confirmed Security Incident has occurred, in which case Customer may request one (1) additional audit directly related to that incident within the same calendar year.

(b) **Notice.** Customer must provide StarTex with no less than thirty (30) days' prior written notice of a requested audit.

(c) **Cost Allocation.** StarTex will bear its internal costs for facilitating the audit. Customer will bear all costs for any third-party auditor engaged by Customer, and will reimburse StarTex for any reasonable out-of-pocket costs incurred by StarTex in connection with the audit.

(d) **Confidentiality.** Any audit results, findings, and reports will be treated as Confidential Information of both parties and subject to a mutually executed NDA prior to commencement of the audit.

(e) **Scope Limitation.** Audits will be conducted during normal business hours and in a manner that minimizes disruption to StarTex's operations. Customer and any third-party auditor must comply with StarTex's reasonable security and confidentiality requirements.

If StarTex declines to follow any instruction requested by Customer regarding audits, Customer is entitled to terminate the Agreement in accordance with its terms.

12. **Transfers of Personal Data.**

12.1 **Regions.** Customer can specify the location(s) where Customer Data will be processed within the StarTex Network (each a "**Region**"). Once Customer has made its choice, StarTex will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body.

12.2 **Application of Standard Contractual Clauses.** The Standard Contractual Clauses will only apply to Customer Data that is transferred, either directly or via onward transfer, to any Third Country, (each a "**Data Transfer**").

12.3 When Customer is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.

13. **Liability and Indemnity.**

13.1 **Mutual Indemnification.** StarTex indemnifies Customer and holds harmless Customer against all third-party claims, losses, damages, and reasonable legal expenses directly arising from StarTex's material breach of this DPA or the GDPR. Customer indemnifies,

and holds StarTex harmless against all third-party claims, losses, damages, and reasonable legal expenses directly arising from Customer's material breach of this DPA or the GDPR.

- 13.2 **Liability Cap.** Each party's total aggregate liability to the other under or in connection with this DPA, whether arising in contract, tort (including negligence), breach of statutory duty, or otherwise, will not exceed the liability cap set forth in the Agreement. Where the Agreement does not specify a liability cap, each party's total aggregate liability will not exceed the total fees paid or payable by Customer to StarTex in the twelve (12) months immediately preceding the event giving rise to the claim.
- 13.3 **Exclusion of Consequential Damages.** To the maximum extent permitted by applicable law, neither party will be liable to the other for any indirect, incidental, special, punitive, or consequential damages, or for any loss of profits, loss of revenue, loss of data, or loss of business opportunity, arising under or in connection with this DPA, even if advised of the possibility of such damages.
- 13.4 **Customer-Caused Losses.** StarTex will have no indemnification obligation under this Section 13 to the extent that a claim or loss arises from: (i) Customer's misconfiguration of the Services; (ii) Customer's failure to implement any of the Customer Security Measures, whether or not Customer elected to implement them; (iii) Customer's use of the Services in violation of the Agreement; or (iv) acts or omissions of Customer's authorized users.
- 13.5 **Exceptions.** Nothing in this Section 13 shall exclude or limit either party's liability to the extent such liability cannot be excluded or limited under applicable law.
14. **Termination of the DPA.** This DPA will continue in force until the termination of the Agreement (the "Termination Date").
15. **Return or Deletion of Customer Data.** Upon the earlier of (a) termination or expiration of this DPA or (b) Customer's written request, the following will apply:
- (i) **Customer Election.** Customer may, within thirty (30) days of the Termination Date, submit a written request to either: (A) receive an export of Customer Data in a machine-readable format used by the Services at the time of the request, provided that StarTex reserves the right to charge Customer at its then-current professional services rates for exports exceeding 100 GB in size or requiring custom extraction, and StarTex will notify Customer of any such charges before proceeding; or (B) receive written confirmation that Customer Data has been securely deleted or destroyed.
 - (ii) **Deletion Timeline.** StarTex will complete the export or deletion, as elected by Customer, within forty-five (45) days of the Termination Date.
 - (iii) **Default Deletion.** If Customer does not submit a written election within thirty (30) days of the Termination Date, StarTex may securely delete or destroy all Customer Data without further notice. StarTex will have no obligation to retain Customer Data beyond sixty (60) days of the Termination Date under any circumstances.
 - (iv) **Retained Copies.** Notwithstanding the foregoing, StarTex may retain Customer Data (A) to the extent required by applicable law, regulation, or binding governmental order, or (B) in the form of routine system backups, provided that such backup copies are subject to the confidentiality and security obligations of this DPA and are overwritten or deleted in the ordinary course of StarTex's backup rotation schedule.
 - (v) **Third-Party Sub-processors.** StarTex will use commercially reasonable efforts to cause Sub-processors to delete or return Customer Data consistent with the timeline in this Section.

16. Duties to Inform. Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by StarTex, StarTex will inform Customer without undue delay. StarTex will, without undue delay, notify all relevant parties in such action (for example, creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer's property and area of responsibility and that Customer Data is at Customer's sole disposition.

17. Entire Agreement; Conflict. This DPA, together with the Agreement and the Standard Contractual Clauses (incorporated by reference), constitutes the entire agreement between the parties with respect to the Processing of Personal Data. Except as amended by this DPA, the Agreement will remain in full force and effect. In the event of conflict between the Agreement and this DPA with respect to data protection matters, the terms of this DPA will control. In the event of conflict between this DPA and the Service Terms, the Service Terms will control. Nothing in this DPA varies or modifies the Standard Contractual Clauses.

18. General Provisions

18.1 Amendments. StarTex may update or modify this DPA from time to time to reflect changes in applicable law, regulatory guidance, or its data processing practices. StarTex will provide notice of any material changes by: (a) posting the updated DPA to its website at https://www.ehsinsight.com/gdpr_dpa (or successor location); and (b) sending email notice to Customer's contact information on record, in each case no less than thirty (30) days before the changes take effect (the "Notice Period"). Changes will become binding on Customer at the end of the Notice Period. Customer's continued use of the Services after the Notice Period constitutes Customer's acceptance of the updated DPA. If Customer does not wish to continue under the updated DPA, Customer's sole remedy is to terminate the Agreement in accordance with its terms prior to the end of the Notice Period. If you would like to receive an email notification when we update the Agreement, complete the form found at <https://www.ehsinsight.com/dpa-and-subprocessor-change-notification>.

18.2 Severability. If any provision of this DPA is held by a court of competent jurisdiction to be invalid, illegal, or unenforceable, that provision will be modified to the minimum extent necessary to make it enforceable, or if modification is not possible, it will be severed from this DPA. The remaining provisions of this DPA will continue in full force and effect. The invalidity or unenforceability of any provision in one jurisdiction will not affect its validity or enforceability in any other jurisdiction.

18.3 Waiver. No failure or delay by either party in exercising any right or remedy under this DPA will constitute a waiver of that right or remedy. A waiver of any breach of this DPA will not constitute a waiver of any subsequent breach.

18.4 Governing Law and Jurisdiction.

(a) **General.** This DPA and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) will be governed by and construed in accordance with the governing law specified in the Agreement.

(b) **GDPR Matters.** To the extent this DPA involves the Processing of Personal Data subject to the GDPR or UK GDPR, nothing in this Section limits the jurisdiction of any supervisory authority under applicable Data Protection Requirements.

(c) **Fallback.** Where the Agreement does not specify a governing law, this DPA will be governed by the laws of the State of Texas, without regard to its conflict of law

provisions, and the parties submit to the exclusive jurisdiction of the state and federal courts located in Harris County, Texas.

19. **Definitions.** Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below:

“**CCPA**” means the California Consumer Privacy Act of 2018 together, as amended by the California Privacy Rights Act of 2020, with any subordinate legislation or regulations.

“**controller**” has the meaning given to it in the GDPR.

“**Controller-to-Processor Clauses**” means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at https://www.ehsinsight.com/gdpr_c2p_scc.

“**Customer Data**” means all electronic data or information submitted or uploaded by Customer or a User in connection with the Services, which may contain the “Personal Data” (as defined herein).

“**Customer Security Measures**” means the technical and organizational security measures that StarTex strongly recommends Customer implement in connection with its use of the Services, as described in Sections 5.2 and 8 of this DPA and further detailed in the Documentation. The Customer Security Measures represent industry best practices for securing Customer Data. Customer's decision whether to implement any or all of the Customer Security Measures is solely Customer's, and StarTex bears no liability for losses arising from Customer's failure to implement them.

“**Data Protection Requirements**” means the General Data Protection Regulation, and any applicable laws, regulations, and other legal requirements relating to (a) privacy, data security, and protection of Personal Data; and (b) the Processing of any Personal Data. Data Protection Requirements may include, but are not limited to, UK GDPR, the Swiss Federal Act on Data Protection 2020, Lei Geral de Proteção de Dados (Brazil's General Data Protection Law), the CCPA, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act.

“**Data Subject**” means any individual person whose Personal Data you process pursuant to this Agreement.

“**Documentation**” means StarTex's user manuals or other documentation regarding the Services, accessible via Customer's account management section within the StarTex website at <http://www.ehsinsight.com> and <http://support.ehsinsight.com> (or successor location), as may be updated by StarTex from time to time upon written notice to Customer.

“**EEA**” means the European Economic Area.

“**GDPR**” means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

“**Personal Data**” means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an

online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person, as further defined in Article 4(1) of the GDPR. For purposes of the CCPA Addendum (Annex 2), "Personal Information" has the meaning set forth in §1798.140 of the CCPA.

"Processing" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

"Processor" has the meaning given to it in the GDPR.

"Security Incident" means a breach of StarTex's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

"Service Controls" means the controls, including security features and functionalities, that the Services provide, as described in the Documentation.

"Standard Contractual Clauses" means the Controller-to-Processor Clauses.

"StarTex Network" means certain data center facilities, servers, networking equipment, and host software systems (for example, virtual firewalls) that are utilized by StarTex to provide the Services. No physical access is implied by this definition.

"StarTex Security Standards" means the security standards attached to the Agreement, or if none are attached to the Agreement, attached to this DPA as Annex 1.

"Third Country" means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

"UK GDPR" means the UK General Data Protection Regulation, amended by the Data Protection Act 2018.

"UK Personal Data" means Personal Data the sharing of which pursuant to this Agreement is regulated by the UK GDPR.

Annex 1 StarTex Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

1. **Information Security Program.** StarTex will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the StarTex Network, and (c) minimize security risks, including through risk assessment and regular testing. StarTex will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:
 - 1.1 **Network Security.** The StarTex Network will be electronically accessible to employees, contractors, and any other person as necessary to provide the Services. StarTex will maintain access controls and policies to manage what access is allowed to the StarTex Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. StarTex will maintain corrective action and incident response plans to respond to potential security threats.
 - 1.2 **Physical Security.** Physical components of the StarTex Network are housed in AWS facilities (the “Facilities”). AWS employs physical barrier controls to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. StarTex maintains no physical facilities for the purpose of hosting Services, and no local networks are connected directly to the StarTex Network.
2. **Continued Evaluation.** StarTex will conduct periodic reviews of the security of its StarTex Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. StarTex will continually evaluate the security of its StarTex Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

Annex 2
To EHS INSIGHT GDPR DATA PROCESSING ADDENDUM
California Consumer Privacy Act

This CCPA/CPRA Addendum (the “Addendum”) reflects the requirements of the California Consumer Privacy Act of 2018 and its implementing regulations, as amended or superseded from time to time. For the purposes of this Addendum StarTex is acting as a Service Provider for CCPA purposes.

This Addendum is an addendum to the DPA between StarTex and Customer and shall remain in effect for so long as StarTex maintains Personal Information (as defined in and to the extent protected by the CCPA) provided by Customer or which is collected on behalf of Customer by StarTex. This Addendum shall only apply and bind the Parties if and to the extent StarTex is a Business under the CCPA. This Addendum prevails over any conflicting terms of the Agreement but does not otherwise modify the Agreement. All capitalized terms not defined in this Addendum shall have the meanings set forth in the CCPA.

1. Interpretations.

“Affiliate” means an entity that directly or indirectly controls, is controlled by or is under common control with an entity.

“Authorized Affiliate” means any of Customer’s Affiliate(s) permitted to or otherwise receiving the benefit of the Services pursuant to the Agreement.

“Business”, “Collects”, “Consumer”, “Business Purpose”, “Sell”, “Service Provider”, and “Share” shall have the meanings given to them in §1798.140 of the CCPA.

“California Consumer Privacy Act” or “CCPA” means Title 1.81.5 California Consumer Privacy Act of 2018 (California Civil Code §§1798.100—1798.199), as amended or superseded from time to time.

“Personal Information” means personal information as defined by §1798.140 of the CCPA submitted to StarTex for processing pursuant to the Agreement.

“Services” shall have the meaning set forth in the Agreement.

2. Scope and Applicability of this Addendum.

2.1. This Addendum applies to the collection, retention, use, and disclosure of the Personal Information from California residents pursuant to the Agreement.

2.2. StarTex is a Service Provider within the meaning of CCPA who is appointed to process the Personal Information on behalf of Customer. Customer is responsible for compliance with the requirements of the CCPA applicable to Businesses.

2.3. Customer’s collection, retention, use, or disclosure of Personal Information for its own purposes independent of providing the Services specified in the Agreement are outside the scope of this Addendum.

3. Restrictions on Processing.

3.1. StarTex is prohibited from retaining, using, or disclosing the Personal Information for any purpose other than for the specific purpose of performing the Services specified in the

Agreement for Customer, as set out in this Addendum, or as otherwise permitted by the CCPA.

- 3.2. StarTex shall not further collect, sell, or use the Personal Information except as necessary to perform the Business Purpose. For the avoidance of doubt, StarTex shall not use the Personal Information for the purpose of providing services to another person or entity, except that StarTex may combine Personal Information received from one or more entities to which it provides similar services to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.
4. **Consumer Rights.**
 - 4.1 **Assistance.** StarTex will, upon Customer's reasonable written instructions, use commercially reasonable efforts to assist Customer in: (i) deleting Personal Information in accordance with a verified Consumer request, except to the extent StarTex is permitted to retain such Personal Information pursuant to an exemption under the CCPA and/or CPRA; and (ii) responding to verified Consumer requests to access or receive information relating to the collection of Personal Information for the Business Purpose.
 - 4.2 **Standard Assistance.** StarTex will provide the assistance described in Section 4.1 at no additional charge for up to six (6) verified Consumer requests per calendar year per Customer account.
 - 4.3 **Excess Requests.** For verified Consumer requests exceeding the threshold in Section 4.2, StarTex reserves the right to charge Customer at StarTex's then-current professional services rates, provided StarTex notifies Customer before incurring such charges and Customer approves the work in writing.
 - 4.4 **Verification.** StarTex's obligation to assist is conditioned on Customer providing StarTex with sufficient information to identify the relevant Personal Information and confirm the request has been verified by Customer in accordance with CCPA requirements. StarTex is not responsible for verifying the identity of Consumers, which remains Customer's obligation.
 - 4.5 **Regulatory Correspondence.** StarTex will, upon Customer's instruction and upon proof of such a communication, provide reasonable assistance to Customer to enable Customer to respond to any correspondence, inquiry, or complaint received from a Consumer or the California Attorney General in connection with the collection and processing of the Personal Information.
 - 4.6 **Deletion Upon Termination.** Data return and deletion of Personal Information upon termination of the Agreement is governed exclusively by Section 14 of this DPA, the terms of which are incorporated into this Addendum by reference. In the event of any conflict between this Addendum and Section 14 with respect to data return or deletion, Section 14 shall control.
 5. **Data Security.** StarTex shall implement and maintain reasonable security procedures and practices appropriate to the nature of the Personal Information it will process to protect the Personal Information from and against unauthorized or illegal access, destruction, use, modification, or disclosure. StarTex shall notify Customer without undue delay (and in time to fulfil any applicable reporting obligations) after becoming aware of an accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access of or to the Personal Information, and provide timely information relating to such, as it becomes known or is reasonably requested by Customer.
 6. **Mergers, Sale, or Other Asset Transfer.** In the event that either Party transfers to a third party the Personal Information of a Consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of such Party to the

Agreement, that information shall be used or shared consistently with applicable law. If a third party materially alters how it uses or shares the Personal Information of a Consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the Consumer in accordance with applicable law.