

TERMS OF SERVICE

Effective as of July 21, 2026.

These Terms of Service together with its Exhibits (the "**Agreement**") are entered into by and between TopK, Inc., a Delaware corporation (the "**Provider**") and the entity or person placing an order for or accessing any Services (the "**Customer**"). If you are accessing or using the Services on behalf of your company, you represent that you are authorized to accept this Agreement on behalf of your company, and all references to "you" or "Customer" reference your company.

The "**Effective Date**" of this Agreement is the date which is the earlier of (a) Customer's initial access to any Services (as defined below) or (b) the effective date of the first Order Form referencing this Agreement.

BY INDICATING YOUR ACCEPTANCE OF THIS AGREEMENT OR ACCESSING OR USING ANY SERVICES, YOU ARE AGREEING TO BE BOUND BY ALL TERMS, CONDITIONS, AND NOTICES CONTAINED OR REFERENCED IN THIS AGREEMENT. IF YOU DO NOT AGREE TO THIS AGREEMENT, PLEASE DO NOT USE ANY SERVICES. FOR CLARITY, EACH PARTY EXPRESSLY AGREES THAT THIS AGREEMENT IS LEGALLY BINDING UPON IT. THIS AGREEMENT CONTAINS MANDATORY ARBITRATION PROVISIONS THAT REQUIRE THE USE OF ARBITRATION TO RESOLVE DISPUTES, RATHER THAN JURY TRIALS. PLEASE READ IT CAREFULLY.

1. DEFINITIONS

Other than the terms defined in the body of this Agreement, these terms have the following meaning:

"**Affiliate**" means any entity under the control of a Party where "control" means ownership of or the right to direct greater than 50% of the voting securities of such entity.

"**Beta Offerings**" mean pre-release services, features, or functions identified as alpha, beta, preview, early access, or words or phrases with similar meanings.

"**Code**" means software development kits (SDKs), command line interfaces (CLIs), or other code provided by the Provider for deployment on Customer Properties.

"**Contractor**" means an independent contractor or consultant of the Customer who is not a competitor of the Provider.

"**Customer Data**" means any data of any type that is submitted to the Services by or on behalf of the Customer, including without limitation data submitted, uploaded, or imported to the Services by the Customer (including from Third-Party Platforms).

"**Customer Properties**" mean Customer's websites, servers, apps, or other offerings owned and operated by (or for the benefit of) Customer through which Customer uses the Services.

"**Dashboard**" means Provider's user interface for accessing and administering the Services that Customer may access via the web or the Apps.

"**DPA**" means the data processing addendum attached hereto as Exhibit A.

"**Documentation**" means the technical user documentation provided with the Services.

"Feedback" means comments, questions, suggestions, or other feedback relating to the Services, but excluding any Customer Data.

"Initial Term" means a set term designated in an Order Form during which the Services are provided to the Customer.

"Intellectual Property Rights" include all valid patents, trademarks, copyrights, trade secrets, moral rights, feedback, and other intellectual property rights, as may exist now or hereafter come into existence, and all renewals and extensions thereof, and all improvements to any of the foregoing, regardless of whether any of such rights arise under the laws of any state, country, or other jurisdiction.

"Laws" mean all applicable local, state, federal, and international laws, regulations, and conventions.

"Order Form" means a written or electronic form to order the Services referencing this Agreement. Upon execution by the authorized parties each Order Form will be subject to the terms and conditions of this Agreement.

"Party" means either The Provider or the Customer; the **"Parties"** both The Provider and the Customer.

"Permitted User" means an employee or a Contractor of the Customer or its Affiliate who is authorized to access the Services.

"Renewal Term" means successive periods equal to Initial Term, beginning after the then-current Subscription Term.

"Sensitive Personal Information" means any of the following: (i) credit, debit or other payment card data subject to the Payment Card Industry Data Security Standards (**"PCI DSS"**); (ii) patient, medical or other protected health information regulated by the Health Insurance Portability and Accountability Act (**"HIPAA"**), if applicable; or (iii) any other personal data of an EU citizen deemed to be in a "special category" (as identified in the EU General Data Protection Regulation or any successor Laws).

"Services" mean the Provider's proprietary software-as-a-service solution, including all products, services, and software provided by the Provider to the Customer.

"Subscription Term" means either the Initial Term or then-current Renewal Term.

"Support" means standard technical support and maintenance as further set forth under the Service Level Agreement attached to the Order Form (if applicable).

"Taxes" mean any sales, use, GST, value-added, withholding, or similar taxes or levies, whether domestic or foreign, other than taxes based on the income of the Provider.

"Third-Party Platform" means any software, software-as-a-service, data sources or other products or services not provided by the Provider that are integrated with or otherwise accessible through the Services.

2. PROVIDER SERVICES

2.1. Provision of Services. The Services are provided on a subscription basis for a Subscription Term. The Customer will purchase, and the Provider will provide the Services identified and agreed upon in the applicable Order Form.

2.2. Access to Services. The Customer may access and use the Services solely for its own benefit and in accordance with the terms and conditions of this Agreement, the Documentation, and any scope of use restrictions designated in the applicable Order Form. Use of and access to the Services is permitted only by Permitted Users. If Customer is given API keys or passwords to access the Services on the Provider's systems, the Customer will require that all Permitted Users keep API keys, user ID and password information strictly confidential and not share such information with any unauthorized person. User IDs are granted to individual, named persons, and may not be shared. If the Customer is accessing the Services using credentials provided by a third party (e.g., Google), then the Customer will comply with all applicable terms and conditions of such third-party regarding provisioning and use of such credentials. The Customer will be responsible for all actions taken using Customer's accounts and passwords. If a Permitted User who has access to a user ID is no longer an employee or Contractor of the Customer, then the Customer will promptly delete such user ID and otherwise terminate such Permitted User's access to the Services.

2.3. Contractors and Affiliates. The Customer may permit its Affiliates and Contractors to serve as Permitted Users, provided the Customer remains responsible for compliance by such individuals with all the terms and conditions of this Agreement, and all use of the Services by such individuals is for the sole benefit of the Customer.

2.4. General Restrictions. The Customer will not (and will not permit any third party to): (a) rent, lease, provide access to, or sublicense the Services to a third party; (b) resell, sublicense, or provide the Services to a third party on a standalone basis; provided that Customer may use the Services as a component of Customer's own products or services made available to its customers and end users; (c) reverse engineer, decompile, disassemble, or otherwise seek to obtain the source code or non-public APIs to the Services, except to the extent expressly permitted by applicable law (and then only upon advance notice to The Provider); (d) copy or modify the Services or any Documentation, or create any derivative work from any of the foregoing; (e) remove or obscure any proprietary or other notices contained in the Services (notices on any reports or data printed from the Services); or (f) publicly disseminate information regarding the performance of the Services.

2.5. Provider APIs. If Provider makes APIs available as part of the Services, Provider may monitor Customer's API usage and enforce the usage limits set forth in the applicable Order Form or Documentation. Provider may temporarily limit API usage to prevent material harm to the security, availability, operability, or integrity of the Services. Where practicable, Provider will notify Customer before imposing such limitation and will restore normal access promptly after the applicable risk has been resolved.

2.6. Apps. To the extent the Provider provides applications for use with the Services (the "**Apps**"), subject to all the terms and conditions of this Agreement, the Provider grants to the Customer a limited, non-transferable, non-sublicensable, non-exclusive license only during an applicable Subscription Term to use the object code form of the Apps internally, but only in connection with the Customer's use of the Services and otherwise in accordance with the Documentation and this Agreement.

2.7. Deployment of the Code. Subject to all the terms and conditions of this Agreement, the Provider grants to the Customer a limited, non-transferable, non-sublicensable, non-exclusive license only during an applicable Subscription Term to copy the Code in the form provided by the Provider on Customer Properties solely to support the Customer's use of the Services and otherwise in accordance with the Documentation and this Agreement. The Customer must implement the Code on the Customer Properties to enable features of the Services. The Customer will implement all the Code in strict accordance with the Documentation and other instructions provided by

the Provider. The Customer acknowledges that any changes made to the Customer Properties after initial implementation of the Code may cause the Services to cease working or function improperly and that the Provider will have no responsibility for the impact of any such change.

2.8. Trial Subscriptions. If the Customer receives free access or a trial or evaluation subscription to the Services (a "**Trial Subscription**"), then the Customer may use the Services in accordance with the terms and conditions of this Agreement for a period of fourteen (14) days or such other period granted by the Provider (the "**Trial Period**"). Trial Subscriptions are permitted solely for the Customer's use to determine whether to purchase a paid subscription to the Services. Trial Subscriptions may not include all functionality and features accessible as part of a paid Subscription Term. If the Customer does not enter into a paid Subscription Term, this Agreement and the Customer's right to access and use the Services will terminate at the end of the Trial Period. The Provider has the right to terminate a Trial Subscription at any time for any reason. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, THE PROVIDER WILL HAVE NO WARRANTY, LIABILITY, INDEMNITY, SUPPORT, OR OTHER OBLIGATIONS WITH RESPECT TO TRIAL SUBSCRIPTIONS.

2.9. Beta Offering. From time to time, the Provider may make Beta Offerings available to the Customer at no charge. The Customer may elect to try such Beta Offering in its sole discretion. Beta Offerings are intended for evaluation purposes and not for production use, are not supported, and may be subject to additional terms. Beta Offerings are not considered "Services" under this Agreement; however, all restrictions, our ownership and the Customer obligations concerning the Services shall apply. Unless otherwise stated or communicated to the Customer, any Beta Offerings trial period will expire upon the date that a version of the Beta Offerings becomes generally available without the applicable Beta Offerings designation. The Provider may discontinue Beta Offerings at any time in its sole discretion and may never make them generally available. Beta Offerings may not be supported and may be modified at any time without notice. Beta Offerings may not be as reliable, available, or subject to the same security requirements as in the Security Policy (as defined below).

3. CUSTOMER DATA

3.1. Data Processing by the Provider. All data processing activities by the Services will be governed by the DPA.

3.2. Rights in Customer Data. As between the parties, the Customer will retain all right, title, and interest (including all Intellectual Property Rights) in and to the Customer Data as provided to the Provider. Subject to the terms of this Agreement, the Customer hereby grants to the Provider a non-exclusive, worldwide, royalty-free right to use, copy, store, transmit, modify, and display the Customer Data solely to the extent necessary to provide the Services to the Customer.

3.3. Storage of Customer Data. Provider is not an archival or permanent backup service. During the applicable Subscription Term, Provider will use commercially reasonable measures designed to protect Customer Data against accidental loss, deletion, or corruption and to restore availability following a physical or technical incident. Customer remains responsible for maintaining independent backups of Customer Data where appropriate.

3.4. Customer Obligations.

a) In General. The Customer is solely responsible for the accuracy, content, and legality of all Customer Data. The Customer represents and warrants to the Provider that the Customer has all necessary rights, consents, and permissions to collect, share, and

use all Customer Data as contemplated in this Agreement (including granting the Provider the rights in Section 3.2 (Rights in Customer Data)) and that no Customer Data will violate or infringe (i) any third party Intellectual Property Rights or publicity, privacy, or other rights, (ii) any Laws, or (iii) any terms of service, privacy policies or other agreements governing Customer's accounts with any Third-Party Platforms. The Customer further represents and warrants that all Customer Data complies with the Agreement. The Customer will be fully responsible for all Customer Data submitted to the Services by any person as if it was submitted by the Customer.

b) No Sensitive Personal Information. Except as otherwise expressly agreed between the Parties in writing, the Customer specifically agrees not to use the Services to collect, store, process, or transmit any Sensitive Personal Information. The Customer acknowledges that the Provider is not a payment card processor and that the Services are not PCI DSS compliant. Except for the Provider's obligations as a business associate pursuant to this Agreement, the Customer shall be responsible for any Sensitive Personal Information it inadvertently submits to the Services, and the Provider will treat such submissions as Customer Data as defined in this Agreement such that the Provider is not subject to any additional obligations that apply to Sensitive Personal Information.

c) Compliance with Laws. The Customer agrees to comply with all applicable Laws in its use of the Services. Without limiting the generality of the foregoing, the Customer will not engage in any unsolicited advertising, marketing, or other activities using the Services, including without limitation any activities that violate the applicable Laws.

3.5. Indemnification by Customer. The Customer will defend the Provider from and against any claim arising from or relating to any Customer Data, Customer's use of a Third Party Platform, or Customer's use of the Services in violation of Laws and will indemnify and hold the Provider harmless from and against any damages and costs awarded against the Provider or agreed in settlement by the Customer (including reasonable attorneys' fees) resulting from such claim, provided that the Customer will have received from the Provider: (i) prompt written notice of such claim (but in any event notice in sufficient time for the Customer to respond without prejudice); (ii) the exclusive right to control and direct the investigation, defense and settlement (if applicable) of such claim; and (iii) all reasonably necessary cooperation of the Provider (at the Customer's expense). Notwithstanding the foregoing sentence, (a) the Provider may participate in the defense of any claim by counsel of its own choosing, at its cost and expense; and (b) the Customer will not settle any claim without the Provider's prior written consent, unless the settlement fully and unconditionally releases the Provider and does not require the Provider to take any action or admit any liability.

3.6. Anonymized Data. Notwithstanding anything to the contrary herein, the Customer agrees that the Provider may obtain and aggregate technical and other data about Customer's use of the Services that is non-personally identifiable with respect to the Customer ("**Anonymized Data**"), and the Provider may use the Anonymized Data to analyze, improve, support, and operate the Services and otherwise for any business purpose during and after the term of this Agreement, including without limitation to generate industry benchmark or best practice guidance, recommendations, or similar reports for distribution to and consumption by the Customer and other the Provider customers. For clarity, this Section 3.6 does not give the Provider the right to identify the Customer as the source of any Anonymized Data.

3.7. Artificial Intelligence. Provider will not use Customer Data to train or fine-tune any artificial intelligence or machine learning model made available to other customers or third parties without Customer's prior written consent. Provider may use Customer Data to operate, support, secure, and improve the Services for Customer, including evaluating service quality, provided that such use is consistent with the DPA and

Customer's documented instructions. Provider may use Anonymized Data in accordance with Section 3.6.

4. SECURITY

The Provider agrees to use commercially reasonable technical and organizational measures designed to prevent unauthorized access, use, alteration, or disclosure of the Services or Customer Data, as further described in the Provider's Technical and Organizational Measures set forth as Schedule B to the DPA (the "**Security Policy**"). However, the Provider will have no responsibility for errors in transmission, unauthorized third-party access, or other causes beyond the Provider's control.

5. THIRD-PARTY INTEGRATIONS

The Services may support integrations with certain Third-Party Platforms. To enable the Services to access and receive Customer's information from a Third-Party Platform, the Customer may be required to input its credentials for such Third-Party Platform. By enabling use of the Services with any Third-Party Platform, the Customer authorizes The Provider to access Customer's accounts with such Third-Party Platform for the purposes described in this Agreement. The Customer is responsible for complying with any relevant terms and conditions of the Third-Party Platform and for maintaining appropriate accounts in good standing with the providers of the Third-Party Platforms. Customer acknowledges and agrees that the Provider has no responsibility or liability for any Third-Party Platform, or how a Third-Party Platform uses or processes Customer Data after such is exported to a Third-Party Platform. The Provider cannot ensure that the Services will maintain integrations with any Third-Party Platform and the Provider may disable integrations of the Services with any Third-Party Platform at any time with or without notice to the Customer. For clarity, this Agreement governs Customer's use of and access to the Services, even if accessed through an integration with a Third-Party Platform. TO THE EXTENT THE CUSTOMER USES FEATURES IN THE SERVICES THAT INTEGRATE WITH A THIRD-PARTY PLATFORM AND THE CUSTOMER REQUESTS THAT THE PROVIDER INTEGRATE WITH SUCH THIRD-PARTY PLATFORM'S BETA OR PRE-RELEASE FEATURES (the "**THIRD-PARTY BETA RELEASES**"), THE PROVIDER WILL HAVE NO LIABILITY ARISING OUT OF OR IN CONNECTION WITH THE PROVIDER'S PARTICIPATION IN SUCH THIRD-PARTY BETA RELEASES OR CUSTOMER'S USE OF SUCH INTEGRATED FEATURES.

6. OWNERSHIP

6.1. Provider's Technology. This is a subscription agreement for access to and use of the Services. The Customer acknowledges that it is obtaining only a limited right to the Services and that irrespective of any use of the words "purchase", "sale", or like terms in this Agreement, no ownership rights are being conveyed to the Customer under this Agreement. The Customer agrees that the Provider or its suppliers retain all right, title, and interest (including all Intellectual Property Rights) in and to the Services and all Documentation, Professional Services' deliverables and all related and underlying technology and documentation and any derivative works, modifications or improvements of any of the foregoing, including Feedback (collectively, the "**Provider's Technology**"). Except as expressly set forth in this Agreement, no rights in the Provider's Technology are granted to the Customer. Further, the Customer acknowledges that the Services are offered as an on-line, hosted solution, and that the Customer has no right to obtain a copy of any of the Services, except for the Code and the Apps in the format provided by the Provider.

6.2. Feedback. The Customer may, from time to time, submit Feedback to the Provider. The Provider may freely use or exploit Feedback in connection with the

Services and may also disclose such Feedback to third party. The Provider shall not disclose the name of the Customer in any use or exploitation of the Feedback.

7. SUBSCRIPTION TERM, FEES & PAYMENT

7.1. Subscription Term and Renewals. The Subscription Term and Renewal Term will be as set forth in the applicable Order Form. Unless otherwise specified in an applicable Order Form, each Subscription Term will automatically renew for the Renewal Term set forth in such Order Form unless either party gives the other written notice of termination at least thirty (30) days prior to expiration of the then-current Subscription Term.

7.2. Fees and Payment. All fees are as set forth in the applicable Order Form and will be paid by the Customer in accordance with the payment terms set forth in the Order Form. Except as expressly set forth in Section 9 (Limited Warranty), Section 13 (Indemnification), or Section 16.7 (Modifications to this Agreement), all fees are non-refundable. The Customer is responsible for paying all Taxes, and all Taxes are excluded from any fees set forth in the applicable Order Form. If the Customer is required by Law to withhold any Taxes from Customer's payment, the fees payable by the Customer will be increased as necessary so that after making any required withholdings, the Provider receives and retains (free from any liability for payment of Taxes) an amount equal to the amount it would have received had no such withholdings been made. Any late payments will be subject to a service charge equal to 1.5% per month of the amount due or the maximum amount allowed by law, whichever is less.

7.3. Suspension of Service. Without limiting the Provider's termination or other rights hereunder, the Provider reserves the right to suspend Customer's access to the applicable Services (and any related Professional Services and Support) in whole or in part, without liability to the Customer: (i) if Customer's account is thirty (30) days or more overdue; (ii) for Customer's breach of Sections 2.4 (General Restrictions) or 3.4 (Customer Obligations); or (iii) to prevent harm to other customers or third parties or to preserve the security, availability or integrity of the Services. Where practicable, Provider will provide Customer with prior notice of a suspension and a reasonable opportunity to resolve the applicable issue. Provider will use commercially reasonable efforts to limit any suspension to the affected accounts, users, data, or components and to minimize disruption to Customer. Provider will promptly notify Customer of an emergency suspension and restore access as soon as the grounds for suspension have been resolved.

8. TERM AND TERMINATION

8.1. Term. This Agreement is effective as of the Effective Date and expires on the date of expiration or termination of all Subscription Terms.

8.2. Termination for Cause. Either party may terminate this Agreement (including all related Order Forms) if the other party (a) fails to cure any material breach of this Agreement (including with respect to the Customer any of the events set forth in Section 7.3 (Suspension)) within thirty (30) days after written notice; (b) ceases operation without a successor; or (c) seeks protection under any bankruptcy, receivership, trust deed, creditors' arrangement, composition, or comparable proceeding, or if any such proceeding is instituted against that party (and not dismissed within sixty (60) days thereafter).

8.3. Effect of Termination. Upon any expiration or termination of this Agreement, the Customer will immediately cease all use of and access to all Services (including all related Provider's Technology) and delete (or, at the Provider's request, return) all copies of the Documentation, all passwords or access codes and all other Provider's Confidential

Information in its possession. For thirty (30) days following expiration or termination, Customer may access and export Customer Data using the standard export functionality of the Services, unless the Agreement was terminated due to Customer's unlawful use of the Services or continued access would create a material security risk. Upon Customer's written request during that period, Provider will provide reasonable migration assistance at Provider's then-current professional services rates. Except where an exclusive remedy is specified, the exercise of either party of any remedy under this Agreement, including termination, will be without prejudice to any other remedies it may have under this Agreement, by law or otherwise.

8.4. Survival. The following Sections will survive any expiration or termination of this Agreement: 2.4 (General Restrictions), 2.8 (Trial Subscriptions), 3.3 (Storage of Customer Data), 3.5 (Indemnification by Customer), 3.6 (Aggregated Anonymous Data), 3.7 (AI Data), 6 (Ownership), 7.2 (Fees and Payment), 8 (Term and Termination), 9.1 (Warranty Disclaimer), 12 (Limitation of Remedies and Damages), 13 (Indemnification), 14 (Confidential Information), and 16 (General Terms).

9. LIMITED WARRANTY

9.1. Limited Warranty. The Provider warrants, for Customer's benefit only, that the Services will operate in substantial conformity with the applicable Documentation and in accordance with applicable law. The Provider's sole liability (and Customer's sole and exclusive remedy) for any breach of this warranty will be, at no charge to the Customer, for the Provider to use commercially reasonable efforts to correct the reported non-conformity, or if the Provider determines such remedy to be impracticable, either Party may terminate the applicable Subscription Term and the Customer will receive as its sole remedy a refund of any fees the Customer has pre-paid for use of such Services for the terminated portion of the applicable Subscription Term. The limited warranty set forth in this Section 9.1 will not apply: (i) unless the Customer makes a claim within thirty (30) days of the date on which the Customer first noticed the non-conformity, (ii) if the error was caused by misuse, unauthorized modifications, or third-party hardware, software, or services, or (iii) to use provided on a no-charge, trial, or evaluation basis.

9.2. Warranty Disclaimer. EXCEPT FOR THE LIMITED WARRANTY IN SECTION 9.1, ALL SERVICES, SUPPORT, AND PROFESSIONAL SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE" (SUBJECT TO OBLIGATIONS IN SERVICE LEVEL AGREEMENT), THE PROVIDER AND ITS AFFILIATES DISCLAIM ALL OTHER WARRANTIES, CONDITIONS, GUARANTEES, OR UNDERTAKINGS, WHETHER EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, QUALITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE PROVIDER DOES NOT WARRANT THAT CUSTOMER'S USE OF THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT IT WILL MEET ITS NEEDS. THE PROVIDER SHALL NOT BE LIABLE FOR DELAYS, INTERRUPTIONS, SERVICES' FAILURES OR OTHER PROBLEMS INHERENT IN USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS, THIRD-PARTY PLATFORMS, OR OTHER SYSTEMS OUTSIDE THE REASONABLE CONTROL OF THE PROVIDER. PARTIES ALSO EXCLUDE THE APPLICATION OF BUSINESS PRACTICES.

10. AVAILABILITY, SERVICE LEVELS, AND SUPPORT

Provider will provide the Services and Support in accordance with the service levels set forth in the applicable Order Form or Service Level Agreement. If no Service Level Agreement is attached to the applicable Order Form, Provider will use commercially reasonable efforts to keep the Services available.

11. PROFESSIONAL SERVICES

The Provider will provide professional consulting services (the "**Professional Services**") purchased in the applicable Order Form. The scope of Professional Services will be as set forth in a Statement of Work referencing this Agreement and executed by both parties describing the work to be performed, fees and any applicable milestones, dependencies and other technical specifications or related information (an "**SOW**"). Unless the Professional Services are provided on a fixed-fee basis, the Customer will pay the Provider at the per-hour rates set forth in the Order Form (or, if not specified, at the Provider's then-standard rates) for any excess services. The Customer will reimburse the Provider for reasonable travel and lodging expenses as incurred. The Customer may use anything delivered as part of the Professional Services in support of authorized use of the Services and subject to the terms regarding Customer's rights to use the Services set forth in Section 2 (Provider Services) and the applicable SOW, but the Provider will retain all right, title, and interest in and to any such work product, code, or deliverables and any derivative, enhancement, or modification thereof created by the Provider. For any Professional Services provided to the Customer at no charge, the Customer further acknowledges and agrees that the Provider will not warrant the performance of such Professional Services.

12. LIMITATION OF REMEDIES AND DAMAGES

12.1. Consequential Damages Waiver. EXCEPT FOR EXCLUDED CLAIMS (DEFINED BELOW), NEITHER PARTY (NOR ITS AFFILIATES) SHALL HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOSS OF USE, LOST DATA, LOST PROFITS, FAILURE OF SECURITY MECHANISMS, INTERRUPTION OF BUSINESS, OR ANY INCIDENTAL, PUNITIVE, EXEMPLARY, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

IF THE CUSTOMER IS IN THE EUROPEAN ECONOMIC AREA, REFERENCES TO "INCIDENTAL, PUNITIVE, EXEMPLARY, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES" SHALL ALSO MEAN ANY LOSSES OR DAMAGES WHICH: (A) WERE NOT REASONABLY FORESEEABLE BY BOTH PARTIES; (B) WERE KNOWN TO THE CUSTOMER BUT NOT TO THE PROVIDER; OR (C) WERE REASONABLY FORESEEABLE BY BOTH PARTIES BUT COULD HAVE BEEN PREVENTED BY THE CUSTOMER SUCH AS, FOR EXAMPLE, LOSSES CAUSED BY VIRUSES, MALWARE, OR OTHER MALICIOUS PROGRAMS, OR LOSS OF OR DAMAGE TO CUSTOMER DATA.

12.2. Liability Cap. EXCEPT FOR EXCLUDED CLAIMS (DEFINED BELOW), EACH PARTY'S ENTIRE LIABILITY TO THE OTHER ARISING OUT OF OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED IN AGGREGATE THE AMOUNT ACTUALLY PAID OR PAYABLE BY THE CUSTOMER TO THE PROVIDER UNDER THIS AGREEMENT IN THE 12 MONTHS PRIOR TO ACT THAT GAVE RISE TO LIABILITY.

12.3. Limitations to Exclusions. NOTHING IN THIS SECTION SHOULD BE CONSTRUED AS LIMITING A PARTY'S LIABILITY FOR DEATH OR BODILY HARM, WILFUL MISCONDUCT, OR GROSS NEGLIGENCE. ADDITIONALLY, SOME JURISDICTIONS DO NOT ALLOW OTHER EXCLUSIONS OR LIMITATIONS OF LIABILITY SPECIFIED IN THIS SECTION 12. IN SUCH CASE THESE EXCLUSIONS AND LIMITATIONS WILL BE ENFORCED TO THE GREATEST EXTENT PERMITTED BY APPLICABLE LAW.

12.4. Excluded Claims. "**Excluded Claims**" means any claim arising (a) under Section 2.4 (General Restrictions); (b) 3.4 (Customer Obligations), 3.5 (Indemnification by Customer); or (c) from a party's breach of its obligations in Section 14 (Confidential Information) (but excluding claims relating to Customer Data).

12.5. Nature of Claims and Failure of Essential Purpose. The parties agree that the waivers and limitations specified in this Section 12 apply regardless of the form of action, whether in contract, tort (including negligence), strict liability or otherwise and will survive and apply even if any limited remedy specified in this Agreement is found to have failed of its essential purpose.

13. INDEMNIFICATION

The Provider will defend the Customer from and against any claim by a third party alleging that the Services infringes any Intellectual Property Right and will indemnify and hold the Customer harmless from and against any damages and costs finally awarded against the Customer or agreed in settlement by the Provider (including reasonable attorneys' fees) resulting from such claim, provided that the Provider will have received from the Customer: (i) prompt written notice of such claim (but in any event notice in sufficient time for the Provider to respond without prejudice); (ii) the exclusive right to control and direct the investigation, defense, and settlement (if applicable) of such claim; and (iii) all reasonable necessary cooperation of Customer. Notwithstanding the foregoing sentence, (a) the Customer may participate in the defense of any claim by counsel of its own choosing, at its cost and expense and (b) the Provider will not settle any claim without Customer's prior written consent, unless the settlement fully and unconditionally releases the Provider and does not require the Customer to take any action or admit any liability. If the Customer's use of the Services is (or in the Provider's opinion is likely to be) enjoined, if required by settlement or if the Provider determines such actions are reasonably necessary to avoid material liability, the Provider may, in its sole discretion: (a) substitute substantially functionally similar products or services; (b) procure for the Customer the right to continue using the Services; or if (a) or (b) are not commercially reasonable, (c) terminate this Agreement and refund to the Customer the fees paid by the Customer for the portion of the Subscription Term that was paid by the Customer but not rendered by the Provider. The foregoing indemnification obligation of the Provider will not apply: (1) if the Services are modified by any party other than the Provider, but solely to the extent the alleged infringement is caused by such modification; (2) if the Services are combined with products or processes not provided by the Provider, but solely to the extent the alleged infringement is caused by such combination; (3) to any unauthorized use of the Services; (4) to any action arising as a result of Customer Data; (5) to any action arising from Customer's use of the Third-Party Platform; or (6) if the Customer settles or makes any admissions with respect to a claim without the Provider's prior written consent. THIS SECTION SETS FOR THE PROVIDER'S AND ITS AFFILIATES' SOLE LIABILITY AND THE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM OF INTELLECTUAL PROPERTY INFRINGEMENT.

14. CONFIDENTIAL INFORMATION

Each party (as "**Receiving Party**") agrees that all code, inventions, know-how, business, technical and financial information it obtains from the disclosing party (the "**Disclosing Party**") constitute the confidential property of the Disclosing Party (the "**Confidential Information**"), provided that it is identified as confidential at the time of disclosure or should be reasonably known by the Receiving Party to be confidential or proprietary due to the nature of the information disclosed and the circumstances surrounding the disclosure. Any Provider's Technology, performance information relating to the Services, and the terms and conditions of this Agreement will be deemed Confidential Information of The Provider without any marking or further designation. Except as expressly authorized herein, the Receiving Party will (1) hold in confidence and not disclose any Confidential Information to third parties and (2) not use Confidential Information for any purpose other than fulfilling its obligations and exercising its rights under this Agreement. The Receiving Party may disclose Confidential Information to its employees, agents, contractors and other representatives having a

legitimate need to know (including the Provider's Affiliates and the subcontractors referenced in Section 10 (Subcontractors)), provided that such representatives are bound to confidentiality obligations no less protective of the Disclosing Party than this Section 14 and that the Receiving Party remains responsible for compliance by any such representative with the terms of this Section 14. The Receiving Party's confidentiality obligations will not apply to information that the Receiving Party can document: (i) was rightfully in its possession or known to it prior to receipt of the Confidential Information; (ii) is or has become public knowledge through no fault of the Receiving Party; (iii) is rightfully obtained by the Receiving Party from a third party without breach of any confidentiality obligation; or (iv) is independently developed by employees of the Receiving Party who had no access to such information. The Receiving Party may make disclosures to the extent required by law or court order, provided the Receiving Party notifies the Disclosing Party in advance and cooperates in any effort to obtain confidential treatment. The Receiving Party acknowledges that disclosure of Confidential Information would cause substantial harm for which damages alone would not be a sufficient remedy, and therefore that upon any such disclosure by the Receiving Party the Disclosing Party will be entitled to seek appropriate equitable relief in addition to whatever other remedies it might have at law. These confidentiality obligations will apply during the term and for five (5) years thereafter; provided that obligations relating to trade secrets will continue for so long as such information remains a trade secret under applicable law. Customer Data will be deemed Customer's Confidential Information without any marking or further designation.

15. PUBLICITY

Neither party may issue a press release naming the other party or use the other party's name, trademarks, or logos in public marketing materials without the other party's prior written consent. Notwithstanding the foregoing, Provider may identify Customer as a customer in non-public discussions with prospective customers, investors, and professional advisors, subject to confidentiality obligations, unless Customer notifies Provider otherwise in writing.

16. GENERAL TERMS

16.1. Assignment. This Agreement will bind and inure to the benefit of each party's permitted successors and assigns. Neither party may assign this Agreement without the advance written consent of the other party, except that either party may assign this Agreement in connection with a merger, reorganization, acquisition, or other transfer of all or substantially all of such party's assets or voting securities. Any attempt to transfer or assign this Agreement except as expressly authorized under this Section 16.1 will be null and void.

16.2. Severability. If any provision of this Agreement will be adjudged by any court of competent jurisdiction to be unenforceable or invalid, that provision will be limited to the minimum extent necessary so that this Agreement will otherwise remain in effect.

16.3. Governing Law; Dispute Resolution.

a) Governing Law. This Agreement is construed and governed by the Laws of the State of Delaware, without reference to applicable jurisdiction's conflict of laws principles.

b) Direct Dispute Resolution. In the event of any dispute, claim, question, or disagreement arising from or relating to this Agreement, whether arising in contract, tort or otherwise, (the "**Dispute**"), the parties shall first use their best efforts to resolve the Dispute. If a Dispute arises, the complaining party shall provide written notice to the other party in a document specifically entitled "Initial Notice of Dispute," specifically

setting forth the precise nature of the dispute (the "**Initial Notice of Dispute**"). If an Initial Notice of Dispute is being sent to the Provider, it must be emailed to contact@topk.io.

Following receipt of the Initial Notice of Dispute, the parties shall consult and negotiate with each other in good faith and, recognizing their mutual interest, attempt to reach a just and equitable solution of the Dispute that is satisfactory to both parties ("**Direct Dispute Resolution**"). If the parties are unable to reach a resolution of the Dispute through Direct Dispute Resolution within thirty (30) days of the receipt of the Initial Notice of Dispute, then the Dispute shall subsequently be resolved by litigation as set forth below.

c) Litigation. Any lawsuit will be filed in any courts located in Wilmington, Delaware, and both Parties consent to personal jurisdiction in such courts for resolution on Disputes and agree that such venue is appropriate.

d) Construction and Joinder. THIS AGREEMENT MUST BE CONSTRUED AS IF IT WAS JOINTLY WRITTEN BY BOTH PARTIES. BOTH THE CUSTOMER AND THE PROVIDER AGREE THAT EACH MAY BRING OR PARTICIPATE IN CLAIMS AGAINST THE OTHER ONLY IN THEIR RESPECTIVE INDIVIDUAL CAPACITIES, AND NOT AS A PLAINTIFF OR CLASS MEMBER IN ANY PURPORTED CLASS. NO ARBITRATION OR CLAIM UNDER THIS AGREEMENT SHALL BE JOINED TO ANY OTHER ARBITRATION OR CLAIM, INCLUDING ANY ARBITRATION OR CLAIM INVOLVING ANY OTHER CURRENT OR FORMER USER OF THE SERVICES, AND NO CLASS ARBITRATION PROCEEDINGS SHALL BE PERMITTED.

e) Injunctive Relief. Notwithstanding the above provisions, the Provider may apply for injunctive remedies (or an equivalent type of urgent legal relief) in any jurisdiction.

16.4. Notice. Any notice or communication required or permitted under this Agreement will be in writing to the parties at the addresses set forth on the Order Form or at such other address as may be given in writing by either party to the other in accordance with this Section and will be deemed to have been received by the addressee (i) if given by hand, immediately upon receipt; (ii) if given by overnight courier service, the first business day following dispatch or (iii) if given by registered or certified mail, postage prepaid and return receipt requested, the second business day after such notice is deposited in the mail or (iv) next business day if sent by email.

16.5. Amendments; Waivers. No supplement, modification, or amendment of this Agreement will be binding, unless (i) modified in accordance with Section 16.7; or (ii) executed in writing by a duly authorized representative of each party to this Agreement. No waiver will be implied from conduct or failure to enforce or exercise rights under this Agreement, nor will any waiver be effective unless in a writing signed by a duly authorized representative on behalf of the party claimed to have waived. No provision of any purchase order or other business form employed by the Customer will supersede the terms and conditions of this Agreement, and any such document relating to this Agreement will be for administrative purposes only and will have no legal effect.

16.6. Entire Agreement. This Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements and communications relating to the subject matter of this Agreement.

16.7. Modifications to this Agreement. From time to time, The Provider may modify this Agreement. Unless otherwise specified by The Provider, changes become effective for the Customer upon renewal of Customer's current Subscription Term or entry into a new Order Form. The Provider will use reasonable efforts to notify Customer of the changes through communications via Customer's account, email or other means. In any

event, continued use of the Services after the updated version of this Agreement goes into effect will constitute Customer's acceptance of such updated version. If The Provider specifies that changes to the Agreement will take effect prior to Customer's next renewal or order (such as for legal compliance or product change reasons) and the Customer objects to such changes within 10 calendar days, The Provider may either (i) move the effective date of a change of the Agreement to Customer's next renewal or order; or (ii) terminate the applicable Subscription Term and give to the Customer as its sole remedy a refund of any fees the Customer has pre-paid for use of the applicable Services for the terminated portion of the Subscription Term, commencing on the date notice of termination was received or a different date the Parties agree on. The Provider may make changes to the Services, and the Provider will update the applicable Documentation accordingly. The support, security and service level availability terms described Service Level Agreement and in the Security Policy may be updated from time to time upon reasonable notice to the Customer to reflect process improvements or changing practices (but the modifications will not materially decrease the Provider's obligations as compared to those reflected in such terms as of the Effective Date).

16.8. Force Majeure. Neither party will be liable to the other for any delay or failure to perform any obligation under this Agreement (except for a failure to pay fees) if the delay or failure is due to unforeseen events that occur after the signing of this Agreement and that are beyond the reasonable control of such party, such as a strike, blockade, war, act of terrorism, riot, natural disaster, failure or diminishment of power or telecommunications or data networks or services, or refusal of a license by a government agency.

16.9. Hardship. If continued performance has become excessively onerous due to an event beyond a party's reasonable control which it could not reasonably have been expected to have taken into account (a "**Hardship**"), the Parties will in good faith negotiate alternative terms which reasonably allow for the consequences of such event. The Parties expressly exclude the ability of a court to adapt, amend, or terminate the Agreement in case of Hardship, and assume such risk.

16.10.Subcontractors. The Provider may use the services of subcontractors and permit them to exercise the rights granted to the Provider in order to provide the Services under this Agreement, provided that the Provider remains responsible for (i) compliance of any such subcontractor with the terms of this Agreement, (ii) for the overall performance of the Services as required under this Agreement and (iii) compliance with the terms of the DPA.

16.11.Court Orders. Nothing in this Agreement prevents the Provider from disclosing Customer Data to the extent required by law, subpoenas, or court orders, but the Provider will use commercially reasonable efforts to notify the Customer where permitted to do so.

16.12.Independent Contractors. The parties to this Agreement are independent contractors. There is no relationship of partnership, joint venture, employment, franchise, or agency created hereby between the parties. Neither party will have the power to bind the other or incur obligations on the other party's behalf without the other party's prior written consent.

16.13.Export Control. In its use of the Services, the Customer agrees to comply with all export and import laws and regulations of the applicable jurisdictions. Without limiting the foregoing, (i) the Customer represents and warrants that it is not listed on any US, UK, or EU government list of prohibited or restricted parties or located in (or a national of) a country that is subject to a US, UK, or EU government embargo or that has been designated by the US, UK, or EU government as a "terrorist supporting" country, (ii) the Customer will not (and will not permit any of its users to) access or use

the Services in violation of any US, UK, or EU export embargo, prohibition or restriction, and (iii) the Customer will not submit to the Services any information that is controlled under the U.S. International Traffic in Arms Regulations.

16.14. Counterparts. This Agreement may be executed in counterparts, each of which will be deemed an original and all of which together will be considered one and the same agreement.

Exhibit A

DATA PROCESSING ADDENDUM

1. INITIAL PROVISIONS

1.1. Agreement. This Data Processing Addendum including its annexes and the Standard Contractual Clauses, (the "**DPA**") is made by and between TopK Inc. (the "**Provider**"), and Customer, pursuant to the Master SaaS Subscription Agreement, the Terms of Service or other written or electronic agreement between the parties (as applicable) (the "**Agreement**").

1.2. Data Processing Agreement. By entering into the Agreement with the Provider You, the Customer, acknowledge that you have read and understood this DPA and agree to be bound by it.

2. DEFINITIONS

Any capitalized term used but not defined in this DPA has the meaning provided to it in the Agreement.

"**Account Data**" means Personal Data that relates to Customer's relationship with Provider, including to access Customer's account and billing information, identity verification, maintain or improve performance of the Services, provide support, investigate and prevent system abuse, or fulfill legal obligations.

"**Applicable Data Protection Legislation**" refers to laws and regulations applicable to Provider's processing of personal data under the Agreement, including but not limited to (a) the GDPR, (b) 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 2019 ("**UK GDPR**") and the Data Protection Act 2018 (together, "**UK Data Protection Laws**"), (c) the Swiss Federal Data Protection Act and its implementing regulations ("**Swiss DPA**"), (d) CCPA & CPRA, and (e) Australian Privacy Principles and the Australian Privacy Act (1988), in each case, as may be amended, superseded or replaced.

"**CCPA**" or "**CCPA and CPRA**" means the California Consumer Privacy Act of 2018 and any binding regulations promulgated thereunder, in each case, as may be amended from time to time. This includes but it is not limited to the California Privacy Rights Act of 2020.

"**Controller**" or "**controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. It shall have the same meaning ascribed to "controller" under the GDPR and other equivalent terms under Applicable Data Protection Legislation (e.g., "Business" as defined under the CCPA), as applicable.

"**Customer Personal Data**" means Personal Data that Provider processes as a Processor on behalf of Customer.

"**Europe**" means for the purposes of this DPA the European Economic Area ("**EEA**"), the United Kingdom ("**UK**") and Switzerland, or another country which ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of Personal Data, as determined by the European Commission in the case that EU Data Protection Law applies respectively as determined by the ICO in the case that UK Data Protection Law applies.

"GDPR" means 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 data (General Data Protection Regulation).

"Personal Data" or **"personal data"** or **"personal information"** means any information, including personal information, relating to an identified or identifiable natural person ("data subject") or as defined in and subject to Applicable Data Protection Legislation.

"Processor" or **"processor"** means the entity which processes Personal Data on behalf of the Controller. It shall have the meaning ascribed to "processor" under the GDPR and other equivalent terms under other Applicable Data Protection Legislation (e.g., "Service Provider" as defined under the CCPA), as applicable.

"Processing" or **"processing"** (and **"Process"** or **"process"**) means any operation or set of operations performed upon Personal Data, whether or not by automated means, means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

"Restricted Transfer" means: (i) where the GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

"Security Breach" means a breach of security leading to any accidental, unauthorized or unlawful loss, disclosure, destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data transmitted, stored or otherwise processed by Provider. A Security Incident shall not include an unsuccessful attempt or activity that does not compromise the security of Customer Personal Data, including (without limitation) pings and other broadcast attacks of 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.

"Standard Contractual Clauses" or **"SCCs"** means (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN> ("**EU SCCs**"); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c), or (d) where the UK GDPR means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as such Addendum may be revised under Section 18 therein ("**UK SCCs**") and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the "**Swiss SCCs**") (in each case, as updated, amended or superseded from time to time).

"Sub-processor" or "sub-processor" means (a) Provider, when Provider is processing Customer Personal Data and where Customer is itself a processor of such Customer Personal Data, or (b) any third-party Processor engaged by Provider or its affiliates to assist in fulfilling Provider's obligations under the Agreement and which processes Customer Personal Data. Sub-processors may include third parties or Provider affiliates but shall exclude Provider employees, contractors or consultants.

"Third Party Request" means any request, correspondence, inquiry, or complaint from a data subject, regulatory authority, or third party.

"UK Addendum" means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as such Addendum may be revised under Section 18 therein. This is found in Schedule D below.

3. APPLICABILITY AND SCOPE

3.1. Applicability. This DPA will apply only to the extent that Provider processes, on behalf of Customer, Personal Data to which Applicable Data Protection Legislation applies.

3.2. Scope. The subject matter of the data processing is the provision of the Services, and the processing will be carried out for the duration of the Agreement. Schedule A (Details of Processing) sets out the nature and purpose of the processing, the types of Personal Data Provider processes and the categories of data subjects whose Personal Data is processed.

3.3. Provider as a Processor. The parties acknowledge and agree that regarding the processing of Customer Personal Data, Customer may act either as a controller or processor and Provider is a processor. Provider will process Customer Personal Data in accordance with Customer's instructions as set forth in Section 3 (Customer Instructions).

3.4. Provider as a Controller of Account Data. The parties acknowledge that, regarding the processing of Account Data, Customer is a controller and Provider is an independent controller, not a joint controller with Customer. Provider will process Account Data as a controller (a) in order to manage the relationship with Customer; (b) carry out Provider's core business operations; (c) in order to detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services; (d) identity verification; (e) to comply with Provider's legal or regulatory obligations; and (f) as otherwise permitted under Applicable Data Protection Legislation and in accordance with this DPA, the Agreement, and the Privacy Policy.

4. PROVIDER AS A PROCESSOR

4.1. Customer Instructions. Customer appoints Provider as a processor to process Customer Personal Data on behalf of, and in accordance with, Customer's instructions (a) as set forth in the Agreement, this DPA, and as otherwise necessary to provide the Services to Customer (which may include investigating security incidents, and detecting and preventing exploits or abuse); (b) as necessary to comply with applicable law, including Applicable Data Protection Legislation; and (c) as otherwise agreed in writing between the parties ("**Permitted Purposes**").

4.2. Lawfulness of Instructions. Customer will ensure that its instructions comply with Applicable Data Protection Legislation. Customer acknowledges that Provider is

neither responsible for determining which laws are applicable to Customer's business nor whether Provider's Services meet or will meet the requirements of such laws. Customer will ensure that Provider's processing of Customer Personal Data, when done in accordance with Customer's instructions, will not cause Provider to violate any applicable law, including Applicable Data Protection Legislation. Provider will inform Customer if it becomes aware, or reasonably believes, that Customer's instructions violate applicable law, including Applicable Data Protection Legislation.

4.3. Additional Instructions. Additional instructions outside the scope of the Agreement or this DPA will be mutually agreed to between the parties in writing.

4.4. Purpose Limitation. Provider will process Customer Personal Data in order to provide the Services in accordance with the Agreement. Schedule A (Details of Processing) of this DPA further specifies the nature and purpose of the processing, the processing activities, the duration of the processing, the types of Personal Data and categories of data subjects.

4.5. Responding to Third Party Requests. In the event any Third Party Request is made directly to Provider in connection with Provider's processing of Customer Personal Data, Provider will promptly inform Customer and provide details of the same, to the extent legally permitted. Provider will not respond to any Third Party Request, without prior notice to Customer and an opportunity to object, except as legally required to do so or to confirm that such Third Party Request relates to Customer.

5. COMPLIANCE

Customer shall be responsible for ensuring that: a) all such notices have been given, and all such authorizations have been obtained, as required under Applicable Data Protection Legislation, for Provider (and its affiliates and Sub-processors) to process Customer Personal Data as contemplated by the Agreement and this DPA; b) it has complied, and will continue to comply, with all applicable laws relating to privacy and data protection, including Applicable Data Protection Legislation; and c) it has, and will continue to have, the right to transfer, or provide access to, Customer Personal Data to Provider for processing in accordance with the terms of the Agreement and this DPA.

6. SUBPROCESSORS

6.1. Authorization for Sub-processing. Customer agrees that (a) Provider may engage Sub-processors as listed at <https://trust.topk.io/subprocessors> (the "**Sub-processor Page**") which may be updated from time to time and Provider affiliates; and (b) such affiliates and Sub-processors respectively may engage third party processors to process Customer Personal Data on Provider's behalf. Customer provides a general authorization for Provider to engage onward sub-processors that is conditioned on the following requirements: (x) Provider will restrict the onward sub-processor's access to Customer Personal Data only to what is strictly necessary to provide the Services, and Provider will prohibit the sub-processor from processing the Customer Personal Data for any other purpose. (y) Provider agrees to impose contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any sub-processor it appoints that require such sub-processor to protect Customer Personal Data to the standard required by Applicable Data Protection Legislation; and (z) Provider will remain liable and accountable for any breach of this DPA that is caused by an act or omission of its sub-processors.

6.2. Current Sub-processors. Customer understands that effective operation of the Services may require the transfer of Customer Personal Data to Provider affiliate or to Provider's Sub-processors, see Schedule C. Customer hereby authorizes the transfer of Customer Personal Data to locations outside Europe (Provider's primary processing

facilities are in the United States of America), including to Provider affiliates and Sub-processors, subject to continued compliance with this DPA throughout the duration of the Agreement. Customer hereby provides general authorization to Provider engaging additional third-party Sub-processors to process Customer Personal Data within the Services for the Permitted Purposes.

6.3. Notification of Sub-processor Additions. Provider may, by giving reasonable notice to the Customer, add to the Sub-processor Page. Provider will notify Customer if it intends to add or replace Sub-processors from the Sub-Processor Page at least 10 days prior to any such changes. To receive such notification, Customers can follow link <https://trust.topk.io/subprocessors> to join Provider's distribution list. If Customer objects to the appointment of an additional Sub-processor within thirty (30) calendar days of such notice on reasonable grounds relating to the protection of the Customer Personal Data, then Provider will work in good faith with Customer to find an alternative solution. In the event that the parties are unable to find such a solution, Customer may terminate the Agreement at no additional cost.

7. IMPACT ASSESSMENTS AND CONSULTATIONS

Provider shall, to the extent required by Applicable Data Protection Legislation, provide Customer with reasonable assistance (at Customer's cost and expense) with data protection impact assessments or prior consultations with data protection authorities that Customer is required to carry out under such legislation.

8. SECURITY

8.1. Security Measures. Provider has in place and will maintain throughout the term of this Agreement appropriate technical and organizational measures designed to protect Customer Personal Data against Security Breaches. These measures shall at a minimum comply with applicable law and include the measures identified in Schedule B (Technical and Organizational Security Measures). Customer acknowledges that the security measures are subject to technical progress and development and that Provider may update or modify the security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

8.2. Staff. Provider will ensure that any person authorized to process Customer Personal Data (including its staff, agents, and subcontractors) shall be subject to a duty of confidentiality.

8.3. Security Breach. Upon becoming aware of a Security Breach involving Customer Personal Data processed by Provider on behalf of Customer under this DPA, Provider shall notify Customer without undue delay and shall provide such information as Customer may reasonably require, including to enable Customer to fulfil its data breach reporting obligations under Applicable Data Protection Legislation. Provider's notification of or response to a Security Breach shall not be construed as an acknowledgement by Provider of any fault or liability with respect to the Security Breach.

8.4. Customer is solely responsible for its use of the Services, including (a) making appropriate use of the Service to ensure a level of security appropriate to the risk in respect of Customer Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Service; and (c) backing up Customer Personal Data.

9. RETURN OR DELETION OF CUSTOMER'S PERSONAL DATA

Upon termination or expiry of this Agreement, Provider will (at Customer's election) delete or return to Customer all Customer Personal Data (including copies) in its possession or control as soon as reasonably practicable and within a maximum period of 30 days of termination or expiry of the Agreement, save that this requirement will not apply to the extent that Provider is required by applicable law to retain some or all of the Customer Personal Data, or to Customer Personal Data it has archived on back-up systems, which Customer Personal Data Provider will securely isolate and protect from any further processing, except to the extent required by applicable law.

10. AUDITS

10.1. Acknowledgment. The parties acknowledge that when Provider is acting as a processor on behalf of Customer, Customer must be able to assess Provider's compliance with its obligations under Applicable Data Protection Legislation and this DPA.

10.2. Previous Audits. Upon written request and at no additional cost to Customer, Provider shall provide Customer, or its appropriately qualified third-party representative (collectively, the "**Auditor**"), access to reasonably requested documentation evidencing Provider's compliance with its obligations under this DPA in the form of the relevant audits or certifications.

10.3. Customer Audit. While it is the parties' intention ordinarily to rely on the provision of the documentation to demonstrate Provider's compliance with this DPA and the provisions of Article 28 of the GDPR, Provider shall permit Customer or its Auditor to carry out an audit, at Customer's cost and expense, (including, without limitation, the costs and expenses of Provider), of Provider's processing of Customer Personal Data under the Agreement upon Customer's written request for an audit, subject to the terms of this Section. Following Provider's receipt of such request, Provider and Customer shall mutually agree in advance on the details of the audit, including the reasonable start date, scope and duration of any such audit. Any such audit shall be subject to Provider's security and confidentiality terms and guidelines, may only be performed a maximum of once annually and will be restricted to only data relevant to Customer. Where the Auditor is a third-party, Provider may object in writing to such Auditor, if in Provider's reasonable opinion, the Auditor is not suitably qualified or is a direct competitor of Provider. Any such objection by Provider will require Customer to either appoint another Auditor or conduct the audit itself. Any expenses incurred by an Auditor in connection with any review of reports or an audit shall be borne exclusively by the Auditor. For clarity, the exercise of audit rights under the SCCs shall be as described in this Section 10.3.

11. TRANSFERS

11.1. Location of Processing. Customer acknowledges that Provider and its Sub-processors may transfer and process personal data to and in the United States of America and other locations in which Provider, its affiliates or its Sub-processors maintain data processing operations, as more particularly described in the Sub-processor Page. Provider shall ensure that such transfers are made in compliance with Applicable Data Protection Legislation and this DPA.

11.2. Transfer Mechanism. The parties agree that when the transfer of personal data from Customer (as "data exporter") to Provider (as "data importer") is a Restricted Transfer, Applicable Data Protection Legislation requires that appropriate safeguards are put in place. For the purposes of such Restricted Transfers from Customer to Provider, the parties rely on Provider's certification under the EU-U.S Data Privacy Framework, the Swiss-US Data Privacy Framework and the UK-US Data Privacy Framework (together, the "**DPF**") operated by the U.S. Department of Commerce. To the extent that the DPF is invalidated or ceases to be an appropriate safeguard under Article 46 GDPR for transfers

to the United States, then, such transfer shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form part of this DPA, as follows:

- a) In relation to transfers of Customer Personal Data that is protected by the GDPR, the EU SCCs shall apply, completed as follows:
 - i. Module Two or Module Three will apply (as applicable);
 - 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 Sub-processor changes shall be as set out in section 6.3 of this DPA;
 - iv. in Clause 11, the optional language will not apply;
 - v. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of the EU Member State in which the data exporter is established and if no such law by Irish law;
 - vi. in Clause 18(b), disputes shall be resolved before the courts of the EU Member State in which the data exporter is established and otherwise Ireland;
 - vii. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule A to this DPA;
 - viii. and Subject to section 8.1 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule B to this DPA,
- b) In relation to transfers of Account Data protected by the GDPR and processed in accordance with Section 3.4 of this DPA, the EU SCCs shall apply, completed as follows:
 - i. Module One will apply;
 - ii. in Clause 7, the optional docking clause will apply;
 - iii. in Clause 11, the optional language will not apply;
 - iv. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
 - v. in Clause 18(b), disputes shall be resolved before the courts of Ireland;
 - vi. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule A to this DPA;
 - vii. and Subject to section 8.1 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule B to this DPA;
- c) In relation to transfers of Account Data protected by the GDPR and processed in accordance with Section 3.4 of this DPA, the EU SCCs shall apply, completed as follows:
 - i. references to "Regulation (EU) 2016/679" shall be interpreted as references to UK Privacy Laws or the Swiss DPA (as applicable);
 - ii. references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of UK Privacy Laws or the Swiss DPA (as applicable);
 - iii. references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "UK" or "Switzerland", or "UK law" or "Swiss law" (as applicable);

- iv. the term "member state" shall not be interpreted in such a way as to exclude data subjects in the UK or Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., the UK or Switzerland);
 - v. Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the UK Information Commissioner or Swiss Federal Data Protection Information Commissioner (as applicable);
 - vi. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Information Commissioner" and the "courts of England and Wales" or the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" (as applicable);
 - vii. in Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales or Switzerland (as applicable);
 - viii. and with respect to transfers to which UK Privacy Laws apply, Clause 18 shall be amended to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts", and with respect to transfers to which the Swiss DPA applies, Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland;
- d) To the extent that and for so long as the EU SCCs as implemented in accordance with sub-paragraph a)-c) above cannot be used to lawfully transfer Customer Personal Data and Account Data in accordance with the UK GDPR to Provider, the UK SCCs shall be incorporated into and form an integral part of this DPA and shall apply to transfers governed by the UK GDPR. For the purposes of the UK SCCs, the relevant annexes, appendices or tables shall be deemed populated with the information set out in Schedules A and B of this DPA. In relation to data that is protected by the UK GDPR, the EU SCCs will apply as follows:
- i. apply as completed in accordance with paragraph 7(a) above; and
 - ii. be deemed amended as specified by Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of this DPA.

In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Schedule A and Schedule B of this DPA and table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

11.3. SCC Conflict. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

11.4. Alternative Transfer Mechanism. To the extent that Provider adopts an alternative data export mechanism (including any new version of or successor to the DPF or Standard Contractual Clauses adopted pursuant to Applicable Data Protection Legislation) ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall upon notice to Customer and an opportunity to object, apply instead of any

applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Applicable Data Protection Legislation applicable to Europe and extends to territories to which Customer Personal Data and Account Data is transferred).

12. COOPERATION AND DATA SUBJECT RIGHTS

12.1. Data Subject Rights. Provider provides Customer with a number of self-service features via the Services, including the ability to delete, obtain a copy of, or restrict use of Customer Personal Data. Customer may use such self-service features to assist in complying with its obligations under Applicable Data Protection Law with respect to responding to Third Party Requests from data subjects via the Services at no additional cost. Upon Customer's request, Provider shall, taking into account the nature of the processing, provide reasonable assistance to Customer where possible and at Customer's cost and expense, to enable Customer to respond to requests from a data subject seeking to exercise their rights under Applicable Data Protection Legislation. In the event that such request is made directly to Provider, if Provider can, through reasonable means, identify the Customer as the controller of the Customer personal data of a data subject, Provider shall promptly inform Customer of the same. As between the Parties, Customer shall have sole discretion and responsibility in responding to the rights asserted by any individual in relation to Customer Personal Data.

12.2. Cooperation. In the event that either party receives (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Legislation or (b) any Third Party Request relating to the processing of Account Data or Customer Personal Data conducted by the other party, such party will promptly inform the other party in writing. The parties agree to cooperate, in good faith, as necessary to respond to any Third Party Request and fulfill their respective obligations under Applicable Data Protection Legislation.

13. NO SALE OR SHARING

To the extent that the processing of Customer Personal Data is subject to U.S. data protection laws, Provider is prohibited from: (a) selling Customer Personal Data or otherwise making Customer Personal Data available to any third party for monetary or other valuable consideration; (b) sharing Customer Personal Data with any third party for cross-behavioral advertising; (c) retaining, using, or disclosing Customer Personal Data for any purpose other than for the business purposes specified in this DPA or as otherwise permitted by U.S. data protection laws; (d) retaining, using or disclosing Customer Personal Data outside of the direct business relationship between the parties, and; (e) except as otherwise permitted by U.S. data protection laws, combining Customer Personal Data with personal data that Provider receives from or on behalf of another person or persons, or collects from its own interaction with the data subject. Provider will notify Customer promptly if it makes the determination that it can no longer meet its obligations under applicable U.S. data protection laws.

14. MISCELLANEOUS

14.1. If there is a conflict between the Agreement and this DPA, the terms of this DPA will prevail. The order of precedence will be: (a) this DPA; (a) the Agreement; and (c) the Privacy Policy. To the extent there is any conflict between the Standard Contractual Clauses, and any other terms in this DPA, the Agreement, or the Privacy Policy, the provisions of the Standard Contractual Clauses will prevail.

14.2. The parties agree that this DPA shall replace and supersede any prior data processing addendum that Provider and Customer may have previously entered into in connection with the Services.

14.3. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

14.4. In no event does this DPA restrict or limit the rights of any data subject or of any competent supervisory authority.

14.5. In the event (and to the extent only) of a conflict (whether actual or perceived) among Applicable Data Protection Legislation, the parties (or relevant party as the case may be) shall comply with the more onerous requirement or standard which shall, in the event of a dispute in that regard, be solely determined by Provider.

14.6. Notwithstanding anything else to the contrary in the Agreement, Provider reserves the right to make any modification to this DPA as may be required to comply with Applicable Data Protection Legislation.

14.7. Notwithstanding anything in the Agreement or any order form entered in connection therewith, the parties acknowledge and agree that Provider access to Customer Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

14.8. In no event shall this DPA benefit or create any right or cause of action on behalf of a third party (including a Third-Party Controller), but without prejudice to the rights or remedies available to Data Subjects under Data Protection Laws or this DPA (including the DPF and SCCs).

Schedule A
Description of the Processing Activities / Transfer

Schedule A(1) List of Parties:

Data Exporter	Data Importer
Name: Customer, as identified in the Order Form	Name: Provider, as identified in the Agreement
Address: As identified in the Order Form	Address: As identified in the Agreement
Contact details: As identified in the Order Form	Contact details: As identified in the Agreement
Activities relevant to the transfer: See Schedule A(2) below	Activities relevant to the transfer: See Schedule A(2) below
Role: Controller	Role: Processor

Schedule A(2) Description of Transfer

	Description
Categories of data subjects:	• Permitted users – any of Customer's employees or other personnel, suppliers and other third parties authorised under the Agreement to use the Services. • employees, contractors, business partners, customers or other individuals having Personal Data stored, transmitted to, made available to, accessed or otherwise processed by The Provider.
Categories of personal data:	• Permitted users – contact data • Customer determines the categories of Personal Data which could be processed in The Provider's Platform.
Sensitive data:	The Provider does not require any special categories of data to provide the Services and does not intentionally collect or process such data in connection with the provision of the Services.
Frequency of the transfer:	Continuous
Nature and subject matter of processing:	The Personal Data may be subject to the following processing activities: • storage (hosting) and other processing necessary to provide, maintain and improve the Services provided to Customer under the Agreement,

	• technical support provided to the Customer on a case by case basis, • disclosures in accordance with the Agreement and the DPA, as compelled by law, and • collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
Duration of the processing:	Processing Term.
Purpose(s) of the data transfer and further processing:	(i) Processing to provide, maintain, support, and improve the Services provided to the Customer in accordance with the Agreement; (ii) Processing initiated by the Permitted users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by the Customer (e.g., via email) where such instructions are consistent with the Agreement of the Agreement (including this DPA).
Retention period (or, if not possible to determine, the criteria used to determine that period):	Processing Term

Schedule A(3): Competent supervisory authority

With respect to EU Data the competent supervisory authority is The Office of the Information Commissioner of Ireland (the "**Supervisory Authority**").

Schedule B
Technical and Organizational Measures

The technical and organisational measures implemented by the Provider (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, are described at [Data Management Policy](#) and:

Type of measure	Implemented measure
Measures of pseudonymisation and encryption of personal data	Customer Data is encrypted in transit and at rest using approved industry-standard cryptography. Data masking, pseudonymisation or anonymisation is applied where appropriate.
Measures for ensuring ongoing confidentiality of processing systems and the Services	Access to Customer Data is restricted by least privilege, RBAC and business need. Privileged production access requires MFA, and production environments are segregated from development and testing.
Measures for ensuring ongoing integrity of processing systems and the Services	Production changes are documented, tested, reviewed and approved. Systems are hardened, default credentials are changed, unnecessary services are disabled and vulnerabilities are remediated under defined timelines.
Measures for ensuring ongoing availability and resilience of processing systems and the Services	Provider monitors system capacity and maintains backup, recovery, continuity and incident-response procedures designed to support service availability.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Provider performs annual risk assessments and penetration testing, quarterly vulnerability scanning of public-facing production systems, periodic audits and annual incident-response testing.
Measures for user identification and authorization	Users have unique accounts. Access requires documented approval, follows least privilege and RBAC, and is promptly revoked when no longer required. Privileged access requires MFA.
Measures for the protection of Data during storage	Confidential Data and backups are encrypted at rest. Access is restricted, and storage media is securely erased or destroyed before reuse or disposal.

Measures for ensuring physical security of locations at which personal data are processed	Customer Data is processed using approved facilities and cloud providers subject to contractual, security and vendor-management controls. Devices containing Confidential Data are encrypted and securely disposed of.
Measures for ensuring events logging	Production systems log authentication, administrative activity, security changes and access to Customer Data. Logs are protected from tampering, monitored and retained according to policy.
Measures for ensuring system configuration, including default configuration	Systems are configured using documented hardening standards. Default accounts and passwords are removed or changed, unnecessary functionality is disabled and production network access is restricted.
Measures for internal IT and IT security governance and management	Provider maintains documented security, privacy, risk, access-control, cryptography, development, operations and incident-response policies, with assigned owners and approved exception processes.
Measures for certification/assurance of processes and products	Provider evaluates controls through audits, risk assessments, vulnerability scans, penetration tests and documented remediation activities.
Measures for ensuring data minimization	Data collection, access and disclosure are limited to what is necessary for legitimate business purposes. Production Customer Data is not used in test environments without authorization and appropriate protection.
Measures for ensuring data quality	Development, testing, change-management and release procedures are used to reduce errors and protect data integrity.
Measures for ensuring limited data retention	Personal Data is retained only for documented business, contractual, regulatory or legal purposes and is deleted or de-identified when no longer required.

Measures for ensuring accountability	Access changes, privileged activity, production changes, vulnerabilities, incidents, exceptions and data restorations are recorded in auditable systems.
Measures for allowing data portability and ensuring erasure	Provider maintains processes to return, export or delete Customer Personal Data in accordance with the Agreement, documented instructions and applicable law.

Schedule C
Approved Sub-processors

Amazon Web Services, Inc. (or any of its affiliates in the respective locations)	Cloud computing provider
Google Cloud (or any of its affiliates in the respective locations)	Cloud computing provider
Google Workspace	Identity provider
Auth0	Identity provider
GitHub	Version control

Schedule D
UK Addendum to the EU Commission Standard Contractual Clauses

1. Date of this Addendum: This Addendum is effective from the same date as the DPA.
2. Background: The Information Commissioner considers this Addendum to provide appropriate safeguards for the purposes of transfers of personal data to a third country or an international organization in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors.
3. Interpretation of this Schedule 4. Where this Addendum uses terms that are defined in the Annex those terms shall have the same meaning as in the Annex. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Clauses.
The Annex	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
UK	The United Kingdom of Great Britain and Northern Ireland.

1. This Addendum shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that it fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR.
2. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.
3. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.
4. Hierarchy: In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.
5. Incorporation of the Clauses: This Addendum incorporates the Clauses which are deemed to be amended to the extent necessary so they operate:
 - a. for transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that transfer; and
 - b. to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.
6. The amendments required by Section 7 above, include (without limitation):

- a. References to the "Clauses" means this Addendum as it incorporates the Clauses.
 - b. Clause 6 Description of the transfer(s) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer".
 - c. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.
 - d. References to Regulation (EU) 2018/1725 are removed.
 - e. References to the "Union", "EU" and "EU Member State" are all replaced with the "UK".
 - f. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner.
 - g. Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".
 - h. Clause 18 is replaced to state: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."
 - i. The footnotes to the Clauses do not form part of the Addendum.
7. Amendments to this Addendum
- a. The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of Scotland or Northern Ireland.
 - b. The Parties may amend this Addendum provided it maintains the appropriate safeguards required by Art 46 UK GDPR for the relevant transfer by incorporating the Clauses and making changes to them in accordance with Section 7 above.
8. Executing this Addendum
- a. The Parties may enter into the Addendum (incorporating the Clauses) in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in the Clauses. This includes (but is not limited to):
 - i. By attaching this Addendum as Schedule 4 to the Provider DPA.
 - ii. By adding this Addendum to the Clauses and including in the following above the signatures in Annex 1A:

"By signing we agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses dated:" and add the date (where all transfers are under the Addendum)

"By signing we also agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses dated" and add the date (where there are transfers both under the Clauses and under the Addendum) (or words to the same effect) and executing the Clauses;
or

- iii. By amending the Clauses in accordance with this Addendum and executing those amended Clauses.