Nelio Services
Data Processing Addendum (DPA)

Introduction

This Data Processing Agreement ("**DPA**") is entered between Nelio Software S.L. (**"Nelio"**) and Customer (**"Customer"**), together referred to as the "**Parties**".

The Parties agree that this Nelio Services Data Processing Agreement ("DPA") sets forth their obligations with respect to the processing and security of Customer Data, and Personal Data subject to Applicable Data Protection Laws in connection with the Services. The DPA is incorporated by reference into the Agreement.

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. Definitions

"**Nelio**" means Nelio Software S.L.

"**Applicable Data Protection Laws**" means, to the extent applicable:

(i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR"), Directive 2002/58/EC ("e-Privacy Directive"), the UK GDPR, the UK Data Protection Act 2018, and any other data protection or privacy laws and regulations of the European Union, the European Economic Area, their Member States, Switzerland, and the United Kingdom; and
(ii) any other applicable privacy and data protection laws and regulations worldwide (whether national, state, provincial, local or otherwise) applicable to the Processing of Personal Data under the Agreement, as may be amended, replaced, or re-enacted from time to time, including without limitation any jurisdiction-specific provisions set out in the relevant Annexes.

"**Agreement**" means Nelio's Common Terms and Conditions, the applicable Specific Terms and Conditions, the Privacy and Cookies Policy, and any other relevant documents governing the provision of the Services to Customer, as may be updated from time to time.

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

"**Customer Data"** means any Personal Data and other information that is submitted to the Services by or on behalf of the Customer or its Users, including information relating to Users, End Users, or other individuals. Customer Data includes any content or data stored, transmitted, or processed through the Services.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

"**Personal Data**" means "any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person", as defined under the General Data Protection Regulation 2016/679 and includes any equivalent definition in the Applicable Data Protection Laws;

"Personal Data Breach" means a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data, as defined under Article 4(12) of the GDPR or any equivalent definition under Applicable Data Protection Laws.

"**Process**, **Processing or Processed**" means "any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction", as defined under the General Data Protection Regulation 2016/679 and includes any equivalent definition in the Applicable Data Protection Laws;

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

"**Sensitive Information**" means any Personal Data that is defined as sensitive information or sensitive data under Applicable Data Protection Laws and that requires additional protections, safeguards or security measures under such applicable laws. Sensitive Information includes, but is not limited to, 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 offenses.

"**Standard Contractual Clauses**" or "**SCCs**" means the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as adopted by the European Commission on 4 June 2021 (Commission Implementing Decision (EU) 2021/914). Where transfers are subject to the UK GDPR, the SCCs shall be read together with, and supplemented by, the UK Addendum as set out in Annex V.

"**Sub-processor**" means any Processor engaged by Nelio to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA.

"**Supervisory Authority**" means an independent statutory regulatory authority with respect to Personal Data privacy under Applicable Data Protection Laws.

"**Third Country**" means any country, organization or territory not recognied under Applicable Data Protection Laws as providing an adequate level of data protection.

"**TOMs**" means Nelio's technical and organizational security measures as outlined in Section 3.2.

"**UK Addendum to the SCCs**" means the United Kingdom Addendum B.1.0 to the Standard Contractual Clauses issued by the United Kingdom Commissioner's Office.

2. Processing of Personal Data

2.1 Roles of the Parties. The Parties acknowledge and agree that, for the purposes of this DPA and the Applicable Data Protection Laws:

- the **Customer** acts as the **Controller** (or, where applicable, as a Processor acting on behalf of its own third-party Controller); and
- **Nelio** acts as the **Processor** processing Personal Data on behalf of the Customer in connection with the provision of the Services.

Nelio may engage Sub-processors in accordance with Section 8 as listed in **Annex III** of this DPA.

2.2 Compliance with Applicable Data Protection Laws. The Parties shall comply with their respective obligations under **Applicable Data Protection Laws**. This DPA sets out the terms under which Nelio will Process Personal Data on behalf of the Customer and assist the Customer in meeting its legal obligations as Controller.

2.3 Nelio's Processing of Personal Data. Nelio shall Process Personal Data only on documented instructions from the Customer, unless otherwise required by Applicable Data Protection Laws. In such a case, Nelio shall inform the Customer of that legal requirement before Processing, unless prohibited by law.

Nelio shall Process Personal Data solely for the following purposes:
(i) to provide the Services in accordance with the Agreement;
(ii) as initiated by Users in their use of the Services; and
(iii) to comply with other reasonable documented instructions provided by the Customer, provided that such instructions are consistent with the Agreement and Applicable Data Protection Laws.

2.4 Customer's Processing of Personal Data. The Customer is solely responsible for:
(a) ensuring that its instructions to Nelio comply with Applicable Data Protection Laws;
(b) determining the lawfulness, accuracy, quality, and adequacy of the Personal Data provided to Nelio;
(c) obtaining any necessary consents and providing required notices to Data Subjects;
(d) ensuring that any transfers of Personal Data to third parties (other than Nelio and authorized Sub-processors) comply with Applicable Data Protection Laws; and
(e) determining the legal basis for the Processing of Personal Data, including any processing of Sensitive Information.

2.5 Customer's Responsibility for Third-Party Transfers. Where the Customer enables or integrates third-party services in connection with the Services, the Customer acknowledges that such third parties act independently and are not under Nelio's control. The Customer is solely responsible for ensuring that any such third-party Processing complies with Applicable Data Protection Laws.

2.6 Notification of Non-Compliance. If the Customer becomes aware that any Processing of Personal Data through the Services does not comply with Applicable Data Protection Laws, it shall notify Nelio without undue delay. Nelio may, where reasonably necessary, suspend the affected Processing activities until the issue is resolved.

2.7 Details of the Processing. The subject matter, duration, nature, and purpose of Processing, as well as the types of Personal Data and categories of Data Subjects, are described in Annex I to this DPA.

3. Obligations of Processor

3.1 Nelio Personnel and Access Controls

3.1.1 Confidentiality. Nelio shall ensure that all personnel involved in Processing Personal Data are subject to binding confidentiality obligations, have received appropriate training on data protection requirements, and understand the sensitive nature of the data they access. These confidentiality obligations shall survive the end of employment or engagement.

3.1.2 Reliability. Nelio shall take commercially reasonable measures to verify the reliability of any personnel with access to Personal Data.

3.1.3 Assistance with Compliance. Nelio shall provide reasonable cooperation and assistance to Customer, upon written request, to help Customer meet its obligations related to cross-border transfers or other data protection requirements under Applicable Data Protection Laws.

3.1.4 Limitation of Access. Nelio shall restrict access to Personal Data strictly to those personnel who require it to perform their duties under the Agreement.

3.2 Security Measures and Controls

3.2.1 Technical and Organizational Measures (“**TOMs**”). Nelio shall implement and maintain appropriate technical and organizational measures to ensure the security, confidentiality, and integrity of Customer Data. The applicable TOMs are outlined in **Annex II** of this DPA and may be updated periodically.

3.2.2 Monitoring and Maintenance. Nelio regularly monitors the effectiveness of its TOMs and updates them as needed to address emerging risks, changes in legal requirements, and technological developments.

3.2.3 Continuous Improvement. TOMs may be modified over time for continuous improvement, provided that any changes maintain or enhance the existing level of security for Personal Data. Individual measures may be replaced by equivalent or superior alternatives without diminishing protection.

3.2.4 Documentation and Audit Rights. Nelio shall make available to the Customer, upon written request, all information reasonably necessary to demonstrate compliance with this DPA, subject to appropriate confidentiality obligations and safeguards for Nelio’s legitimate business interests.

Where required by Applicable Data Protection Laws, and subject to Section 7 (DPA Audits), Nelio shall allow for and contribute to audits, including inspections, conducted by the Customer or an independent auditor mandated by the Customer, provided that such auditor is not a direct competitor of Nelio and that any such audit is conducted in a manner that does not unreasonably interfere with Nelio's business operations.

3.3 Personal Data Breach Notification and Management

Nelio shall notify Customer without undue delay, and in any event within seventy-two (72) hours after becoming aware of a Personal Data Breach affecting Customer Data. The notification shall include, to the extent known at the time:
(i) a description of the nature of the breach, including, where possible, the categories and approximate number of affected Data Subjects and records;

(ii) the likely consequences of the breach;

(iii) the measures taken or proposed to address the breach and mitigate its effects; and

(iv) whether notification to a supervisory authority or affected individuals has been made or is planned (noting that such notifications, where required, remain the Customer's responsibility unless otherwise agreed).

Nelio shall provide reasonable cooperation to Customer in managing any such breach, in accordance with Applicable Data Protection Laws.

3.4 Return or Deletion of Customer Data

Upon Customer's written request, or within thirty (30) days following termination or expiration of the Agreement, Nelio shall permanently delete all copies of Personal Data in its possession (in any form) using industry-standard destruction methods, unless retention is required by applicable law. Upon request, Nelio shall return Customer Data in a readable format. Any costs related to reformatting returned data to Customer specifications shall be borne by the Customer.

4. Obligations of Controller

4.1 Compliance with Data Protection Laws. The Customer, acting as the Controller, shall comply with all applicable Data Protection Laws in relation to its Processing of Personal Data. This includes ensuring that any instructions provided to Nelio are lawful, documented, and consistent with the legal requirements governing the Personal Data.

4.2 Duty to Inform Nelio. The Customer shall promptly notify Nelio of any errors, irregularities, or concerns relating to the Processing of Personal Data under this Agreement, particularly if any processing activity is identified that may violate Section 5 (Restrictions) or Applicable Data Protection Laws. Where requested by Nelio, the Customer shall take immediate corrective measures to ensure that its use of the Services aligns with applicable legal and contractual requirements.

4.3 Responsibility for Implementation. Nelio provides the Services as technical tools. The Customer is solely responsible for the proper implementation, configuration, and customization of the Services within its own environment ("Implementation"). Nelio assumes no responsibility or liability for any issues, non-compliance, or legal consequences arising from the Customer's Implementation of the Services.

5. Restrictions

5.1 Compliance with Laws. Nelio shall process Customer Data solely to perform the Services, for the purposes described in this DPA, and in accordance with the Customer's documented, lawful instructions, or as otherwise permitted or required under Applicable Data Protection Laws. Nothing in this DPA shall require Nelio to process Customer Data in a way that would breach applicable legal obligations.

5.2 Processing of Sensitive Information. The Services provided by Nelio are not designed for, nor intended to process, Sensitive Information. The Customer is solely responsible for determining whether its use of the Services to process Sensitive Information, including Special Categories of Data as defined in Article 9 of the GDPR, complies with Applicable Data Protection Laws.

If the Customer elects to process such data, it must first conduct and document a risk assessment to confirm that Nelio's technical and organizational measures are appropriate for the intended processing.

In particular, the Customer must refrain from submitting Sensitive Information into any prompts, inputs, or other submissions involving Nelio AI features. The Customer assumes full responsibility for ensuring that no Sensitive Information is processed through such features in violation of this DPA.

To the extent permitted by applicable law, Nelio shall not be liable for any consequences arising from the Customer's decision to process Sensitive Information in connection with the Services in breach of this Section.

6. Data Subject Rights

6.1 Data Subject Request. As between the Parties, the Customer is solely responsible for managing and responding to any requests from individuals to exercise their rights under Applicable Data Protection Laws ("**Data Subject Requests**" or "**DSRs**") regarding their Personal Data.
Nelio will promptly forward any DSR received by Nelio or its Sub-processors to the Customer. Nelio may advise the individual to contact the Customer directly for resolution.

6.2 Assistance with Data Subject Requests. Taking into account the nature of the processing, Nelio shall provide the Customer with self-service tools within the Services or reasonable additional assistance as needed to enable the Customer to fulfill its obligations to respond to DSRs, as required by Applicable Data Protection Laws.

6.3 Completeness and Avoidance of Duplicates. The Customer shall ensure that any assistance requests submitted to Nelio in relation to DSRs are complete, clear, and not duplicative. Nelio is not required to act on vague, incomplete, or repetitive requests.

6.4 Scope of Nelio's Assistance. Nelio's obligation to assist with DSRs is limited to Personal Data processed within the scope of the Services provided by Nelio. Nelio has no responsibility or obligation to assist with DSRs related to Personal Data processed outside the Services.

7. DPA Audits

7.1 Audit Rights.
Subject to Section 3.2.4, upon written request and no more than once per year, the Customer or its authorized representative may audit Nelio's compliance with this DPA. Such audits will typically consist of a review of relevant documentation, certifications, audit reports, and other information reasonably necessary to demonstrate compliance.

7.2 Remote Audits.
Audits shall be conducted remotely, unless otherwise required by Applicable Data Protection Laws or a competent Supervisory Authority. Nelio shall provide reasonable cooperation through the provision of documentation, written responses, and, where appropriate, video or conference calls.

7.3 On-Site Audits (Exceptional Circumstances).
On-site audits of Nelio may only be conducted where:

- (i) required by Applicable Data Protection Laws or a competent Supervisory Authority, and
- (ii) a remote audit is insufficient to meet such requirements.
  Any on-site audits shall be subject to reasonable prior notice, mutually agreed scope, confidentiality obligations, and shall be conducted in a manner that minimizes disruption to Nelio's business operations.

7.4 Costs.
Each party shall bear its own costs related to any audit, unless otherwise required by Applicable Data Protection Laws.

8. Sub-processing

8.1 Authorized Sub-processors and Notification of New Sub-processor. The Customer authorizes Nelio to engage third-party Sub-processors to support the delivery of the Services. A current list of Sub-processors is maintained in **Annex III**.

Nelio may update its Sub-processors from time to time. Where required by Applicable Data Protection Laws, Nelio will provide notice of material changes to Sub-processors.

8.2 Sub-processor obligations. Nelio shall:

- Enter into written agreements with Sub-processors imposing data protection obligations at least equivalent to those in this DPA.
- Remain fully responsible for the performance of Sub-processors and for any breach of this DPA caused by a Sub-processor.

Customer acknowledges that Nelio fulfills its obligations under the SCCs by complying with this Section 8. Due to confidentiality restrictions, Nelio may not be able to disclose full copies of Sub-processor agreements but will provide sufficient information upon request.

8.3 Sub-processors List. The list of Sub-processors is published in Annex III of the DPA (also accessible via https://neliosoftware.com/legal-information/data-processing-agreement/) and is subject to updates as described above.

8.4 Right to Object. The Customer may object in writing to the appointment of a new Sub-processor within thirty (30) calendar days of receiving notice, provided the objection is based on reasonable data protection grounds.
In such cases, the parties will work together in good faith to find a resolution. If no resolution

is possible, the Customer may suspend or terminate the affected Services in accordance with the Agreement.

9. International Transfers

9.1 Application of Standard Contractual Clauses (SCCs). To the extent that Nelio processes Personal Data that is transferred from the European Economic Area (EEA), the United Kingdom (UK), or Switzerland to a country not recognized as providing an adequate level of data protection under Applicable Data Protection Laws, the Parties agree that such transfers shall be governed by the applicable **Standard Contractual Clauses (SCCs)** set forth in **Annex IV** of this DPA.

The SCCs shall apply:

- To any direct or onward transfers of Personal Data to countries lacking adequacy decisions, including transfers to Sub-processors located in such countries.
- In accordance with the role of each Party (Controller-to-Processor or Processor-to-Processor) as required by the nature of the Processing under the Agreement.

The Parties agree that by entering into this DPA, they are deemed to have executed the SCCs as incorporated in Annex IV without the need for separate signature.

9.2 Supplementary Measures
Where necessary, Nelio and the Customer will work together in good faith to implement additional technical, contractual, or organizational measures to ensure an essentially equivalent level of protection for Personal Data in accordance with guidance from competent Supervisory Authorities and Applicable Data Protection Laws.

9.3 UK Addendum
For transfers subject to the UK GDPR, the **UK Addendum to the SCCs** (set out in **Annex V**) shall apply and form an integral part of this DPA.

10. Duties to Inform, Mandatory Written Form, Choice of Law, Additional terms

10.1 Seizure and Third-Party Access. If Customer's Personal Data becomes subject to search, seizure, attachment, confiscation, bankruptcy, insolvency measures, or any similar actions by third parties while under Nelio's control, Nelio shall promptly inform Customer unless prohibited by law. Where legally permissible, Nelio will immediately notify the relevant

third parties that such Personal Data belongs solely to Customer and that Customer, as the Controller, retains full responsibility and decision-making authority under Applicable Data Protection Laws.

10.2 DPA Updates and Changes. When Customer renews or purchases a new subscription to the Services, the then-current version of this DPA shall apply, unless otherwise agreed in writing by the Parties.
Where the DPA is not separately executed by the Parties, it shall become legally binding upon Customer's acceptance of the Terms of Service or continued use of the Services.
Nelio reserves the right to amend this DPA as necessary to comply with updates to Applicable Data Protection Laws, including the introduction of new or replacement Standard Contractual Clauses. Nelio shall provide Customer with at least ninety (90) days' prior written notice of any material amendments, unless a shorter notice period is required to comply with applicable law.
If Nelio introduces new features, add-ons, or related software not previously covered by the Services, specific terms and corresponding updates to this DPA may apply to those offerings. Such updates shall apply only to the extent Customer elects to use the relevant features.

10.3 Severability. If any provision of this DPA is found to be invalid, illegal, or unenforceable, the remaining provisions shall remain valid and binding. The invalid provision shall be replaced by a valid one that most closely reflects the Parties' original intent and economic purpose.

10.4 Additional GDPR Specific Provisions:

10.4.1 GDPR Compliance. Nelio shall process Personal Data in accordance with the GDPR to the extent directly applicable to Nelio's provision of the Services.

10.4.2 Transfer Impact Assessments (TIA). Upon Customer's reasonable written request, Nelio shall provide commercially reasonable assistance to enable Customer to conduct a **Transfer Impact Assessment (TIA)**, as required under Applicable Data Protection Laws. This assistance is limited to information reasonably available to Nelio.

10.4.3 Cooperation with Supervisory Authorities.
Nelio shall also provide reasonable assistance to Customer in any cooperation or consultations with Supervisory Authorities concerning Customer's use of Nelio Services, where such cooperation relates specifically to Nelio's role as Processor.

ANNEXES

The following Annexes I–VI form an integral part of this DPA.

- **ANNEX I: DETAILS OF THE PROCESSING**
- **ANNEX II: TECHNICAL AND OPERATIONAL MEASURES**
- **ANNEX III: LIST OF SUB-PROCESSORS**
- **ANNEX IV – STANDARD CONTRACTUAL CLAUSES**
- **ANNEX V: UK ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES**
- **ANNEX VI: CCPA/CPRA ADDENDUM**

The Parties agree that the details in these Annexes shall govern the respective areas they address.

ANNEX I – DETAILS OF THE PROCESSING

This Annex I to the DPA includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

1. List of Parties

Controller / Data Exporter:

Name:	
Address:	
Contact person's name and contact details	
Activities relevant to the data transferred under the SCCs:	Receipt of the Services
Signature and date:	
Role (controller/processor):	Controller

Processor / Data Importer:

Name:	Nelio Software S.L.
Address:	Pomaret 83 08017 Barcelona, Spain

Contact person's name and contact details	Ruth Raventós CEO Email: legal@neliosoftware.com
Activities relevant to the data transferred under the SCCs:	Provision of the Services
Signature and date:	
Role (controller/processor):	Processor

2. Description of Transfer

2.1 Categories of Data Subjects

Nelio processes Personal Data of the following categories of Data Subjects:

- Customer authorized users (including but not limited to Customer employees, freelancers or contractors) from time to time to whom the Customer has granted the right to use the Services in accordance with the Agreement;
- End-users and visitors to the Customer's websites, online stores, or digital properties who interact with the Services;
- Individuals whose data is provided to Nelio via the Services by or at the direction of the Customer.

2.2 Categories of Personal Data Processed

Nelio may process the following categories of Personal Data in the course of the provision of all the Services:

- Personal identification information (such as name, etc.);
- Contact details (such as address, email address, phone number etc.);
- Console logs and errors;

- Billing and invoicing information provided by the applicable payment or merchant-of-record provider (such as FastSpring or Shopify, where applicable), excluding full payment card details.

Nelio Content Service

Nelio may process the following categories of Personal Data in the course of the provision of Nelio Content Service:

- Social media accounts connection information (such as username, account ids, profile image, display name, username/page ID or profile ID, access token);
- Social media information published (such as Customer authorized users published posts and social messages) and collected (such as click rates, likes, and general engagement counts in their social networks).

Nelio A/B Testing Service

Nelio may process the following categories of Personal Data in the course of the provision of Nelio A/B Testing Service:

- Aggregated or pseudonymized usage metrics relating to end-user interactions;
- Statistics on end-users' device type, browser, screen size, operating system, and country, per page and aggregated daily;
- Statistics on time spent on each page, bounce rate, scroll depth, of end-users per page and aggregated daily;
- Statistics on end-user actions (clicks, selections), per page and aggregated daily.

Nelio Session Recording

Nelio may process the following categories of Personal Data in the course of the provision of Nelio Session Recordings Service (either used as a standalone plugin or as a Nelio A/B Testing addon)**:**

Data collected in a pseudonymized manner, without Nelio being able to directly identify Data Subjects:

- End-users' device type, browser, screen size, operating system, referring URL and domain, and country;
- End-users pages visited and time spent on each page, bounce rate, scroll depth;
- End-users actions (clicks, selections and mouse movements), per page.

2.3 Sensitive Information processed

Nelio does not want to, nor does it intentionally, collect or process any Sensitive Information in connection with the provision of the Services.

2.4 Frequency of Processing

Data will be transferred on a continuous basis for the duration of the Agreement.

2.5 Purpose of the Processing

Nelio shall only process Customer Data for the purposes in accordance with the Agreement (including this DPA), which shall include: (i) Processing as necessary to provide the Services in accordance with the Agreement; (ii) Processing initiated by Customer in its use of the Services; and (iii) Processing to comply with any other reasonable instructions provided by Customer (e.g., via email or support tickets) that are consistent with the terms of the Agreement.

For Customers who use Nelio AI features, the processing includes the transfer of Customer-provided content (such as text prompts, store content, or related context submitted through Nelio AI features) to third-party AI services for the purpose of generating content suggestions or analysis. Such processing is strictly limited to the requested AI features.

2.6 Duration of Processing

Data processing will continue for the term specified in the Agreement. Following expiration or termination, processing shall be subject to Section 3.4 (Return or Deletion of Customer Data) of this DPA.

2.7 Data Deletion

Nelio will process Customer Data as outlined in Section 3.4 (Return or Deletion of Customer Data) of this DPA.

2.8 Sub-processors

Nelio may engage Sub-processors to provide parts of the Service. Nelio will ensure Sub-processors only access and use the Customer's Personal Data to provide Nelio's Services and not for any other purpose. The Sub-processors currently engaged by Nelio and authorized by Customer are available and published, and may be updated from time to time, in Annex III of the DPA.

3. Competent Supervisory Authority

Spanish Data Protection Authority:

Agencia Española de Protección de Datos (AEPD)
C/ Jorge Juan, 6. 28001 – Madrid
Tel. 901 100 099 – 912 663 517

ANNEX II: TECHNICAL AND OPERATIONAL MEASURES

Nelio Software S.L. implements the following technical and organizational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR:

---

1. **Access Control**

- Access to systems and Personal Data is restricted to authorized personnel only.
- Role-based access control (RBAC) is enforced to ensure least-privilege access.
- Multi-factor authentication (MFA) is required for all administrative accounts, including access to cloud infrastructure (e.g., AWS, SiteGround).
- Access rights are reviewed regularly and immediately revoked upon employee termination or role change.

2. **Data Encryption**

- **Encryption in Transit:** All Personal Data is transmitted using strong encryption protocols such as TLS 1.2 or higher.
- **Encryption at Rest:** All stored Personal Data, including databases and backups, is encrypted using industry-standard algorithms (e.g., AES-256).
- Encryption keys are securely managed following best practices.

3. **Confidentiality and Employee Controls**

- All employees are bound by confidentiality obligations through employment contracts or separate agreements.
- Security awareness training is provided to staff regularly.
- Access to Personal Data is limited to personnel who require it to fulfill their job responsibilities.

4. **Physical Security**

- Nelio's infrastructure is hosted with reputable third-party providers (e.g., AWS, SiteGround) that implement strong physical security at their data centers, including controlled access, surveillance, and environmental controls.

5. **System and Network Security**

- Firewalls, intrusion detection systems, and security group configurations are used to protect systems and networks.
- All systems are regularly patched and updated to address security vulnerabilities through a formal patch management process.
- Anti-malware protection is in place where applicable.

6. **Logging, Monitoring, and Incident Response**

- Security-relevant events and system access are logged and centrally monitored.
- Logs are retained for at least 12 months and reviewed as part of security operations.
- Nelio maintains an incident response plan to detect, respond to, and remediate security incidents.
- In case of a Personal Data Breach, Nelio will notify the Customer in accordance with Section 3.3 of the DPA.

7. **Data Backup, Business Continuity, and Disaster Recovery**

- Regular encrypted backups of critical systems and Personal Data are performed and stored in geographically separate locations within the EU.
- Backups are tested periodically to ensure recoverability.
- Nelio maintains business continuity and disaster recovery plans to minimize disruption in the event of system failures or incidents.

8. **Data Minimization and Retention**

- Nelio collects and processes only the minimum amount of Personal Data necessary to provide the Services.
- Personal Data is retained only as long as needed to fulfill contractual obligations or comply with legal requirements.

9. **Data Deletion and Disposal**

- Upon termination of the Agreement or when requested by the Customer, Nelio securely deletes or returns all Personal Data in accordance with Section 3.4 of the DPA.
- Secure deletion processes include data wiping and deletion from all backups within established retention periods.

10. **Sub-processor Oversight**

- All Sub-processors used by Nelio are contractually obligated to implement equivalent security measures as described in this Annex.
- Sub-processor compliance is reviewed periodically.

ANNEX III: LIST OF SUB-PROCESSORS

Customer has authorized the use by Nelio of the Sub-processors detailed below.

Nelio enters into written agreements with each Sub-processor containing data protection obligations no less protective than those set out in this DPA.

Where Personal Data is transferred outside the EEA, such transfers are conducted in compliance with Chapter V of the GDPR, including reliance on adequacy decisions (where applicable), the EU-US Data Privacy Framework (where applicable), and/or the Standard Contractual Clauses adopted by the European Commission, supplemented where necessary by additional safeguards.

Sub-Processor Name	**Location of Processing**	**Service Provided**	**Safeguards/Transfer Mechanism**
Amazon Web Services (AWS)	Data centers in EU (primarily Ireland and Germany)	Cloud infrastructure and hosting services	Data stored in the EU; reliance on adequacy decisions where applicable; SCCs in place for any transfers outside the EU
FastSpring (Bright Market, LLC)	United States	Merchant of Record (payment processing and subscription management)	Standard Contractual Clauses (SCCs)
Freshworks Inc.	United States with EU data center	Customer support ticketing system	Standard Contractual Clauses (SCCs); EU data center option available

Google Workspace (Google LLC)	Data centers worldwide, with EU storage option	Email, internal communications, and document storage	EU-US Data Privacy Framework (self-certified); SCCs; EU Data Region commitments
Google Analytics 4 (GA4) (Google LLC)	Data centers worldwide, primarily in the United States	Web analytics services for service improvement and usage statistics	EU-US Data Privacy Framework (self-certified); SCCs; IP anonymization and EU data controls
Intuit Mailchimp (The Rocket Science Group LLC)	United States	Email marketing and customer communication platform	EU-US Data Privacy Framework (self-certified); SCCs
SiteGround Spain S.L.	Data centers in the EU (primarily Frankfurt, Germany)	Web hosting and server management	Data stored in EU; no international transfer
OpenAI, L.L.C.	United States	Optional AI processing provider, used only when Customer enables Nelio AI features	Standard Contractual Clauses (SCCs); optional feature activated by Customer

ANNEX IV: STANDARD CONTRACTUAL CLAUSES

SECTION 1

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); and

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 organizational 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 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 organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, 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 organizational 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 authorized 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 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 noncompliance. 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 subprocessors

(a) The data importer has the data exporter's general authorization for the engagement of subprocessor(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 subprocessors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the subprocessor(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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the subprocessor 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 subprocessor contract and to instruct the subprocessor 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 authorized 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 organizational 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 authorized 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, organization 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 subprocessor 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 subprocessor), 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 subprocessor to avoid its own liability.

Clause 13

Supervision

(a) 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, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, 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 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 authorizing 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 authorizing 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 organizational 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 organizational 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 minimization

(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 PROVISION

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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Kingdom of Spain.

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 and Tribunals of the City of Barcelona (the Kingdom of Spain).

(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 to the Standard Contractual Clauses

This Appendix forms part of the Clauses. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

ANNEX I.

A. LIST OF PARTIES

Data exporter. The data exporter is the Customer, as defined in the Annex I to the DPA.

Data importer. The data importer is Nelio, as defined in the Annex I to the DPA.

B. DESCRIPTION OF TRANSFER

The details regarding the description of transfer can be found in Annex I to the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Spanish Data Protection Authority:

Agencia Española de Protección de Datos (AEPD)
C/ Jorge Juan, 6. 28001 – Madrid
Tel. 901 100 099 – 912 663 517

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

The details of the technical and organizational measures applicable to the Services being provided by Nelio to Customer can be found in Annex II to the DPA.

ANNEX III. LIST OF SUBPROCESSORS

Customer has authorized the use by Nelio of the subprocessors detailed at Annex III to the DPA which are applicable to the Services being provided by Nelio to Customer.

ANNEX V: UK ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

In cases of data transfer from and to the United Kingdom the following provisions, this Annex V applies in addition to the Standard Contractual Clauses in Annex IV of the Nelio DPA.

PART 1: TABLES

Table 1: Parties

Start date	---Effective Date (See Order Form)	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number and any company number or similar identifier can be found in the Nelio Subscription Order Form	Full legal name: Nelio Software S.L. TIN: ESB66034794
Key Contact	Job Title and Contact details including email can be found in the Nelio Subscription Order Form	Job Title and Contact details: CEO, Ruth Raventós, legal@neliosoftware.com

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information available at https://neliosoftware.com/legal-information/data-processing-agreement/

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in the Data Processing Agreement available at https://neliosoftware.com/legal-information/data-processing-agreement/

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum: Importer and Exporter

PART 2: MANDATORY CLAUSES

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2 Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.

UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9 Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum

EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

"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";

c. Clause 6 (Description of the transfer(s)) is replaced with:

“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;

d. Clause 8.7(i) of Module 1 is replaced with:

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

f. References to “Regulation (EU) 2016/679”, “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)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;

j. Clause 13(a) and Part C of Annex I are not used;

k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

ANNEX VI: CCPA/CPRA ADDENDUM (FOR CALIFORNIA RESIDENTS)

1. Purpose and Scope

This **CCPA/CPRA Addendum** ("Addendum") forms part of the **Data Processing Agreement (DPA)** between **Nelio Software, S.L.** ("Nelio") and the Customer, where Nelio Processes **Personal Information** of California residents on behalf of the Customer in the course of providing the Services. This Addendum applies solely to Personal Information that is subject to the **California Consumer Privacy Act of 2018 (CCPA)**, as amended by the **California Privacy Rights Act of 2020 (CPRA)** and any implementing regulations.

All capitalized terms not defined in this Addendum shall have the meanings set forth in the DPA or under applicable law.

2. Definitions

- **Personal Information**: Has the meaning set forth in Cal. Civ. Code § 1798.140(v), including any information that identifies, relates to, describes, or is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California consumer or household.
- **Sensitive Personal Information**: Has the meaning set forth in Cal. Civ. Code § 1798.140(ae), including information such as government identifiers, precise geolocation, racial or ethnic origin, religious beliefs, union membership, genetic data, biometric information, health data, and sexual orientation.
- **Service Provider**: Has the meaning set forth in Cal. Civ. Code § 1798.140(ag) and refers to Nelio acting solely for the business purposes described in this Agreement and the Services.
- **Sale** and **Sharing**: Have the meanings assigned in Cal. Civ. Code § 1798.140(ad) and (ah), respectively. For the avoidance of doubt, "sharing" refers to disclosure for cross-context behavioral advertising.

3. Service Provider Obligations

Nelio agrees that when acting as a **Service Provider** on behalf of the Customer:

a. Nelio shall not **sell** or **share** Personal Information, including for cross-context behavioral advertising purposes.

b. Nelio shall not retain, use, or disclose Personal Information:

- For any purpose other than for the specific business purpose of performing the Services;
- For any commercial purpose other than providing the Services;
- Outside of the direct business relationship between Nelio and the Customer.

c. Nelio shall not combine Personal Information received from the Customer with Personal Information collected from other sources, except as expressly permitted under CCPA § 1798.140(ag)(1).

4. Customer Obligations

The Customer represents and warrants that:

a. It has provided all necessary notices and obtained all required consents under the CCPA/CPRA to enable lawful transfer of Personal Information to Nelio for processing.

b. It shall not instruct or request Nelio to process Personal Information in violation of applicable California privacy laws.

5. Consumer Rights Assistance

Taking into account the nature of the Services, Nelio shall provide reasonable assistance to the Customer in fulfilling verified consumer requests related to:

- The right to know/access;
- The right to correct inaccurate Personal Information;
- The right to deletion;
- The right to opt-out of sale or sharing (if applicable—note that Nelio does not engage in such activities);
- The right to limit the use of Sensitive Personal Information.

Requests from California consumers received directly by Nelio shall be promptly forwarded to the Customer.

6. Security Measures

Nelio shall implement and maintain reasonable security procedures and practices appropriate to the nature of the Personal Information to protect it from unauthorized access, destruction, use, modification, or disclosure, in compliance with CCPA § 1798.150(a)(1).

7. Limitation of Liability

This Addendum supplements the DPA. All limitations of liability and disclaimers set forth in the Agreement and DPA apply equally to this Addendum.

8. Additional Rights

If the Customer is also subject to other Applicable Data Protection Laws (e.g., GDPR), the stricter standard shall apply where legally required.

SIGNATURES

IN WITNESS WHEREOF, the Parties have caused this Data Processing Agreement to be executed by their duly authorized representatives.

For the Customer (Controller)

Company Name: _____

By: _____
Name: _____
Title: _____
Email: _____
Date: _____

For Nelio Software S.L. (Processor)

Company Name: Nelio Software S.L.
Registered Address: Pomaret 83, 08017 Barcelona, Spain
TIN: ESB66034794

By: _____
Name: Ruth Raventós
Title: CEO
Email: legal@neliosoftware.com
Date: _____

This Data Processing Agreement shall become legally binding upon execution by both Parties or, where not separately executed, upon Customer's acceptance of the Agreement or continued use of the Services, and shall be effective as of the Effective Date of the Agreement.