

# WEBVIZIO DATA PROCESSING ADDENDUM

Updated 05/01/2023

This Data Processing Addendum (“**DPA**”) supplements the Webvizio Terms of Service available at <https://webvizio.com/documents/webvizio-terms-of-service>, as updated from time to time, between Customer and Webvizio, or other agreement between Customer and Webvizio governing Customer’s use of the Webvizio service (the “**Agreement**”) when the Data Protection Law apply to your use of the Webvizio services (“**Service**”) to process Customer Data. This DPA is an agreement between you and the entity you represent (“**Customer**,” “**you**” or “**your**”) and Webvizio (“**Webvizio**”) under the Agreement. Unless otherwise defined in this DPA or in the Agreement, all capitalised terms used in this DPA will have the meanings given to them in Section 15 of this DPA.

## 1. Data Processing.

1.1 **Scope and Roles.** This DPA applies when Customer Data is processed by Webvizio. In this context, Webvizio will act as processor of Customer Data.

1.2 **Obligations Under Data Protection Laws.** Customer can contact Webvizio to assist it with its obligations under the Data Protection Law, including its obligations to respond to requests from data subjects. Customer confirms that it is unlikely that Webvizio is aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated. However, if Webvizio becomes aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will promptly inform Customer. Webvizio will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Standard Contractual Clauses by providing the Service Controls that Customer can use to erase or rectify Customer Data.

### 1.3 Details of Data Processing.

1.3.1 **Subject matter.** The subject matter of the data processing under this DPA is Customer Data.

1.3.2 **Duration.** As between Webvizio and Customer, the duration of the data processing under this DPA is determined by Customer.

1.3.3 **Purpose.** The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.

1.3.4 **Nature of the processing:** Store and such other Services as described in the Agreement, Documentation and initiated by Customer from time to time.

1.3.5 **Type of Customer Data.** Customer Data uploaded to the Services under Customer’s Webvizio accounts.

1.3.6 **Categories of data subjects.** The data subjects could include Customer



individually, Customer's customers, employees, suppliers and end users.

- 1.4 **Compliance with Webvizio.** Each party will comply with all rules and regulations applicable to it and binding on it in the performance of this DPA, including the Data Protection Law.
2. **Customer Instructions.** The parties agree that this DPA and the Agreement (including Customer providing instructions via configuration tools such as the Webvizio App settings made available by Webvizio as a part of the Services) constitute Customer's documented instructions regarding Webvizio's processing of Customer Data ("**Customer Instructions**"). Webvizio will process Customer Data only in accordance with Customer Instructions (which if Customer is acting as a processor, could be based on the instructions of its controllers). Additional instructions outside the scope of the Customer Instructions (if any) require prior written agreement between Webvizio and Customer, including agreement on any additional fees payable by Customer to Webvizio for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if Webvizio declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA. If Webvizio forms such an opinion, it will immediately inform Customer, in which case, Customer is entitled to withdraw or modify its Customer Instructions.
3. **Confidentiality of Customer Data.** Webvizio will not access or use, or disclose to any third party Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body including a subpoena or court order. If a governmental body sends Webvizio a demand for Customer Data, Webvizio will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, Webvizio may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then Webvizio will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Webvizio is legally prohibited from doing so. Webvizio restricts its personnel from processing Customer Data without authorisation by Webvizio as described in the Webvizio Security Standards as described in Attachment 1. Webvizio imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.
4. **Security of Data Processing**
  - 4.1 Webvizio has implemented and will maintain the technical and organisational measures for the Webvizio Network as follows:
    - (a) security of the Webvizio Network as set out in Attachment 1 of the Webvizio Security Standards;
    - (b) physical security of the facilities as set out in Attachment of the Webvizio Security Standards;

- (c) measures to control access rights for Webvizio employees and contractors to the Webvizio Network as set out in Attachment 1, of the Webvizio Security Standards; and
  - (d) processes for regularly testing and evaluating the effectiveness of the technical and organizational measures as described in Attachment 1 of the Webvizio Security Standards.
- 4.2 Customer can elect to implement the following technical and organizational measures to protect Customer Data as made available by Webvizio or a third party supplier:
- (a) pseudonymisation and encryption;
  - (b) measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are operated by Customer;
  - (c) measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident.

## 5. Sub-processing.

- 5.1 **Authorised Sub-processors.** Customer provides general authorisation to Webvizio's use of sub-processors to provide processing activities on Customer Data on behalf of Customer ("**Sub-processors**") in accordance with this Section. The Webvizio website [lists Sub-processors](#) that are currently engaged by Webvizio. At least 30 days before Webvizio engages a Sub-processor, Webvizio will update the applicable website and provide Customer with a mechanism to obtain notice of that update. To object to a Sub-processor, Customer can: (i) terminate the Agreement pursuant to its terms; or (ii) cease using the Service for which Webvizio has engaged the Sub-processor.
- 5.2 **Sub-processor Obligations.** Where Webvizio authorises a Sub-processor as described in Section 5.1:
- (i) Webvizio will restrict the Sub-processor's access to Customer Data only to what is necessary to provide or maintain the Services in accordance with the Documentation, and Webvizio will prohibit the Sub-processor from accessing Customer Data for any other purpose;
  - (ii) Webvizio will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services provided by Webvizio under this DPA, Webvizio will impose on the Sub-processor the same contractual obligations that Webvizio has under this DPA; and
  - (iii) Webvizio will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the

Sub-processor that cause Webvizio to breach any of Webvizio's obligations under this DPA.

6. **Webvizio Assistance with Data Subject Requests.** Taking into account the nature of the processing, the Service Controls are the technical and organizational measures by which Webvizio will assist Customer in fulfilling Customer's obligations to respond to data subjects' requests under the Data Protection Law. If a data subject makes a request to Webvizio, Webvizio will promptly forward such request to Customer once Webvizio has identified that the request is from a data subject for whom Customer is responsible. Customer authorises on its behalf, and on behalf of its controllers when Customer is acting as a processor, Webvizio to respond to any data subject who makes a request to Webvizio, to confirm that Webvizio has forwarded the request to Customer. The parties agree that Customer's use of the Service Controls and Webvizio forwarding data subjects' requests to Customer in accordance with this section, represent the scope and extent of Webvizio's required assistance.
7. **Optional Security Features.** Webvizio makes available many Service Controls that Customer can elect to use. Customer is responsible for (a) implementing the measures described in Section 4.2, as appropriate, (b) properly configuring the Services, (c) using the Service Controls to allow Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident (for example backups and routine archiving of Customer Data), and (d) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorised access and measures to control access rights to Customer Data.
8. **Security Incident Notification.**
  - 8.1 **Security Incident.** Webvizio will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and (b) take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident.
  - 8.2 **Webvizio Assistance.** To enable Customer to notify a Security Incident to supervisory authorities or data subjects (as applicable), Webvizio will cooperate with and assist Customer by including in the notification under Section 8.1(a) such information about the Security Incident as Webvizio is able to disclose to Customer, taking into account the nature of the processing, the information available to Webvizio, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Security Incident.
  - 8.3 **Unsuccessful Security Incidents.** Customer agrees that:

- (i) an Unsuccessful Security Incident will not be subject to this Section 8. An **“Unsuccessful Security Incident”** is one that results in no unauthorised access to Customer Data or to any of Webvizio’s equipment or facilities storing Customer Data, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers) or similar incidents; and
- (ii) Webvizio’s obligation to report or respond to a Security Incident under this Section 8 is not and will not be construed as an acknowledgement by Webvizio of any fault or liability of Webvizio with respect to the Security Incident.

8.4 **Communication.** Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer’s administrators by any means Webvizio selects, including via email. It is Customer’s sole responsibility to ensure Customer’s administrators maintain accurate contact information in the Webvizio App settings and secure transmission at all times.

## 9. Audits.

9.1 **Customer Audits.** If Customer chooses to conduct any GDPR-related audit, including any inspection of adequacy of its security measures of Webvizio Network, it has the right to request or mandate on its own behalf (and on behalf of its controllers when Customer is acting as a processor, under the GDPR or the Standard Contractual Clauses) that Webvizio carries out such audit. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending Webvizio written notice as provided for in the Agreement. If Webvizio declines to follow any instruction requested by Customer regarding audits, including inspections, Customer is entitled to terminate the Agreement in accordance with its terms.

9.2 **Privacy Impact Assessment.** Subject to parties executing a non-disclosure agreement, and taking into account the nature of the processing and the information available to Webvizio, Webvizio will assist Customer in complying with Customer’s obligations in respect of data protection impact assessments and relevant prior consultation, by providing the information that is available to Webvizio and that does not violate Webvizio’s confidentiality or privacy obligations to third parties.

## 10. Transfers of Personal Data.

10.1 **Application of Standard Contractual Clauses.** The Standard Contractual Clauses will only apply to Customer Data that is transferred, either directly or via onward transfer, to any Third Country, (each a **“Data Transfer”**).



- 10.1.1 When Customer is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.
- 10.1.2 When Customer is acting as a processor, the Processor-to-Processor Clauses will apply to a Data Transfer. Taking into account the nature of the processing, Customer agrees that it is unlikely that Webvizio will know the identity of Customer's controllers because Webvizio has no direct relationship with Customer's controllers and therefore, Customer will fulfil Webvizio's obligations to Customer's controllers under the Processor-to-Processor Clauses.
- 10.2 **Alternative Transfer Mechanism.** The Standard Contractual Clauses will not apply to a Data Transfer if Webvizio has adopted Binding Corporate Rules for Processors or an alternative recognised compliance standard for lawful Data Transfers.

11. **Termination of the DPA.** This DPA will continue in force until the termination of the Agreement (the “**Termination Date**”).
12. **Return or Deletion of Customer Data.** At any time up to the Termination Date, and for 90 days following the Termination Date, subject to the terms and conditions of the Agreement, Webvizio will return or delete Customer Data when Customer uses the Service Controls to request such return or deletion. No later than the end of this 90-day period, Customer will close all Webvizio accounts containing Customer Data.
13. **Duties to Inform.** If Webvizio receives a legal notice that Customer Data is subject to bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by Webvizio, Webvizio will inform Customer without undue delay. Webvizio will, without undue delay, notify all relevant parties in such action (for example, creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer’s property and responsibility and that Customer Data is at Customer’s sole disposition.
14. **Entire Agreement; Conflict.** This DPA incorporates the Standard Contractual Clauses by reference. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control. Nothing in this document varies or modifies the Standard Contractual Clauses.
15. **Definitions.** Unless otherwise defined in the Agreement, all capitalised terms used in this DPA will have the meanings given to them below:
  - “**Controller**” has the meaning given to it in the Data Protection Law.
  - “**Controller-to-Processor Clauses**” means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at [this link](#).
  - “**Customer Data**” means the “personal data” (as defined in the Data Protection Laws) that is uploaded to the Services and/or Webvizio Network under Customer’s Webvizio accounts.
  - “**Data Protection Law(s)**” means all laws and regulations applicable to the Processing of Customer Data under the Agreement, including, as applicable, the laws and regulations of the United States, the European Union, the EEA and their member states, Switzerland and the United Kingdom, including as applicable the General Data Protection Regulation (EU) 2016/679 (“Data Protection Law”), and the California Consumer Privacy Act of 2018 (“CCPA”) as amended.
  - “**EEA**” means the European Economic Area.
  - “**Processing**” has the meaning given to it in the applicable Data Protection Law.
  - “**Processor**” has the meaning given to it in the applicable Data Protection Law.





**“Processor-to-Processor Clauses”** means the standard contractual clauses between processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at [this link](#).

**“Security Incident”** means a breach of Webvizio’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

**“Service Controls”** means the controls, including security features and functionalities, that the Services provide, as described in the Documentation.

**“Standard Contractual Clauses”** means (i) the Controller-to-Processor Clauses, or (ii) the Processor- to-Processor Clauses, as applicable in accordance with Sections 10.1.1 and 10.1.2.

**“Third Country”** means a country outside the EEA not recognised by the European Commission as providing an adequate level of protection for personal data (as described in the Data Protection Law).

**“Webvizio Network”** means Webvizio’s data center facilities, servers, networking equipment, and host software systems (for example, virtual firewalls) that are within Webvizio’s control and are used to provide the Services.

**“Webvizio Security Standards”** means the security standards attached to this DPA as Attachment 1.



## Attachment 1

### Webvizio Security Standards

**Information Security Program.** Webvizio will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the Webvizio Network, and (c) minimise security risks, including through risk assessment and regular testing. Webvizio will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

- 1.1 **Continued Evaluation.** Webvizio will conduct periodic reviews of the security of its Webvizio Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. Webvizio will continually evaluate the security of its Webvizio Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.
- 1.2 **Network Security.** The Webvizio Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. Webvizio will maintain access controls and policies to manage what access is allowed to the Webvizio Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Webvizio will maintain corrective action and incident response plans to respond to potential security threats.
- 1.3 **Physical Security**
  - 1.3.1 **Physical Access Controls.** Physical components of the Webvizio Network are housed in nondescript facilities (the “**Facilities**”).
  - 1.3.2 **Limited Employee and Contractor Access.** Webvizio provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee or contractor of Webvizio or its affiliates.
  - 1.3.3 **Physical Security Protections.** All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. Webvizio also maintains electronic intrusion detection systems designed to detect unauthorised access to



the Facilities, including monitoring points of vulnerability (for example, primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.