DATA PROCESSING AGREEMENT FOR SUPPLIERS

Fenix24, Inc., or one of its affiliates (the applicable entity will be referred to as, "**Fenix24**") and Supplier have entered into an agreement (as may be amended from time to time) (the "**Services Agreement**") under which Supplier may process Fenix24 Personal Data in connection with the provision of Services. This Data Protection Agreement, including the Annexes attached hereto and the Standard Contractual Clauses ("**DPA**") governs Supplier's processing of that data and shall form part of and be incorporated by reference into the Services Agreement with Fenix24 for providing the Services – PROVIDED THAT any additional promises or protections from Supplier to Fenix24 in any other portion of the Parties' agreement(s) shall remain in place and are not superseded or waived by Fenix24 herein. This DPA shall be effective on the effective date of the Services Agreement. At all times, Supplier shall, and shall cause its Subprocessors to, comply with this DPA. Fenix24 (and its affiliate entering into any agreement with Supplier) and Supplier may each be referred to as a "**Party**" and together as the "**Parties**".

Notwithstanding expiry or termination of the Services Agreement, this DPA will remain in effect until, and will terminate automatically upon, deletion by Supplier and its Subprocessors of all Fenix24 Personal Data covered by this DPA, in accordance with this DPA.

1. Definitions and Interpretation

"**Affiliate**" means any entity under the control of a party where **"control"** means ownership of, or the power to vote, directly or indirectly, a majority of any class of voting securities of a corporation or limited liability company, or the ownership of any general partnership interest in any general or limited partnership or as otherwise defined in the Services Agreement to which the DPA relates.

"**Authorized Personnel**" means any natural person who Processes Fenix24 Personal Data on Supplier's behalf, including Supplier's employees, officers, partners, principals, contractors, and Subprocessors.

"**Controller**" means an entity that alone or jointly with others determines the purposes and means of Processing of Personal Data. For the purposes of this DPA, a Controller includes a "business" as such term is defined by the CCPA, or a similar designation under Data Protection Legislation.

"**Cross-Border Transfer**" means any cross-border transfer directly or via onward transfer (including initiation of a transfer) of Fenix24 Personal Data including both physical transfer and remote access to Personal Data from another country.

"**Fenix24 Personal Data**" means any Personal Data provided or made available by or on behalf of Fenix24 to Supplier and/or collected or otherwise obtained by Supplier in connection with Supplier's performance of Services to Fenix24 and Processed by Supplier as a Processor, as more particularly described in the DPA and **Annex A**.

"**Data Protection Legislation**" means any applicable global laws relating to data protection and privacy and the Processing of Fenix24 Personal Data that is protected by applicable law in any relevant jurisdiction, including but not limited to: (i) EU/UK Data Protection Law; and (ii) US Data Protection Law.

"**EU/UK Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such Personal Data (General Data Protection Regulation) (the "**GDPR**"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); (iii) in respect of the UK, the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European

Union (Withdrawal) Act 2018 (the "**UK GDPR**"), the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 as they continue to have effect by virtue of section 2 of the European Union (Withdrawal) Act 2018, and any other laws in force in the UK applicable (in whole or in part) to the Processing of Personal Data (together, "**UK Data Protection Law**"); (iv) the Swiss Federal Act on Data Protection of 2020 and its Ordinance ("**Swiss FADP**"); and (v) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii), (iii) and (iv) above; in each case as may be amended, superseded or replaced from time to time.

"**Europe**" means, for the purposes of this DPA, the member states of the European Economic Area, the United Kingdom ("**UK**") and Switzerland.

"**Personal Data**" means all information relating to an identified or identifiable natural person or consumer ("**Data Subject**"), including any data or information that is deemed "personal data", "personally identifiable information" and/or "personal information" under Data Protection Legislation.

"**Process**," "**Processes**," "**Processing**," "**Processed**" means any operation or set of operations which is performed on 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, destruction, or creating information from, Personal Data.

"**Processor**" means an entity that Processes Personal Data on behalf, and in accordance with the instructions, of a Controller. For purposes of this DPA, a Processor includes a "service provider" as such term is defined by the CCPA, or any similar or analogous designation under Data Protection Legislation.

"**Restricted Transfer**" means a transfer (directly or via onward transfer) of Personal Data that is subject to EU/UK Data Protection Law to a country outside Europe which is not subject to an adequacy determination by the European Commission, United Kingdom or Swiss authorities (as applicable).

"**Security Incident**" means any actual or suspected breach of security leading to, or reasonably believed to have led to, the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Fenix24 Personal Data or similar incident involving Fenix24 Personal Data.

"**Services**" means any product or service provided by Supplier to Fenix24 pursuant to and as more particularly described in the Services Agreement.

"**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission's Implementing Decision 2021/914 of 4 June 2021, as updated or amended from time to time.

"**Subprocessor**" means any third party that has access to Fenix24 Personal Data and which is engaged directly or indirectly by Supplier to assist in fulfilling Supplier's obligations with respect to providing the Services pursuant to the Services Agreement or the DPA. Subprocessors may include Supplier's Affiliates but shall exclude Supplier's employees, contractors and consultants who are natural persons.

"**Supervisory Authority**" means any regulatory, supervisory, governmental, state agency, Attorney General or other competent authority with jurisdiction or oversight over compliance with Data Protection Legislation.

"**Supplier**" means the means the party from which Fenix24 is purchasing solutions and its Affiliates.

"**Term**" means the term of the Services Agreement and any period after the termination or expiry of the Services Agreement during which Supplier and/or its Subprocessors Processes Fenix24 Personal Data, until Supplier has destroyed or returned such Fenix24 Personal Data in accordance with the terms of the DPA.

"**UK Addendum**" means the International Data Transfer Addendum to the Standard Contractual Clauses (version B1.0) issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as it is revised under Section 18 therein; as may be amended, superseded or replaced from time to time.

"**US Data Protection Law**" means all relevant U.S. federal and state privacy laws (including any implementing regulations and amendment thereto) effective as of the date of this DPA, including but not limited to (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("**CCPA**"); (ii) the Virginia Consumer Data Protection Act ("**CDPA**"); (iii) the Colorado Privacy Act ("**CPA**"); (iv) the Utah Consumer Privacy Act ("**UCPA**"); (v) the Connecticut Data Privacy Act ("**CTDPA**"); in each case as may be amended, superseded or replaced from time to time.

2. Scope of this DPA and Relationship of the Parties

2.1 Supplier as a Processor. For the purposes of the GDPR and similar Data Protection Legislation, the Parties agree that Supplier will Process Fenix24 Personal Data as a Processor acting on behalf of Fenix24 (whether a Controller itself or acting on behalf of (a) an Affiliate or (b) a third-party Controller) and only in accordance with Fenix24's written instructions, as further described in Annex A attached hereto, and this DPA shall apply accordingly.

2.2 Sale or Sharing of Fenix24 Personal Data Prohibited. Supplier will not (a) sell Fenix24 Personal Data to a Subprocessor or any other third parties, as the term "sell" is defined under US Data Protection Law; (b) share Fenix24 Personal Data to a Subprocessor or any other third parties, as the term "share" is defined by the CCPA; (c) retain, use, disclose or transfer the Fenix24 Personal Data for any purposes other than for performing Supplier's obligations under the Services Agreement and this DPA, in particular, the Permitted Purpose (as defined below), including to retain, use or disclose Fenix24 Personal Data for a commercial purpose other than performing its Services under the Services Agreement and this DPA; (d) retain, use, or disclose the Fenix24 Personal Data outside the direct business relationship between the Parties; or (e) combine Fenix24 Personal Data received with Personal Data that Supplier receives from other sources or that it collects from its own interaction with the Data Subject, except as otherwise permitted by the Services Agreement or by US Data Protection Law. The Parties agree that Fenix24's transfer of Fenix24 Personal Data to Supplier is not a sale, and Supplier provides no monetary or other valuable consideration to Fenix24 in exchange for Fenix24 Personal Data. Supplier certifies that it understands the restrictions set out in this Section and will comply with them.

2.3 Compliance with Data Protection Legislation. Each Party shall comply with its obligations under Data Protection Legislation with respect to the Processing of Fenix24 Personal Data. The Parties shall reasonably assist each other in meeting their respective obligations under Data Protection Legislation. Supplier shall not perform its obligations under the Services Agreement or the DPA in such a way as to cause Fenix24 to breach any of its obligations under Data Protection Legislation. Supplier shall promptly notify Fenix24 in writing if it believes that it can no longer meet its obligations under any Data Protection Legislation.

2.4 Remediation. Fenix24 has the right to take reasonable and appropriate steps to ensure that Supplier uses Fenix24 Personal Data in a manner that is consistent with a business's obligations under US Data Protection Law and other Data Protection Legislation, which may include asking survey questions or for audits or interviews of appropriate personnel during ordinary business hours.

3. Processing Instructions

3.1 Supplier will Process the Fenix24 Personal Data as a Processor only in accordance with the written instructions from Fenix24 and in compliance with Data Protection Legislation. Such instructions may be specific or of a general nature as set out in this DPA, the Services Agreement, an SOW, or as otherwise notified by Fenix24 to Supplier in writing from time to time.

3.2 Fenix24 instructs Supplier to Process Fenix24 Personal Data as a Processor for the following purposes: (a) to provide the Services and all other Processing necessary for Supplier to perform its obligations under the Services Agreement and the DPA; (b) to comply with any other reasonable instructions provided by Fenix24 (e.g., via email or support tickets) that are consistent with the terms of the Services Agreement and the DPA; (c) to comply with Supplier's legal obligations under applicable law, including Data Protection Legislation; and (d) any other purpose expressly authorised by Fenix24 under the Services Agreement (collectively and individually the "**Permitted Purpose**").

3.3 Supplier shall not Process Fenix24 Personal Data for its own or for any other purposes except (i) as otherwise specified in this DPA or (ii) to the extent applicable, as required by Union or Member State law to which the Supplier is subject. If (ii) applies, Supplier shall inform Fenix24 of the legal requirement before Processing, unless that law prohibits such information on important grounds of public interest and, where permitted, Supplier shall only Process Fenix24 Personal Data as strictly necessary to comply with such law. Supplier certifies that it understands the restrictions set out in this Section 3.3 and will comply with them.

3.4 Supplier shall make available to Fenix24 all information necessary to demonstrate compliance with the obligations laid down in this DPA. Supplier will inform Fenix24 prior to the Processing of Fenix24 Personal Data -- unless prohibited by law from doing so -- if it: becomes aware of or believes that any instruction from Fenix24 violates Data Protection Legislation; and/or is unable to comply with Fenix24's instructions for any reason.

4. Security

4.1 Supplier represents and warrants that it has implemented and shall maintain appropriate technical and organisational measures to protect the Fenix24 Personal Data against Security Incidents and to preserve the security and confidentiality of Fenix24 Personal Data. These measures shall take into account the current industry standards, state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Without prejudice to the foregoing, such measures shall include, at a minimum, those set out in **Annex B** attached hereto. Supplier may change the measures outlined in **Annex B** hereto so long as it maintains a comparable or better level of security. Material changes must be communicated to Fenix24 in writing at: LegalNotices@fenix24.com. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Fenix24 Personal Data.

4.2 Supplier shall ensure that any person who Processes Fenix24 Personal Data on Supplier's behalf: (a) is required to protect and Process Fenix24 Personal Data in a manner consistent with the terms of the Services Agreement and the DPA; and (b) will receive appropriate training by Supplier regarding the protection of Fenix24 Personal Data prior to receiving access to Fenix24 Personal Data.

4.3 Supplier will take reasonable steps to ensure the reliability and competence of any of its and its Subprocessors' Authorized Personnel, including regular training of those with access to Fenix24 Personal Data in applicable security and data privacy measures. Supplier will ensure that all such Authorized Personnel are subject to a strict legal duty of confidentiality and that they Process the Fenix24 Personal Data only for the purpose of delivering the Services to Fenix24 in accordance with this DPA.

5. Subprocessing

5.1 Supplier will not give access to or transfer any Fenix24 Personal Data to any third party (including any of Supplier's Affiliates, group companies or Subprocessors) without the prior written consent of Fenix24. Notwithstanding the foregoing, where Supplier is a Processor, Fenix24 does consent to Supplier engaging a Subprocessor to Process Fenix24 Personal Data provided that:

(a) Supplier conducts appropriate due diligence to ensure it retains Subprocessors which present sufficient guarantees in terms of confidentiality, security and data protection in accordance with Data Protection Legislation;

(b) Supplier provides at least 30 days' prior written notice to Fenix24 of the engagement of any new Subprocessor (including details of the Processing and location) and Supplier shall update the list of all Subprocessors engaged to Process Fenix24 Personal Data under the DPA and send such updated version to Fenix24 prior to the engagement of the Subprocessor;

(c) Supplier must ensure the Subprocessor is a "service provider" as such term is defined under US Data Protection Law or any similar or analogous designation under Data Protection Legislation;

(d) Supplier must ensure the reliability and competence of such Subprocessor, and of its Authorized Personnel who may have access to Fenix24 Personal Data;

(e) Supplier imposes in its contract with such Subprocessor provisions which are at least as protective of Fenix24 as those in the DPA and the Services Agreement and as required by Data Protection Legislation; and

(f) Supplier is fully liable to Fenix24 for any breach of the DPA and the Services Agreement caused by an act, error or omission of a Subprocessor including Authorized Personnel.

5.2 If Fenix24 objects to the engagement of any Subprocessor on data protection grounds, then either Supplier will not engage the Subprocessor to Process Fenix24 Personal Data or Fenix24 may elect to immediately suspend or terminate the Services Agreement or the Processing of Fenix24 Personal Data under the Services Agreement, in each case without penalty.

6. Cooperation

6.1 Supplier will take all reasonable steps to assist Fenix24 in meeting Fenix24's (or its Affiliates) obligations under Data Protection Legislation, including Fenix24's obligations: (a) to respond to requests by Data Subjects to exercise their rights with respect to Fenix24 Personal Data (including its right of access, correction, objection, erasure/deletion and data portability, as applicable); (b) to adhere to data security obligations; and (c) to consult with Supervisory Authorities.

6.2 Supplier will promptly inform Fenix24 in writing if it receives: (a) a request from a Data Subject concerning any Fenix24 Personal Data; or (b) a complaint, communication, or request relating to Fenix24's obligations under Data Protection Legislation. Supplier shall not respond to such communication without Fenix24's express authorization, except to confirm that the request relates to Fenix24. Regarding requests from Data Subjects seeking to exercise their rights, Supplier will inform Fenix24 in writing without undue delay (but in no case longer than five (5) business days) of receiving a request from a Data Subject concerning the Processing of Fenix24 Personal Data. Where the request concerns Personal Data covered under the CCPA or other US Data Protection Law, Supplier shall inform the requestor that the request cannot be acted upon because the request has been sent to a service provider, as this term is defined under US Data Protection Law, and that the request is or has been referred to Fenix24.

6.3 Supplier will provide all reasonable assistance required by Fenix24 or its Affiliate to conduct a data protection impact assessment, risk assessment, cybersecurity audit or similar under Data Protection Legislation and/or inquiry, complaint or prior consultation with any applicable Supervisory Authorities.

6.4 If Supplier receives a subpoena, court order, warrant or other legal demand from a third party (including law enforcement or other governmental, regulatory or judicial authorities) seeking the disclosure of Fenix24 Personal Data, Supplier shall not disclose any information but shall immediately notify Fenix24 in writing of

such request, and reasonably cooperate with Fenix24 if Fenix24 wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable laws.

6.5 Supplier shall have in place, maintain and comply with a policy governing Personal Data access requests from government authorities, which addresses the obligations herein and at minimum prohibits: massive, disproportionate or indiscriminate disclosure of Personal Data relating to Data Subjects in Europe; and disclosure of Personal Data relating to Data Subjects in Europe to a government authority without a subpoena, warrant, writ, decree, summons or other legally binding order that compels disclosure of such Personal Data.

7. Deletion or return

7.1 Supplier acting as a Processor. At the end of the Services, or upon Fenix24's request, Supplier will securely destroy or return to Fenix24 the Fenix24 Personal Data in Supplier's possession or control (including any Fenix24 Personal Data Processed by its Subprocessors) that Supplier processes as a Processor.

7.2 The requirements above shall not apply to the extent that Supplier is required by any applicable law to retain some or all of the Fenix24 Personal Data, in which case Supplier shall isolate and protect the Fenix24 Personal Data from any further Processing except to the extent required by such law. Supplier shall delete such retained data without undue delay when technically feasible and/or allowed by the applicable law, and shall confirm such deletion in a signed writing upon request.

7.3 The obligations placed upon Supplier under this DPA shall survive so long as Supplier and/or its Subprocessors Process Fenix24 Personal Data.

8. Transfers

8.1 International transfers. Supplier shall be entitled to Process and transfer the Fenix24 Personal Data, including by using Subprocessors, in or to a territory other than the territory in which the Fenix24 Personal Data was first collected as permitted only by and in compliance with Data Protection Legislation and this DPA.

8.2 Restricted or Cross-Border Transfers. Supplier shall not conduct a Restricted Transfer of Fenix24 Personal Data, or a Cross-Border Transfer, unless it first takes all such measures as are necessary to ensure the transfer is in compliance with all applicable laws including EU/UK Data Protection Law. Any movement of Fenix24 Personal Data out of the United States or processing by Supplier outside of the United States must be expressly identified to Fenix24 in the applicable SOW or order or a signed written agreement. Measures necessary to ensure compliance may include (without limitation) transferring Fenix24 Personal Data to a recipient that: (a) is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for personal data; (b) has achieved binding corporate rules authorization; or (c) has executed with Supplier appropriate Standard Contractual Clauses, including the adoption of supplementary measures, if required to ensure an adequate level of protection; in each case as adopted or approved in accordance with applicable EU/UK Data Protection Law.

8.3 Where Fenix24 transfers (directly or via onward transfer) Fenix24 Personal Data to Supplier, the Parties agree to be subject to the Standard Contractual Clauses, which shall be incorporated by reference as form an integral part of this DPA, as follows:

(a) Supplier as a Processor. In relation to Fenix24 Personal Data that is protected by the EU GDPR and is Processed in accordance with this DPA, the SCCs shall apply completed as follows: (i) Module Two (Controller-to-Processor or Module Three (Processor-to-Processor, as applicable) will apply; (ii) in Clause 7, the optional docking clause will apply, (iii) in Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes shall be as set out in Section 6 (Subprocessing) of this DPA; (iv) in Clause 11, the optional language will not apply; (v) in Clause 17, Option 1 will apply, and the SCCs will be governed by the law of the Netherlands; (vi) in Clause 18(b), disputes shall be

resolved before the courts of the Netherlands; (vii) Annex I of the SCCs shall be deemed completed with the information set out in **Annex A** attached hereto; and (viii) subject to Section 5.1 of this DPA, Annex II of the SCCs shall be deemed completed with the information set out in **Annex B** attached hereto.

(b) UK Transfer Mechanism. For the purposes of Fenix24 Personal Data that is protected by UK Data Protection Law, the SCCs as implemented above will also apply with the following modifications: (i) the SCCs to be deemed amended as specified by Part 2 of the UK Addendum; (ii) tables 1 to 3 in Part 1 of the UK Addendum to be deemed completed respectively with the information set out in Annexes A, B and C attached hereto (as applicable); and (iii) table 4 in Part 1 of the UK Addendum to be deemed completed by selecting "neither party".

(c) Swiss Transfer Mechanism. For the purposes of Fenix24 Personal Data that is protected by the Swiss FADP, the SCCs as implemented above will also apply with the following modifications: (i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss FADP; (ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss FADP; (iii) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" or "Swiss law"; (iv) the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland); (v) Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the Swiss Federal Data Protection Information Commissioner; (vi) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland"; (vii) in Clause 17, the SCCs shall be governed by the laws of Switzerland; and (viii) Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.

8.4 Supplier agrees to implement and maintain any additional contractual, technical or organisational measures to supplement the safeguards under the SCCs which are required from time to time by Fenix24 in order to protect the Fenix24 Personal Data, so long as such safeguards are consistent with requirements under Data Protection Legislation. If Supplier is unable to implement and maintain such supplementary measures, Fenix24 may immediately terminate the Services Agreement and the DPA (in whole or in part) without penalty. Supplier shall promptly notify Fenix24 if it makes a determination that it can no longer meet its obligations under this Section, and in such event but without prejudice to any other right or remedy available to Fenix24, Supplier shall:

(a) remediate (if remediable) any Processing until such time as the Processing meets the level of protection as is required by Data Protection Legislation and this Section 9; and/or

(b) immediately cease (and require that all Subprocessors immediately cease) Processing such Fenix24 Personal Data if in Fenix24's sole discretion, Fenix24 determines that Supplier has not or cannot correct any non-compliance with this Section within a reasonable time frame.

8.5 It is not the intention of either Party, nor the effect of the DPA, to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses. Accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses shall prevail. In no event does the DPA restrict or limit the rights of any Data Subject or of any competent Supervisory Authority.

8.6 The Parties agree that, in the event that a Supervisory Authority and/or EU/UK Data Protection Law no longer allow the lawful transfer of Fenix24 Personal Data to Supplier and/or requires that Fenix24 adopt an alternative transfer solution that complies with EU/UK Data Protection Law, Supplier will fully co-operate with Fenix24 to enter into an amendment to this DPA to remedy such non-compliance and/or cease Processing of Fenix24 Personal Data. If the Parties, acting in good faith, are unable to agree such changes within thirty (30)

days, Fenix24 may immediately terminate the Services Agreement without any further liability or obligation to Supplier, and Supplier shall refund to Fenix24 any amounts which were paid for work not yet performed under the Services Agreement.

9. Security Reports and Inspections

9.1 Supplier shall maintain records in accordance with ISO 27001 or similar information security management system standards. On request, Supplier shall provide copies of relevant reports, certifications or any information reasonably requested by Fenix24 to demonstrate compliance with the obligations set out in the DPA. Supplier shall also respond to Fenix24 security and compliance questionnaires and address any reasonable follow up questions. Supplier shall maintain logs of all access, changes, transfers, deletion and processing of Fenix24 Confidential Information and Personal Data for at least two years unless Fenix24 and Supplier expressly agree upon the transfer of those records to Fenix24 so that the records remain available for review.

9.2 While it is the Parties' intention ordinarily to rely on Section 9.1 above to demonstrate Supplier's compliance with the DPA (including the Standard Contractual Clauses as applicable) and Data Protection Legislation, where Fenix24 has reasonable concerns about Supplier's compliance, Supplier will allow Fenix24 or an Affiliate under the DPA and their respective auditors or authorized agents to conduct audits and inspections during the term of the Services Agreement and for 12 months thereafter. Such inspections shall include, where necessary, providing access to the premises, resources and Authorized Personnel, and provide all reasonable assistance in order to assist Fenix24 or an Affiliate under the DPA in exercising its audit rights under this Section. Inspections may only be carried out with reasonable prior notice, during normal business hours. If the audit reveals non-compliance with this DPA, Supplier shall reimburse Fenix24 for the costs of the audit.

10. Security Incidents

10.1 If Supplier becomes aware of any Security Incident, it shall:

(a) without undue delay (and in any event no later than 48 hours of discovery) notify Fenix24 and provide Fenix24 with: a detailed description of the Security Incident; the type of data that was the subject of the Security Incident; the identity of each affected Data Subjects (if determinable), and the steps Supplier has taken or intends to take in order to mitigate and remediate such Security Incident, in each case as soon as such information can be collected or otherwise becomes available (as well as periodic updates to this information and any other information Fenix24 may reasonably request relating to the Security Incident);

(b) take action immediately, at its own expense, to investigate the Security Incident and to identify, prevent and mitigate the effects of the Security Incident and, with the prior written approval of Fenix24, to carry out any recovery or other action necessary to remedy the Security Incident;

(c) reimburse Fenix24 for reasonable costs incurred by Fenix24 (or an Affiliate) to draft, prepare, generate, and send, or otherwise related to, all notifications as required by Data Protection Legislation and, if requested by Fenix24, provide credit monitoring and identity theft protection services to affected Data Subjects; and

(d) not release or publish any filing, communication, notice, press release, or report concerning the Security Incident without Fenix24's prior written approval (except where it is required to do so by law).

11. Liability and Indemnity

11.1 Notwithstanding anything else to the contrary in the Services Agreement, Supplier agrees that:

(a) it shall be liable for any unauthorized use, exposure or loss of data (including Fenix24 Personal Data) arising under or in connection with the Services Agreement and the DPA to the extent such loss results from any failure of Supplier (or its Subprocessors) to comply with its obligations under the DPA and/or applicable law or regulation; and

(b) any exclusion of damages or limitation of liability that may apply to limit Supplier's liability in the Services Agreement shall not apply to Supplier's liability arising under or in connection with the DPA, howsoever caused, regardless of how such amounts or sanctions awarded are characterized and regardless of the theory of liability, which liability shall be expressly excluded from any agreed exclusion of damages or limitation of liability.

11.2 To the fullest extent permitted by applicable law, Supplier shall indemnify, defend, and hold Fenix24, including its Affiliates, and each of its affiliates, partners, principals, officers, directors, employees, subcontractors and agents harmless against any claims, suits, or proceedings and any resulting liabilities, fines, losses, damages, costs and expenses (including reasonable attorney's fees) that Fenix24 may suffer or incur as a result of any act or omission on the part of Supplier or its subcontractors, or anyone acting on their behalf, that leads to Fenix24 being liable for breach of Data Protection Legislation or a third-party contract.

11.3 In the event there is any act, error or omission on the part of Supplier and/or its Subprocessors which leads to Fenix24 being liable for breach of Data Protection Legislation or any third-party contract, then Supplier shall indemnify Fenix24 for any damages, losses, liabilities, costs, harm or expenses (including reasonable legal fees) suffered by Fenix24 as a result.

11.4 The Parties acknowledge and agree that any breach by Supplier of the DPA shall constitute a material breach of the Services Agreement, in which event and without prejudice to any other right or remedy available to it, Fenix24 may elect to immediately terminate the Services Agreement in accordance with the termination provisions in the Services Agreement.

11.5 Nothing in the DPA is intended to limit any Data Subject rights, as third-party beneficiaries, under the Standard Contractual Clauses against any Party arising out of such Party's breach of the Standard Contractual Clauses, where applicable.

12. Documentation and Records of Processing

12.1 Each Party is responsible for its compliance with its documentation requirements, in particular maintaining records of Processing, where required under Data Protection Legislation. Each Party shall reasonably assist the other Party in its documentation requirements, including providing the information the other Party needs from it in a manner reasonably requested by the other Party (such as using an electronic system) in order to enable the other Party to comply with any obligations relating to maintaining records of Processing.

13. General

13.1 The DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Services Agreement, unless and to the extent required otherwise by the Data Protection Legislation or, where applicable, the Standard Contractual Clauses.

13.2 If Supplier accesses, retains, is exposed to, or becomes aware of "Protected Health Information" as defined in 45 C.F.R. § 164.501 in the course of providing service, Supplier and Fenix24 hereby agree to and Supplier shall comply with the HIPAA US Subcontractor Agreement and the HIPAA Business Associate Agreement, attached as Annex C.

13.3 The Parties acknowledge and agree that the DPA is incorporated into and forms a part of the Services Agreement between Fenix24 and Supplier. For matters not addressed under the DPA, the terms of the Services

Agreement apply. If and to the extent the DPA conflicts with any provision of the Services Agreement, the DPA shall control and prevail. Conflicts between the terms of the DPA and the Standard Contractual Clauses are addressed in Section 9.5 above, as further subject to Section 9.6 above.

13.4 The Parties acknowledge that either Party may disclose this DPA (and any other relevant privacy terms or agreements entered between the Parties) to the US Department of Commerce, the Federal Trade Commission, European data protection authorities or any other US, EU, Swiss or UK judicial or regulatory body upon their request.

13.5 The Parties acknowledge and agree that any breach by Supplier of the DPA shall constitute a material breach of the Services Agreement, in which event and without prejudice to any other right or remedy available to it, Fenix24 may elect to immediately terminate the Services Agreement (in whole or in part) in accordance with the termination provisions in the Services Agreement.

Annex A
Description of the Processing Activities / Transfer

Annex 1(A) List of Parties:

Data Exporter	**Data Importer**
Name: The Fenix24 entity executing the Services Agreement and the DPA	**Name:** Supplier as this term is defined in the DPA and/or Services Agreement
Address: As identified in the Services Agreement	**Address:** As identified in the Services Agreement
Contact Person's Name, position and contact details: privacy@fenix24.com	**Contact Person's Name, position and contact details:** As provided for in the Services Agreement or otherwise Supplier's publicly-available email address for receiving privacy-related notices.
Activities relevant to the transfer: See **Annex 1(B)** below	**Activities relevant to the transfer:** See **Annex 1(B)** below
Role: Controller or Processor	**Role:** Processor

Annex 1(B) Description of transfer:

	Description
Categories of data subjects:	As needed in order for Supplier to perform the Services, which may include: ● Employees and applicants ● Customers and end users ● Suppliers, agents, and contractors
Categories of personal data:	As needed in order for Supplier to perform the Services, which may include: ● Direct identifiers such as first and last name, date of birth, & home address; ● Communications data such as home telephone number, cell telephone number, email address, postal mail, and fax number; ● Family and other personal circumstance information such as age, date of birth, marital status, spouse or partner, and number and names of children; ● Employment information such as employer, work address, work email and phone, job title and function, salary, manager, employment ID, system usernames and passwords, performance information, and CV data; ● Other data such as financial, goods or services purchased, device identifiers, online profiles, and IP address; ● Details of user's interaction with the data importer's systems and with systems for which the data importer provides computing services; ● Information that the data exporter or its users choose to include in files stored on or routed through data importer's applications; and ● Other personal data to which the parties provide to each other in connection with the provision of the Services.
Sensitive data transferred (if applicable) and applied restrictions:	Personal data transferred may include sensitive data such as government identifier, or any other sensitive data necessary to be processed in order to perform the Services.
Frequency of the transfer:	Continuous
Nature of the Processing:	The performance of Services under the Services Agreement and the DPA.
Duration of the Processing:	The term of the Services Agreement and any period after the termination or expiry of the Services Agreement during which Supplier Processes Fenix24 Personal Data, until Supplier has deleted, destroyed or returned such Personal Data in accordance with the terms of the DPA (the "**Processing Term**").
Purpose(s) of the data transfer and further Processing:	The Permitted Purpose (as defined in the DPA).
Retention period (or, if not possible to determine, the criteria used to determine that period):	The Processing Term.

For transfers to Subprocessors, also specify subject matter, nature and duration of the Processing:	The nature is the provision of the Services as described in the Services Agreement. The subject matter is the personal data as described above. The duration will be in accordance with Section 9 of the DPA.

Annex 1(C) Competent supervisory authority:
The competent supervisory authority, in accordance with Clause 13 of the SCCs, shall be determined in accordance with EU/UK Data Protection Law.

Annex B

Technical and organizational measures

Supplier shall implement the following minimum technical and organizational measures (including any relevant certifications) to ensure an appropriate level of security taking into account the nature, scope, context and purposes of the processing, and the risks for the rights and freedoms of natural persons:

Type of Measure	**Implemented Measure**
1. Measures of encryption of personal data	● Encryption of the Fenix24 Personal Data while at rest and in transit consistent with industry standards and at a minimum of 256-bit encryption.
2. Measures for ensuring ongoing confidentiality, integrity and resilience of processing systems and services	● Confidentiality Obligations. Ensure employees are required to sign a confidentiality agreement when accepting a new hire offer and contractors who access the facilities and/or data required to sign a confidentiality or non-disclosure agreement. ● Training. Implement and maintain security and privacy awareness training for all employees and contractors regarding the handling and securing of confidential information and Fenix24 Personal Data consistent with applicable law (including Data Protection Legislation). ● Background Checks. Supplier shall conduct a criminal background check on each of all employees and contractors with access to Fenix24 Personal Data. Supplier shall not provide access to Fenix24 Personal Data to any employee or contractor who: (a) has any felony convictions or misdemeanor convictions involving violence or dishonesty, or its international equivalents; (b) has a restriction (e.g. a court order or restrictive covenant) that would prevent the person from providing services or impose limitations on the services that the person is able to provide to Fenix24 or a customer of Fenix24; (c) may present a higher than normal security risk to Fenix24 or a customer of Fenix24; or (d) do not meet other guidelines specified by Fenix24 or the customers of Fenix24 from time to time. ● Remote access to systems must utilize secure applications, i.e., VPN. Access to remote resources must be authenticated using multiple authentication factors (MFA). ● Identify appropriately defined organizational roles for security and incident response. ● Include appropriate controls addressing (A) critical asset identification and asset management; (B) access controls and management; (C) physical and environmental security; (D) communications and operations security and management; (E) systems acquisition, development, and maintenance; (F) third-party risk management; (G) configuration and change management for software systems; (H) incident response, planning, and management, including appropriate maintenance, monitoring and analysis of audit logs; and (I) business continuity management, disaster recovery, and contingency planning/redundancy. ● Segregation of the Fenix24 Personal Data from all other third-party data. ● Proper user authentication for all employees and contractors with access to the Fenix24 Personal Data, including, without limitation, by assigning each employee/contractor unique access credentials for access to any system on which the Fenix24 Personal Data can be accessed and prohibiting employees/contractors from sharing such access credentials.

	● Restrict and track access to the Fenix24 Personal Data by only those employees/contractors whose access is necessary to performing the services and implement and maintain logging and monitoring technology to help detect and prevent unauthorized access attempts to networks and production systems. ● Conduct periodic reviews of changes affecting systems' handling authentication, authorization, and auditing, and privileged access to production systems. ● Upon termination of any employee/contractor, ensure the terminated employee/contractor's access to any Fenix24 Personal Data on Supplier's systems will be immediately revoked. ● If Supplier or any authorized person is granted access to or connects to any computing system, network, platform, facilities or telecommunications or other information system (the "Systems") owned, controlled, or operated by or on behalf of Fenix24 or any of its Affiliates, then Supplier and any applicable authorized person will be subject to and shall comply with all then-current Fenix24 policies, including without limitation, all security, privacy, safety, environmental, information technology, legal and business conduct policies. Any such access or connection to the Systems is strictly for the purpose of Supplier's performance of the Services under and in accordance with the Agreement. Supplier agrees that Fenix24 may perform periodic network assessments and should any such assessment reveal inadequate security by Supplier, Fenix24, in addition to other remedies it may have, may suspend Supplier's access to the Systems until such security issue has been eliminated. ● Supplier that not allow any generative Artificial Intelligence (A.I.) (NLP, deep learning, machine learning) that either (a) trains on or (b) does not guarantee Fenix24's sole ownership and confidentiality of the following, without Fenix24's prior explicit written consent: Fenix24 Personal Data or information from or about any Fenix24 customer or supplier or any Confidential Information. Supplier must use human oversight for all material actions taken by, or output delivered from, AI. Supplier must be willing to identify which elements of any deliverables or services provided to Fenix24 were created by AI, upon request. Any processing of Fenix24 Personal Data by AI shall be included in the scope of Subprocessors identified in writing by Supplier to Fenix24.
3. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	● Business Continuity Plan. Maintain internal practices, plans or procedures that are designed to reasonably ensure Supplier's products and services are uninterrupted during the term of the Agreement. Supplier's plans shall be designed around at minimum a recovery time objective of 24 hours for critical systems and 5 days for all others and recovery point objective of 24 hours unless otherwise expressly agreed in a signed writing. ● Maintain: (i) daily backups (including backup encryption) of production file systems and databases; and (ii) a formal disaster recovery plan for the production data center and conduct regular testing on the effectiveness of such plan.
4. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	● Section 5 of the DPA. ● Regularly conduct internal security audits and obtain at least annual external security assessments and penetration tests of Supplier systems including, without limitation, cloud architecture, business processes and procedures, access controls and encryption measures. ● Implement and maintain a risk assessment program to help identify foreseeable internal and external risks to Supplier's information resources and determine if existing controls, policies, and procedures are adequate.

5. Measures for user identification and authorization	● Proper user authentication for all employees and contractors with access to the Fenix24 Personal Data, including, without limitation, by assigning each employee/contractor unique access credentials for access to any system on which the Fenix24 Personal Data can be accessed and prohibiting employees/contractors from sharing such access credentials. ● Restrict and track access to the Fenix24 Personal Data to only those employees/contractors whose access is necessary to performing the services and implement and maintain logging and monitoring technology to help detect and prevent unauthorized access attempts to networks and production systems. ● Conducts periodic reviews of all user and service accounts — including privileged and third-party accounts — to verify that access remains appropriate, authorized, and consistent with each user's current role. Accounts inactive for 30 days are flagged for deactivation; accounts inactive for 45 days are disabled. Service account passwords are rotated on a minimum six-month cycle. ● Conduct periodic reviews of changes affecting systems' handling authentication, authorization, and auditing; and privileged access to production systems.
6. Measures for protection of Data during storage	● Encryption at rest. See Section 1 above. ● Multifactor authentication enabled for user access to production environment. ● Not store the Fenix24 Personal Data on any personal device (e.g., a home computer) or removable storage devices.
7. Measures for ensuring physical security of locations at which personal data are processed	● Establish limits on physical access to information systems and facilities using physical controls (e.g., coded badge access) that provide reasonable assurance that access to data centers is limited to authorized individuals. ● Install camera or video surveillance systems at all external and at critical internal entry points. ● All access logs and cameras shall be monitored 24x7. Alerts to unauthorized access or activities are responded to immediately by a designated incident response team. Record retention shall be maintained for 6 months if permitted under applicable law.
8. Measures for ensuring events logging	● All activities impacting the Fenix24 Personal Data, the management of this data, and changes to access shall be logged and reviewed on a regular schedule for unauthorized access or activities. These logs shall be securely stored and processed by a security event and incident management system, which shall be configured to alert for suspicious or unauthorized activities 24x7. A designated team shall be responsible to manage and monitor these systems and logs.
9. Measures for ensuring system configuration, including default config	● Implement and maintain policies and procedures for managing changes to production systems, applications and databases, including without limitation, processes for documenting testing and approval of changes into production, security patching, and authentication. ● Any security or privacy related patch addressing any Critical vulnerability or risk must be implemented within 72 hours or there must be compensating controls in place by that time, with full remediation within 7 calendar days; and for any High vulnerability or risk the deadline shall be not slower than 14–30 days.
10. Measures for internal IT and IT security governance and management	● Maintain and implement security policies and procedures designed to ensure employees and contractors process the Fenix24 Personal Data in accordance with the Standard Contractual Clauses, this DPA and Data Protection Legislation. ● Implement and enforce disciplinary measures against employees and contractors for failure to abide by its security policies and procedures.
11. Measures for certification/assurance of processes and products	● Certifications. See Section 4 above. ● All information security roles and responsibilities are defined and allocated. Minimization of opportunities for unauthorized or unintentional modification or misuse of assets and data.

12. Measures for ensuring data minimization and accountability	● Section 3 of the DPA. ● Detailed privacy assessments are performed related to implementation of new products/services and processing of personal data by Supplier and third parties. ● Security measures are in place to provide only the minimum amount of access necessary to perform required functions. ● Data retention time limits restricted.
13. Measures for ensuring data quality	● Exercise of rights. See Section 7 of the DPA. ● Secure development environment. Development environments are protected from malicious or accidental development and update of code that may create vulnerabilities or compromise confidentiality, integrity, and availability of the platform. Production data of Fenix24 or its customers may not be used in development or testing.
14. Measures for ensuring limited data retention	● Section 8 and Annex A of the DPA.
15. Measures for allowing data portability and ensuring erasure	● Sections 7 and 8 of the DPA.

Annex C: HIPAA

BUSINESS ASSOCIATE AGREEMENT

Fenix24 and/or its Affiliates ("**Fenix24**" or "**Business Associate**") and Supplier, or Supplier's affiliate, have entered or are entering into an agreement pursuant to which Fenix24 may purchase services or products from Supplier (the "Services Arrangement") and Supplier performs services on Fenix24's behalf ("Supplier Agreement"). This Business Associate Agreement ("**BAA**") is attached to and made a part of the Data Protection Agreement ("**DPA**") between Fenix24 and Supplier.

RECITALS

WHEREAS, Business Associate has arrangements with certain clients which may subject Business Associate to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, as amended and supplemented by Subtitle D of the Health Information Technology for Economic and Clinical Health Act, and the regulations promulgated pursuant to the foregoing statues under 45 C.F.R. Parts 160 and 164 (collectively "HIPAA");

WHEREAS, in connection with the Services Arrangement, Supplier may create, receive, maintain, or transmit Protected Health Information (as defined below); and

WHEREAS, Business Associate and Supplier desire to protect the privacy, security, and integrity of all such Protected Health Information pursuant to this BAA in accordance with HIPAA.

NOW THEREFORE, effective upon the earlier of Supplier agreeing to incorporate the DPA or upon any cross-reference to this BAA in a purchase agreement or order of Fenix24, this BAA shall apply (the "BAA Effective Date"). Business Associate and Supplier do hereby covenant and agree as follows:

1. Definitions

(a) "Breach" shall have the same meaning as the term "breach" in 45 C.F.R. Part 164, Subpart D (the "Breach Notification Rule").

(b) "Disclosure" or "Disclose" shall have the same meaning as the term "disclosure" in HIPAA.

(c) "Designated Record Set" shall have the same meaning as the term "designated record set" in HIPAA.

(d) "Discovery" shall have the same meaning as the term "discovery" in 45 C.F.R. § 164.410(a)(2).

(e) "Electronic Protected Health Information" shall have the same meaning as the term "electronic protected health information" in HIPAA, limited to the information created or received by Supplier from or on behalf of Business Associate or from or on behalf of any "covered entity" or "business associate" (as defined under HIPAA) client of Business Associate.

(f) "Individual" shall have the same meaning as the term "individual" in HIPAA and shall include a person who qualifies as a personal representative in accordance with HIPAA.

(g) "Information Blocking" shall have the meaning given to such term in the 21st Century Cures Act, including without limitation 45 C.F.R. § 171.103.

(h) "Protected Health Information" shall have the same meaning as the term "protected health information" in HIPAA, limited to the information created or received by Supplier from or on behalf of Business Associate or from or on behalf of any "covered entity" or "business associate" (as defined under HIPAA) client of Business Associate.

(i) "Required By Law" shall have the same meaning as the term "required by law" in HIPAA.

(j) "Secretary" shall mean the Secretary of the United States Department of Health and Human Services ("HHS").

(k) "Security Incident" shall have the same meaning as the term "security incident" in HIPAA.

(l) "Transaction" shall have the same meaning as the term "transaction" in 45 C.F.R. Parts 160 and 162 (the "Transactions Rule").

(m) "Unsecured Protected Health Information" shall have the same meaning as the term "unsecured protected health information" in the Breach Notification Rule.

(n) "Use" shall have the same meaning as the term "use" in HIPAA.

Unless otherwise provided in this BAA, all terms have the same meaning as set forth in HIPAA, as amended. All citations to the Code of Federal Regulations set forth in this BAA shall include all subsequent, updated, amended and/or revised provisions thereto.

2. Obligations and Activities of Supplier.

(a) Except as otherwise limited in this BAA, Supplier may Use or Disclose Protected Health Information to fulfill its obligations to Business Associate under the Services Arrangement. Supplier agrees to not Use or Disclose Protected Health Information other than as permitted or required by this BAA or as Required By Law.

(b) Supplier agrees to use appropriate safeguards and comply, where applicable, with Subpart C of 45 C.F.R. Part 164 with respect to Electronic Protected Health Information, to prevent Use or Disclosure of Protected Health Information other than as provided for by this BAA.

(c) Supplier agrees to report, in writing (see Section 7), to Business Associate, within three (3) days of Discovery, any Use or Disclosure of Protected Health Information not provided for by this BAA of which it becomes aware, including any Breach of Unsecured Protected Health Information, as required by 45 C.F.R. §164.410, and any Security Incident. For reports of incidents constituting a Breach, the report shall include, to the extent available and promptly thereafter as soon as information becomes available, the identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by Supplier to have been, accessed, acquired, used, or disclosed during such Breach as well as any other information a covered entity would be required to include in notifications to Individuals under 45 C.F.R. § 164.404(c). For incidents that do not rise to the level of a Breach, the report shall identify the date of the Security Incident or impermissible Use or Disclosure (collectively "Occurrence"), the scope of the Occurrence, Supplier's response to the Occurrence, and the identification of the party responsible for causing the Occurrence, if known.

(d) Supplier agrees to mitigate, to the extent practicable, any harmful effect that is known to Supplier or Business Associate, of a Use or Disclosure of Protected Health Information in violation of this BAA or HIPAA.

(e) In accordance with 45 C.F.R. §§164.308(b)(2) and 164.502(e)(1)(ii), Supplier agrees to ensure that any subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of Supplier agree in writing to the same restrictions, conditions, and requirements that apply pursuant to this BAA to Supplier with respect to such information.

(f) Supplier agrees to make available, in a time and manner specified by Business Associate, Protected Health Information in a Designated Record Set to Business Associate, to any Covered Entity client of Business Associate if so directed by Business Associate, or to an Individual if so directed by Business Associate, as necessary to satisfy a covered entity's obligations under 45 C.F.R. §164.524 and applicable state law. In the event an Individual requests such access directly from Supplier, Supplier shall forward such request to Business Associate promptly, and within no more than two (2) days.

(g) Supplier agrees to make any amendment, in a time and manner specified by Business Associate, to Protected Health Information in a Designated Record Set as requested or agreed to by Business Associate or any covered entity or business associate client of Business Associate pursuant to 45 C.F.R. §164.526, or to take other measures as necessary to satisfy a covered entity's obligations under 45 C.F.R. §164.526 and applicable state law. In the event an Individual requests an amendment directly from Supplier, Supplier shall forward such request to Business Associate promptly, and within no more than two (2) days.

(h) Supplier agrees to maintain and make available, in a time and manner specified by Business Associate, the information required to provide an accounting of Disclosures to Business Associate, to any covered entity or business associate client of Business Associate if so directed by Business Associate, or to an Individual if so directed by Business Associate, in accordance with 45 C.F.R. §164.528 or HIPAA. In the event an Individual requests an accounting directly from Supplier, Supplier shall forward such request to Business Associate promptly, and within no more than two (2) days.

(i) To the extent Supplier is to carry out one or more of Business Associate's or any covered entity or business associate client's obligation(s) under Subpart E of 45 C.F.R. Part 164 or other provisions of HIPAA, Supplier agrees

to comply with the requirements of Subpart E and HIPAA that apply to Business Associate or any covered entity or business associate client of Business Associate, as applicable, in the performance of such obligation(s).

(j) Supplier agrees to make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information available to (i) Business Associate, upon written request, and (ii) the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining Supplier's, Business Associate's or any Business Associate client's compliance with HIPAA. If the Secretary requests such access, Supplier shall promptly notify Business Associate and shall consult and cooperate with Business Associate concerning the proper response to such request. Notwithstanding the foregoing, nothing in this section shall impose upon Business Associate any obligation to review Supplier's practices, books or records.

(l) Unless Business Associate agrees, in writing, that this requirement is infeasible with respect to particular data, Supplier shall secure all Protected Health Information by a technology standard that renders Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals and is developed in accordance with Department of Health and Human Services' applicable guidance and other applicable laws and regulations.

(m) Except to the extent prohibited by law, Supplier shall immediately notify Business Associate if it receives a request for Disclosure of Protected Health Information with which Supplier believes it is Required by Law to comply. Supplier shall provide Business Associate with a copy of such request and shall consult and cooperate with Business Associate concerning the proper response to such request. Supplier shall immediately notify Business Associate of any litigation or administrative proceedings commenced against Supplier or its agents or contractors in connection with this BAA or the Services Arrangement.

(n) To the extent that, under the Services Arrangement, Supplier conducts on behalf of Business Associate all or part of a Transaction, Supplier shall comply with, and shall cause any of its agents or subcontractors to comply with, the Transactions Rule.

(o) Supplier shall not engage in any practice that would constitute Information Blocking, with respect to Supplier, Business Associate or a client of Business Associate, shall cooperate in good faith with Business Associate to prevent or mitigate any practice that would constitute Information Blocking and shall otherwise comply with all laws with respect to Information Blocking.

3. ***Permitted Uses and Disclosures of Protected Health Information by Supplier.***

(a) Supplier may Use or disclose Protected Health Information as necessary to perform the services for, or on behalf of, Business Associate as set forth in the Services Arrangement and as provided in this BAA provided such Use or Disclosure complies with HIPAA. Supplier acknowledges and agrees that it acquires no title or ownership rights to the Protected Health Information, including any de-identified information, as a result of this BAA.

(b) Supplier agrees to Use, Disclose and make requests for Protected Health Information consistent with the requirements in HIPAA regarding minimum necessary Uses and Disclosures.

(c) Supplier may not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by a Covered Entity.

(d) Supplier agrees that it will not de-identify any Protected Health Information received from Business Associate without the express written consent of Business Associate.

(e) Supplier shall create, receive, maintain, or transmit Protected Health Information on behalf of Business Associate only within the United States of America.

4. Termination and Survival.

(a) ***Term.*** The term of this BAA shall begin as of the BAA Effective Date and shall terminate upon the termination or expiration of the Services Arrangement and completion of all services thereunder or upon the termination of this BAA pursuant to Section 4(b) below.

(b) ***Termination for Cause.*** Upon Business Associate's knowledge of a material breach or violation of this BAA by Supplier, Business Associate may either: (i) provide an opportunity for Supplier to cure the breach or end the violation and terminate, without penalty, this BAA and the Services Arrangement if Supplier does not cure the breach or end the violation within thirty (30) days of receiving notice of such breach or violation from Business

Associate; (ii) immediately terminate, without penalty, this BAA and the Services Arrangement if Supplier has breached or violated a material term of this BAA and Business Associate reasonably determines that cure is not feasible; or (iii) if Business Associate reasonably determines neither termination nor cure are feasible, Business Associate may report the breach or violation to the Secretary.

(c) ***Effect of Termination.***

(i) Upon termination of this BAA:

(A) Supplier shall, within thirty (30) days of the termination of this BAA, return to Business Associate, or upon Business Associate's written request destroy in a HIPAA-compliant manner, all Protected Health Information received from Business Associate, or created or received by Supplier on behalf of Business Associate, that Supplier still maintains in any form and shall retain no copies of Protected Health Information; and

(B) In the event Supplier determines that returning or destroying any such Protected Health Information is infeasible, Supplier shall provide to Business Associate notification of the conditions that make return or destruction infeasible. If Business Associate agrees with such infeasibility determination, Supplier may retain such Protected Health Information, extending the protections of this BAA to such retained Protected Health Information and limiting further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Supplier maintains such Protected Health Information.

This Section 4(c)(i) also shall apply to Protected Health Information that is in the possession of subcontractors or agents of Supplier.

5. ***Definitions*****.** A regulatory reference in this BAA to a section of HIPAA or to HIPAA, generally, means the section or HIPAA as in effect or as amended. Any ambiguity or inconsistency in this BAA shall be interpreted to permit compliance with HIPAA.

6. ***Independent Contractors.*** The parties agree that they are independent contractors and not agents of each other, except as otherwise required by law or regulation.

7. ***Notices*****.** Any and all notices or other communications required or permitted by this BAA or by law to be served on or given to either party hereto by a party to this BAA shall be consistent with notice provisions in the applicable Services Arrangement and – if to Fenix24 – shall be copied to LegalNotices@fenix24.com.

8. ***Indemnification.*** In addition to any additional indemnification rights available under applicable law or the Services Arrangement, unless otherwise expressly agreed in writing, Supplier hereby agrees to indemnify and hold harmless Business Associate (including, without limitation, each of its employees, agents, successors and assigns) from and against any and all claims, causes of action, liabilities, damages, costs, or expenses (including without limitation, attorneys' fees, court costs, notification and monitoring costs, costs of administrative or other proceedings, and costs of investigation) arising out of any act or omission pertaining to the creation, receipt, maintenance or transmission of Protected Health Information, or any breach of the terms and provisions of this BAA or HIPAA, by Supplier or any party acting by or through Supplier (including, without limitation, Supplier's agents, employees, representatives, contractors or subcontractors).

9. ***Insurance Coverage.*** In addition to any additional insurance provisions in the Services Arrangement, Supplier shall procure and maintain, at its sole cost and expense, all insurance coverage required by applicable law and, in any event, cyber liability insurance, including first party and third party coverage, with limits no less than one million dollars ($2,000,000) per incident and no less than five million dollars ($5,000,000) in the aggregate for all claims each policy year. Such insurance shall name Business Associate as an additional insured and be issued by an insurance company with a Best's Rating of no less than A-VII, and must provide that the insurance carrier will give Business Associate at least thirty (30) days' prior written notice of any cancellation or non-renewal of coverage prior to any such cancellation or non-renewal of coverage, Supplier shall have new insurance policies in place that meet the requirements of this section. Upon Business Associate's written request, Supplier will provide Business Associate with copies of the certificates of insurance and policy endorsements for the insurance policies required by this section. To the extent any insurance coverage required under this section is purchased on a "claims made" basis, such insurance shall be continuously maintained until at least six (6) years beyond the termination or cancellation of this BAA.

10. ***Entire Agreement; Amendment*****.** This BAA supersedes all previous contracts and constitutes the entire agreement of whatever kind or nature existing between the parties with respect to the subject matter hereof, and no party shall be entitled to benefits other than those specified herein. As between the parties, no oral statement or prior written material

not specifically incorporated herein shall be of any force and effect; and the parties specifically acknowledge that in entering into and executing this BAA, the parties rely solely upon the representations and agreements contained in this BAA and no others.

11. ***Interpretation; Waiver.*** In the event that a provision of this BAA conflicts with a provision of the Services Arrangement, the provision of this BAA shall control; provided, however, that to the extent that any provision within the Services Arrangement imposes more stringent requirements than that required in the BAA, the parties agree to adhere to the terms of the Services Arrangement. Otherwise, this BAA shall be construed under, and in accordance with, the terms of the Services Arrangement. The failure of either party to enforce at any time any provision of this BAA shall not be construed as a waiver of such provision, nor in any way affect the validity of this BAA or the right of either party thereafter to enforce each as every such provision. Waiver of a breach of any provision of this BAA shall not be deemed a waiver of any other breach of the same or any different provision.

12. ***Survival.*** Any provision of this BAA which by its terms imposes an obligation which continues following termination of this BAA shall survive the termination of this BAA and shall continue to be binding on the parties, including but not limited to Section 4(c), Section 8, Section 9, Section 13 and Section 19 of this BAA.

13. ***Injunctive Relief.*** Supplier understands and acknowledges that any Use or Disclosure of Protected Health Information in violation of this BAA will cause Business Associate irreparable harm, the amount of which may be difficult to ascertain, and therefore agrees that Business Associate shall have the right to apply to a court of competent jurisdiction for specific performance and/or an order restraining and enjoining any such further Use or Disclosure and for such other relief as Business Associate shall deem appropriate. Such right of Business Associate is to be in addition to the remedies otherwise available to Business Associate at law or in equity. Supplier expressly waives the defense that a remedy in damages will be adequate and further waives any requirement in an action for specific performance or injunction for the posting of a bond by Business Associate.

14. ***Assignment; Binding Effect.*** No assignment of the rights or obligations of either party under this BAA shall be made without the express written consent of the other party, which consent shall not be unreasonably withheld – provided that Fenix24 may assign to an affiliate of Fenix24 upon providing notice to Supplier in writing. This BAA shall be binding upon and shall inure to the benefit of the parties, their respective successors and permitted assignees. An "affiliate" shall mean any entity with at least 50% common direct or indirect ownership or control.

15. ***Counterparts.*** This BAA shall be effective upon incorporation by reference to the DPA to which it is attached. If the Parties prefer, they may also mutually execute a copy but such execution rather than incorporation by reference shall not be required in order for this BAA to be effective. If executed, it may be executed in any number of counterparts, each of which shall be deemed an original, but which together shall constitute one and the same instrument.

16. ***No Third Party Beneficiaries.*** Nothing express or implied in this BAA is intended to confer, nor shall anything herein or therein confer, upon any person other than Business Associate and Supplier and their respective successors or assigns in interest, any rights, remedies, obligations, or liabilities whatsoever.

17. ***Modification For Change in Law.*** Upon the occurrence of changes or amendments to the regulations or other law that affect the legality of or any provision in this BAA, Business Associate and Supplier agree to modify this BAA to comport with such changes or amendments. Any such modification of this BAA shall be in writing and signed by Business Associate and Supplier.

18. ***Other Requirements.*** Business Associate and Supplier agree that to the extent not incorporated or referenced in this BAA, other applicable requirements under HIPAA that are required to be incorporated by reference in a business associate agreement are incorporated into this BAA as if set forth in this BAA in their entirety and are effective as of the applicable date for each such requirement on which HHS will require business associates to comply with such requirement. Supplier shall comply with such requirements prescribed by HIPAA commencing on such applicable date of each such requirement.

19. ***Governing Law.*** This BAA shall be governed and construed in accordance with HIPAA and the laws of the State of Tennessee, without regard to conflicts of law provisions that would require application of the law of another jurisdiction.

20. ***Severability.*** If any provision of this BAA is rendered invalid or unenforceable by the decision of any court, arbitrator or administrative body, such invalid or unenforceable provision shall be severed from this BAA and all other provisions of this BAA shall remain in full force and effect.