

Product Addendum: Meta CAPI Gateway

Dit Product Addendum (“Addendum”) regelt het gebruik van de TAGGRS Meta Conversions API Gateway dienst (het “Product”). Dit Addendum wordt aangegaan tussen TAGGRS B.V. (“TAGGRS”) en de Klant en vormt een aanvulling op de TAGGRS Algemene Servicevoorwaarden (“Voorwaarden”).

Door gebruik te maken van dit Product gaat de Klant akkoord met dit Addendum, de Voorwaarden, de Verwerkersovereenkomst (Bijlage 1) en de Service Level Agreement (Bijlage 2).

In geval van strijdigheid tussen dit Addendum en de Algemene Servicevoorwaarden prevaleren de bepalingen van dit Addendum voor het gebruik van dit specifieke Product.

1. Het Product

1.1. TAGGRS biedt een softwareoplossing die fungeert als een Meta Conversions API Gateway (het “Product”). Met deze software kan event data veilig en betrouwbaar rechtstreeks vanaf het domein van de Klant naar de servers van Meta worden verzonden.

1.2. De Klant kan via het TAGGRS-dashboard een CAPI Gateway-endpoint aanmaken. Dit endpoint wordt gebruikt om event data van de website van de Klant te ontvangen en door te sturen naar Meta.

2. Vergoedingen

2.1. De Klant betaalt aan TAGGRS een vergoeding (de “Vergoeding”) voor het gebruik van het Product, op basis van het door de Klant gekozen abonnementspakket. Elk pakket bevat een specifieke limiet voor zowel het aantal unieke Meta Pixels dat is gekoppeld aan de CAPI Gateway als het totale aantal maandelijks verwerkte events.

2.2. De standaardprijspakketten zijn gepubliceerd op de TAGGRS CAPI Gateway-pagina (<https://taggrs.io/meta-capi-gateway-hosting>). Indien er een maatwerk prijsafspraken van toepassing is, wordt deze vermeld in een afzonderlijke offerte die door TAGGRS wordt verstrekt.

2.3. TAGGRS is gerechtigd de Vergoeding eenzijdig aan te passen indien er sprake is van fluctuaties in serverkosten. TAGGRS zal de Klant informeren over dergelijke wijzigingen in de Vergoeding.

3. Gratis Accounts

3.1. Voor gratis accounts geldt dat elke Gateway met minder dan 100 requests per maand gedurende twee opeenvolgende maanden als inactief wordt aangemerkt en wordt losgekoppeld van het platform.

3.2. Inactieve Gateways kunnen door de Klant via het dashboard opnieuw worden geactiveerd, waarmee de actieve status met nog eens twee maanden wordt verlengd.

3.3. Indien er geen heractivatie plaatsvindt, wordt de inactieve Gateway na twee extra maanden tijdelijk verwijderd en na vier maanden permanent verwijderd. TAGGRS zal tijdens dit proces per e-mail meldingen verstrekken aan de Klant.

4. Verplichtingen en Verantwoordelijkheden van de Klant

4.1. De Klant is verantwoordelijk voor het leveren en onderhouden van de benodigde deugdelijke hardware waarop het Product kan worden gebruikt.

4.2. Zonder voorafgaande schriftelijke toestemming van TAGGRS zal de Klant niet:

- a. Wijzigingen aanbrengen in het Product.
- b. Het Product overdragen aan derden, hetzij via een (sub)licentie of anderszins.
- c. Enige andere partij toegang verlenen tot het Product.

4.3. De Klant vrijwaart TAGGRS van en tegen alle aanspraken, vorderingen, schade, kosten en boetes van derden indien de Klant dit Addendum, de Voorwaarden of de Verwerkersovereenkomst niet naleeft. De Klant zal TAGGRS alle daarmee samenhangende kosten vergoeden, waaronder redelijke juridische kosten. Deze vrijwaring is niet van toepassing voor zover de aanspraak voortvloeit uit een schending door TAGGRS van dit Addendum, de Voorwaarden of toepasselijke wetgeving.

4.4. Indien de Klant enige verplichting uit dit Artikel 4 niet naleeft, is de Klant aan TAGGRS een boete verschuldigd gelijk aan de totale Vergoeding die de Klant verschuldigd zou zijn voor een periode van één (1) jaar. Deze boete wordt opeisbaar na een hersteltermijn van tien (10) dagen en laat het recht van TAGGRS om aanvullende schadevergoeding te vorderen onverlet.

5. Beëindiging van de Dienst

5.1. Na beëindiging of afloop van de overeenkomst vervalt het recht van de Klant om het Product te gebruiken. De Klant is zich ervan bewust dat het Product na beëindiging niet langer functioneel zal zijn.

6. Bijlagen

De volgende bijlagen vormen een integraal onderdeel van dit Addendum:

Annex 1: Verwerkersovereenkomst

Annex 2: Service Level Agreement (SLA)

Annex 1: Verwerkersovereenkomst

Deze Verwerkersovereenkomst wordt gesloten tussen TAGGRS B.V. (de “Verwerker”) en de Klant (de “Verwerkingsverantwoordelijke”) en vormt een bijlage bij het Product Addendum voor de Meta CAPI Gateway. Deze overeenkomst vormt een aanvulling op de Algemene Servicevoorwaarden van TAGGRS (de “Voorwaarden”).

Inleiding

- A. De Verwerkingsverantwoordelijke wenst gebruik te maken van de diensten van de Verwerker en heeft daartoe de Voorwaarden en het toepasselijke Product Addendum aanvaard (gezamenlijk de “Overeenkomst”).
- B. Bij de uitvoering van de Overeenkomst verwerkt de Verwerker Persoonsgegevens namens de Verwerkingsverantwoordelijke.
- C. Partijen wensen de voorwaarden voor de verwerking van Persoonsgegevens schriftelijk vast te leggen zodat beide Partijen kunnen voldoen aan hun verplichtingen onder de Algemene Verordening Gegevensbescherming (AVG).
- D. Deze Verwerkersovereenkomst vervangt alle eerdere verwerkersovereenkomsten van vergelijkbare strekking tussen Partijen.

1. Definities

De met een hoofdletter geschreven termen in deze Verwerkersovereenkomst hebben de hieronder vermelde betekenis of, indien van toepassing, de betekenis zoals gedefinieerd in de AVG.

Overeenkomst	De combinatie van de TAGGRS Algemene Servicevoorwaarden en het toepasselijke Product Addendum of Addenda die door Partijen zijn overeengekomen.
Verwerkingsverantwoordelijke	De natuurlijke persoon of rechtspersoon die een account aanmaakt op het TAGGRS-platform, ook wel aangeduid als “Klant”
Datalek	Een inbreuk op de beveiliging die leidt tot de toevallige of onrechtmatige vernietiging, het verlies, de wijziging, of de ongeoorloofde openbaarmaking van, of toegang tot, Persoonsgegevens die zijn verzonden, opgeslagen of anderszins verwerkt.
Betrokkene	De geïdentificeerde of identificeerbare natuurlijke persoon op wie de Persoonsgegevens betrekking hebben.
Europese Economische Ruimte (EER)	Alle landen van de Europese Unie, plus Liechtenstein, Noorwegen en IJsland.
AVG	Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, inclusief de implementatiewetgeving.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon zoals gedefinieerd in de AVG

Verwerking	Elke bewerking of elk geheel van bewerkingen dat wordt uitgevoerd op Persoonsgegevens.
Verwerker	TAGGRS B.V., statutair gevestigd te Heerenveen, Nederland
Subverwerker	Elke niet-ondergeschikte derde partij die door de Verwerker wordt ingeschakeld om Persoonsgegevens te verwerken onder de Overeenkomst.
Toezichthoudende Autoriteit	De Autoriteit Persoonsgegevens of een andere relevante toezichthoudende autoriteit krachtens de AVG.

2. Onderwerp van deze Overeenkomst

2.1. Deze Verwerkersovereenkomst is van toepassing op alle Verwerkingen van Persoonsgegevens die door de Verwerker namens de Verwerkingsverantwoordelijke worden uitgevoerd op grond van de Overeenkomst.

2.2. De Verwerkingsverantwoordelijke is de “data controller” en de Verwerker is de “data processor” in de zin van de AVG.

3. Verwerking van Persoonsgegevens

3.1. De Verwerker zal Persoonsgegevens uitsluitend verwerken op basis van schriftelijke instructies van de Verwerkingsverantwoordelijke, inclusief de instructies die zijn vastgelegd in deze Verwerkersovereenkomst en in Bijlage 1.

3.2. De Verwerkingsverantwoordelijke garandeert dat de voor Verwerking aangeleverde Persoonsgegevens juist zijn en dat de instructies met betrekking tot de Verwerking van Persoonsgegevens voldoen aan de AVG en overige toepasselijke wet- en regelgeving. De Verwerkingsverantwoordelijke is als enige verantwoordelijk voor de rechtmatigheid van de Verwerking.

3.3. De specifieke Persoonsgegevens die worden verwerkt, de categorieën van betrokkenen, en de aard en doeleinden van de Verwerking zijn beschreven in Bijlage 1 van deze Verwerkersovereenkomst.

3.4. De Verwerker zal de Verwerkingsverantwoordelijke, waar redelijkerwijs mogelijk, bijstaan bij het nakomen van diens verplichtingen onder de AVG, waaronder het afhandelen van verzoeken van betrokkenen en het uitvoeren van gegevensbeschermingseffectbeoordelingen (DPIA's).

3.5. De Verwerker zal Persoonsgegevens in beginsel uitsluitend verwerken binnen de Europese Economische Ruimte (EER).

4. Duur

Deze Verwerkersovereenkomst blijft van kracht zolang de Verwerker Persoonsgegevens verwerkt namens de Verwerkingsverantwoordelijke op grond van de Overeenkomst.

5. Beveiligingsmaatregelen

De Verwerker zal passende technische en organisatorische maatregelen treffen en handhaven om Persoonsgegevens te beschermen tegen vernietiging, verlies, wijziging, ongeoorloofde toegang of enige andere vorm van onrechtmatige verwerking, zoals nader omschreven op de beveiligingspagina van de website van de Verwerker (<https://taggrs.io/security/>).

6. Audits

De Verwerkingsverantwoordelijke heeft het recht om éénmaal per kalenderjaar een audit uit te voeren om de naleving van deze Verwerkersovereenkomst door de Verwerker te controleren. De kosten van een dergelijke audit komen voor rekening van de Verwerkingsverantwoordelijke, tenzij uit de audit

blijkt dat sprake is van een wezenlijke schending door de Verwerker. In dat geval zal de Verwerker de kosten die verband houden met het vaststellen van de schending vergoeden. De Verwerkingsverantwoordelijke dient ten minste één (1) week vooraf schriftelijk kennis te geven van de voorgenomen audit.

7. Melding van Datalekken

7.1. In het geval van een Datalek zal de Verwerker de Verwerkingsverantwoordelijke zonder onredelijke vertraging op de hoogte stellen zodra hij hiervan kennis heeft genomen.

7.2. De melding zal, voor zover mogelijk, de aard van het Datalek bevatten, de categorieën van getroffen Persoonsgegevens, de waarschijnlijke gevolgen, en de genomen of voorgenomen maatregelen om het Datalek aan te pakken.

7.3. De Verwerkingsverantwoordelijke is als enige verantwoordelijk voor het beoordelen of een Datalek moet worden gemeld aan de Toezichhoudende Autoriteit en/of aan de getroffen Betrokkenen.

8. Vertrouwelijkheid

De Verwerker is verplicht om de door de Verwerkingsverantwoordelijke verstrekte Persoonsgegevens vertrouwelijk te behandelen. Alle werknemers van de Verwerker die betrokken zijn bij de Verwerking zijn gebonden aan een geheimhoudingsplicht.

9. Subverwerkers

9.1. De Verwerkingsverantwoordelijke verleent de Verwerker hierbij een algemene schriftelijke toestemming om Subverwerkers in te schakelen voor de uitvoering van de Verwerking.

9.2. Een actuele lijst van Subverwerkers is opgenomen in Bijlage 1. De Verwerker zal de Verwerkingsverantwoordelijke informeren over voorgenomen wijzigingen met betrekking tot de toevoeging of vervanging van Subverwerkers, waarbij de Verwerkingsverantwoordelijke de mogelijkheid krijgt om bezwaar te maken.

9.3. Wanneer de Verwerker een Subverwerker inschakelt, legt de Verwerker aan die Subverwerker dezelfde verplichtingen inzake gegevensbescherming op als opgenomen in deze Verwerkersovereenkomst..

10. Aansprakelijkheid

10.1. De aansprakelijkheid van de Verwerker die voortvloeit uit enige schending van deze Verwerkersovereenkomst is beperkt overeenkomstig het aansprakelijkheidsartikel in de Algemene Servicevoorwaarden.

10.2. De Verwerkingsverantwoordelijke is aansprakelijk jegens de Verwerker voor alle schade die voortvloeit uit het niet-naleven van deze Verwerkersovereenkomst, de AVG of andere toepasselijke privacywetgeving door de Verwerkingsverantwoordelijke.

10.3. De Verwerkingsverantwoordelijke vrijwaart de Verwerker tegen alle aanspraken, boetes en sancties van derden, Betrokkenen of een Toezichhoudende Autoriteit die voortvloeien uit het niet-naleven van wettelijke of contractuele verplichtingen door de Verwerkingsverantwoordelijke.

11. Teruggave en verwijdering van Gegevens

Na beëindiging van de Overeenkomst zal de Verwerker, naar keuze van de Verwerkingsverantwoordelijke, alle Persoonsgegevens aan de Verwerkingsverantwoordelijke retourneren of verwijderen. Dit zal plaatsvinden binnen dertig (30) dagen na beëindiging, tenzij wettelijke bewaartermijnen anders vereisen.

12. Toepasselijk recht en forumkeuze

Het op deze Verwerkersovereenkomst toepasselijke recht en de bevoegde rechter zijn dezelfde als vermeld in de Algemene Servicevoorwaarden.

Bijlage 1 Subverwerkers CAPI Gateway

Deze bijlage bevat een overzicht van de persoonsgegevens die door de Verwerker namens de Verwerkingsverantwoordelijke worden verwerkt. Binnen dit overzicht zijn er twee categorieën Subverwerkers: hostingproviders en overige Subverwerkers.

Omschrijving diensten	Aard van de verwerking	Soort persoonsgegevens	Categorieën van betrokkenen	Doeleinden van de verwerking	Subverwerkers	Bewaartermijnen
Het aanbieden van een directe en veilige gateway om event data naar Meta te verzenden zonder technische setup.	Het ontvangen, verwerken en doorsturen van event data vanuit de server-side setup van de Klant naar Meta's Conversions API.	Naam, contactgegevens, geboortedatum, geslacht, IP-adres, locatiegegevens, apparaatgegevens, surfgedrag, voorkeuren (alleen de data die afhankelijk is van de (zelf) ingestelde setup).	Websitebezoekers / app-gebruikers van de Klant.	Het veilig doorgeven van tracking-data aan Meta ten behoeve van verbeterde advertentie-tracking, attributie en optimalisatie.	Meta / Google Cloud	Geen data opgeslagen
Gebruik van ondersteunende tools voor communicatie, klantenbeheer en e-mailmarketing.	Verwerking omvat communicatie, klantcontact, facturatie, ondersteuning en e-mailverzending	Naam, contactgegevens, communicatiegegevens, betalingsgegevens, gebruikersgegevens, voorkeuren	Werknemers	Het doel van deze subverwerkers is het ondersteunen van interne operationele processen zoals klantenservice, verkoop, facturering en automatisering.	- Front - Klaviyo - Zapier - HubSpot - Stripe	1 jaar

Annex 2: Service Level Agreement (SLA)

Deze Service Level Agreement (“SLA”) is een bijlage bij het Product Addendum voor de Meta CAPI Gateway en beschrijft de serviceniveaus die van toepassing zijn op het Product.

1. Definities

In deze SLA hebben met een hoofdletter geschreven termen de onderstaande betekenis.

Beschikbaarheid	De totale tijd waarin het Product daadwerkelijk beschikbaar was voor de Klant, uitgedrukt als een percentage van de totale tijd binnen de Serviceperiode.
Incident	Een storing waardoor het Product niet presteert in overeenstemming met zijn specificaties.
Kantooruren	Maandag tot en met vrijdag van 08:30 tot 17:00 uur (Nederlandse tijd), met uitzondering van algemeen erkende feestdagen in Nederland.
Prioriteitsniveau	De prioriteit die door TAGGRS wordt toegekend aan een Incident, gebaseerd op de impact en urgentie ervan.
Melding	Een melding die door de Klant wordt ingediend via de TAGGERS-klantenservice met betrekking tot een mogelijk Incident.
Responstijd	De tijd tussen het ontvangen van een Melding door TAGGRS en het moment waarop TAGGRS de Klant informeert dat de Melding in behandeling is genomen.
Hersteltijd	The time between TAGGRS's acknowledgement of a Report and the implementation of a remedy or workaround.
Service Desk	Het centrale aanspreekpunt van TAGGRS waar de Klant Meldingen kan indienen.
Serviceperiode	De periode waarover de Beschikbaarheid wordt gemeten en gerapporteerd door TAGGRS (meestal maandelijks).

2. Beschikbaarheid

2.1. TAGGRS streeft naar de hoogst mogelijke Beschikbaarheid van het Product. Indien TAGGRS de gegarandeerde Beschikbaarheid van 99,85% niet behaalt, zal TAGGRS een krediet toekennen op de vergoedingen die in die maand in rekening zijn gebracht, overeenkomstig onderstaande tabel:

Beschikbaarheid	Crediteringspercentage
Tussen 95.00% en 99.85%	25%
Tussen 90.00% en 94.99%	50%
Lager dan 90.00%	100%

2.2. Kredieten worden uitsluitend toegepast op de maandelijkse vergoedingen voor het Product en niet op implementatiekosten of andere eenmalige kosten

2.3. Het recht van de Klant op het ontvangen van een krediet zoals beschreven in dit artikel vormt de enige en exclusieve remedie bij het niet behalen van de Beschikbaarheids verplichting door TAGGRS.

3. Servicedesk

3.1. TAGGRS biedt ondersteuning bij Incidents via de Servicedesk, die bereikbaar is via de “customer support”-kanalen op de website van TAGGRS (taggrs.io).

3.2. De Servicedesk is beschikbaar tijdens de Kantooruren. Meldingen die buiten de Kantooruren worden ingediend, worden door TAGGRS opgepakt tijdens de eerstvolgende Kantooruren.

4. Priority Levels

De opvolging van een Incident is afhankelijk van het Prioriteitsniveau dat door TAGGRS wordt toegewezen.

Prioriteitsniveau	Betekenis
Prioriteit 1	Volledige uitval van de dienst.
Prioriteit 2	Dataproblemen of onbeschikbaarheid van kernfunctionaliteiten.
Prioriteit 3	Individuele onderdelen van de dienst functioneren niet naar behoren.

5. Incidentbeheer

5.1. TAGGRS zal zich inspannen om de volgende Responstijden en Hersteltijden voor Incidents na te leven, gemeten tijdens Kantooruren.

Priority level	Response time	Follow-up time
Prioriteit 1	Binnen 2 uur	Binnen 8 uur
Prioriteit 2	Binnen 4 uur	Binnen 2 werkdagen
Prioriteit 3	Binnen 8 uur	Binnen 5 werkdagen

5.2. TAGGRS heeft aan de Responstijd voldaan indien de Klant binnen de genoemde tijd is geïnformeerd over de voorgestelde oplossing of vervolgstappen van TAGGRS. De genoemde Hersteltijden zijn afhankelijk van de tijdige aanlevering van alle noodzakelijke informatie door de Klant voor het oplossen van het Incident.

6. Reporting

TAGGRS zorgt voor een correcte en toegankelijke registratie van de resultaten binnen deze SLA. De actuele status en historische uptime zijn beschikbaar op status.taggrs.io.

7. Availability Exclusions

De volgende gebeurtenissen worden **niet** meegenomen in de berekening van de Beschikbaarheid:

- a. Tijdelijke onbeschikbaarheid veroorzaakt door overmacht, waaronder overheidsingrijpen, grootschalige internet storingen of sabotage van het Product door derden.
- b. Tijdelijke onbeschikbaarheid als gevolg van vooraf aangekondigd onderhoud.