HIGHLIGHT AI

DATA PROCESSING ADDENDUM

Download a PDF

Effective Date: 2/20/26

This Data Processing Addendum ("**DPA**") supplements and is incorporated into and forms part of the Highlight US Inc.'s Terms of Service, available at https://highlightai.com/terms ("**Terms of Service**"), and any other agreement between you ("**Customer**," "**your**," or "**you**") and Highlight US Inc. ("**Company**", "**we**", "**our**", "**us**") that references this DPA. The Terms of Service and any such separate agreement referencing this DPA are collectively referred to as the "**Agreement**."

This DPA applies to Company's processing of Customer Data (defined below) under the Agreement and Company Privacy Policy, available at https://highlightai.com/privacy-policy ("**Privacy Policy**").

You hereby represent you are lawfully able to enter into this DPA and, if you are entering into the DPA for an entity, that it has legal authority to bind that entity. By creating an account, subscribing to our Services or otherwise using the Services, you agree to this DPA.

1. DEFINITIONS

"**Applicable Data Protection Laws**" means all local, state, national and/or foreign data protection and privacy laws, treaties and/or regulations applicable to the collection, use, transfer, storage, correction, disclosure, deletion, and other processing of Customer Data under this DPA, including, where applicable, any U.S. Data Protection Law(s) and any European Data Protection Laws.

"**Control**" (for purposes of Customer Affiliate definition) means direct or indirect ownership or control of more than 50% of voting interests.

"**Controller**" and "**processor**" include "**business**" and "**service provider**", respectively, as required by Applicable Data Protection Laws.

"**Customer Affiliate**" means an affiliate of Customer that (a) is permitted to use the Services pursuant to the Agreement between Company and Customer, and (b) directly or indirectly controls, is controlled by, or is under common control with the subject entity.

"**Customer Data**" means Personal Data submitted through the Services by or on behalf of Customer or a Customer Affiliate, or otherwise provided by or at the direction of Customer to Company or its Sub-Processors under the DPA, as more particularly identified in Appendix A **(Processing Particulars)**.

"**Data Subject**" means a natural person who has been or is identified or identifiable, directly or indirectly, by reference to (i) one or more identifiers such as a name, an identification number, location data, an online identifier and/or (ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person or as otherwise defined under Applicable Data Protection Laws.

"**European Data Protection Laws**" means all EU and U.K. regulations or other legislation regarding data protection applicable (in whole or in part) to the processing of Customer Data by Company under the Agreement, such as Regulation (EU) 2016/679 (the "**GDPR**"), the national laws of each European Economic Area (EEA) member state and the U.K. implementing any EU directive applicable (in whole or in part) to the Processing of Data (such as Directive 2002/58/EC); and any other national laws of each EEA member state and the U.K. applicable (in whole or in part) to the processing of Customer Data; in each case as amended or superseded from time to time.

"**Personal Data**" means any information relating to a Data Subject, the processing of which is governed by Applicable Data Protection Laws. Where the CPRA applies, the term "**Personal Data**" includes "**personal information**" as defined by the CPRA. Personal Data does not include anonymous or de-identified information or aggregated information derived from Personal Data, which does not otherwise qualify as Personal Data.

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

"**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses for the transfer of personal data to third countries approved by the European Commission pursuant to Article 46(2)(c) of the GDPR; those terms set forth in the European Commission's Implementing Decision of June 4, 2021 on standard contractual clauses, selecting Module Two between controllers and processors (where Customer is a data controller) or Module Three between processors (where Customer is a data processor) and excluding optional clauses (except as selected herein), under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council dated June 4, 2021, and any replacement, amendment or restatement of the foregoing issued by the European Commission, incorporated herein by reference.

"**Sub-Processor**" means a third party engaged by or on behalf of a data processor or any further sub-contractor to process Personal Data on behalf of and under the instructions of the data controller.

"**Sub-Processor List**" means the list available at the following address https://highlightai.com/privacy/subprocessors.

"**Sub-Processors**" means the sub-processors engaged by Company to process Customer Data in connection with the Services.

"**Supervisory Authority**" means an independent public authority established by an EU Member State pursuant to Article 51 of the GDPR.

"**U.S. Data Protection Law**" means all federal and state laws, rules, regulations or other legislation regarding data protection applicable (in whole or in part) to the processing of Customer Data by Company under the Agreement, which may include (without limitation) the California Consumer Privacy Act of 2018, as codified at California Civil Code Sections 1798.100 through 1798.199.100, and its associated regulations ("**CCPA**"), as amended by the California Privacy Rights Act of 2020, effective January 1, 2023 ("**CPRA**") in each case as amended or superseded from time to time.

Capitalized terms, which are not defined in the DPA have the meanings provided in the Terms of Service.

2. PROCESSING OF CUSTOMER DATA

2.1. **Purpose of DPA:** Each party acknowledges and agrees that all Customer Data is disclosed by Customer hereunder only for those limited and specified purposes set forth in the Agreement, Privacy Policy, and this DPA.

2.2. **Scope of DPA.** The subject matter, nature, purpose, and duration of this processing, as well as the types of Customer Data collected and categories of Data Subjects, are described in Appendix A. As between the parties, Customer is the data controller and Company is the data processor of Customer Data.

2.3. **Instructions for Processing.** Unless required by applicable law to which Company is subject, Company will only process Customer Data to provide or maintain the Services, and in compliance with Customer's documented instructions, including as provided under the Agreement and this DPA. Customer shall only give instructions that comply with Applicable Data Protection Laws. Customer hereby instructs Company to process Customer Data as necessary to provide and maintain the Service in accordance with the Agreement and this DPA. Company shall inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Laws.

2.4. **Processing of Customer Data under U.S. Data Protection Law.** Company will not (i) "sell" Customer Data, as defined by Applicable Data Protection Laws; (ii) retain, use, or disclose Customer Data outside of the direct business relationship and for any purpose other than specified under the Agreement and this DPA, or as otherwise permitted by Applicable Data Protection Laws; and, except as otherwise permitted by Applicable Data Protection Laws; or (iii) combine Customer Data with Personal Data that Company receives from or on behalf of another person or persons. The terms "sale," and "sell" are defined in Section 1798.140 of the CPRA. Company will notify Customer if Company determines it can no longer meet its obligations under Applicable Data Protection Laws.

2.5. **Rightful Processing of Customer Data**. Customer represents and warrants that: (i) Customer has and will continue to have the right to allow processing of Customer Data by Company, its affiliates and Sub-Processors in accordance with the Agreement and this DPA; (ii) all Customer Data provided to Company for processing has been and shall be collected and provided in accordance with Applicable Data Protection Laws, and Customer shall ensure that all notifications and approvals required by Applicable Data Protection Law for such processing are obtained and/or maintained; and (iii) Customer will not transfer any sensitive/special categories of Personal Data (as defined under Applicable Data Protection Laws) to Company.

2.6. **Anonymization of Customer Data.** Company may anonymize or deidentify Customer Data in accordance with Applicable Data Protection Laws ("**Deidentified Data**"), provided Company (i) implements technical safeguards that prohibit re-identification of the Data Subject to whom the information may pertain; (ii) implements business processes that specifically prohibit reidentification of the Deidentified Data and prevent the inadvertent release of Deidentified Data; and (iii) makes no attempt to reidentify the Deidentified Data.

3. DISCLOSURES TO AUTHORITIES

3.1. **Disclosure**. Company shall not knowingly disclose Customer Data to an authority in a massive, disproportionate, and indiscriminate manner that goes beyond what is necessary in a democratic society, and shall not knowingly disclose Customer Data to an authority without a subpoena, warrant, writ, decree, summons or other legally binding order that compels disclosure of Customer Data.

3.2. **Company's Notice Obligations**. If Company receives notice from any law enforcement, regulatory, judicial or governmental authority (each an "**Authority**") that such Authority wishes to obtain access to any or all of Customer Data, then Company shall (unless legally prohibited): (a) promptly notify Customer of such Authority's data access request; and (b) inform the Authority that requests for access to Customer Data should be notified to or served upon Customer in writing.

3.3. **Conditions upon Company's Disclosure Obligations**. If Company makes a disclosure of Customer Data to an Authority (whether with Customer's authorization or due to a mandatory legal compulsion), Company shall only disclose such Customer Data to the extent Company is legally required to do so.

3.4. **Exceptions**. Sections 3.2 and 3.3 shall not apply to the extent that Company has a reasonable and good-faith belief that providing access to Customer Data to the requesting Authority is necessary to prevent imminent risk of serious harm to any individual. In such event, Company shall notify Customer as soon as possible following such Authority's access and provide Customer with full details of the same, unless and to the extent Company is legally prohibited from doing so.

4. AUTHORIZED SUB-PROCESSORS

4.1. Customer hereby grants Company general authorization to engage the Sub-Processors identified in the Sub-Processor List available at https://highlightai.com/privacy/subprocessors, as well as any additional Sub-Processors. Company shall provide Customer with reasonable prior notice of any new Sub-Processor, and Customer may object to such engagement by providing written notice to Company within fifteen (15) calendar days of receipt of such notice. Any objection must be based on reasonable data privacy or data security concerns. If Customer does not provide a timely objection, Customer shall be deemed to have consented to the engagement of the new Sub-Processor. In the event of an objection, the parties shall cooperate in good faith to resolve the objection in a mutually acceptable manner.

4.2. Company will: (a) enter into a contractual agreement with each Sub-Processor imposing data protection obligations that are substantially as protective as Company's obligations under this DPA to the extent applicable to the nature of the services provided by Sub-Processor; and (b) remain liable to Customer for each Sub-Processors' acts and omissions related to this DPA to the extent Company is liable for its own and consistent with the Agreement, including its limitation of liability provisions.

5. INTERNATIONAL TRANSFERS OF CUSTOMER DATA

5.1. **Applicable Standard Contractual Clauses**. For Customer Data subject to European Data Protection Laws, the terms of the Standard Contractual Clauses SCCs Module Two (controller to processor) or, if applicable, Module Three (processor to processor), as described in Appendix D of this DPA, are hereby incorporated by reference and will be deemed

to have been executed by the parties. To the extent required by Applicable Data Protection Laws, the jurisdiction-specific addenda to the SCCs set out in Appendix D are also incorporated herein by reference and will be deemed to have been executed by the parties. Company is the "data importer" and Customer is the "data exporter" (notwithstanding that Customer may itself be located outside the EEA/UK and/or a processor acting on behalf of a third-party data controller).

5.2. **Conflict with Standard Contractual Clauses**. It is not the intention of either party, nor the effect of this DPA, to contradict or restrict any provision of the Standard Contractual Clauses. To the extent that any provision of the Standard Contractual Clauses conflicts with this DPA, the Standard Contractual Clauses shall prevail to the extent of such conflict with respect to Customer Data which is subject to the Standard Contractual Clauses. In no event does this DPA restrict or limit the rights of any Data Subject or of any competent Supervisory Authority.

5.3. **Data Impact Transfer Assessment**. To the extent that Customer requires Company's assistance to meet its obligations under Articles 35 and 34 of the GDPR to carry out a data protection impact assessment and/or consultation with the competent Supervisory Authority (as defined in Appendix C) related to Customer's use of the Service, and taking into account the nature of the processing and the information available to Company, Company shall provide Customer with reasonable and timely assistance with any data protection impact assessments as required by Applicable Data Protection Laws.

6. RIGHTS OF DATA SUBJECTS

6.1. **Responses to Data Subjects**. Customer is responsible for responding to requests from Data Subjects to exercise their rights with respect to Customer Data (collectively "Data Subject Request(s)"), which may include, as applicable, the rights of access, rectification, erasure, data portability, restriction or cessation of processing, withdrawal of consent to processing, and/or objection to being subject to processing that constitutes automated decision-making.

6.2. **Company's Obligations Regarding Data Subject Requests**. If Company receives a Data Subject Request in relation to Customer Data, Company will promptly inform Customer by providing full details of the same and shall not respond to the communication unless specifically required by law or authorized by Customer. Company will provide reasonable and timely assistance to enable Customer to respond to Data Subject Requests.

7. INFORMATION RIGHTS

7.1. **Information Rights.** To the extent required by Applicable Data Protection Laws and upon Customer's written request, the Company shall provide copies of certifications or reports demonstrating the Company's compliance with data security standards applicable to the processing of Customer Data, along with such other information as the Customer may reasonably request from the Company for the purpose of demonstrating each party's compliance with Applicable Data Protection Laws and this DPA.

7.2. **Audit Report.** In addition to the information rights set forth in Section 7.1, to the extent required by Applicable Data Protection Laws, Company shall provide, upon Customer's written request, a copy of the audit report from Company's most recent certification audit, as conducted by an independent third party ("**Audit Report**"). If documentation or information beyond the Audit Report and the information provided by Company under Section 7.1 are

necessary to fulfill Customer's obligations under Applicable Data Protection Laws (such as Article 28(3)(h) of the GDPR where applicable), then Company shall permit Customer to audit Company's compliance with this DPA, subject to the terms below:

7.2.1. Customer shall not be entitled to more than one audit of Company per calendar year, except (i) following the occurrence of a Security Incident, or (ii) upon instructions from a Supervisory Authority.

7.2.2. such audit is (i) conducted by Customer or a third-party auditor designated by Customer that has executed an appropriate confidentiality agreement with Company, and (ii) Customer and Company mutually agree on reasonable details of the audit, including the start date, scope and duration of, and security and confidentiality controls applicable to such audit.

7.2.3. Customer will pay any reasonably incurred costs and expenses incurred by Company in the event Customer performs an audit that is not (a) required by Applicable Data Protection Laws or (b) in response to a Security Incident.

7.2.4. Customer may use the results of an audit only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of the DPA.

8. SECURITY OF CUSTOMER DATA; SECURITY INCIDENTS

8.1. **Company's Security Measures**. Company shall implement appropriate technical and organizational measures to protect Customer Data from (i) accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to Customer Data. At a minimum, such measures shall include the security measures identified in Appendix B. With respect to the evaluation of the appropriate level of security for the processing of Customer Data, Company:

8.1.1. It has taken due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for Customer Data; and

8.1.2. It has evaluated the use of encryption and/or pseudonymization for Customer Data and has determined that the level provided by Company is appropriate for Customer Data.

8.2. **Obligations in Security Incident**. Upon becoming aware of a Security Incident, Company shall:

8.2.1. notify Customer of the Security Incident without undue delay, but no later than required under the Applicable Data Protection Laws;

8.2.2. provide such cooperation and reasonably available information as to enable Customer to fulfill its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Laws; and

8.2.3. take such steps as are necessary and reasonable to remediate such Security Incident, and to the extent required by Applicable Data Protection Laws, to

cooperate with Customer to minimize the harmful effects on the Data Subjects whose Personal Data was disclosed.

9. DELETION OR RETURN OF CUSTOMER DATA

9.1. **Retrieval Period.** Upon termination of this DPA, Company shall make all Customer Data available for download by Customer through the Services or other mutually agreed means for a period of thirty (30) calendar days following the effective date of termination (the "Retrieval Period"). Customer is solely responsible for downloading and retaining copies of any Customer Data it wishes to preserve during the Retrieval Period. Company shall provide reasonable assistance to Customer in downloading Customer Data upon request.

9.2. **Deletion after Retrieval Period.** Upon the earlier of (i) expiration of the Retrieval Period, or (ii) Customer's written confirmation that it has retrieved all Customer Data, Company shall securely delete or destroy all Customer Data in its possession or control, including all copies residing in Company's systems and any Sub-Processor systems.

9.3. **Legal Retention**. Notwithstanding the foregoing, if Company is required or authorized by applicable laws to retain any Customer Data, Company shall only retain such Customer Data for as long as required under applicable laws, and shall continue to comply with Applicable Data Protection Laws during such retention period. Company shall notify Customer of any such legal retention requirement.

9.4. **No Liability.** Company shall have no obligation to retain, store, or provide access to any Customer Data following expiration of the Retrieval Period. Company shall not be liable for any loss, damage, or costs arising from Customer's failure to download Customer Data during the Retrieval Period.

10. MISCELLANEOUS

10.1. **Termination.** The term of this DPA will terminate automatically without requiring any further action by either party upon the later of (i) the termination of the Agreement, or (ii) when all Customer Data is removed from Company's systems and records, and/or is otherwise rendered unavailable to Company for further processing.

10.2. **Conflict; Invalidation.** This DPA is subject to the terms of the Agreement; provided that, in the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA shall prevail with regard to the parties' data protection and privacy obligations. If any provision of this DPA is deemed invalid or unenforceable, the invalid or unenforceable provision shall be either (i) amended to ensure its validity and enforceability while preserving the parties' intentions as closely as possible; or (ii) if that is not possible, then construed in a manner as if the invalid or unenforceable part had never been included herein. Any remaining provisions of this DPA which have not been deemed invalid or unenforceable shall remain valid and in force.

10.3. **Changes to this DPA.** Company may revise this DPA from time to time, including when required to comply with changes in Applicable Data Protection Laws or regulatory guidance. Company will provide Customer with written notice of any material changes to this DPA. For material changes, Company will endeavor to provide advance notice of at least thirty (30) calendar days prior to the effective date of such changes, except where a shorter notice period is required by Applicable Data Protection Laws or regulatory authorities. What constitutes a "material change" will be determined by Company in good faith using

reasonable judgment and in accordance with Applicable Data Protection Laws. The updated DPA will be posted at https://highlightai.com/privacy/dpa and the effective date of the changes will be clearly indicated.

APPENDIX A – PROCESSING PARTICULARS

A. LIST OF PARTIES

Data exporter(s): The data exporter is the Customer and/or Customer Affiliates exporting Customer Data.

Data importer(s):

Highlight US Inc

200 Spectrum Center Drive
Suite 300
Irvine, CA 92618
United States

B. DESCRIPTION OF TRANSFER

Categories of Customer Data: Customer may submit Personal Data to the Services, the categories of which will depend upon Customer's use of the Services which is determined and controlled by Customer in its sole discretion, but it may include, but is not limited to names, contact information, demographic information, or any other information provided by Customer's end users as specified in the Privacy Policy available at https://highlightai.com/privacy-policy.

Categories of Data Subjects: The Data Subjects may include, but are not limited to Customer's employees, customers, suppliers and end users.

Special categories of Personal Data/ sensitive Personal Data (if applicable): No sensitive Personal Data is intended to be transferred unless the end-user of the Services shares it with Company. Due to the nature of our Services, Company may inadvertently collect sensitive Personal Data through screenshots or audio data. The Privacy Policy instructs end users to temporarily disable our Services when accessing sensitive information on an end user's device or discussing sensitive information near their device.

Duration and Frequency of Processing: Processing occurs continuously throughout the term of the Agreement, with the frequency determined by Customer.

Retention: The duration is the term of the Agreement, and the 30-day Retrieval Period after the termination. Personal Data is retained by Company for no longer than necessary to provide the services set out in the Agreement and this DPA, subject to exemptions as set forth in the DPA.

Subject Matter and Nature of the Processing: Performing the Services on behalf of Customer which involves processing of Personal Data as part of an artificial intelligence assistant tool, as further described in the Agreement; verifying or maintaining the quality, security, and integrity of the Services; debugging to identify and repair errors that impair existing intended functionality.

Company transfers the Personal Data described above to the Sub-Processors identified in Sub-Processor List solely for the purpose of enabling Company to perform its obligations under the Agreement. Company ensures that each Sub-Processor processes such Personal Data only on documented instructions from Company and retains the Personal Data for no longer than is necessary to provide the relevant sub-processing services, unless a longer retention period is required by applicable law.

APPENDIX B – SPECIFIC SECURITY MEASURES

TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF CUSTOMER DATA

Description of the technical and organizational measures implemented by the Data Importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. **Measures of pseudonymization and encryption of personal data; measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services**

Company has implemented a number of input control measures to maintain confidentiality and integrity, including an authorization policy for the input, reading, alteration and deletion of Customer Data, requiring authentication of any authorized personnel, installation of measures to prevent end users from reading, altering, or deleting stored data without authorization, utilization of unique authentication credentials or codes, automatic log-off of user IDs that have not been used for a substantial period of time, and electronic recording of entries.

Customer Data collected for different purposes is processed separately via mechanisms such as separating levels of application security for the appropriate users, installing modules within Company's database to separate data used for differing purposes, storing data in different normalized tables, separated per module or function they support; and using interfaces, batch processes and reports designed for only specific purposes and functions.

Company's security program adheres to the principles of "deny all", "need to know" and "least privilege" classification of user information as confidential or non-confidential, internal computer systems with isolation of confidential information to limited, classified systems, prevention of external access to classified systems, and providing access on a "need to know basis". In the event of disciplinary action, separation, leave, or termination of an employee or contractor, logon IDs and passwords will be deactivated so that access to information systems and Customer Data is taken away as soon as reasonably possible.

2. **Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing**

Company has implemented and maintains a formal information security program, consisting of internal security administration and operations policies in accordance with relevant industry standards as appropriate to confidentiality of information.

Company provides data privacy training to all members of its workforce upon hiring. Annually, Company provides all employees with copies of its current information security program internal policies and procedures which may include: Access Control and Termination Policy, Encryption and Key Management Policy, Vulnerability and Patch Management Policy, Information Security Policy, Data Retention and Disposal Policy, Network Security Policy, Privacy and Data Protection Policy, Security Incident Response Plan, Data Classification Policy, Physical Security

Policy, Processing Integrity Policy, Risk Assessment and Treatment Policy, Secure Development Policy, and Vendor Management Policy.

Company requires each employee to sign an acknowledgement of receipt and understanding of those terms. As necessary, senior management from the information security team provides relevant security awareness information to Company employees.

Company implements measures such as infrastructure redundancy and alternative backup storage systems in case of failure of the primary system. Additionally, Company implements measures to monitor and restrict access to Company's system administrators, including:

- Registering system administrators' access logs to the infrastructure and keeping them secure, accurate and unmodified;
- Annual audits of system administrators' activity to assess compliance with assigned tasks and instructions;
- Keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned.

Authorized personnel are only able to access Customer Data within the scope and to the extent covered by their respective access permission (authorization) and that Customer Data cannot be read, copied, modified or removed without authorization. Employees are trained with respect of each employee's access rights to Customer Data; further, Company allocates individual terminals, and can identify characteristics exclusive to specific functions.

Upon Customer's written request and subject to execution of Company's standard confidentiality agreement, Company will provide Customer with a copy of Company's most recent SOC 2 Type 2 report within thirty (30) calendar days of such request.

Company will notify Customer within thirty (30) calendar days of any material adverse changes to Company's security certifications or the results of security audits that could reasonably affect the security of Customer Data.

3. Measures for the protection of data during transmission; Measures for the protection of data during storage

Company implements measures to prevent Customer Data from being read, copied, altered or deleted by unauthorized parties during transmission or at rest via use of industry standard firewall and VPNs. All data is encrypted in transmission and at rest, and systems generate a user alert upon incomplete transfer of data (end to end check). All data transmissions are logged, monitored, and tracked. Company systems are set to implement automatic temporary lock-out of user terminal if left idle, with identification and password required to reopen.

When Company controls the transmission of information electronically, encryption is used for Customer Data at rest, in transit and in use and include the following measures:

- Customer Data is never stored in unencrypted form, even temporarily;
- Encryption of Customer Data during any electronic transmission across electronic communication networks;
- Company requires that the encryption of data-at-rest should only include strong encryption methods (AES-256 or a minimally equivalent protocol).

- Company uses security key management and other measures to ensure encrypted Data is not lost or irretrievable should the encryption keys become unavailable. Keys are stored in a separate location from the Customer Data.
- Company uses industry standard encryption technology and protocols to transfer Customer Data, performing server verification to verify the identity of a server before establishing a connection with such server, and implementing certificate pinning in any software applications that process any Customer Data.
- Company maintains a firewall at all logical demilitarized zones and Internet connection points, with access control restricted to those levels required for authorized use of Company systems and applications.
- Company regularly monitors the servers, internal network and laptop security to ensure that security measures are operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Customer Data.
- External reviews of Company's security program and audits of adherence to security compliance standards, no less than annually.

Company's systems use industry-standard and up-to-date antivirus, antimalware, firewall, and intrusion detection system software with baseline security configuration on all company laptops and workstations. Additionally, Company's internal software uses built-in, up-to-date firewall protection for network traffic which includes a baseline security configuration.

4. Measures for ensuring security of locations at which Customer Data is processed

Unauthorized persons are restricted from access to the data processing equipment (namely telephones, database and application servers and related hardware) through established security areas and physical controls, protection and restriction of access paths, and requiring access authorizations for employees and third parties. All access to the data center where Customer Data is hosted is logged, monitored, and tracked, and the data center where Customer Data is hosted is secured by a security alarm system, and other appropriate security measures.

APPENDIX C – COMPETENT SUPERVISORY AUTHORITY

Identification of Competent Supervisory Authority: In accordance with Clause 13 of the Standard Contractual Clauses, the competent supervisory authority shall be identified as follows:

1. Data Exporter Established in an EU Member State

Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer is the competent supervisory authority.

2. Data Exporter Not Established in the EU with an Appointed Representative

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established is the competent supervisory authority.

3. Data Exporter Not Established in the EU Without an Appointed Representative

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of the GDPR: The Irish Data Protection Commission is the competent supervisory authority.

APPENDIX D - INTERNATIONAL DATA TRANSFERS

European Union International Data Transfer Addendum

Elections for the purposes of Module Two and Module Three of the Standard Contractual Clauses:

Clause 7 (Docking clause) – does not apply.

Audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with the audit provisions detailed in Section 7.2 of this DPA.

Clause 9 (Use of Sub-Processors) – Option 2 (General written authorization) will apply, and the time period is as specified in Section 4.1 of the DPA.

Clause 11 (Redress) – optional wording does not apply.

Clause 17 (Governing Law) – Option 1 will apply and the governing law will be the law of the Republic of Ireland.

Clause 18 (Choice of forum and jurisdiction) – the applicable choice of forum and jurisdiction will be the Republic of Ireland.

For the purpose of Annex I of the Standard Contractual Clauses, Part A of Appendix A contains the specifications regarding the parties, Part B of Appendix A contains the description of transfer for Module Two and Module Three, and Appendix C contains information on the competent Supervisory Authority.

For the purpose of Annex II of the Standard Contractual Clauses, Appendix B of this DPA contains technical and organizational measures including technical and organizational measures to ensure the security of the data.

For the purpose of Annex III of the Standard Contractual Clauses, the list of Sub-Processors are set out in Appendix E or as otherwise determined by Section 4 (Authorized Sub-Processors) of this DPA. The Sub-Processor's contact person, and contact details will be provided by Company upon request.

UK International Data Transfer Addendum

1. Definitions. For the purposes of this UK Addendum:

(a) "Approved Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, Version B1.0, issued by the Information Commissioner under Section 119A(1) of the Data Protection Act 2018, and laid before Parliament on 2 February 2022, as it may be revised under Section 18 of those Addendum EU SCCs (as defined in the Approved Addendum).

(b) "Approved EU SCCs" means the Standard Contractual Clauses set out in Appendix D of this DPA.

(c) "UK GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (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, and as amended by the Data Protection,

Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

(d) "Mandatory Clauses" means Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with Section 119A of the Data Protection Act 2018.

2. Incorporation of UK Addendum

With respect to any transfers of Customer Data that fall within the scope of the UK GDPR from Customer (as Data Exporter) to Company (as Data Importer), the parties agree as follows:

(a) To the extent required by the UK GDPR and applicable UK data protection laws, the Approved Addendum as further specified in this Appendix is hereby incorporated into and forms an integral part of this DPA.

(b) The Approved Addendum shall be deemed completed as follows:

3. Completion of Tables in Part 1 of the Approved Addendum

Table 1: Parties: The parties' details for the purposes of Table 1 of the Approved Addendum are as set forth in Appendix A (Processing Particulars), Part A (List of Parties) of this DPA.

Table 2: Selected SCCs, Modules and Selected Clauses: For the purposes of Table 2 of the Approved Addendum:

Addendum EU SCCs: The version of the Approved EU SCCs, as set out above in this Appendix D.

Selected Modules: Module Two (Controller to Processor) where Customer is a Controller, and/or Module Three (Processor to Processor) where Customer is a Processor, as applicable to the specific transfer.

Table 3: Appendix Information

The Appendix Information for the purposes of Table 3 of the Approved Addendum is set out in:

Annex I. A (List of Parties): Appendix A, Part A of this DPA

Annex I. B (Description of Transfer): Appendix A, Part A of this DPA

Annex II (Technical and Organizational Measures): Appendix B of this DPA

Annex III (List of Sub-Processors): Appendix E of this DPA

Table 4: Ending this Addendum when the Approved Addendum Changes: for the purposes of Table 4 of Part 1 of the Approved Addendum, Company (as Data Importer) may end the Approved Addendum.

Alternative approach: Not applicable.

4. Competent Supervisory Authority

For the purposes of Clause 13 of the Approved EU SCCs and the UK Addendum, the competent supervisory authority for data transfers subject to the UK GDPR shall be the Information Commissioner's Office (ICO) of the United Kingdom.

ICO Contact Information:

Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow, Cheshire SK9 5AF
United Kingdom
Website: https://ico.org.uk
Telephone: +44 (0) 303 123 1113
Email: casework@ico.org.uk

Swiss International Data Transfer Addendum

1. Scope. This Swiss Addendum applies to processing of Customer Data subject to Swiss Data Protection Laws alone or in conjunction with the GDPR.
2. Definitions:

- "Swiss Data Protection Laws" means the Swiss Federal Act on Data Protection (FADP) of 19 June 1992, the Swiss Ordinance of 14 June 1993, the revised FADP of 25 September 2020, and any successor legislation.
- "FDPIC" means the Swiss Federal Data Protection and Information Commissioner.

3. Interpretation. This Swiss Addendum shall be interpreted to provide appropriate safeguards under Article 46 GDPR and/or Article 6(2)(a) FADP. Terms defined in the Standard Contractual Clauses have the same meaning unless otherwise specified. In case of conflict, provisions providing the most protection to Data Subjects prevail.
4. Amendments to Standard Contractual Clauses

(a) For Transfers Subject Exclusively to Swiss Data Protection Laws:

The Standard Contractual Clauses are amended as follows:

(i) References to "GDPR" or "Regulation (EU) 2016/679" are replaced with "Swiss Data Protection Laws"

(ii) References to "EU", "Union", and "EU Member State" are replaced with "Switzerland"

(iii) References to Regulation (EU) 2018/1725 are removed

(iv) Clause 6: Details of transfers are specified in Appendix A where Swiss Data Protection Laws apply

(v) Clause 13(a): The competent supervisory authority is the FDPIC

(vi) Clause 17: Governing law is the laws of Switzerland

(vii) Clause 18: Disputes shall be resolved by Swiss courts; Data Subjects may bring proceedings in their place of habitual residence in Switzerland

(b) For Transfers Subject to Both Swiss Data Protection Laws and GDPR: The Standard Contractual Clauses apply (i) as written for GDPR compliance, and (ii) as amended per Section 3(a) above for Swiss compliance, except Clause 17 remains unamended.

5. Customer Warranty: Customer warrants it has made all required notifications to the FDPIC under Swiss Data Protection Laws.

6. Contact Information

FDPIC:

Feldeggweg 1, CH-3003 Bern, Switzerland
Website: https://www.edoeb.admin.ch
Email: info@edoeb.admin.ch

APPENDIX E– SUB-PROCESSORS

Company's list of Sub-Processors is available at https://highlightai.com/privacy/subprocessors.