WPML

Auftragsverarbeitungsvertrag (DPA)

This Agreement (the "**DPA**") is dated at the earliest date on which we began providing the Services to you (the "Commencement Date"), and supplements our Terms and Conditions (henceforth the "**Terms**") and our Privacy Policy (henceforth the "**Privacy Policy**"), as updated from time to time between you and us, or other agreement governing your use of the Services (altogether with the DPA, the Terms and the Privacy Policy, the "**Agreement**"). This DPA is an agreement between you and the entity you represent ("Customer", "you" or "your") and OnTheGoSystems Limited ("**we**," "**us**," or "**our**") under the Agreement.

THE PARTIES AGREE AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

1.1. The definitions below will have the following meaning:

"**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" (including the derivatives "**Processed**" and "**Process**") and "**Processor**", have the meanings given in the GDPR or, where relevant, the meaning of the essentially equivalent terms in other applicable Data Protection Laws;

"**Data Protection Laws**" means any applicable law relating to the Processing, privacy, and use of Personal Data including: (i) the GDPR; (ii) the UK GDPR; (iii) any laws that implement, replace, extend, re-enact, consolidate, or amend any of the foregoing laws; (iv) any corresponding national laws or regulations; and (v) corresponding guidance, codes or certification mechanisms of the relevant regulatory authority regarding such laws;

"**(Your) Personal Data**" means Personal Data provided or made available to us by (or collected or created for) you in connection with this Agreement.

1.2. All capitalised words not referred to in the above clause 1.1 will have the meaning and definition given to them in either the Privacy Policy or the Terms and Conditions.

1.3. Reference to laws includes subordinate legislation and means that law as amended or re-enacted from time to time.

1.4. In the event of any inconsistencies, overlaps or redundancies between this DPA and the Terms or the Privacy Policy, the terms set out in this DPA shall prevail in all cases.

1.5. Where the Processing of your Personal Data is subject to the GDPR, a reference to a "legal obligation" in this Agreement means an obligation pursuant to European Union or Member State law.

2. PROCESSING OF YOUR PERSONAL DATA

2.1 For the purposes of this Agreement, You act as the Controller and We act as the Processor with respect to the Processing of Personal Data described in Appendix 1, unless otherwise expressly stated. We shall Process Personal Data only (1) as provided for in this DPA, the Terms and/or the Agreement, (2) as required by applicable legal obligations, in which case We shall inform You of that legal requirement unless prohibited by law, or (3) on documented instructions from You. If We are required by applicable law to Process Personal Data other than on Your instructions, We shall inform You of that legal requirement before Processing, unless prohibited by law from doing so. The subject matter, duration, nature and purpose of Processing, the types of Personal Data, and categories of Data Subjects are set out in Appendix 1. No special categories of Personal Data will be Processed without Your prior written approval.

2.2 The parties acknowledge that, in addition to Processing Personal Data as a Processor on Your behalf, We may process certain Personal Data as an independent Controller for the following limited purposes: (i)

management and administration of Your account, (ii) billing and payment processing, (iii) compliance with legal and regulatory obligations applicable to Us, and (iv) internal service administration, security, fraud prevention, service monitoring, product analytics, product improvement, and service development. Such processing is carried out in accordance with our Privacy Policy and applicable Data Protection Laws, and falls outside the scope of this DPA.

2.3 We will only Process Your Personal Data in accordance with this Agreement as necessary to provide the Services.

2.4 We shall: (i) comply with and Process all Your Personal Data in accordance with applicable Data Protection Laws; (ii) co-operate and assist the Customer with any data protection impact assessments and consultations with (or notifications to) or responding to questions from or investigations by regulators or supervisory authorities; (iii) ensure that its policies, measures and procedures meet, perform, and comply with the Data Protection Laws and will ensure that it has all necessary appropriate measures to make sure the data processing is being performed based on a legal basis and that it seeks consents, where necessary, and makes sure all the required notices are in place to enable the lawful transfer of Your Personal Data to any third party recipient for the duration and purposes of this Agreement, and (iv) process Personal Data only insofar as provided for in clause 2.1 above. We shall regularly review the notices and policies and keep them up to date, where necessary, to ensure that the information requirements are met and that any changes are communicated to data subjects in an immediate manner.

2.5 You shall: (i) guarantee that the processing commissioned under this Agreement, and the sharing of personal data involved, is carried out in strict compliance with applicable Data Protection Laws; (ii) deliver Your Personal Data to us; (iii) ensure, prior to and throughout the processing, that we comply with Data Protection Laws; (iv) supervise the processing, including carrying out inspections, audits or consultation; (v) reciprocally comply with the obligations set out in this Agreement insofar as applicable, and (vi) any other obligations arising from current and applicable legislation.

3. OUR PERSONNEL

3.1 We shall ensure that our personnel are subject to an appropriate contractual or statutory duty of confidentiality in relation to Your Personal Data.

3.2 We shall cease Processing Your Personal Data when it is no longer necessary to provide the Services unless retention is required by applicable law. Upon termination or expiry, and at Your option, We shall delete or return Your Personal Data within thirty (30) days of Your written request. Where deletion is required, We shall take reasonable steps to securely delete such Personal Data, including from backups, in accordance with our retention practices. In any case, deletion or return of Your Personal Data shall be subject and conditional to applicable legal obligations to Us that may restrict our capacity to do so. Any Personal Data retained pursuant to such legal obligations shall remain subject to the protections of this Agreement.

3.3 We shall ensure that any personnel authorized to process Your Personal Data are subject to appropriate confidentiality obligations and shall process such Personal Data only as necessary to provide the Services.

4. SECURITY

4.1. The Parties warrant they have implemented and shall maintain appropriate technical and organisational measures to protect Your Personal Data against a Personal Data Breach, which shall at all times satisfy, at a minimum, the standards required by Data Protection Laws.

4.2. We shall ensure that we have in place appropriate technical and organisational security measures, as described in Appendix 2, to protect Your Personal Data against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might

result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it.

5. NOTIFICATION AND PERSONAL DATA BREACHES

5.1. If we receive any complaint, claim, or request in relation to the Processing of Your Personal Data (particularly those relating to the exercise of Data Subject rights under applicable laws), we shall, without undue delay, forward such to you and cooperate and assist you with responding to such as directed by you.

5.2 If we become aware of any Personal Data Breach, we shall without undue delay (and in any event within 36 hours) notify you, investigate the Personal Data Breach, remediate/mitigate any damage and prevent re-occurrence (providing you with detailed related information throughout), and cooperate in informing the relevant supervisory authorities or affected Data Subjects.

5.3 We shall, taking into account the nature of the Processing, assist You by appropriate technical and organisational measures, insofar as this is possible, in fulfilling Your obligation to respond to requests for exercising Data Subject rights under applicable Data Protection Laws, including rights of access, rectification, erasure, restriction, portability, and objection. We shall notify You of any such request without undue delay and in any event within five (5) business days of receipt, and shall provide reasonable cooperation to enable You to respond within the timeframes required by applicable Data Protection Laws.

6. SUBCONTRACTORS

6.1 You provide a general authorization for Us to engage subprocessors to process Your Personal Data in connection with the Services.

6.2 We shall ensure that any subprocessor is bound by written obligations that provide at least the same level of protection for Your Personal Data as those set out in this DPA.

6.3 We shall remain liable to You for the performance of any subprocessor and for any acts or omissions of such subprocessor in relation to the Processing of Your Personal Data as Our own, in the terms of this DPA and the Agreement.

6.4 We may update the list of subprocessors from time to time. Any intended addition or replacement of subprocessors shall be notified by updating the applicable subprocessor list or privacy notice made available through the Services or our website. You may object to such changes on reasonable grounds related to data protection within fourteen (14) days of such update. If You raise a reasonable objection and We cannot reasonably accommodate such objection, either Party may terminate the affected Services in accordance with the Agreement.

7. TRANSFERS OF DATA

7.1. We (or any subcontractor) shall only transfer Your Personal Data to a country outside the EEA or an international organisation where such transfer is subject to appropriate safeguards and otherwise complies with Data Protection Laws.

7.2. Where such transfers are made, We shall implement appropriate safeguards, including the use of standard contractual clauses adopted by the European Commission (including Commission Implementing Decision (EU) 2021/914), or other valid transfer mechanisms under applicable Data Protection Laws.

8. RECORDS

8.1 We shall make available to You all information reasonably necessary to demonstrate compliance with this Agreement and applicable Data Protection Laws, and shall allow for and contribute to audits conducted by

You or an independent auditor, subject to reasonable prior notice and confidentiality obligations.

8.2 We may satisfy such obligations by providing relevant certifications, reports, or other independent assessments.

9. TERM AND TERMINATION

9.1. This Agreement shall start on the Commencement Date and shall continue indefinitely unless terminated by either of the parties in accordance with the terms of our collaboration and any obligations relating to the Services.

9.2. The Confidentiality under section 10 of this Agreement shall survive termination or expiry of this Agreement and continue indefinitely.

10. CONFIDENTIALITY

The Parties shall not disclose, without the prior, written consent of the other party, any information disclosed or made available, in any form or medium, directly or indirectly before or after the date of this Agreement, in connection with the processing as well as the information relating to the business Services, financial plans, intellectual property rights, clients, suppliers, employees, plans; the know-how, designs, trade secrets, technical information or software; any other information which each of us wishes to protect against unrestricted disclosure and which is marked as confidential or proprietary or is, by its nature, clearly confidential; and any findings, data or analysis derived from such information, unless it is required to be disclosed in a judicial or administrative proceeding or required to be disclosed by law. In such case Parties shall inform each other in advance to perform any necessary legal precautions to ensure information is protected within the scope of mandatory disclosure.

11.INDEMNITY

11.1 Each Party shall indemnify and hold harmless the other Party against any direct losses, damages, costs, and expenses (including reasonable legal fees) arising from a material breach by the indemnifying Party of its obligations under this Agreement or applicable Data Protection Laws, provided that: (i) the indemnifying Party's liability shall be limited to losses directly attributable to its own acts or omissions; (ii) neither Party shall be liable to the other for any indirect, incidental, special, or consequential damages, including loss of profits, revenue, or business opportunity, howsoever arising; and (iii) the indemnifying Party’s liability for acts or omissions of subprocessors shall be determined in accordance with applicable Data Protection Laws, this Agreement, and the liability limitations set out herein.

11.2 Notwithstanding anything to the contrary in this Agreement, the aggregate liability of each Party arising out of or in connection with this DPA, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, shall not exceed the total fees paid or payable by You to Us under the Agreement in the twelve (12) month period immediately preceding the event giving rise to the claim. This limitation shall apply to the fullest extent permitted by applicable law but shall not limit either Party's liability for losses arising from wilful misconduct or gross negligence, or any liability that cannot be excluded or limited under applicable Data Protection Laws.

11.3 Notwithstanding the above, in the event that We as the Processor fail to comply with the stipulations of this Agreement as a direct result of Your acts, omissions, or instructions, You shall bear responsibility for any resulting non-compliance and shall indemnify Us against any direct losses, damages, costs, and expenses arising therefrom, including any claims by Data Subjects or sanctions imposed by the competent supervisory authorities attributable to such acts, omissions, or instructions.

12. GOVERNING LAW

12.1. This Agreement and any dispute or claim arising out of, or in connection with it, its subject matter or formation (including non-contractual disputes or claims), shall be governed by, and construed in accordance

with, the laws of Spain, and the Parties hereby submit to the exclusive jurisdiction of the courts of Madrid, Spain.

13. NOTICES

13.1 All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post, or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13.2 For any questions regarding the processing of Personal Data under this Agreement, You may contact us at hello@wpml.org or such other contact as we may notify from time to time.

Appendix 1

- **NATURE AND PURPOSE OF THE PROCESSING:**

The Processing of Personal Data is carried out for the purpose of delivering the Services offered by OnTheGoSystems, including but not limited to:

- Provision and support of OTGS software products (WPML, Toolset, PTC, and related services), as specified in the corresponding Terms and Conditions,
- Communication necessary to provide and support the Services,
- Technical operations, including hosting, storage, backup, and system monitoring,
- Security logging, access control, abuse prevention, debugging, product improvement, and usability analysis,

Where required, personal data may also be processed to comply with legal obligations or to exercise or defend legal claims.

- **DURATION OF PROCESSING:**

Your Personal Data will be Processed for the duration of the Agreement between the parties, and:

- As long as necessary for the specific purpose it was collected for,
- Or as required by applicable laws (e.g., accounting or tax record retention),
- After termination, data will be returned or deleted as per Section 3 of the DPA unless otherwise required by law.

- **PERSONAL DATA IN SCOPE:**

We may process the following types of Personal Data on your behalf:

Category	Examples
Identification data	Full name, username, user ID, profile photo
Contact data	Email address, phone number, billing/shipping address
Account credentials	Login details (hashed), language preferences
Payment information	Card numbers, billing address, currency
Transactional data	Purchase history, subscription info, invoices

Communication data	Messages, support tickets, chat logs, feedback
Technical metadata	IP address, browser/user agent, access logs, usage behavior, time zone, interactions with designated WPML administration interfaces (including navigation paths and configuration actions)
Document content	Files or text submitted via OTGS services or during support interactions

Special categories of Personal Data are not intentionally collected or processed by OTGS as part of the services. In the event such data is included in user-generated content or embedded within customer data, its processing is incidental and subject to the controller's instructions and applicable legal requirements.

- **PERSONS AFFECTED (DATA SUBJECTS):**

The group of Data Subjects affected by the Processing of their Personal Data consists of end users of Our software, clients and customers, website visitors, and service providers. In case You are not the Data Subject affected by our Processing of their Personal Data, you hereby warrant that You have obtained all necessary consents and authorizations from and/or, if applicable, informed, the Data Subjects of Our Processing of their Personal Data.

Appendix 2: Technical and Organisational Measures (TOMs)

We implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as described below.

1. Organisational Measures

- Information security and data protection responsibilities are defined and periodically reviewed
- Access to systems is restricted to authorized personnel based on role and necessity (least privilege)
- Personnel with access to Personal Data are subject to confidentiality obligations
- Security awareness and privacy training is provided internally
- Incident management and response procedures are in place
- Vendors and infrastructure providers are assessed from a security and data protection perspective
- Periodic risk assessments are performed
- Measures are reviewed and updated to reflect changes in risk, technology, and regulatory requirements
- Data protection principles such as privacy by design and by default are applied
- A personal data breach management and notification process is in place

2. Technical Measures

- Personal Data in transit is encrypted using secure protocols (e.g., HTTPS/TLS)
- Access to infrastructure is protected by means of authentication controls and logging
- Systems are subject to regular updates, patching, and vulnerability management
- Monitoring and logging are implemented to detect and respond to security incidents
- Backup and recovery procedures are in place to ensure availability and resilience
- Changes to production systems follow defined change management processes
- Production and non-production environments are segregated

3. Subprocessor and Infrastructure Measures

We rely on established infrastructure providers and subprocessors that implement appropriate security

measures, including:

- Physical security of data centers
- Network and infrastructure protection
- Redundancy, availability, and resilience controls
- Independent certifications and audits (e.g., ISO 27001, SOC reports)

We rely on these providers under appropriate contractual and data protection terms and periodically review their security commitments.

4. Shared Responsibility

Where the Services are integrated into Customer-controlled environments, You are responsible for:

- Securing your systems, infrastructure, and hosting environment
- Managing user access, authentication, and roles
- Applying updates and patches
- Managing data retention and deletion

5. Data Minimisation

We process only the Personal Data necessary to provide the Services, such as content submitted for processing, licensing information, and operational metadata. We do not use customer content to train AI models and do not retain it beyond what is necessary to provide the Services.

Appendix 3: Subprocessors

In accordance with the Agreement, the current authorised subcontractors and/or transfers of Your Personal Data are set out in the table below.

Name (registered seat)	Processing location / transfers	Description of services provided by the subprocessor
Amazon Web Services, Inc. (Seattle, Washington, US)	US (us-east-1). International transfers are conducted in accordance with clause 7 of the DPA (EU Standard Contractual Clauses).	Cloud hosting of the Services and their database, file storage for support uploads, transactional and newsletter email, message queues; our self-hosted team chat runs on this account; language models used to process and translate content submitted through the Services.
Google LLC (Mountain View, California, US)	US. International transfers are conducted in accordance with clause 7 of the DPA (EU Standard Contractual Clauses).	Cloud infrastructure and artificial intelligence services: language models used to process and translate content submitted through the Services, the model that translates support messages between a client and a supporter, and the reporting of a new account's first order to Google Ads as an offline conversion (account identifier and order time, no message content).
Microsoft Corporation (Redmond, Washington, US)	US. International transfers are conducted in accordance with clause 7 of the DPA (EU Standard Contractual Clauses).	Cloud infrastructure and artificial intelligence services, including language models used to process and translate content submitted through the Services.

DeepL SE (Cologne, Germany)	EU (Germany). No international transfer.	Machine translation services used to process and translate content submitted through the Services.
Stripe Payments Europe, Limited, and Stripe Technology Europe, Limited (Dublin, Ireland)	Ireland / global. International transfers are conducted in accordance with clause 7 of the DPA (EU Standard Contractual Clauses).	Card payments and saved payment methods for your payments for the Services. We never see or store the card number.
PayPal Hong Kong Limited (Hong Kong), with PayPal, Inc. (San Jose, California, US)	Hong Kong and US. International transfers are conducted in accordance with clause 7 of the DPA (EU Standard Contractual Clauses).	PayPal payments and billing agreements for your payments for the Services.
PostHog, Inc. (San Francisco, California, US)	US. International transfers are conducted in accordance with clause 7 of the DPA (EU Standard Contractual Clauses).	Product analytics and session replay in designated WPML administration interfaces.
Anthropic, PBC (San Francisco, California, US)	US. International transfers are conducted in accordance with clause 7 of the DPA (EU Standard Contractual Clauses).	The language models behind Maiya, the support assistant: the support messages you write, the account facts she reads to answer them, and the attachments she is allowed to read.
OpenAI, L.L.C. (San Francisco, California, US)	US. International transfers are conducted in accordance with clause 7 of the DPA (EU Standard Contractual Clauses).	Maiya's fallback language models during an outage of the primary provider: the same support messages, only while the fallback is active.
JetBrains s.r.o. (Prague, Czech Republic), YouTrack Cloud, EU region	EU. No international transfer.	The issue tracker where a reported problem, the site address it concerns and the supporter's notes are filed for our developers.
Serper (serper.dev, US)	US. International transfers are conducted in accordance with clause 7 of the DPA (EU Standard Contractual Clauses).	A web search used to build a new customer's company profile: the buyer's name and company name are the search terms.

OnTheGoSystems Limited

22/F 3 Lockhart Road

Wanchai Hong Kong

October 16th, 2026

Unterschriftsdatum: 27. Oktober 2026