Data Processing Agreement

Last update: November 3, 2026

This Data Processing Agreement (the “DPA”) supplements the Terms of Service concluded between you (“Client”, “you”, “your”) and Upgrade Parade Corp, a Florida corporation operating the WebinOne platform, (“WebinOne”, “Company”, “we”, “us”, “our”) for provision of WebinOne and TeamOne Services, and/or is incorporated into the other written or electronic agreement between us regarding the provision of WebinOne Services (including the service level agreement). The Terms of Service and/or the other agreement between us regarding the provision of WebinOne Services (depending on which is applicable) are referred to as the “Agreement” for the purposes of this DPA. In the event of any conflict or inconsistency between any of the terms of the Agreement, the provisions of DPA shall prevail.

This DPA governs the processing of Personal Data that the Client provides to WebinOne in connection with the provision of WebinOne Services or any Personal Data that WebinOne obtains in connection with the performance of the Services. Further in this text, you and we individually are referred to as a “Party” and collectively as the “Parties”. For the purpose of ensuring compliance with the Data Protection Laws and Regulations, the Parties have entered into this DPA, which forms an integral part of the Agreement.

1. Definitions

“Standard Contractual Clauses (“SCCs”)” means Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

“General Data Protection Regulation (“GDPR”)” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

“Controller”, “processor”, “data subject”, “personal data”, and “processing” have the meanings given in the GDPR and Other Data Protection Laws and Regulations.

“Client Data” means personal data that the Client, acting as a data controller, provides to WebinOne, acting as a data processor, in connection with the services offered by WebinOne and requested by the Client, or any other personal data for which the Client is a data controller and the Company is a data processor, including personal data that the Client processes as a processor on behalf of its own customer.

“Other Data Protection Laws and Regulations” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, the United

Kingdom, the United States, and its states, applicable to the processing of personal data, such as the UK and US Data Protection Laws, or other applicable laws and regulations.

“Subprocessor” means any entity that provides processing services to WebinOne in furtherance of WebinOne’s processing on behalf of the Client or the respective data controller.

“Public Authority” means a government agency or law enforcement authority, including judicial authorities.

“Supervisory Authority” means an independent public authority to be responsible for monitoring the application of data protection legislation.

2. Roles

The Client acknowledges and agrees that with regard to data processing under this DPA, the Client and WebinOne have the roles under the GDPR and the Other Data Protection Laws and Regulations specified in this Section of the DPA. This DPA shall not apply to situations where WebinOne acts as a controller in accordance with our Privacy Policy.

When WebinOne processes the Client Data provided by the Client or to which it may otherwise have access under this DPA (for example, data about the Client’s customers, end users, etc.), WebinOne acts as a data processor, and the Client acts as a data controller under the GDPR and the Other Data Protection Laws and Regulations.

Where the Client processes Client Data on behalf of its own customer (for example, as a Platform User providing the Services to its Clients), the Client acts as a processor and WebinOne acts as the Client's sub-processor. In that case, the Client warrants that its instructions, including the engagement of WebinOne, have been authorized by the relevant controller, and WebinOne's obligations under this DPA apply equally for the benefit of that controller.

3. Instructions

The Parties agree that this DPA and the Agreement between the Parties (including Terms of Service and any other agreements that the Parties have entered into based on Terms of Service) constitute the Client’s complete and final documented instructions regarding the processing of the Client Data on the Client’s behalf (the “Instructions”), where the Client acts as a data controller, and WebinOne acts as a data processor under the GDPR and Other Data Protection Laws and Regulations. Any additional or alternate instructions must be consistent with the Terms of Service of this DPA and the Agreement between the Parties.

4. Obligations

4.1. WebinOne Obligations

4.1.1. When acting as a data processor

4.1.1.1. General Obligations

With regard to the processing of the Client Data, WebinOne shall:

(i) process the Client Data only for established purposes, using appropriate technical and organizational security measures, and in compliance with the instructions received from the Client subject to Section 3 of this DPA;

(ii) inform the Client if WebinOne cannot comply with its obligations under this DPA, in which case the Client may terminate the agreement between the Parties or take any other reasonable actions, including suspending data processing operations;

(iii) inform the Client if, at WebinOne's discretion, the Client's Instruction may be in violation of the provisions of the GDPR or Other Data Protection Laws and Regulations;

(iv) follow the Client's instructions regarding the collection of the Client Data (including with regard to the provision of notice and exercise of choice) in case WebinOne is obtaining the Client Data from data subjects on behalf of the Client under the agreement between the Parties;

(v) take reasonable steps to ensure that any subprocessor to whom WebinOne authorizes access to the Client Data on its behalf complies with respective provisions of the Agreement between the Parties and this DPA;

(vi) make available to the Client all information necessary to demonstrate compliance with WebinOne's obligations under this DPA, the GDPR, and Other Data Protection Laws and Regulations.

4.1.1.2. Notices to the Client.

Upon becoming aware, WebinOne shall inform the Client of any legally binding request for disclosure of the Client Data by a Public Authority, unless WebinOne is otherwise forbidden by law to inform the Client, for instance, to preserve the confidentiality of investigation by a Public Authority. WebinOne will inform the Client if it becomes aware of any notice, inquiry, or investigation by a Supervisory Authority with respect to the processing of the Client Data under this DPA or the Agreement.

4.1.1.3. Security Measures.

WebinOne shall implement and maintain appropriate technical and organizational measures to protect the Client Data from personal data breaches (the "Security Incidents") in accordance with WebinOne's security standards set out in Schedule 2 of this DPA. The Client acknowledges that security measures are subject to technical progress so that WebinOne may modify or update Schedule 2 at its discretion, provided that such modification or update does not result in a material degradation in the security measures offered by Schedule 2 of this DPA at the time of signing this DPA.

4.1.1.4. Security Incident.

Upon becoming aware of a Security Incident, WebinOne shall:

(i) notify the Client by email without undue delay, and in any event within forty-eight (48) hours, after it becomes aware of a Security Incident affecting Client Data;

(ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by the Client, including the nature of the Security Incident, the categories and approximate number of data subjects and personal data records concerned (where possible), the likely consequences, measures taken or proposed to be taken by the Client to address the Security Incident (including, where appropriate, measures to mitigate its possible adverse effects), and the contact details of WebinOne's privacy contact (privacy@webinone.com) where more information can be obtained;

(iii) promptly take reasonable steps to contain and investigate any Security Incident so that the Client can notify competent authorities and/or affected data subjects of the Security Incident. WebinOne’s notification of or response to a Security Incident shall not be construed as an acknowledgment by WebinOne of any fault or liability regarding the Security Incident.

4.1.1.5. Confidentiality.

WebinOne will not access, use, or disclose to any third party any Client Data, except, in each case, as necessary to maintain or as necessary to comply with contractual and legal obligations or binding order of a public body (such as a subpoena or court order). WebinOne shall ensure that any employee/contractor to whom it authorizes access to the Client Data on its behalf (if applicable) is subject to appropriate confidentiality contractual or statutory duty obligations with respect to the Client Data, including after the end of their respective employment or termination or expiration of the contract.

4.1.1.6. Return or Deletion of the Client Data.

At the choice of the Client, WebinOne shall, and shall cause any subprocessors to, delete or return all the personal data to the Client after the end of the provision of services relating to processing and delete existing copies, unless the GDPR or Other Data Protection Laws and Regulations (whichever is applicable) require the storage of the personal data.
The Client can permanently delete Client Data at any time using the site administration tools; Client Data deleted in this way is removed from WebinOne's production systems immediately. Where the Client deletes a site without first deleting its Client Data, or creates a backup of a site, the site backup, including any Client Data it contains, is retained for up to six (6) months so the site can be restored, and is then permanently deleted. On the Client's written request, WebinOne will delete such a backup earlier. In addition, WebinOne takes daily infrastructure backups, which are retained for thirty (30) days and then permanently deleted; Client Data deleted from production systems or site backups therefore no longer exists in any WebinOne backup after thirty (30) days. If the Client's subscription ends, the site and its Client Data are deleted thirty (30) days after the end of the subscription. A backup of the site is then retained for up to one hundred eighty (180) days so the site can be restored, and is then permanently deleted. On the Client's written request, WebinOne will delete it earlier.

4.1.1.7. Reasonable Assistance.

WebinOne agreed to provide reasonable assistance to the Client regarding:

(i) any request from a data subject in respect of access to or the rectification, erasure, restriction, portability, blocking, or deletion of the Client Data that WebinOne processes on behalf of the Client. If a data subject sends such a request directly to WebinOne, Section 5 of this DPA shall apply;

(ii) the investigation of Security Incidents and communication of necessary notifications regarding such Security Incidents subject to Section 4.1.1.4 of this DPA;

(iii) preparation of data protection impact assessments and, where necessary, consultation of the Client with the Supervisory Authority under Articles 35 and 36 of the GDPR.

4.1.1.8. Audit and Certification.

4.1.1.8.1. Supervisory Authority Audit.

If a Supervisory Authority requires an audit of the data processing facilities from which WebinOne processes the Client Data to ascertain or monitor the Client's compliance with the GDPR or Other Data Protection Laws and Regulations, WebinOne will cooperate with such audit. The Client is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any time WebinOne expends for any such audit, in addition to the costs for services performed by WebinOne.

4.1.1.8.2. Audits.

The Client may, prior to the commencement of processing and at regular intervals after that, audit the technical and organizational measures taken by the Company. If the Client is the controller with respect to the personal data processed by the Company on its behalf, upon reasonable and timely advance agreement, during regular business hours and without interruption to the Company's business operations, the Company may provide the Client with all information necessary to demonstrate compliance with its obligations laid down in the Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client with respect to such processing.

The Company shall, upon the Client's written request and within a reasonable period, provide the Client with all information necessary for such audit, to the extent that such information is within the Company's control and the Company is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

4.2. Client's Obligations

4.2.1. When acting as a data controller

Within the scope of the DPA, the Client, as a data controller, shall be responsible for complying with all requirements that apply to the Client as a data controller under the GDPR and Other Data Protection Laws and Regulations. The Client represents and warrants that the Client shall be responsible for:

(i) the accuracy, quality, integrity, confidentiality, and security of collected Client Data;

(ii) complying with all necessary transparency, lawfulness, fairness, and other requirements under GDPR and Other Data Protection Laws and Regulations for the collection and use of personal data by:

1. establishing and maintaining the procedure for the exercise of the rights of the data subjects whose personal data are processed on behalf of the Client;
2. providing WebinOne only with personal data that has been lawfully and validly obtained and ensuring that such personal data will be relevant and proportionate to the respective uses;
3. ensuring compliance with the provisions of this DPA and the Agreement by the Client's personnel or by any third party accessing or using the Client Data on the Client's behalf.

(iii) ensuring that the Client's Instructions to WebinOne regarding the processing of the Client Data comply with the GDPR and Other Data Protection Laws and Regulations, including complying with principles of data minimization, purpose, and storage limitation; and

(iv) complying with all applicable laws, rules, and regulations (including the GDPR and Other Data Protection Laws and Regulations) in respect to any Instructions the Client issues to WebinOne.

5. Data Subject Request

If a data subject contacts WebinOne with regard to the exercise of their rights under the GDPR and Other Data Protection Laws and Regulations (in particular, requests for access to, rectification, or blocking of the Client Data), WebinOne shall notify the Client of such request.

WebinOne, as a data processor, will make all reasonable efforts to forward such requests to the Client and provide assistance where and to the extent necessary to comply with the requirements of the GDPR and Other Data Protection Laws and Regulations.

If WebinOne is legally required or authorized by the Client to respond to such a request, it shall immediately notify the Client and provide the Client with a copy of the request unless WebinOne is legally prohibited from doing so.

6. Subprocessors

The Client agrees that WebinOne may engage Subprocessors to fulfill our obligations regarding the provision of WebinOne Services under the Agreement. The current list of Subprocessors is set forth below in Schedule 3 of this DPA.

If authorization for the engagement of Subprocessors is required by applicable Data Protection Laws and Regulations, the Client hereby grants WebinOne prior, general authorization to engage Subprocessors for processing personal data, provided that WebinOne enters into a data processing agreement with each Subprocessor containing data protection obligations relevant to the nature of the processing provided by such Subprocessor no less protective than those in this DPA.

WebinOne will notify the Client at least thirty (30) days before a new Subprocessor begins processing Client Data, by email to the Client's account contact and by updating Schedule 3. The Client may object in writing within that period. If the Parties cannot resolve the objection in good faith, the Client may terminate the affected Services.

7. Applicable Law

The law applicable to this DPA is specified in the Agreement between WebinOne and the Client unless otherwise required by the GDPR or Other Data Protection Laws and Regulations.

8. Data Transfers

8.1. Transfers of the Client Data

The Parties agree that when the processing of the Client Data constitutes a transfer from the Client as a data controller or processor to WebinOne as a data processor under the GDPR and Other Data Protection Laws and Regulations and appropriate safeguards are required, such processing will be subject to the Standard Contractual Clauses which are deemed to be incorporated into and form part of this DPA as further described in subsections 8.1.1. of this DPA. If and to the extent the EU SCCs conflict with any provision of the DPA, the EU SCCs shall prevail to the extent of such conflict.

8.1.1. Transfers under GDPR

When the processing of the Client Data constitutes a “transfer” under the GDPR and in other cases under this DPA, Module Two of the EU SCCs shall apply. Where the Client acts as a processor on behalf of its own customer, Module Three of the EU SCCs shall apply.

For the purpose of Module Two of the EU SCCs, the Client is a “data exporter”, and WebinOne is a “data importer”.

The relevant provisions in the EU SCCs are incorporated by reference herein and remain an integral part of this DPA. Clauses and annexes of the EU SCCs deemed to be completed are as follows:

1. in Clause 7, the optional docking clause shall not apply;
2. in Clause 9, Option 2 (General Written Authorisation) shall apply. For the purpose of Clause 9(a), the time period for informing the data exporter in advance of any intended changes to the sub-processors list through the addition or replacement of sub-processors shall be 30 days;
3. in Clause 11, the optional provision shall not apply;
4. in Clause 13, the following rules must apply:
    1. where the Client is established in an EU Member State, the Supervisory Authority with responsibility for ensuring compliance by the data exporter with the GDPR as regards the data transfer shall act as competent Supervisory Authority;

2. where the Client is not established in an EU Member State but falls within the territorial scope of application of the GDPR, in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR, the Supervisory Authority of the Member State in which the representative is established shall act as competent Supervisory Authority;
3. where the Client is not established in an EU Member State but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without however having to appoint a representative, 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, shall act as competent Supervisory Authority;

5. in Clause 17, Option 1 shall apply. The Parties agree that the governing law shall be the law of the Republic of Ireland.
6. In Clause 18(b), disputes shall be resolved by the courts of the EU Member State which law applies to this Agreement under Option 1 of Clause 17 as provided hereabove;
7. Annex I of the EU SCCs is deemed completed with the information set out in Schedule 1 of this DPA;
8. Annex II of the EU SCCs is deemed completed with the information set out in Schedule 2 of this DPA;

9. DPA Duration

This DPA shall remain in effect until the Agreement between the Parties is terminated.

SCHEDULE 1 - DESCRIPTION OF PROCESSING

1. LIST OF PARTIES

Data exporter

Name: Client, also referred to as “you” in the DPA and Terms of Service.

Address: the relevant information is contained in the Agreement and payment processing documentation.

Contact person’s name, position and contact details: the relevant information is contained in the Agreement and payment processing documentation.

Activities relevant to the data transferred under these Clauses: data processing in the context of the provision of services by WebinOne to the Client, such as website hosting, content management, CRM, email marketing, e-commerce and AI-assisted site editing (AgentOne) under the Agreement between the Parties.

Signature and date: By entering into the Agreement, the data exporter is deemed to have signed the EU SCCs incorporated herein, including Annexes, as of the effective date of the Agreement.

Role: controller, or processor where the Client acts on behalf of its own customer.

Data importer

Name: Upgrade Parade Corp (WebinOne)

Address: 4107 Tamiami Trail, PO Box 112, South Venice, FL 34293, USA

Contact person's name, position and contact details: Oleksii Iagolnyk, CEO, privacy@webinone.com.

Activities relevant to the data transferred under these Clauses: data processing in the context of the provision of services by WebinOne to the Client, such as website hosting, content management, CRM, email marketing, e-commerce and AI-assisted site editing (AgentOne) under the Agreement between the Parties.

Signature and date: By entering into the Agreement, the data importer is deemed to have signed the EU SCCs incorporated herein, including Annexes, as of the effective date of the Agreement.

Role: processor.

2. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred:
    1. Clients, potential clients, employees and contractors of the Client, Client representatives, and other persons engaged by the Client in the processing of personal data;
    2. other data subjects whose personal data is provided by the Client.
2. Categories of personal data transferred:
    1. personal data of visitors, form submitters, registered members, customers and newsletter recipients of the Client's sites, such as names, contact details, account credentials (stored hashed), order history, form submissions, IP addresses and technical logs;
    2. any other personal data the Client provides and instructs WebinOne to process under the Terms of Service and other agreements between the Parties.
3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved: the data importer does not knowingly request to obtain access to the special categories of data (sensitive data) unless the Client provides and instructs Webinone to process such data. The data importer takes technical and organizational measures, included in Schedule 2, to protect personal data, including sensitive personal data, if any is transferred.
4. The frequency of the transfer: the personal data is transferred on a continuous basis.
5. Nature of the processing:
    1. collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, alignment or combination, restriction, erasure or destruction to the extent necessary to comply with the Terms of Service and any other agreements the Parties have entered into;
    2. performing any other lawful data processing activities that the Client has instructed WebinOne to perform.

6. Purpose(s) of the data transfer and further processing: the main purpose of the data transfer and further processing is to provide the services by the data importer to the data exporter based on the Terms of Service and any other agreements the Parties have entered into.
7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: the personal data shall be stored for the duration of service(s) provided under the Terms of Service and any other agreements the Parties have entered into unless otherwise agreed in writing, this DPA, and legal obligations imposed on the data importer or data exporter, provided that the data exporter has instructed the data importer to act in accordance with such legal obligation.
8. For transfers to (sub-) processors, also specify subject-matter, nature, and duration of the processing:
    1. subject-matter: the performance of services necessary for the performance of services based on Terms of Service or any other agreements between the Client and WebinOne;
    2. nature: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, alignment or combination, restriction, erasure or destruction to the extent necessary for the performance of services based on Terms of Service or any other agreements between the Client and WebinOne;
    3. duration: the performance of the services for the data importer by the subprocessor under the service agreement concluded between the data importer and such subprocessor.

3. COMPETENT SUPERVISORY AUTHORITY

In accordance with Clause 13, the competent supervisory authority under these Clauses is the Supervisory Authority specified under the rules provided in the DPA.

SCHEDULE 2 - TECHNICAL AND ORGANIZATIONAL MEASURES

TECHNICAL AND ORGANIZATIONAL MEASURES, INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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

1. Hosting and data location: Client sites, databases, backups and logs for sites hosted in the EU are stored in AWS eu-central-1 (Frankfurt, Germany). No content delivery network is used, and data is not replicated to other regions. Emails are sent via Amazon SES in AWS us-west-2 (Oregon, USA).
2. Encryption: all data in transit is encrypted with TLS (HTTPS is enforced on all sites, with automatically renewed certificates). Data at rest is encrypted using AWS EBS encryption.
3. Access control: access to production systems and Client Data is limited to a small number of authorized personnel, granted individually on a least-privilege basis. Shared credentials are stored in a company password manager.

4. Network security: AWS Virtual Private Cloud, security groups and access control lists restrict network access to production systems.
5. Logging: AWS CloudTrail activity logging is enabled. AgentOne AI request logs are retained for 30 days.
6. Backups and availability: daily infrastructure backups are retained for 30 days. Site backups are retained as described in Section 4.1.1.6.
7. Personnel: everyone with access to Client Data is bound by written confidentiality and data-protection obligations. Access is revoked when a person leaves.
8. Incident response: Clients are notified without undue delay, and in any event within 48 hours of WebinOne becoming aware of a Security Incident affecting their data, by a status message sent by email and by posting the incident report in the WebinOne Partners Slack channel.

Technical and organizational measures to be taken by the (sub-)processor to be able to provide assistance to the controller and, for transfers from a processor to a subprocessor, to the data exporter, will include the following:

1. the transfer of personal data to a third party (the (sub-)processor) is only made if a corresponding contract exists and only for specific purposes;
2. such a contract shall contain the same or similar security measures as specified in Schedule 2, and the subprocessor shall provide a level of protection of personal data that is not lesser than the one provided under this DPA;
3. the data importer ensures that an adequate level of data protection exists at the target location and(or) organization in accordance with the European Union's data protection requirements, e.g. by employing agreements based on the EU SCCs.

SCHEDULE 3 - LIST OF SUBPROCESSORS

To deliver the WebinOne Services, WebinOne may use the following Subprocessors to process Client Data.

Subprocessor	Purpose	Location	Contact	Transfer mechanism
Amazon Web Services, Inc. (EC2, EBS, S3)	Hosting, storage and backups of Client sites and Client Data.	The AWS region in which the Client's site is hosted. For sites hosted in the EU: eu-central-1, Frankfurt, Germany.	410 Terry Avenue North, Seattle, WA 98109-5210, USA 1-888-280-4331 cs-reply@amazon.com	Amazon Data Processing Agreement, incorporating the EU Standard Contractual Clauses
Amazon Web Services, Inc. (Amazon SES)	Sending emails, including workflows, autoresponders and system emails.	AWS region us-west-2 (Oregon, USA), for all sites.	410 Terry Avenue North, Seattle, WA 98109-5210, USA 1-888-280-4331 cs-reply@amazon.com	Amazon Data Processing Agreement, incorporating the EU Standard Contractual Clauses

Subprocessor	Purpose	Location	Contact	Transfer mechanism
Amazon Web Services, Inc. (Amazon Bedrock)	AI features of AgentOne, when AgentOne is enabled for a site.	Requests are sent from eu-central-1 (Frankfurt, Germany) and processed within AWS regions in the European Union.	410 Terry Avenue North, Seattle, WA 98109-5210, USA 1-888-280-4331 cs-reply@amazon.com	Amazon Data Processing Agreement, incorporating the EU Standard Contractual Clauses

Third-party integrations

The Client may connect its sites to third-party services of its own choice (for example, Mailchimp or Zapier) through the WebinOne API or integrations. Such services are engaged by the Client, not by WebinOne; they are not Subprocessors of WebinOne, and the Client is responsible for its agreements with them and for any personal data it shares with them.