

## XTM DATA PROCESSING AGREEMENT

### 1. Definitions and Interpretation

In addition to capitalised words and phrases in the Definitions Schedule (available at <https://go.xtm.cloud/legal/definitions-schedule>) which continue to apply, the following definitions and rules of interpretation apply to this XTM Data Processing Agreement (“**DPA**”):

**Business Purposes** means the Services provided to You or any other purpose specifically identified in Annex A.

**Controller, Processor, Process, Data Subject, Personal Data and Personal Data Breach and Supervisory Authority** have the meanings given to them in the GDPR.

**Controller to Processor Clauses** means the standard contractual clauses between controllers and processors, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and available at <https://go.xtm.cloud/legal/standard-contractual-clauses-controller-to-processor-clauses>.

**Data Protection Supervising Authority** means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws.

**EEA** means the European Economic Area.

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

**International Data Transfer Addendum** means the international data transfer addendum to the standard contractual clauses issued by the Information Commissioner’s Office under section 119A of the Data Protection Act 2018 on 2 February 2022, and located at <https://go.xtm.cloud/legal/uk-gdpr-addendum>.

**Processor to Processor Clauses** means the standard contractual clauses between processors, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and available at <https://go.xtm.cloud/legal/standard-contractual-clauses-processor-to-processor-clauses>.

**Protected Data** means Personal Data that is processed by Us on Your behalf in connection with the provision of the Services.

**Standard Contractual Clauses** means (1) the Controller to Processor Clauses; and (2) the Processor to Processor Clauses, as applicable in accordance with clause 8 of this DPA.

**UK** means the United Kingdom.

**UK Controller to Processor Clauses** means the Controller to Processor Clauses, as amended by the International Data Transfer Addendum.

**UK Processor to Processor Clauses** means the Processor to Processor Clauses, as amended by the International Data Transfer Addendum.

**UK Protected Data** means any personal data (as defined in the UK GDPR) that is processed by Us on Your behalf in connection with the provision of the Services.

**UK Standard Contractual Clauses** means (i) the UK Controller-to-Processor Clauses, or (ii) the UK Processor-to-Processor Clauses, as applicable in accordance with clause 8 of this DPA.

**UK Third Country** means a country outside the UK not recognised by the Secretary of State or the

Data Protection Act 2018 as providing an adequate level of protection for personal data (as described in the UK GDPR).

- 1.1 This DPA is subject to and incorporated into the XTM Subscription Agreement Terms.
- 1.2 The annexes to this DPA form part of this DPA and shall have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Annexes.
- 1.3 In the case of conflict or ambiguity between:
  - 1.3.1 any provision contained in the body of this DPA and any provision contained in the annexes, the provision in the body of this DPA will prevail;
  - 1.3.2 the terms of any accompanying invoice or other documents annexed to this DPA and any provision contained in the Annexes, the provision contained in the annexes will prevail;
  - 1.3.3 any of the provisions of this DPA and the provisions of the XTM Subscription Agreement Terms, the provisions of this DPA will prevail; and
  - 1.3.4 any of the provisions of (1) this DPA; and (2) the Standard Contractual Clauses, the provisions of the Standard Contractual Clauses will prevail.

## **2. Personal Data Types and Processing Purposes**

- 2.1 We will act as a Processor of any Protected Data provided to Us in delivering the Services to You.
- 2.2 You acknowledge that You may be either a Controller or a Processor of the Protected Data.
- 2.3 To the extent You are not sole Controller of any Protected Data You warrant that You have full authority and authorisation of all relevant Controllers to instruct Us to process the Protected Data in accordance with the Agreement.
- 2.4 Annex A describes the subject matter, duration, nature, and purpose of the processing and the personal data categories and Data Subject types in respect of which We may process the Protected Data on Your behalf to fulfil the Business Purposes.

## **3. Rights and Obligations**

- 3.1 We will immediately notify You if We consider any of Your instructions to be unlawful.
- 3.2 If You issue Us with written notice to amend, transfer, delete or otherwise process the Protected Data, or to stop, mitigate or remedy any unauthorised processing, We will comply with that request within a reasonable period of time.
- 3.3 Except to the extent required by applicable law, We will:
  - 3.3.1 only access and process the Protected Data to the extent and in a manner necessary to fulfil the Business Purposes and in accordance with Your written instructions. We will not process the Protected Data for any other purpose or in a manner which is incompatible with this DPA;
  - 3.3.2 not disclose the Protected Data to third parties without Your authority unless specifically permitted by this DPA. Unless prohibited by applicable law, We will inform You of the disclosure and where possible will give You an opportunity to object or challenge the disclosure; and
  - 3.3.2 provide reasonable assistance and support to You to meet the Controller's compliance obligations under the GDPR, taking into account the nature of Our processing and the information available to Us, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with Supervisory Authorities under the GDPR in compliance with Our obligations under the GDPR.

#### **4. XTM's Employees and Affiliated Personnel**

- 4.1 We will ensure that all employees or persons authorised to process the Protected Data in connection with the Business Purpose:
- 4.1.1 are advised of the confidential nature of the Protected Data and are bound by confidentiality obligations to keep information secure;
  - 4.1.2 are aware of both Our duties and their personal duties and obligations under the Data Protection Law and this DPA; and
  - 4.1.3 we will take reasonable steps to ensure the reliability of any employee or authorised person who may have access to the Protected Data.

#### **5. Sub-processors**

- 5.1 You acknowledge and consent to Us subcontracting the processing of Protected Data to Our Affiliates and to those sub-processors set out in Annex A. We shall remain liable to You for the performance of Our sub-processor's obligations that cause Us to breach any of Our obligations under this DPA.
- 5.2 If We wish to change any of Our sub-processors We will provide reasonable notice to You, including by updating the information on XTM's Website. If You object to the use of any new sub-processor You may terminate the Agreement on giving ninety (90) days' notice provided that such notice is received by Us within thirty (30) days of notice of the change of sub-processor.
- 5.3 We will enter into a written contract with Our sub-processors on terms substantially the same as those set out in this DPA, and We will ensure that they are required to provide appropriate technical and organisational measures in place to secure the Protected Data.

#### **6. Security**

Both We and You shall at all times maintain, evaluate and, where necessary, adapt and update appropriate technical and organisational measures to protect against any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Protected Data transmitted, stored or otherwise processed in accordance with this DPA, including, but not limited to, the security measures set out in Annex B.

#### **7. Personal Data Breach**

- 7.1 We will notify You without undue delay (and in any event within seventy-two (72) hours of becoming aware) of a Personal Data Breach affecting Protected Data and provide You with details of the Personal Data Breach.
- 7.2 The parties will reasonably co-operate with each other in the investigation of the Personal Data Breach.
- 7.3 Unless required by applicable law, We will not inform any third party of any Personal Data Breach without Your prior written consent.

#### **8. Cross-Border Transfers of Personal Data**

- 8.1 You consent to Us transferring and processing Protected Data outside the jurisdiction of the UK and/or the EEA where applicable where such processing is undertaken by Our Affiliate or approved sub-processor.
- 8.2 Where You are acting as a Controller and We are acting as a Processor:
- 8.2.1 the Controller-to-Processor Clauses will apply to any transfer of Protected Data from within the EEA to an EEA Third Country; and

8.2.2 the UK Controller-to-Processor Clauses will apply to any transfer of UK Protected Data from within the UK to a UK Third Country.

8.3 Where You are acting as a Processor and We are acting as a Sub-Processor:

8.3.1 the EU Processor-to-Processor Clauses will apply to any transfer of UK Protected Data from within the EEA to an EEA Third Country; and

8.3.2 the UK Processor-to-Processor Clauses will apply to any transfer of Protected Data from within the UK to a UK Third Country.

You agree that it is possible that We will not know the identity of the Controller because We may not have a direct relationship with the Controller. In these circumstances, You will fulfil Our obligations to the Controller under the EU Processor-to-Processor Clauses or UK Processor-to-Processor Clauses, as applicable.

## **9 Complaints, Data Subject Requests, Third Party Rights**

9.1 Taking into account the nature of the processing, We will, once we have identified that the communication relates to the processing of Protected Data for whom You are responsible, notify You without undue delay:

9.1.1 of any complaint, notice or communication and will provide reasonable co-operation to enable You to respond to such complaint, notice or communication; and

9.1.2 of any request by a Data Subject to access their Personal Data or exercise any of their rights.

9.2 We will reasonably co-operate with You, and assist in responding to any complaint, notice, communication or Data Subject request in compliance with Our obligations under the GDPR.

9.3 You authorise Us to respond to any Data Subject who makes a request to Us to confirm that we have forwarded the communication to You.

## **10 Termination**

10.1 This DPA will remain in full force and effect so long as:

10.1.1 the Agreement is in effect; or

10.1.2 We retain any Protected Data.

## **11 Data Return and Destruction**

11.1 On termination of the Agreement, You will have access to Customer Data for a thirty (30) day period to enable You to copy and extract the Customer Data (including any Protected Data). We reserve the right to charge a reasonable fee for Our time and resources to copy any Customer Data onto media for You to transport and/or for Our time and resources uploading the Customer Data for download.

11.2 Within a reasonable period following the period set out in clause 11.1, We will securely delete or destroy the Customer Data remaining in Our possession or control, unless We are required to retain a copy under applicable law.

## **12 Audit**

12.1 We will make available to You information reasonably required to demonstrate Our compliance with this DPA provided that you ensure that all information obtained or generated by You or Your auditor(s) in connection with such information requests is kept strictly confidential (save for disclosure to a Data Protection Supervisory Authority or as otherwise required by applicable law). In addition, You may conduct an annual audit or inspection on giving Us at least fourteen (14) days' written notice at any time between the hours of 9am and 5pm (GMT) on a Business Day during the term of the Agreement.

We will facilitate reasonable access to records, systems and Our personnel and offer reasonable assistance to You in conducting such audit providing that this can be done with minimal disruption to Our day to day business activities.

- 12.2 The costs of any audit are payable by You, unless the audit reasonably shows that we have materially failed to take appropriate security measures in accordance with this DPA.

## ANNEX A: PERSONAL DATA PROCESSING PURPOSES AND DETAILS

### 1. The Duration of Processing:

The Protected Data shall be processed for as long as the obligation to process the Protected Data under the Agreement continues.

### 2. The Nature and Subject Matter of Processing, and the Business Purposes:

The processing purpose is to provide software solutions operated by Us that allow You to translate electronic documents from a source language to one or more target languages.

We and Our Affiliates and subcontractors shall store and process information entered by Approved Users as required for the Business Purposes and for Our legitimate interests to manage and support the underlying software solutions.

We will only obtain and use Protected Data for the following purposes:

- (i) translating electronic documents (to the extent that those documents contain any Protected Data); and
- (ii) managing user accounts to enable Approved Users to access and use the Subscribed Services.

### 3. Data Categories:

Protected Data uploaded to the Services.

The data categories processed in connection with Your Approved Users could include:

- (i) title;
- (ii) first name;
- (iii) last name;
- (iv) email address;
- (v) default currency;
- (vi) postal address;
- (vii) telephone number;
- (viii) mobile phone number;
- (ix) source and target languages;
- (x) subject matter specialisation;
- (xi) access rights to Supplier (e.g., which Protected Data can be accessed etc.);
- (xii) rating (score card for quality etc.); and
- (xiii) tasks allocated.

### 4. Data Subject Categories:

Authorised Users.

Any third party whose Personal Data is contained within a document translated using the Services.

### 5. Approved sub-processors:

Name: OVH Limited  
Contact Person: Grégory Gitsels - Data Protection Officer  
Phone number: +44 333 370 0425  
Address: Roubaix, France

Name: Amazon Web Services EMEA SARL and Amazon Web Services, Inc.  
Contact: <https://aws.amazon.com>  
Address: 38 Avenue John F. Kennedy, L-1855, Luxembourg

Our Affiliates and personnel engaged by Us as sub-contractors to deliver the Services who are subject to confidentiality restrictions at least as restrictive as those in this DPA and the Agreement.

**7. Notices:**

Notices served under this DPA should be served in accordance with the Agreement.

## **ANNEX B: SECURITY MEASURES**

The technical and organisational data security measures in place are the following:

- (i) The Supplier does not maintain any servers on site. All personal information is stored on secure hosted platforms.
- (ii) The Supplier's staff are only given access to electronic filing systems and folders to the extent that this is necessary to enable each staff member to fulfil his or her duties.
- (iii) Access to hosted data systems is password-protected and only current authorised staff have access.
- (iv) Staff only use laptops provided by the Supplier.
- (v) Staff use their own mobile phones for the Supplier's business. Members of staff who handle Protected Data are obliged to password-protect and encrypt their mobile phones and allow them to be remotely accessed and wiped in the event of loss or theft.
- (vi) Staff are required to log-off from systems and laptops when not in use.
- (vii) Staff are provided with training and guidance on the secure use of electronic devices in public and the associated risks.
- (viii) The Supplier does not maintain any paper records containing Protected Data.
- (ix) The Supplier ensures that its physical premises are secure from theft and other intrusion.
- (x) The management of the Supplier's IT systems is the delegated responsibility of a third-party provider. The Supplier's Chief Executive Officer is responsible for ensuring that these services provide an appropriate level of security. The Supplier's IT systems are reviewed for data security compliance purposes at intervals of no more than twelve (12) months.
- (xi) The Supplier's full security program and policy document is available on request.