GENERAL DATA PROCESSING ADDENDUM

This General Data Processing Addendum ("**GDPA**") attached to the Master Subscription Agreement forms part of the Master Subscription Agreement to which it is attached (the "Agreement") by and between Customer and Company to reflect the parties' agreement with regard to the Processing of Personal Data, in consideration of the mutual covenants and representations set forth in this GDPA, the parties hereby agree as follows.

Unless defined in this GDPA, all capitalized terms used herein shall have the meaning given to them in the Agreement. In the event of any conflict between the Agreement and this GDPA, the terms of this GDPA shall prevail in relation to the Processing of Personal Data set out in this GDPA.

Customer enters into this GDPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Company processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this GDPA only, and except where indicated otherwise, the term "Customer" shall include Customer and its Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

DATA PROCESSING TERMS

1. DEFINITIONS

In this GDPA, the following definitions apply:

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Authorized Affiliate(s)**" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws and Regulations and (b) is permitted to use the Subscription Services pursuant to the Agreement, but has not signed its own order form with Company and is not a "Customer" as defined under the Agreement.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Customer Data" means electronic data and information submitted by Customer in connection with the use of the Subscription Services.

"Data Protection Laws and Regulations" means all laws and regulations, including Graham Leach Bliley Act Title V – Privacy, Subtitle A, section 502, subsection c) and 201 CMR 17 Massachusetts Privacy regulation, laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, including without limitation 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" or "GDPR") and EU Directive 2002/58/EC on Privacy and Electronic Communications ("e-Privacy Directive") or, the superseding Regulation on Privacy and Electronic Communications ("e-Privacy Regulation"), once effective.

"Data Subject" means the identified or identifiable natural person, as defined under Data Protection Laws and Regulations, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Personal Data" means any information relating to a Data Subject that is Processed by Company on behalf of Customer pursuant to the terms of the Agreement.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Company.

"Process," "Processes," "Processed" or "Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller.

“Sub-processor” means any Processor engaged by Company, or a group of its companies, in the provision of the Subscription Services to Customer.
“**Supervisory Authority**” means an independent public authority, which is established by an EU Member State pursuant to the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties.** The parties acknowledge and agree that, with regard to the Processing of Personal Data, Customer is the Controller and appoints Company as the Processor and that Company or its Affiliates may engage Sub-processors pursuant to the requirements set forth in Section 6 (“Sub-processors”) below.. Company does not have independent control over the Personal Data. Company processes the Personal Data solely on the instructions of the Customer within the context of providing the Subscription Services, in line with the purposes and means provided by the Controller and the retention terms stated in main Agreement, and in compliance with the applicable Data Protection Laws and Regulations..

2.2 **Customer’s Processing of Personal Data.** Customer shall, in its use of the Subscription Services, Process Personal Data in accordance with the requirements of the Agreement and all Data Protection Laws and Regulations. For the avoidance of doubt, Customer’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3 **Company’s Processing of Personal Data.** Company shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of, and in accordance with, Customer’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Customer’s end users in their use of the Subscription Services; and (iii) Processing to comply with other documented, commercially reasonable instructions provided by Customer (e.g., via email), where such instructions are consistent with the terms of the Agreement. Company will not process the Personal Data any further than is provided in this clause 2.1. Under no circumstances will Company use the Personal Data for its own purposes or exploit them (or have them exploited) other than as permitted or authorized pursuant to the terms of the Agreement.

2.4 **Details of the Processing.** The subject-matter of Processing of Personal Data by Company is the performance of the Subscription Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this GDPA are further specified in Annex I.B to this GDPA.

2.5 **Cross-Border Transfers**. If Personal Data is transferred under the Agreement from the European Economic Area or Switzerland by Customer as Controller to Company as Processor, or otherwise by Company as Processor, to a jurisdiction which the European Commission or, where relevant, the Swiss Federal Data Protection and Information Commissioner, has not determined ensures an adequate level of protection of Personal Data, then Company and Customer shall execute the Standard Contractual Clauses in Schedule 1.

3. NOTICES AND CONSENTS

3.1 **General**: Customer shall comply with all applicable Data Protection Laws and Regulations, including: (a) providing all required notices and appropriate disclosures to all Data Subjects regarding Customer’s, and Company’s, Processing and transfer of Personal Data; and (b) obtaining all necessary rights and valid consents from Data Subjects to permit Processing by Company for the purposes of fulfilling Company’s obligations, or as otherwise permitted, under the Agreement.

3.2 **Children; Sensitive Data**: Customer is responsible for compliance with all applicable Data Protection Laws and Regulations regarding its content, including without limitation those that regulate content directed toward children (as defined under applicable Data Protection Laws and Regulations; for example, under 13 years old in the United States or under 16 years old in certain other countries). Customer’s use of Company Subscription Services in connection with the distribution of content and/or Processing of sensitive Personal Data of a Data Subject (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or an individual’s genetic data, biometric data, health data, or data regarding sex life or sexual orientation) must be in compliance with all applicable Data Protection Laws and Regulations, including obtaining express consent from Data Subjects whose Personal Data is provided to Company for Processing.

4. RIGHTS OF DATA SUBJECTS

Company shall, to the extent legally permitted, promptly notify Customer if Company receives a request from a Data Subject to exercise the Data Subject's valid right of access, right to rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, to the extent that such Data Subject is entitled to such rights under applicable Data Protection Laws and Regulations (“**Data Subject Inquiry**”). Taking into account the nature of the Processing, Company shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer’s obligation to respond to a Data Subject Inquiry under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Subscription Services, does not have the ability to address a Data Subject Inquiry, Company shall upon Customer’s request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Inquiry, to the extent Company is legally permitted to do so and the response to such Data Subject Inquiry is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Company’s provision of such assistance.

5. COMPANY PERSONNEL

5.1 **Confidentiality.** Company shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Company shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

5.2 **Reliability.** Company shall take commercially reasonable steps to ensure the reliability of any Company personnel engaged in the Processing of Personal Data.

5.3 **Limitation of Access.** Company shall ensure that Company’s access to Personal Data is limited to those personnel, including Sub-processors, providing Subscription Services in accordance with the Agreement. Company only grants its employees and Sub-processors access to the Personal Data insofar as this is required for the performance of the Agreement and with due observance of the confidentiality provisions.

6. SUB-PROCESSORS

6.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) Company’s Affiliates may be retained as Sub-processors; and (b) Company and Company’s Affiliates, respectively, may engage third-party Sub-processors in connection with the provision of the Subscription Services. Company or its Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this GDPA with respect to the protection of Personal Data to the extent applicable to the nature of the services provided by such Sub-processor. A list of approved Sub-processors as of the Effective Date of this GDPA can be found in Annex III of the enclosed Standard Contractual Clauses (Schedule I). Customer may subscribe to receive update alerts when changes are made to the Sub-processor List. Nevertheless, Company or its Affiliate shall specifically inform in writing the Customer of any intended changes of that list through the addition or replacement of Sub-processors at least five (5) business days in advance.

6.2 **Objection Right for New Sub-processors.** If Customer can reasonably show that the appointment of a new Sub-processor will have a material adverse effect on Company’s ability to comply with applicable Data Protection Laws and Regulations, then Customer must promptly notify Company in writing within fifteen (15) business days thereafter of its reasonable basis for objection to the use of a new Sub-processor. Upon receipt of Customer’s written objection, Customer and Company will work together without unreasonable delay to recommend an alternative arrangement. If the following conditions apply: a) a mutually acceptable and reasonable alternative arrangement is not found; b) Customer has a termination right under applicable Data Protection Laws and Regulations, and c) Customer has provided prompt written notice under this Section, then Customer may terminate the Subscription Agreement only with respect to those services that cannot be provided by Company without the use of the new Sub-processor. Unless prohibited by applicable Data Protection Laws and Regulations, in the event of such early termination by Customer, Company can retain or require payment for Services through the end of Customer’s current contract term for the terminated services.

6.3 **Liability.** Company shall be liable for the acts and omissions of its Sub-processors to the same extent Company would be liable if performing the Subscription Services of each Sub-processor directly under the terms of this GDPA, except as otherwise set forth in the Agreement.

7. SECURITY

7.1 **Controls for the Protection of Customer Data.** Company shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data. Company regularly monitors compliance with these measures. Company will not materially decrease the overall security of the Subscription Services during a subscription term. The description of the technical and organizational measures can be found in Annex II of the enclosed Standard Contractual Clauses (Schedule I).

7.2 **Third-Party Certifications and Audits.** Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Company shall make available to Customer that is not a competitor of Company (or Customer's independent, third-party auditor that is not a competitor of Company) a copy of Company's then most recent third-party audits or certifications, as applicable.

8. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

Company shall maintain security incident management policies and procedures and shall, notify Customer without undue delay after becoming aware of any Personal Data Breach. Company shall make reasonable efforts to identify the cause of such Personal Data Breach and take those steps as Company deems necessary and commercially reasonable in order to remediate the cause of such a Personal Data Breach to the extent the remediation is within Company's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's end users.

9. RETURN AND DELETION OF CUSTOMER DATA

Upon termination or expiration of the Agreement or at any time at Customer's written request, Company shall: return to Customer or destroy all Personal Data, except as otherwise permitted by applicable Data Protection Laws and Regulations.

10. LIMITATION OF LIABILITY

Notwithstanding anything contained in this GDPA to the contrary, Customer's remedies and Company's and its Affiliates' obligations, with respect to breach of this GDPA or a Personal Data Breach directly caused by Company and the overall liability of Company arising out of, or in connection with such breach will be subject to the aggregate limitations of liability under Section 9 of the Agreement (the "**Liability Cap**")

FOR THE AVOIDANCE OF DOUBT, THE PARTIES INTEND AND AGREE THAT THE OVERALL AGGREGATE LIABILITY OF COMPANY AND ITS AFFILIATES ARISING OUT OF, OR IN CONNECTION WITH, COMPANY'S BREACH OF THIS GDPA SHALL IN NO EVENT EXCEED THE LIABILITY CAP.

11. EUROPEAN SPECIFIC PROVISIONS

11.1 **Data Protection Impact Assessment.** Upon Customer's request, Company shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Subscription Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Company. COMPANY shall provide commercially reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 2.5 of this GDPA, to the extent required under the GDPR.

STANDARD CONTRACTUAL CLAUSES: The contractual clauses set out in Schedule 1 ("Standard Contractual Clauses"), which are pursuant to the European Commission implementing decision (EU) 2021/915 of 4 June 2021, are incorporated herein and apply to the Processing of Personal Data of residents of the European Union or Switzerland by Company in the course of providing Services to Customer under the Agreement (Module 2 shall apply, Controller-Processor).

SCHEDULE 1

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take 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 the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 5 business days in advance, thereby giving the data exporter 15 business days to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its subprocessor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination - including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Cyprus.\

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Cyprus.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: [ADD]

Address: [ADD]

Contact person's name, position and contact details:

[ADD]

Position: [ADD]

E-Mail: [ADD]

Activities relevant to the data transferred under these Clauses: Data processing for the performance of the agreement

Signature and date: …

Role (controller/processor): Controller

Data importer(s):

Name: [ADD]

Address:

[ADD]

Contact person's name, position and contact details: …Data Privacy Officer dpo@creatio.com

Activities relevant to the data transferred under these Clauses: … Data processing for the performance of the agreement

Signature and date: …

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS PROCESSED

The personal data transferred concern the following categories of data subjects: customers of Customer and any other individuals interacting with the Company's software and services, or as otherwise set forth or referenced in the Agreement and GDPA, or in any Orders or Statements of Work issued pursuant to the Agreement, or as otherwise agreed by the parties.

Customer may submit Personal Data to the Subscription Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's Users authorized by Customer to use the Subscription Services

CATEGORIES OF PERSONAL DATA PROCESSED

The personal data transferred concern the following categories of data subjects: customers of Customer and any other individuals interacting with the Company's software and services, or as otherwise set forth or referenced in the Agreement and GDPA, or in any Orders or Statements of Work issued pursuant to the Agreement, or as otherwise agreed by the parties.

Customer may submit Personal Data to the Subscription Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localisation data

SENSITIVE DATA

Not applicable

NATURE AND PURPOSE OF PROCESSING

Company will Process Personal Data as necessary to perform the Subscription Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Subscription Services.

DURATION OF PROCESSING

Subject to Section 9 of the GDPA, Company will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

C.COMPETENT SUPERVISORY AUTHORITY

Office of the Commissioner for Personal Data Protection

Office address:

[ADD]

Postal address

[ADD]

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational security measures implemented by the Processor during performing the Subscription Services

A. ***Measures of pseudonymisation and encryption of personal data***

Encrypting data when transmitting and\or storing using industry-standard strong encryption.

B. ***Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services***

Each cloud location of our Services has dedicated and separate network, divided into logical segments.

The perimeters of Company Cloud locations is protected with firewall solution with IDS/IPS features.

All hosts protected by endpoint protection solution with antivirus protection, OS integrity controls and additional network protection features (firewall, and intrusion protection system). Endpoint protection solution has up-to-date patches and virus definitions and is set to receive the most current security updates on a regular basis.

Hosts are configured according to internal security requirements based on best practices and recommendations from vendors and leading experts in information security.

Processor keeps up to date the operating systems and applications it uses. Installation of security patches is performed within 1 month from the time patch was released by the vendor.

Access to cloud infrastructure is controlled with the following methods:

- The Company restricts and controls mechanisms for logical and network access.
- Only limited number of cloud administrators have persistent access to the cloud infrastructure to perform infrastructure maintenance tasks.
- Access lists are reviewed on a quarterly basis.
- According to established procedure all Processor’s employee accesses are revoked at dismissal and his/her accounts in all Company’s systems are blocked

Company uses two factor authentication for administrative access.

Each Customer Data is separated from other customers’ data.

C. ***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***

Company regularly backs-up of Customer data. The back-up parameters are further described and aligned in the SLA between Parties. Back-ups are stored for 30 days,and regularly tested to assure integrity and Processor’s processes to restore data in case of destruction or incidents.

Disaster Recovery Plan at Company is kept up to date and regularly tested.

D. ***Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing***

Following regular evaluations and reviews are part of information security processes:

- Regular vulnerability scans are performed at least quarterly on all hosts and components. Scanning is performed both inside and outside of the Company Cloud infrastructure perimeter.
- Regular penetration tests take place at least yearly and are conducted by third-party independent experts.
- Regular, at least yearly, internal reviews of the security policies and procedures.
- Internal access review is performed quarterly.
- Processor performs regular tests of Business Continuity Plan and Disaster Recovery Plans.
- Regular external audits are conducted as part of the compliance processes.

E. ***Measures for user identification and authorisation***

Subscription Services provide capabilities for Customer’s system administrators to enable and configure secure authentication controls that:

- control of user IDs and other identifiers;
- a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

- control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
- restricting access to active users and active user accounts only;
- blocking access to user identification after multiple unsuccessful attempts to gain access;
- requiring authentication for all external requests to Creatio web services;
- Limiting multiple logins under single user credentials.

Subscription Services provide capabilities for secure access control that:

- restrict access to records and files containing personal information to those who need such information to perform their job duties; and
- assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

F. **Measures for the protection of data during transmission**

Customer data in motion is encrypted with TLS protocol.

G. ***Measures for the protection of data during storage***

Customer data during storage is encrypted using industry-standard strong encryption.

H. ***Measures for ensuring physical security of locations at which personal data are processed***

Company's Subprocessors, Amazon Web Services (AWS) and Microsoft Azure, implement controls for physical security, that include datacenter access control, regularly reviewing provided access, and surveillance control of physical access points. Company verifies that its Subprocessors, AWS and Microsoft Azure, maintain valid certificates and reports to demonstrate their compliance with ISO 27001 and SOC2.

I. ***Measures for ensuring events logging***

All security related events in Cloud infrastructure are collected in the log management system and regularly analyzed by Processor's teams.

In Subscription Services the Audit Log allows to register events related to the modification of user roles, distribution of access permissions, change of system setting values and users' authorization in the system. Parameters of the audit log are configurable. Audit Log can be exported for analysis on the Customer's side.

J. ***Measures for ensuring system configuration, including default configuration***

Hosts are configured according to internal security requirements based on best practices and recommendations from vendors and leading experts in information security.

All changes, which are introduced, are following the Processor's internal policies. Changes go through mandatory testing and approval steps before they are implemented in the production environment.

Changes to settings are done exclusively using cloud infrastructure automation tools.

Events related to changes in key configuration parameters are logged and controlled by Creatio teams

K. ***Measures for internal IT and IT security governance and management***

Information security management system is implemented at Company and is certified as compliant to ISO 27001 standard.

Company regularly performs review of actualized risks and adopts appropriate measures for mitigation of the discovered risks.

Company performs regular reviews and makes improvements to the information security controls and processes. Regular training for employees on the proper use of the computer security system, personal data, and aspects of enterprise and personal information security.

L. ***Measures for certification/assurance of processes and products***

Company has been certified under ISO 27001 process and updates that certification. Furthermore, Creatio is SOC2 compliant and certified (SSAE 18). External audits are regularly conducted as part of the ISO27001 and SOC2 certification processes.

M. ***Measures for ensuring data minimisation***

Supplier will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Services

N. ***Measures for ensuring limited data retention***

Subject to Section 10 of the DPA, Supplier will process Personal Data for the duration of the Agreement. The main terms of the data deletion mechanism are defined in the Agreement, namely the process and timeframe for either return and/or deletion of Personal data.

O. ***Measures for allowing data portability and ensuring erasure***

Subscription Services provide the necessary capabilities GDPR Compliance Management which allow to register permissions and denials to process personal data, and perform actions related to right to be forgotten and right to access.

P. ***Measures for ensuring data quality***

Subscription Services allow Customer to update stored personal data. Company as the Processor performing the Subscription Services does not have influence over the content of data as part of the performing the Subscription Services pursuant to the Agreement.

Q. ***Measures for ensuring accountability***

Company Subscription Services are GDPR compliant. Company security processes are designed in accordance with GDPR requirements, and Company regularly evaluates its compliance with GDPR regulation.

The details of Processing of Personal Data by Company is defined in the Master Subscription Agreement between Parties. Based on requests from Controller, within a reasonable timeframe Processor can provide report on the implemented measures as part of performing the Subscription Services pursuant to the Agreement.

ANNEX III – LIST OF SUB-PROCESSORS

A list of approved Sub-processors to GENERAL DATA PROCESSING ADDENDUM.

Company may engage the following entities to carry out specific processing activities. Customer may subscribe to receive update alerts when changes are made to the Sub-processor List. Company will inform Customer of any new Sub-processor engaged during the term of the Subscription Agreement by updating the Sub-processor List.

Affiliated Entity	**Corporate location**
CREATIO BRITAIN LTD	UK
CREATIO EMEA LTD	CY
CREATIO AMERICAS Inc.	USA
CREATIO GLOBAL LTD	CY
CREATIO OCEANIA PTY LTD	AU
CREATIO EUROPE sp. z o.o.	PL

Third Party Entities	**Corporate location**
Amazon Web Services (AWS) and its affiliated entities	As per link provided below (with subsequent updates) https://aws.amazon.com/compliance/sub-processors/?nc1=h_ls
Microsoft Azure and its affiliated entities	As per link provided below (with subsequent updates) https://www.microsoft.com/en-us/trust-center/privacy/data-access

Last Updated: February 22, 2024