trufo

DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM (“DPA”) forms part of and is subject to the Master Services Agreement (the "Principal Agreement") between Trufo Inc. and its Client.

RECITALS

(A) The Client has engaged Trufo to provide content provenance, certificate authority, and related services under the Principal Agreement (the "Services").

(B) In the course of providing the Services, Trufo processes Personal Data on behalf of the Client and, in certain circumstances, as an independent Controller as described in this DPA.

(C) The parties wish to ensure that such processing complies with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the "GDPR") and any applicable national implementing legislation (collectively, "Applicable Data Protection Law").

(D) This DPA sets out the terms upon which Trufo will process Personal Data in connection with the Services, as required by Article 28 of the GDPR.

1. DEFINITIONS

In this DPA, unless the context requires otherwise, the following terms shall have the meanings set out below. Capitalized terms not defined herein shall have the meanings given to them in the Principal Agreement or the GDPR.

"Applicable Data Protection Law" means the UK GDPR, the Data Protection Act 2018, the EU GDPR, together with any applicable national implementing legislation in any EU or EEA Member State, and, to the extent applicable, the data protection laws of any other jurisdiction.

"Controller", **"Processor"**, **"Data Subject"**, **"Personal Data"**, **"Personal Data Breach"**, and **"Processing"** have the meanings given to them in Article 4 of the GDPR.

“CAWG” means the Creator Assertions Working Group, a working group within C2PA responsible for developing specifications for identity assertions and creator metadata in content provenance.

"Certificate Services" means Trufo's Organization Validation ("OV") and Product Validation ("PV") certificate issuance services, operated in accordance with C2PA's Certificate Policy and Trufo's Certification Practices Statement ("CPS").

"C2PA" means the Coalition for Content Provenance and Authenticity, including its technical specifications and Certificate Policy.

"DPF" means the EU-U.S. Data Privacy Framework, as established by the European Commission's adequacy decision of 10 July 2023.

"EDPB" means the European Data Protection Board, established under Article 68 of the GDPR.

“Effective Date” means the date of last signature of this DPA, or, if earlier, the date on which Trufo first processes Personal Data on behalf of the Client under the Principal Agreement.

"MFA" means multi-factor authentication, requiring two or more independent credentials for user verification.

"SCCs" means the Standard Contractual Clauses for the transfer of personal data to third countries, as adopted by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

"Signing Services" means Trufo's application programming interface for C2PA manifest creation and signing, watermark encoding and decoding, fingerprint computation, and content verification, as described in Annex 1.

"Sub-processor" means any third party engaged by Trufo to process Personal Data on behalf of the Client in connection with the Services.

"Technical and Organizational Measures" or **"TOMs"** means the security measures described in Annex 2.

"TOTP" means time-based one-time password, as defined in IETF RFC 6238.

2. SCOPE AND ROLES OF THE PARTIES

2.1. Dual-Role Structure. The parties acknowledge that Trufo operates in two distinct capacities with respect to Personal Data processed in connection with the Services:

(a) **Processor Role (Signing Services).** When providing the Signing Services, Trufo acts as a Processor on behalf of the Client (acting as Controller). In this capacity, Trufo processes Personal Data solely in accordance with the Client's documented instructions as set out in this DPA and Annex 1.

(b) **Independent Controller Role (Certificate Services).** When providing the Certificate Services, Trufo acts as an independent Controller with respect to OV/PV application data. Trufo determines the purposes and means of processing this data as required by C2PA's Certificate Policy and applicable trust service standards. The provisions of Section 3 through Section 12 of this DPA apply to Trufo's processing in its Processor capacity. Section 13 sets out the separate terms applicable to Trufo's Controller capacity for Certificate Services. Sections 3 through 12 of this DPA apply to Trufo's processing of Personal Data in its capacity as a Processor in connection with the Signing Services. Trufo’s obligations as an independent Controller in connection with the Certificate Services are set out in Section 13.

2.2. Processing Details. The subject matter, duration, nature, and purpose of the processing, the types of Personal Data processed, and the categories of Data Subjects are described in Annex 1.

2.3 Limited Independent Processing.

(a) Notwithstanding Trufo's role as Processor for the Signing Services, Trufo may process limited Personal Data as an independent Controller solely for the following purposes: (a) security monitoring and threat detection; (b) fraud and abuse prevention; and (c) platform account authentication and session management. Processing for compliance with applicable law is governed by Article 6(1)(c) of the GDPR and Section 3.1 of this DPA and is not subject to this Section 2.3.

(b) The legal basis for the processing described in (a) through (c) is Article 6(1)(f) of the GDPR (legitimate interests of Trufo in maintaining a secure and reliable service). Trufo has conducted a Legitimate Interests Assessment with respect to this processing, which shall be made available to the Client upon written request. Such processing shall be limited to what is strictly necessary for the stated purposes and shall not include manifest content, media file data, or any Personal Data processed solely on behalf of the Client in Trufo's Processor capacity. The categories of Personal Data and retention periods applicable to this processing are set out in Section C of Annex 1.

(c) Trufo shall provide the Client, upon execution of this DPA, with a written statement containing the information required by Article 14(1) and (2) of the GDPR with respect to Trufo's independent Controller processing described in this Section 2.3. The Client shall incorporate such information into its own privacy notice or otherwise make it available to relevant Data Subjects in accordance with Article 14 of the GDPR. Trufo shall notify the Client at least thirty (30) days in advance of any material change to such information, and shall promptly provide the Client with an updated written statement reflecting such change.

3. PROCESSING INSTRUCTIONS (Article 28(3)(a) GDPR)

3.1. Trufo shall process Personal Data only on documented instructions from the Client, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by European Union or Member State law to which Trufo is subject. In such a case, Trufo shall inform the Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.2. The Client's instructions for processing are set out in this DPA and the Principal Agreement. The Client may issue additional written instructions consistent with the terms of this DPA. If Trufo believes that an instruction from the Client infringes Applicable Data Protection Law, Trufo shall promptly notify the Client.

3.3. The specific categories of Personal Data processed, and the applicable retention periods, default storage behavior, and available configuration options for the Signing Services are described in Section B of Annex 1.

4. CONFIDENTIALITY (Article 28(3)(b) GDPR)

4.1. Trufo shall ensure that all persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.2. Trufo shall ensure that access to Personal Data is limited to those personnel who require such access for the performance of the Services.

5. SECURITY MEASURES (Article 28(3)(c) / Article 32 GDPR)

5.1. Trufo shall implement and maintain the Technical and Organizational Measures described in Annex 2, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects.

5.2. Trufo shall regularly test, assess, and evaluate the effectiveness of the TOMs. Upon the Client's reasonable request, Trufo shall provide documentation evidencing its compliance with this Section 5.

5.3. With respect to API call logging, Trufo shall apply data minimization principles in accordance with Article 5(1)(c) and Article 25 of the GDPR and EDPB Guidelines 4/2019 on Data Protection by Design and by Default. In particular:

(a) Trufo shall minimize Personal Data captured in API logs, using pseudonymization, hashing, or redaction at the point of log creation where feasible;

(b) Manifest content and Personal Data shall be excluded from operational logs by default, unless required for security incident investigation;

(c) API log retention shall not exceed 90 days from the date of the relevant API call, after which logs shall be securely deleted;

(d) Trufo shall document its logging practices, including the specific fields logged and the retention periods applied, and shall make such documentation available to the Client upon request.

6. SUB-PROCESSORS (Article 28(2) and (4) GDPR)

6.1. The Client provides general written authorization for Trufo to engage the Sub-processors listed at https://trufo.ai/legal/subprocessors as of the Effective Date.

6.2. Trufo shall update the published list of Sub-processors at least thirty (30) days prior to engaging any new Sub-processor or replacing an existing Sub-processor.

6.3. The Client may object to a Sub-processor change by notifying Trufo in writing within fifteen (15) days of receiving the Sub-processor update, providing reasonable grounds related to data protection. The parties shall discuss the objection in good faith. If the parties cannot resolve the objection within thirty (30) days, the Client may terminate the affected Services without penalty.

6.4. In accordance with EDPB Opinion 22/2024, Trufo shall maintain and make available to the Client, upon request, the identity of all Sub-processors and any downstream processors in the processing chain, regardless of the risk level of the processing activity.

6.5. Trufo shall remain fully liable to the Client for the performance of each Sub-processor's obligations under the relevant sub-processing agreement.

7. DATA SUBJECT RIGHTS (Article 28(3)(e) GDPR)

7.1. Trufo shall, taking into account the nature of the processing, assist the Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Client's obligation to respond to requests for exercising the Data Subject's rights under Chapter III of the GDPR (including rights of access, rectification, erasure, restriction, data portability, and objection).

7.2. If Trufo receives a request directly from a Data Subject, Trufo shall promptly notify the Client and shall not respond to the request directly unless instructed to do so by the Client or required by Applicable Data Protection Law. For Data Subject requests relating to Certificate Services data, Trufo shall respond in its capacity as Controller in accordance with Section 13.3.

8. ASSISTANCE WITH SECURITY, BREACH NOTIFICATION, AND DPIAs (Article 28(3)(f) GDPR)

8.1. Trufo shall assist the Client in ensuring compliance with the Client's obligations under Articles 32 through 36 of the GDPR, taking into account the nature of processing and the information available to Trufo. This assistance includes:

(a) implementing and maintaining appropriate security measures (Article 32);
(b) notifying the Client of Personal Data Breaches (Article 33), as further described in Section 9 of this DPA;
(c) assisting with Data Protection Impact Assessments ("DPIAs") where required (Article 35); and
(d) assisting with prior consultation with supervisory authorities (Article 36).

8.2. The parties acknowledge that the processing of geolocation data (GPS coordinates and IPTC location fields) embedded in media files, combined with creator identity and behavioral metadata (edit history and timestamps), may give rise to high risks to Data Subjects within the meaning of Article 35 of the GDPR and the criteria set out by the Article 29 Working Party (WP248 rev.01). The Client, as Controller, is responsible for determining whether a DPIA is required. Trufo shall provide such information as is reasonably necessary to support any DPIA conducted by the Client, including information regarding the C2PA-specific privacy risks identified by the World Privacy Forum (2024) and Trufo's mitigating measures.

9. PERSONAL DATA BREACH NOTIFICATION (Articles 33 and 34 GDPR)

9.1. Trufo shall notify the Client without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Personal Data processed on behalf of the Client. This timeline aligns with the Controller's notification obligations under Article 33(1) of the GDPR (72 hours from awareness).

9.2. The notification shall include, to the extent available:

(a) a description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) the name and contact details of Trufo's point of contact for further information;

(c) a description of the likely consequences of the breach; and

(d) a description of the measures taken or proposed to be taken to address the breach, including measures to mitigate its possible adverse effects.

9.3. Where it is not possible to provide all information at the same time, the information may be provided in phases without undue further delay.

9.4. For Personal Data Breaches affecting data processed under Trufo's Controller capacity (Certificate Services), Trufo shall notify the relevant supervisory authority and affected Data Subjects in accordance with Articles 33 and 34 of the GDPR and shall inform the Client of any such breach within a commercially reasonable period, to the extent permitted by law, where the breach may affect the Client's use of the Services.

10. DELETION AND RETURN OF DATA (Article 28(3)(g) GDPR)

10.1. Upon termination or expiry of the Principal Agreement, Trufo shall, at the Client's election: (a) return all Personal Data to the Client in a commonly used, machine-readable format; or (b) securely delete all Personal Data and certify such deletion in writing. The Client shall notify Trufo of its election within thirty (30) days of termination. If no election is made within such period, Trufo shall securely delete all Personal Data within ninety (90) days of termination..

10.2. The obligations in Section 10.1 are subject to the following exceptions:

(a) **OV/PV Certificate Data:** Personal Data processed under Trufo's Controller capacity for Certificate Services is subject to the retention obligations described in Section 13 and Annex 1, Section A.3, and is not subject to the deletion or return obligations of this Section 10.

(b) **Legal Retention:** Trufo may retain Personal Data to the extent required by European Union or Member State law, provided that Trufo shall restrict processing to what is required by such law and shall inform the Client of the retention requirement (unless prohibited by law).

(c) **Backup and Log Data:** Personal Data contained in routine backup media and API logs shall be deleted in accordance with Trufo's standard retention schedules (not to exceed the periods specified in Article 5.3 and Annex 1), provided that such data shall not be actively processed pending deletion.

11. AUDIT AND INSPECTION (Article 28(3)(h) GDPR)

11.1. Trufo shall make available to the Client all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and this DPA, and shall allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client.

11.2. Audits shall be subject to the following conditions:

(a) The Client shall provide at least thirty (30) days' prior written notice of an audit, unless a supervisory authority or Applicable Data Protection Law requires a shorter notice period;

(b) Audits shall be conducted during normal business hours and shall not unreasonably disrupt Trufo's operations;

(c) The Client shall bear the costs of any audit, except where the audit reveals material non-compliance by Trufo;

(d) The Client may conduct no more than one (1) audit per calendar year, unless required by a supervisory authority or in connection with a Personal Data Breach; and

(e) Trufo may satisfy audit requests by providing relevant third-party certifications or audit reports (e.g., SOC 2 Type II), to the extent they address the matters subject to audit.

12. INTERNATIONAL DATA TRANSFERS

12.1. The Client acknowledges that Trufo is established in the United States of America and that the provision of the Services involves the transfer of Personal Data from the European Economic Area to the United States. As of the Effective Date, Trufo is not certified under the EU-U.S. Data Privacy Framework.

12.2. Transfer Mechanism. The parties agree that the following transfer mechanism shall apply to all transfers of Personal Data from the Client to Trufo under this DPA:

(a) **Standard Contractual Clauses:** The Standard Contractual Clauses (Module Two: Controller to Processor), as adopted by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "EU SCCs"), are hereby incorporated into this DPA by reference as Annex 4 and shall constitute the transfer mechanism for all transfers of Personal Data under this DPA.

(b) **Sub-processor Transfers:** Where a Sub-processor is located outside the EEA, Trufo shall ensure that transfers to such Sub-processor are made pursuant to a valid transfer mechanism under Chapter V of the GDPR and that the same data protection obligations as those in this DPA are imposed on the Sub-processor by contract.

12.3. Supplementary Measures. Trufo shall implement and maintain the technical and organizational measures described in Annex 2 as supplementary measures to support the transfers under Clause 12.2, in accordance with the EDPB Recommendations 01/2020 on supplementary measures. These measures include, in particular, Trufo's use of HSM-based key management (where private signing keys never leave the hardware security module boundary) and the C2PA redaction framework that enables removal of personal data from content manifests prior to transfer.

12.4. Data Privacy Framework. In the event that Trufo subsequently obtains certification under the EU-U.S. Data Privacy Framework, Trufo shall promptly notify the Client. Upon such certification, the parties may agree in writing that transfers shall be made in reliance on the applicable adequacy decision, with the SCCs continuing to apply as a supplementary safeguard.

12.5. Transfer Impact Assessment. Trufo represents that, as of the Effective Date, it has carried out a transfer impact assessment in respect of the transfers contemplated by this DPA and has concluded that the supplementary measures described in Article 12.3, together with the contractual safeguards in the SCCs, provide a level of protection that is essentially equivalent to that guaranteed by the GDPR.

12.6. Transfers of Personal Data in Connection with Certificate Services. When providing the Certificate Services, Trufo receives OV/PV application data directly from Data Subjects in its capacity as an independent Controller. To the extent such receipt constitutes a transfer of Personal Data from the European Economic Area to the United States within the meaning of Chapter V of the GDPR, the transfer is necessary for the performance of a contract between the Data Subject and Trufo within the meaning of Article 49(1)(b) of the GDPR, namely the validation and issuance of the requested certificate. Trufo additionally applies the supplementary measures described in Annex 2 to protect such data. In the event Trufo obtains DPF certification, such certification shall also serve as a transfer safeguard for Certificate Services data. The legal basis for the underlying processing is Article 6(1)(b) of the GDPR (performance of a contract), as further described in Section 13.2. Alternatively, to the extent the foregoing derogation is insufficient, such transfers are protected by the supplementary measures described in Annex 2, which the parties have assessed as providing essentially equivalent protection within the meaning of Clause 14 of the SCCs.

13. TRUFO AS CONTROLLER: CERTIFICATE SERVICES

13.1. When providing the Certificate Services (OV and PV certificate issuance), Trufo acts as an independent Controller with respect to the Personal Data described in Section A of Annex 1. Trufo determines the purposes and means of this processing as required by the C2PA Certificate Policy and Trufo's CPS.

13.2. The basis for Trufo's Controller processing is as follows:

(a) **Regulatory and Standards Compliance:** C2PA's Certificate Policy requires Certificate Authorities to collect, verify, and retain certain organizational and individual data as part of the OV and PV validation processes. Trufo processes this data to comply with these requirements and to maintain the integrity and trustworthiness of the certificate ecosystem.

(b) **Retention Obligation:** Trufo is required by C2PA standards to retain copies of OV/PV application data for the duration specified in its CPS. This data will not be shared with any external party except for the information that appears on the issued certificates.

(c) **Legal Basis:** The legal basis for processing Personal Data of individual PV applicants is Article 6(1)(b) of the GDPR (performance of a contract to which the Data Subject is a party). The legal basis for processing Personal Data of organizational representatives submitting OV applications

is Article 6(1)(f) of the GDPR (legitimate interests), specifically Trufo's legitimate interest in verifying organizational identity and maintaining the integrity of the certificate ecosystem as required by C2PA's Certificate Policy, which the parties acknowledge overrides the interests of the relevant Data Subjects given the professional context in which such data is submitted.

13.3. In its capacity as Controller for Certificate Services, Trufo shall:

(a) process OV/PV application data in accordance with its published privacy policy and the C2PA Certificate Policy;

(b) respond directly to Data Subject requests relating to OV/PV data, in accordance with Chapter III of the GDPR;

(c) implement appropriate security measures in accordance with Article 32 of the GDPR;

(d) notify affected Data Subjects and the relevant supervisory authority of any Personal Data Breach involving OV/PV data, in accordance with Articles 33 and 34 of the GDPR;

(e) cooperate with the Client in good faith regarding any data protection matters that affect both the Signing Services and the Certificate Services; and

(f) apply data minimization principles to logging of Certificate Services processing activities, consistent with the practices described in Section 5.3.

13.4. Data Retention. Trufo shall retain OV/PV application data for the period required by C2PA's Certificate Policy and Trufo's CPS. Following expiry of the applicable retention period, Trufo shall securely delete such data unless further retention is required by applicable law.

14. GENERAL PROVISIONS

14.1. Precedence. In the event of a conflict between this DPA and the Principal Agreement, this DPA shall prevail with respect to the processing of Personal Data.

14.2. Governing Law. This DPA shall be governed by and construed in accordance with the laws of the Federal Republic of Germany, without regard to its conflict of laws provisions. For the purposes of the SCCs, the governing law shall be as specified in Annex 4.

14.3. Supervisory Authority. The competent supervisory authority for the purposes of the SCCs shall be the Bavarian State Office for Data Protection Supervision (Bayerisches Landesamt für Datenschutzaufsicht, BayLDA).

14.4. Duration. This DPA shall remain in effect for the duration of the Principal Agreement and for so long thereafter as Trufo continues to process Personal Data on behalf of the Client.

14.5. Amendments. This DPA may be amended only by a written instrument signed by both parties. However, Trufo may update Annex 2 (Technical and Organizational Measures) from time to time to reflect improvements to its security posture, provided that the updated measures do not materially diminish the level of protection afforded to Personal Data.

15. SIGNATURES

IN WITNESS WHEREOF, the parties have executed this Data Processing Addendum as of the Effective Date.

TRUFO Trufo, Inc. Signature: Name: James M. Denaro Title: General Counsel Date: _____	**CLIENT** Client Legal Name: _____ Signature: _____ Name: _____ Title: _____ Date: _____

trufo

ANNEX 1: DESCRIPTION OF PROCESSING

Section A: Certificate Services

A.1 Categories of Data Subjects

Data Subjects include: authorized representatives of organizations applying for Certificates from Trufo.

A.2 Types of Personal Data

In connection with Organization Validation (OV), Individual Validation (IV), and Product Validation (PV) certificate-service processing, Trufo processes the following categories of personal data (and related business data submitted by applicants):

(a) **Authorized representative identity and contact data.** Including but not limited to: First and last name, title, business email, business phone (including country code), representative signature metadata (signer name, signature timestamp).

(b) **PV applicant identity and contact data.** Including but not limited to: First and last name, business email, and business phone (including country code).

(c) **Organization legal/registration and office information.** Including but not limited to: Legal name, registration country/state/city/street/postal code, registry identifiers (such as DUNS or LEI), date formed, DBA name/certificate, physical office address fields, and public contact verification references.

(d) **Validation attestations and authorization records.** Including but not limited to: Agreement/attestation confirmations (e.g., terms, authorization, conformance/security attestations), reviewer decisions/notes, submission and approval timestamps, and status/history records required for validation auditability.

(e) **Product validation technical and contact data.** Including but not limited to: Product name, C2PA CPL record_id, assurance level, applicable specification version, implementation details, and related validation context used for issuance authorization.

(f) **Supporting evidence and uploaded documents.** Including but not limited to: Supporting files and evidence submitted for OV/PV (including proof-of-formation, proof-of-address, opinion-letter/attestation materials, and other supporting documentation). Such materials may contain personal data depending on applicant submissions.

A.3 Retention

OV/PV application data is retained for the period required by C2PA's Certificate Policy and Trufo's CPS. Data appearing on issued certificates is retained for the lifetime of the certificate plus the period required for revocation and audit purposes, as specified in the CPS.

Section B: Signing Services

B.1 Subject Matter and Duration

Trufo processes Personal Data in connection with the provision of C2PA manifest creation and signing, watermark encoding and decoding, fingerprint computation, and content verification services. Processing shall continue for the duration of the Principal Agreement and, for stored manifests, for the retention period specified below.

B.2 Nature and Purpose of Processing

The purpose of processing is to enable the Client to establish verifiable digital provenance for media files through the C2PA standard. Processing operations include and are not limited to: extraction of metadata from media files; creation of cryptographically signed C2PA manifests; embedding of invisible watermarks for content identification; computation of content fingerprints; and verification of existing manifests.

B.3 Categories of Data Subjects

Data Subjects whose Personal Data may be processed include: content creators and photographers whose identity or metadata is embedded in media files; individuals whose names or identifiers appear in author, copyright, or contributor fields; and authorized users of the Client's systems who submit media for processing. For the avoidance of doubt, Personal Data processed by Trufo as an independent Controller in connection with Certificate Services is described in Section A and is not subject to the processing descriptions in this Section B.

B.4 Types of Personal Data and Retention Periods

The following categories of Personal Data may be contained in media files and C2PA manifests submitted by the Client for processing. All fields are optional and present only to the extent the Client includes them in submitted media:

Data Type	Description	Default Retention	Adjustable?
C2PA Manifest	All fields within the C2PA manifest that Trufo generates and signs on behalf of the Client, including creator identity assertions (CAWG identity), content credentials, action history, and related provenance metadata.	Retained for the duration of the Principal Agreement, plus a period of 90 days following termination to allow for orderly return or deletion.	Yes, adjustable in Settings to disable storage of C2PA manifests.
Assets to Process	Images, video, audio, and other files that the Client sends to Trufo to process.	No retention beyond the duration of the API request.	Yes, adjustable in Settings to store forensic copy or thumbnail.

Asset Metadata	Including but not limited to EXIF, IPTC, and other metadata embedded in or associated with the assets submitted for processing.	No retention beyond the duration of the API request.	Yes, adjustable to allow Trufo to read, parse, and store asset metadata into the C2PA manifest.

Section C: Limited Independent Processing (Security, Service Integrity, and Platform Authentication)

C.1 Categories of Data Subjects: Users of the Client's systems who interact with the Signing Services; individuals who maintain accounts on the Trufo platform; individuals whose Personal Data appears in API requests processed by Trufo.

C.2 Types of Personal Data: Platform account registration data (name, business email, company affiliation, assigned role); authentication data (hashed credentials, MFA configuration metadata, session identifiers, login and failed-attempt timestamps); and operational data (IP addresses, device identifiers, API authentication tokens, request timestamps, user agent strings, and error logs). No manifest content or media file data is processed for these purposes. API keys used for programmatic access to the Signing Services are organizational credentials and are documented in Section B.

C.3 Purpose of Processing: Security monitoring and threat detection; fraud and abuse prevention; compliance with applicable law; maintaining service integrity and availability; platform account creation, authentication, and access management.

C.4 Legal Basis: Article 6(1)(f) of the GDPR (legitimate interests of Trufo in maintaining a secure and reliable service).

C.5 Retention: Platform account registration data is retained for the duration of the active account plus thirty (30) days following deactivation. Authentication event logs and operational data are retained for no longer than 90 days, except where extended retention is required for an active security investigation or legal obligation.

ANNEX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

Trufo implements the following measures to protect Personal Data in accordance with Article 32 of the GDPR:

1. Database Security

Trufo uses secure MongoDB databases or secure AWS logging services for data storage. Database instances are encrypted at rest using AES-256 encryption via AWS-managed keys. For large media files, Trufo operates an AWS S3 bucket upload/download system with server-side encryption enabled; storage of the media file is transient. Automated backups are performed daily and encrypted at rest.

2. Key Management (HSM-Based)

Production signing keys associated with the Client via CAWG identities are managed through AWS Key Management Service (KMS) with hardware security module (HSM) backing. Private keys never leave the HSM boundary; all signing operations are performed within the HSM. Supported key types: P-256 (ES256) and P-384 (ES384) elliptic curve keys. Key access is controlled through AWS IAM policies with role-based access controls. Encryption keys are subject to automatic rotation in accordance with AWS KMS key rotation policies.

3. Access Controls

Accounts are protected by MFA (passkey or TOTP) and require email activation. Administrator users of an organization can set role-based permissions within said organization. Access to production systems and Personal Data is granted on a least-privilege basis. Personnel with access to Personal Data receive security awareness training upon onboarding and annually thereafter.

4. Encryption in Transit

All API communications are encrypted using TLS 1.2 or higher. All communications with AWS KMS are over HTTPS.

5. Incident Detection and Response

Trufo maintains centralized logging, alerting, and documented incident response procedures for security events. Incident response procedures are reviewed following each material incident and at least annually.

6. Secure Deletion

When Personal Data is due for deletion under this DPA, Trufo uses cryptographic erasure or secure overwrite procedures. Transient data (media files processed via API) is deleted automatically upon completion of the API request unless the Client has configured extended retention.

ANNEX 3: LIST OF SUB-PROCESSORS

Trufo engages the Sub-processors listed at: https://trufo.ai/legal/subprocessors.

ANNEX 4: STANDARD CONTRACTUAL CLAUSES

This Annex 4 incorporates by reference the Standard Contractual Clauses adopted by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, Module Two (Controller to Processor) (the "EU SCCs"). The EU SCCs constitute the operative transfer mechanism for all international transfers of Personal Data under this DPA as of the Effective Date.

Module Selected: Module Two (Transfer Controller to Processor)

Clause 7 (Docking Clause): Included. Additional parties may accede to these SCCs.

Clause 9(a) (Sub-processor Authorization): Option 2 (General written authorization), consistent with Article 6 of this DPA.

Clause 11(a) (Redress): Not included. The parties have determined that alternative redress mechanisms under the Principal Agreement and applicable law provide adequate protection for Data Subjects.

Clause 13(a) (Supervision): The competent supervisory authority shall be the Bavarian State Office for Data Protection Supervision (Bayerisches Landesamt für Datenschutzaufsicht, BayLDA).

Clause 15 (Obligations of the data importer in case of access by public authorities): Included. The data importer shall comply with the obligations set out in Clause 15.

Clause 17 (Governing Law): The SCCs shall be governed by the laws of the Federal Republic of Germany.

Clause 18(b) (Forum): Disputes shall be resolved before the courts of Nürnberg, Germany.

Annex I.A (List of Parties):

Data Exporter: The Client, as identified on the signature page of this DPA.

Data Importer: Trufo, as identified on the signature page of this DPA.

Annex I.B (Description of Transfer): As set out in Section B of Annex 1 to this DPA.

Annex I.C (Competent Supervisory Authority): The Bavarian State Office for Data Protection Supervision (Bayerisches Landesamt für Datenschutzaufsicht, BayLDA).

Annex II (Technical and Organizational Measures): As set out in Annex 2 to this DPA.

Annex III (List of Sub-processors): As set out in Annex 3 to this DPA.

The full text of the SCCs is available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj. In the event of any conflict between the SCCs and this DPA, the SCCs shall prevail to the extent of such conflict.