Elestio Data Processing Agreement

Last Modified: Feb 06, 2025

1. Background

This Data Processing Agreement (‘’DPA’’) is attached to the General Terms (available at https://elest.io/terms and forms an inseparable part of the Agreement entered into by Elestio limited (hereinafter “Elestio”) and the Customer. This DPA shall set out the terms and conditions for the processing of Personal Data by Elestio on behalf of the Customer under the Agreement.

2. Scope and conflict of rules

To the extent the Customer inputs Personal Data into the Cloud Services and Elestio processes such Personal Data, the Parties acknowledge that the Customer acts as a Data Controller and Elestio is a Data Processor processing Personal Data on behalf of the Customer for the purpose of providing the Cloud Services.

In the event of any discrepancy between this DPA and the Agreement, this DPA prevails.

3. Definitions

Unless otherwise defined in this DPA or in the Agreement, terms used in this DPA, such as "Data Controller", "Data Processor", "Data Subject" and "Personal Data" have the meanings as defined in the Data Protection Regulation.

Data Protection Regulation means all applicable laws relating to data protection, including without limitation the GDPR and the laws implementing EU Directive 2002/58/EC and any amendments to or replacements for such laws and regulations.

GDPR means the General Data Protection Regulation (EU) 2016/679.

Personal Data Breach means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Standard Contractual Clauses means the contractual clauses issued by the European Commission by the decision 2021/914/EU for international transfers of Personal Data.

Subprocessor means third parties: i) providing back-end services for Elestio and/or ii) selected by the Customer to provide the hosting services for the data Customer inputs to the Cloud Services. The Subprocessors and their services are listed on the Website.

Website means Elestio's website available at Elest.io and the Elestio console through which the Customer may use the Cloud Services.

4. Processing of personal data

Processing of Personal Data under this DPA is for the purpose of providing the Cloud Services to the Customer. Processing of Personal Data in this context refers to storage, maintenance and other processing activities initiated by the Customer, depending on which Cloud Services the Customer has chosen to order from time to time. The categories of Data Subjects and the types of Personal Data processed are defined in the Appendix 1 (Details of processing).

Personal Data may be processewed as long as the Cloud Services are provided under the Agreement and after that if required by applicable law or contractual obligations or rights of either Party.

5. Customer's instructions

The Elestio shall process Personal Data in accordance with the Customer's written instructions as established in this DPA. The Parties agree that this DPA is the Customer's complete written instruction to the Elestio in the Customer's role as the Data Controller. Additional instructions require prior written agreement between the Parties.

6. Elestio’s general obligations

Elestio shall, at the Customer's written request and the Customer's sole cost and expense, assist the Customer by providing such readily available information, or creating such information, as the Customer may reasonably require and which the Customer does not have, in complying with the requests of the Data Subjects or supervisory authority or any other law enforcement or regulatory authority.

Elestio shall inform the Customer, as soon as reasonably practicable, if it receives a request from a Data Subject seeking to exercise his or her rights under the Data Protection Regulation.

Elestio shall maintain records of processing activities under its responsibility to ensure Elestio's own compliance as a Data Processor with the Data Protection Regulation, and upon the Customer's written request Elestio shall make available to the Customer such records to the extent necessary to demonstrate compliance with Elestio’s obligations set out in this DPA and in the Data Protection Regulation.

7. Data security

Elestio shall implement and maintain appropriate technical and organisational measures to ensure an appropriate level of security of the Personal Data and to protect the Personal Data against

unuthorised or unlawful processing and against accidental loss, destruction, damage, alteration, or disclosure for the purposes of the Cloud Services.

In the event of a Personal Data Breach, Elestio shall notify the Customer without undue delay and at least within 48 hours after becoming aware of the Personal Data Breach and take reasonable steps to mitigate any damage resulting from such breach. The notification shall contain information Elestio is reasonably able to disclose to the Customer, including following information:

1. a description of the nature of the Personal Data breach, including where possible the categories of Data Subjects and the Personal Data concerned;
2. the name and contact details of contact point where more information can be obtained;
3. a description of likely consequences of the Personal Data Breach; and
4. a description of the measures taken or proposed to be taken to address the Personal Data Breach.

The information may be provided in phases if it is not possible to provide the information at the same time.

Elestio shall cooperate with and assist the Customer, at the Customer's written request, in relation to the Personal Data Breach notifications made to supervisory authority as required under the Data Protection Regulation. Elestio shall document the Personal Data Breaches and have the documentation available to the Customer upon the Customer's written request.

8. Controlled Support Access and Data Transfers

8.1 Customer-Controlled Access
Elestio ensures that personal data remains hosted and processed within the EU. Access to customer data is never granted by default—neither Elestio employees inside the EU nor those outside the EU have access unless explicitly authorized by the Customer. Support access is governed by the following conditions:

Customer-Initiated Access Grant: No Elestio employee, whether inside or outside the EU, can access customer data unless the Customer submits a support ticket and explicitly checks the box labeled "Grant Elestio Support team access to your project throughout the duration of this support ticket."
Temporary and Limited Scope: Support access is strictly limited to the duration of the specific support ticket and is automatically revoked upon resolution or ticket closure.
Minimal Necessary Access: Only personnel required for issue resolution will receive access, following the principle of least privilege.

8.2 Legal Basis for Support Access and Non-EU Transfers
In cases where the Customer grants access and Elestio’s support personnel—including those outside the EU—access personal data, such access is considered a restricted transfer under GDPR. Elestio ensures compliance through the following measures:

Standard Contractual Clauses (SCCs): Elestio has implemented SCCs between its EU and non-EU entities or partners, ensuring GDPR-compliant safeguards for data transfers.
Security and Logging: All access requests are logged, monitored, and reviewed to ensure transparency and compliance.
Encryption & Data Protection: Where applicable, personal data remains encrypted at rest and in transit to minimize risks during support access.

8.3 Customer's Control and Revocation Rights
The Customer retains full control over granting and revoking support access. If the Customer does not explicitly grant access, no Elestio employee—whether inside or outside the EU—can access customer data. The Customer may also request an audit log of access events related to their support tickets.

9. Subprocessors

Elestio is entitled to use Subprocessors for the purposes of providing the Cloud Services under the Agreement. Elestio provides information on its Subprocessors at its Website. The Customer can choose a Subprocessor to provide the hosting for the Cloud Services from the options provided by Elestio. Elestio shall inform the Customer in writing of any intended changes of the hosting service provider Subprocessor at least fourteen (14) days in advance, giving the Customer sufficient time to be able to object to such change. The Customer hereby consents to Elestio's use of Subprocessors as described in this section.

Elestio shall use its commercially reasonable efforts to reasonably ensure that its Subprocessors are subject to equivalent requirements regarding data protection, as set out in this DPA. Elestio remains responsible for its Subprocessors and their compliance with the obligations of this DPA.

10. Transfers of personal data

The Customer may choose where the Cloud Services will be hosted. If the Customer has selected a Subprocessor to provide the hosting within the European Economic Area (''EEA''), Elestio shall store the Personal Data within the EEA and transfers outside the EEA are subject to the Customer's prior approval, instruction or request thereto.

If the Customer selects a Subprocessor to provide the hosting services outside the EEA, the Customer accepts that Elestio; (i) performs the international data transfer of Personal Data in accordance with the Standard Contractual Clauses (processor-to-processor module) entered into by Elestio (as a data exporter) and the Subprocessor (as a data importer) or; (ii) agrees the Subprocessor to carry out the transfer in accordance with the Standard Contractual Clauses (processor-to-processor module) entered into by the Subprocessor group companies (Subprocessor's EEA entity as a data exporter and third country entity as a data importer), as applicable, depending on the Subprocessor the Customer chooses.

The Customer warrants to have used reasonable efforts to determine that the Subprocessor acting as data importer, and chosen by Customer, is able through the implementation of appropriate technical and organisational measures, to satisfy data importer’s obligations under the Standard Contractual Clauses for the transfer to be performed as agreed in this DPA. In the event of discrepancies between the Standard Contractual Clauses and this DPA, the Standard Contractual Clauses prevail.

Notwithstanding the foregoing, the Standard Contractual Clauses will not apply if Elestio has adopted alternative safeguards in accordance with Data Protection Regulation for the lawful transfer of Personal Data outside the EEA.

11. Auditing

At the Customer's written request and the Customer's sole cost and expense, the Customer is entitled, once every twelve (12) months, to audit Elestio's compliance with its obligations under the Data Protection Regulation and this DPA.

The audit report and related information shall at all times be deemed as Elestio's confidential information.

12. Data confidentiality

Elestio will not access or use, have visibility or disclose to any third party, any data that the Customer has input into the Cloud Services, except, if specifically requested in writing by the Customer in order to provide customer-specific support services as requested and instructed by the Customer.

If a governmental body sends Elestio a demand for the data input into the Cloud Services, Elestio will do its best efforts to redirect the governmental body to request that data directly from the Customer. If compelled to disclose Customer Data to a governmental body, then Elestio will only disclose the Personal Data strictly to the extent it is legally required to do so and shall give the Customer reasonable notice of the demand to allow the Customer to seek a protective order or other appropriate remedy unless Elestio is legally prohibited from doing so.

13. Term and termination

This DPA shall become effective in parallel with the Agreement and shall continue in force until the termination of the Agreement or as long as Elestio processes Personal Data on behalf of the Customer.

If not instructed otherwise in writing by the Customer and unless legally required to keep the Personal Data, Elestio shall delete and destroy the Personal Data processed hereunder the latest within ninety (90) days' of the termination of the Agreement or after the maximum data retention period permitted by the technology of the relevant Cloud Service. In case the Customer demands that the Personal Data are returned to the Customer or to a third party, the Customer will pay Elestio for any additional costs and expenses arising out of such return of the Personal Data.

Appendix 1 - Details of processing

This Appendix 1 forms part of this DPA describing the details of personal data to be processed by Elestio.

The Customer has full control of what personal data will be processed by uploading such personal data into the Cloud Services. Elestio has no visibility to such personal data provided and uploaded by the Customer.

Data subjects

- Prospects, customers, business partners, and vendors of the Customer (who are natural persons)
- Employees or contact persons of the Customer’s prospects, customers, business partners and vendors
- Employees, agents, advisors, and freelancers of the Customer (who are natural persons)
- Individuals uthorised by the Customer under the Agreement

Categories of personal data

- Full name
- Title, position
- Email address, address
- Phone number

Special categories of personal data - No special categories of Personal Data are processed.

Subject matter of the processing - Hosting, storing and maintenance for the data Customer has input to the Cloud Services.

For clarity, the Customer is the Data Controller of, and this DPA is only applied to, the Personal Data input to the Cloud Services by Customer.

Appendix 2 - Elestio’s technical and organisational safety measures

This Appendix 2 forms a part of this DPA describing Elestio’s technical and organisational safety measures. Description of the technical and organisational security measures implemented by Elestio. Elestio will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data processed on the Cloud Services as applicable to the specific Cloud Service purchased by the Customer. Elestio must report, in an internal document, to be kept updated and available upon request of the Data Controller or the

Guarantor Authority, the identification details of the natural persons who have been assigned the role of System Administrator, with the list of functions assigned to them.

We maintain ISO 27001 and SOC 2 certifications, demonstrating our commitment to industry-leading security standards. These certifications validate our implementation of robust security controls, ensuring the confidentiality, integrity, and availability of personal data.

In accordance with Article 32 of the GDPR, Elestio implements the following security measures to ensure the protection of Personal Data processed through its Cloud Services.

1. Organisational Security Measures

- **Data Protection Policy:** A documented Data Protection Policy is maintained and regularly reviewed.
- **Security Awareness & Training:** All personnel with access to Personal Data undergo mandatory data protection training upon onboarding and annually thereafter.
- **Access Control & Role-Based Authorization:**
  - Access to Personal Data is restricted to authorized personnel based on the principle of least privilege (PoLP).
  - All access permissions are reviewed periodically.
  - Administrative access is subject to multi-factor authentication (MFA).
- **Third-Party Risk Management:** Subprocessors undergo security risk assessments and contractual safeguards are implemented, including data processing agreements.
- **Incident Response Plan:** A formalized incident response plan is in place, detailing responsibilities, detection, containment, eradication, and recovery steps for data breaches.

2. Physical Security Measures

- **Data Center Security:**
  - Cloud Services are hosted in secure data centers certified with **ISO 27001, SOC 2, and/or equivalent standards**.
  - Physical access to servers is restricted to authorized personnel only, with biometric and keycard access controls.
  - Continuous surveillance (CCTV) and intrusion detection systems are implemented.
- **Workstation Security:** Company workstations are encrypted, password-protected, and locked when unattended.

3. Technical Security Measures

- **Encryption:**
  - Personal Data is encrypted **at rest** using AES-256.
  - Personal Data is encrypted **in transit** using TLS 1.2/1.3.
- **Logging & Monitoring:**
  - Access to Personal Data is logged, monitored, and audited for anomalies.
  - System logs are retained for **12 months**.

- **Data Minimization & Anonymization:**
  - Where applicable, Personal Data is pseudonymized or anonymized to reduce risk.
- **Secure Development & Vulnerability Management:**
  - Regular security audits and penetration testing are conducted.
  - Software updates and patches are applied in a timely manner.

4. Business Continuity & Backup

- **Data Backup & Disaster Recovery:**
  - Backups are performed daily and retained for **180 days**.
  - Disaster recovery procedures are tested at least annually.

5. Data Subject Rights & Compliance Measures

- **Handling of Data Subject Requests:**
  - Procedures are in place to respond to requests for data access, rectification, erasure, and portability.
- **Legal & Compliance Audits:** Elestio undergoes periodic external audits to ensure compliance with GDPR and applicable regulations.

Revision #13
Created 30 November 2022 08:18:03 by Joseph Benguira
Updated 6 February 2025 10:19:37 by Joseph Benguira