Product Addendum: Meta CAPI Gateway

This Product Addendum (“Addendum”) governs the use of the TAGGRS Meta Conversions API Gateway service (the “Product”). This Addendum is entered into by and between TAGGRS B.V. (“TAGGRS”) and the Client and supplements the TAGGRS General Terms of Service (“Terms”).

By using this Product, the Client agrees to be bound by this Addendum, the Terms, the Processor Agreement (Annex 1), and the Service Level Agreement (Annex 2).

In the event of a conflict between this Addendum and the General Terms of Service, the provisions of this Addendum shall prevail with respect to the use of this specific Product.

1. The Product
1.1. TAGGRS provides a software solution that acts as a Meta Conversions API Gateway (the "Product"). Through this software, event data can be securely and reliably sent from the Client's domain directly to Meta's servers.
1.2. The Client can create a CAPI Gateway endpoint through the TAGGRS dashboard. This endpoint is used to receive event data from the Client's website and forward it to Meta.

2. Fees
2.1. The Client shall pay TAGGRS a fee (the “Fee”) for the use of the Product, based on the subscription package selected by the Client. Each package includes a specific allowance for both the number of unique Meta Pixels connected to the CAPI Gateway and the total number of events processed monthly.
2.2. Standard pricing is published on the TAGGRS CAPI Gateway page (https://taggrs.io/meta-capi-gateway-hosting). If a custom pricing arrangement applies, it will be specified in a separate quotation provided by TAGGRS.
2.3. TAGGRS is entitled to unilaterally change the Fee at any time due to fluctuations in server costs.TAGGRS shall inform the Client of these changes in the Fee.

3. Free Accounts
3.1. For free accounts, any Gateway with fewer than 100 requests per month for two consecutive months will be marked as inactive and disconnected from the platform.
3.2. Inactive Gateways may be reactivated by the Client via the dashboard, which extends their active status for another two months.
3.3. If no reactivation occurs, the inactive Gateway will be soft-deleted after an additional two months and permanently hard-deleted after a further four months. TAGGRS will provide email notifications throughout this process.

4. Client Obligations and Responsibilities
4.1. The Client shall provide and maintain the necessary sound hardware on which the Product can be used.
4.2. Without prior written consent from TAGGRS, the Client shall not:
    a. Make any changes to the Product.
    b. Transfer the Product to third parties, whether under a (sub)license or otherwise.
    c. Provide any other party with access to the Product.
4.3. The Client shall indemnify TAGGRS against all claims, demands, damages, costs, and fines from third parties if the Client fails to comply with this Addendum, the Terms, or the Processor Agreement. The Client shall reimburse TAGGRS for all related costs, including legal fees. The indemnity shall not apply to the extent the claim arises from TAGGRS’ breach of this Addendum, the Terms, or applicable law.

4.4. If the Client fails to comply with any obligation under this Article 4, the Client shall be liable to TAGGRS for a penalty equal to the total Fee payable by the Client for a period of one (1) year. This penalty is due after a 10-day cure period and is without prejudice to TAGGRS's right to claim further damages.

5. Service Discontinuation
5.1. Upon the termination or expiration date of the agreement, the Client's right to use the Product will be discontinued. The Client is aware that the Product will no longer be functional.

6. Annexes
The following annexes are an integral part of this Addendum:
Annex 1: Processor Agreement
Annex 2: Service Level Agreement (SLA)

Annex 1: Processor Agreement

This Processor Agreement is entered into by and between TAGGRS B.V. (the “Processor”) and the Client (the “Controller”) and is an annex to the Product Addendum for the Meta CAPI Gateway. It supplements the TAGGRS General Terms of Service (the “Terms”).

Introduction
A. The Controller wishes to use the services of the Processor and has for that purpose accepted the Terms and the applicable Product Addendum (collectively the “Agreement”).
B. In performing the Agreement, the Processor processes personal data on behalf of the Controller.
C. The Parties wish to set forth in writing the terms for the processing of personal data so that both Parties can comply with their respective obligations under the General Data Protection Regulation (GDPR).
D. This Processor Agreement supersedes any previous processor agreements of a similar scope between the Parties.

1. Definitions
The capitalized terms in this Processor Agreement shall have the meanings ascribed to them below or as defined in the GDPR.

Agreement	The combination of the TAGGRS General Terms of Service and the applicable Product Addendum(s) agreed to by the Parties.
Controller	The natural person or legal entity who creates an account on the TAGGRS platform, also referred to as “Client”
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.
Data Subject	The identified or identifiable natural person to whom the Personal Data relates.
European Economic Area (EEA)	All countries of the European Union, plus Liechtenstein, Norway, and Iceland.
GDPR	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 its implementing law.
Personal Data	Any information relating to an identified or identifiable natural person as defined by the General Data Protection Regulation (GDPR)
Processing	Any operation or set of operations which is performed on Personal Data.
Processor	TAGGRS B.V., having its registered office in Heerenveen, Netherlands
Sub-processor	Any non-subordinate third party engaged by the Processor to process Personal Data under the Agreement.

Supervisory Authority	The Dutch Data Protection Authority (Autoriteit Persoonsgegevens) or another relevant supervisory authority under the GDPR.

2. Subject of this Agreement
2.1. This Processor Agreement applies to all Processing of Personal Data carried out by the Processor on behalf of the Controller under the Agreement.
2.2. The Controller is the ‘data controller’ and the Processor is the ‘data processor’ within the meaning of the GDPR.

3. Processing of Personal Data
3.1. The Processor shall only process Personal Data based on the written instructions from the Controller, including the instructions documented in this Processor Agreement and its Attachment 1.
3.2. The Controller warrants that the Personal Data provided for Processing is accurate and that its instructions for the Processing of Personal Data will comply with the GDPR and other applicable laws. The Controller is solely responsible for the lawfulness of the Processing.
3.3. The specific Personal Data to be processed, the categories of Data Subjects, and the nature and purposes of the Processing are detailed in Attachment 1 to this Processor Agreement.
3.4. The Processor shall assist the Controller, where reasonably possible, in complying with its obligations under the GDPR, such as responding to Data Subject requests and conducting data protection impact assessments.
3.5. The Processor shall primarily process Personal Data within the European Economic Area (EEA).

4. Duration
This Processor Agreement shall remain in effect for as long as the Processor processes Personal Data on behalf of the Controller under the Agreement.

5. Security Measures
The Processor shall implement and maintain appropriate technical and organizational measures to protect Personal Data against destruction, loss, alteration, unauthorized access, or any form of unlawful processing, as further detailed on the security page of the Processor's website (https://taggrs.io/security/).

6. Audits
The Controller has the right, once per calendar year, to audit the Processor's compliance with this Processor Agreement. The costs of such an audit shall be borne by the Controller, unless the audit reveals a material breach by the Processor, in which case the Processor will reimburse the costs related to identifying the breach.The Controller is required to provide at least one week’s notice before the audit.

7. Data Breach Notification
7.1. In the event of a Data Breach, the Processor shall notify the Controller without unreasonable delay after becoming aware of it.
7.2. The notification will, where possible, include the nature of the breach, the categories of Personal Data affected, the likely consequences, and the measures taken or proposed to be taken to address the breach.
7.3. The Controller is solely responsible for assessing whether a Data Breach needs to be reported to the Supervisory Authority and/or the affected Data Subjects.

8. Confidentiality
The Processor is obligated to keep the Personal Data provided by the Controller confidential. All employees of the Processor involved in the Processing are bound by a duty of confidentiality.

9. Sub-processors
9.1. The Controller hereby grants the Processor general written authorization to engage Sub-processors to perform the Processing.
9.2. A current list of Sub-processors is included in Attachment 1. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-processors, giving the Controller an opportunity to object.
9.3. When engaging a Sub-processor, the Processor shall impose on that Sub-processor the same data protection obligations as set out in this Processor Agreement.

10. Liability
10.1. The liability of the Processor arising from any breach of this Processor Agreement is limited in accordance with the liability article in the General Terms of Service.
10.2. The Controller shall be liable to the Processor for any damages incurred as a result of the Controller's failure to comply with this Processor Agreement, the GDPR, or other applicable privacy laws.
10.3. The Controller shall indemnify the Processor against all claims, fines, and penalties from third parties, Data Subjects, or a Supervisory Authority resulting from the Controller's failure to comply with its legal or contractual obligations.

11. Return and Destruction of Data
Upon termination of the Agreement, the Processor shall, at the choice of the Controller, either return all Personal Data to the Controller or delete it. This will occur within 30 days of termination, unless statutory retention periods require otherwise.

12. Governing Law and Forum
The governing law and competent court for any disputes arising from this Processor Agreement are those specified in the General Terms of Service.

Attachment 1: Details of Processing & Sub-processors

This attachment contains an overview of the personal data processed by the Processor on behalf of the Controller. Within this overview, there are two categories of sub-processors: hosting providers and other sub-processors.

Brief description of services	Nature of processing	Type of personal data	People involved	Purposes of processing	Sub-processors	Retention period
Providing a direct and secure gateway to send conversion data to Meta without technical setup.	Receiving, processing, and forwarding event data from the client's server-side setup to Meta's Conversions API.	Name, contact details, date of birth, gender, IP address, location data, device data, browsing behavior, preferences (Only the data depending on the (self) configured setup.)	Website visitors / app users of the Client.	To securely transmit tracking data to Meta for improved ad campaign tracking, attribution, and optimization.	- Meta - Google cloud	No data stored
Use of supporting tools for communication, customer management, and email marketing.	Processing includes communication, customer contact, invoicing, support, and email sending	Name, contact details, communication data, payment data, user data, preferences	Employees	The purpose of these sub-processors is to support internal operational processes such as customer service, sales, billing, and automation.	- Front - Klaviyo - Zapier - HubSpot - Stripe	1 year

Annex 2: Service Level Agreement (SLA)

This Service Level Agreement (“SLA”) is an annex to the Product Addendum for the Meta CAPI Gateway and details the service levels applicable to the Product.

1. Definitions
Capitalized words and expressions in this SLA have the meanings ascribed to them below.

Availability	The total time during which the Product was actually available to the Client, expressed as a percentage of the total time in the Service Period.
Incident	A failure of the Product to perform in accordance with its specifications.
Office Hours	Monday through Friday from 08:30 to 17:00 (Dutch time), with the exception of recognized public holidays in the Netherlands.
Priority Level	The priority assigned to an Incident by TAGGRS, based on its impact and urgency.
Report	Any notification submitted by the Client via the TAGGRS customer support channels about a possible Incident.
Response Time	The length of time between a Report being received by TAGGRS and TAGGRS notifying the Client that the Report is being processed.
Follow-up Time	The time between TAGGRS's acknowledgement of a Report and the implementation of a remedy or workaround.
Service Desk	TAGGRS's central point of contact for the Client to submit Reports.
Service Period	The time period over which Availability is measured and reported on by TAGGRS (typically monthly).

2. Availability
2.1. TAGGRS strives to achieve the highest possible Availability for the Product. If TAGGRS does not achieve the guaranteed Availability of 99.85%, it shall credit the fees charged for the Product for that month in accordance with the following table:

Availability	Credit rate
Between 95.00% and 99.85%	25%
Between 90.00% and 94.99%	50%
Lower than 90.00%	100%

2.2. Credits will only be applied to the monthly fees for the Product and not to any implementation or other one-time costs.

2.3. The Client's right to receive a credit as described in this article is the sole and exclusive remedy for any failure by TAGGRS to meet its Availability commitment.

3. Service Desk
3.1. TAGGRS will provide support for Incidents through a Service Desk, accessible via the "customer support" channels on its website (taggrs.io).
3.2. The Service Desk is available during Office Hours. Reports submitted outside of Office Hours will be handled by TAGGRS during the next period of Office Hours.

4. Priority Levels
The follow-up on an Incident depends on the Priority Level assigned to it by TAGGRS.

Priority level	Meaning
Priority 1	Complete failure of the Service
Priority 2	Data problems or unavailability of core functions
Priority 3	Individual components of the Service do not work.

5. Incident Management
5.1. TAGGRS will use its best efforts to adhere to the following Response Times and Follow-up Times for Incidents, measured during Office Hours.

Priority level	Response time	Follow-up time
Priority 1	Within 2 hours	Within 8 hours
Priority 2	Within 4 hours	Within 2 working days
Priority 3	Within 8 hours	Within 5 working days

5.2. TAGGRS has met the Response Time if, within the specified time, the Client has been informed of TAGGRS's proposed remedy or next steps. The stated Follow-up Times are dependent on the Client providing all necessary information for resolving the Incident.

6. Reporting
TAGGRS shall ensure the accurate and accessible recording of results under this SLA. The live status and historical uptime can be found at status.taggrs.io.

7. Availability Exclusions
The following events are not included in the calculation of Availability:

a. Any downtime caused by force majeure events, including government interventions, widespread internet failures, or sabotage of the Product by third parties.
b. Any downtime resulting from pre-announced maintenance work.