Data Processing Agreement

Version 3.0 — Effective January 15, 2026

Between	
Data Processor:	**Metricall (a parent organization of Uplint)** The trust layer for incoming data legal@uplint.dev
Data Controller:	**[Your Company Name]** [Your Address] [Your Contact Email]

This Data Processing Agreement ("**DPA**") is entered into between the Data Controller identified above ("**Controller**") and Metricall (a parent organization of Uplint) ("**Processor**"), and supplements the Terms of Service available at uplint.dev/terms (the "**Agreement**").

This DPA reflects the parties' commitment to abide by applicable data protection laws, including the EU General Data Protection Regulation ("**GDPR**"), the UK GDPR, and other applicable privacy legislation.

Contents

Annex D — Standard Contractual Clauses

1. Definitions

"Controller" means the entity that determines the purposes and means of the processing of Personal Data, as identified in this DPA.

"Data Subject" means an identified or identifiable natural person whose Personal Data is processed.

"GDPR" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council.

"Personal Data" means any information relating to a Data Subject that is processed by the Processor on behalf of the Controller in connection with the Agreement.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

"Processing" means any operation performed on Personal Data, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, erasure, or destruction.

"Processor" means Metricall (a parent organization of Uplint), which processes Personal Data on behalf of the Controller.

"Sub-processor" means any third party engaged by the Processor to process Personal Data on behalf of the Controller.

"Standard Contractual Clauses" ("SCCs") means the contractual clauses approved by the European Commission for the transfer of Personal Data to third countries.

"Services" means the file validation, virus scanning, storage, and delivery services provided by Uplint under the Agreement.

2. Scope and Purpose of Processing

2.1 The Processor shall process Personal Data only on behalf of the Controller and in accordance with the Controller's documented instructions, unless required to do so by applicable law. In such case, the Processor shall inform the Controller of that legal requirement before processing, unless prohibited by law.

2.2 The subject matter, duration, nature, and purpose of the processing, as well as the types of Personal Data and categories of Data Subjects, are described in **Annex A**.

2.3 The Processor shall not process Personal Data for any purpose other than as specified in this DPA and the Agreement, and shall not sell, rent, or otherwise make available Personal Data to any third party except as provided herein.

3. Obligations of the Processor

The Processor shall:

3.1 Process Personal Data only in accordance with the Controller's documented instructions, including with regard to transfers of Personal Data to a third country.

3.2 Ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.3 Implement and maintain appropriate technical and organizational measures as set out in **Annex B** to ensure a level of security appropriate to the risk.

3.4 Not engage another processor (Sub-processor) without prior specific or general written authorization of the Controller, subject to Section 5.

3.5 Assist the Controller, taking into account the nature of processing, in responding to requests from Data Subjects exercising their rights under applicable data protection laws.

3.6 Assist the Controller in ensuring compliance with breach notification obligations, data protection impact assessments, and prior consultations with supervisory authorities.

3.7 At the choice of the Controller, delete or return all Personal Data after the end of the provision of Services, and delete existing copies unless applicable law requires storage.

3.8 Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA, and allow for and contribute to audits and inspections.

4. Rights of the Controller

4.1 The Controller retains full ownership of all Personal Data and may instruct the Processor regarding the processing of Personal Data at any time.

4.2 The Controller has the right to request, at any time, information regarding the Processor's processing activities, security measures, and compliance status.

4.3 The Controller may export all Personal Data at any time through the Processor's API or dashboard in standard machine-readable formats (JSON, CSV).

4.4 The Controller may object to changes in Sub-processors as described in Section 5.

5. Sub-processors

5.1 The Controller provides general authorization for the Processor to engage Sub-processors listed in **Annex C**.

5.2 The Processor shall notify the Controller of any intended addition or replacement of Sub-processors at least **30 days** prior to the engagement, providing the Controller an opportunity to object to such changes.

5.3 If the Controller objects to a new Sub-processor on reasonable grounds relating to data protection, the parties shall discuss the objection in good faith. If no resolution is reached within 30 days, the Controller may terminate the affected Services without penalty.

5.4 The Processor shall impose data protection obligations no less protective than those in this DPA on each Sub-processor by way of a written contract.

5.5 The Processor remains fully liable to the Controller for the performance of each Sub-processor's obligations.

6. Data Transfers

6.1 The Processor shall not transfer Personal Data to a country outside the European Economic Area ("EEA") unless appropriate safeguards are in place as required by applicable data protection law.

6.2 For transfers to the United States, the parties agree to the Standard Contractual Clauses (Module 2: Controller to Processor) as approved by European Commission Implementing Decision (EU) 2021/914, incorporated by reference in **Annex D**.

6.3 The Processor implements supplementary measures including encryption in transit (TLS 1.3) and at rest (AES-256-GCM), strict access controls, and regular security audits.

6.4 Enterprise customers may elect EU-only data residency (AWS EU-West-1 Ireland or EU-Central-1 Frankfurt), ensuring no transfer of file data outside the EU.

7. Security Measures

7.1 The Processor shall implement and maintain the technical and organizational security measures described in **Annex B**.

7.2 The Processor shall regularly test, assess, and evaluate the effectiveness of these measures, including through annual SOC 2 Type II audits and regular penetration testing.

7.3 The Processor may update its security measures from time to time, provided that such updates do not materially decrease the overall level of security.

8. Data Breach Notification

8.1 The Processor shall notify the Controller of any Personal Data Breach without undue delay and in any event within **48 hours** after becoming aware of the breach.

8.2 Such notification shall include:

- A description of the nature of the breach, including the categories and approximate number of Data Subjects and Personal Data records concerned;
- The name and contact details of the Processor's data protection contact;
- A description of the likely consequences of the breach;
- A description of the measures taken or proposed to address the breach, including measures to mitigate its possible adverse effects.

8.3 The Processor shall cooperate with the Controller and take reasonable steps to assist in the investigation, mitigation, and remediation of each Personal Data Breach.

9. Data Subject Requests

9.1 The Processor shall promptly notify the Controller if it receives a request from a Data Subject to exercise rights under applicable data protection law.

9.2 The Processor shall not respond to such requests directly unless authorized to do so by the Controller, except to direct the Data Subject to the Controller.

9.3 The Processor shall assist the Controller in fulfilling its obligations to respond to Data Subject requests, including requests for access, rectification, erasure, restriction, portability, and objection.

10. Audit Rights

10.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with this DPA and applicable data protection law.

10.2 The Controller may conduct audits, including inspections, of the Processor's processing activities. Audits shall be conducted with reasonable notice (at least 30 days), during normal business hours, and no more than once per year unless required by a supervisory authority or following a Personal Data Breach.

10.3 The Processor shall provide the Controller with its most recent SOC 2 Type II report upon written request and subject to a non-disclosure agreement.

11. Data Return and Deletion

11.1 Upon termination of the Agreement or upon the Controller's request, the Processor shall, at the Controller's election, return all Personal Data in a standard machine-readable format or securely delete all Personal Data.

11.2 The Processor shall complete deletion within **30 days** of the request and provide written certification of deletion upon the Controller's request.

11.3 The Processor may retain Personal Data to the extent required by applicable law, in which case it shall inform the Controller and continue to protect such data in accordance with this DPA.

12. Term and Termination

12.1 This DPA shall remain in effect for the duration of the Agreement and shall automatically terminate upon termination or expiration of the Agreement.

12.2 The provisions of this DPA that by their nature should survive termination (including Sections 8, 10, 11, and 13) shall survive any termination or expiration.

13. Limitation of Liability

13.1 The total liability of each party under this DPA shall be subject to the limitations and exclusions of liability set out in the Agreement.

13.2 Nothing in this DPA shall limit either party's liability for fraud, gross negligence, willful misconduct, or any liability that cannot be excluded by applicable law.

14. General Provisions

14.1 **Governing Law.** This DPA shall be governed by and construed in accordance with the laws governing the Agreement, unless otherwise required by applicable data protection law.

14.2 **Amendments.** This DPA may only be amended in writing signed by both parties.

14.3 **Conflict.** In the event of a conflict between this DPA and the Agreement, this DPA shall prevail with respect to the processing of Personal Data.

14.4 **Severability.** If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

14.5 **Entire Agreement.** This DPA, together with its Annexes and the Agreement, constitutes the entire agreement between the parties regarding the processing of Personal Data.

Signatures

IN WITNESS WHEREOF, the parties have executed this Data Processing Agreement as of the date last signed below.

DATA PROCESSOR — Metricall (a parent organization of Uplint)

_____

Signature

_____

Name and Title

_____

Date

DATA CONTROLLER — [Your Company Name]

_____

Signature

_____

Name and Title

_____

Date

Annex A — Details of Processing

Category	Details
Subject Matter	Processing of files and associated metadata uploaded by the Controller's end users through the Uplint platform.
Duration	For the term of the Agreement, plus any retention period required for deletion.
Nature of Processing	Collection, storage, validation, virus scanning, encryption, delivery, and deletion of files and metadata.
Purpose	To provide the Controller with file upload validation, security scanning, storage, and delivery services as described in the Agreement.
Types of Personal Data	Files uploaded by end users (which may contain any type of personal data); file metadata (filename, size, type, upload timestamp); user identifiers (API keys, IP addresses); account information (name, email, company).
Categories of Data Subjects	End users of the Controller's applications who upload files through Uplint; the Controller's employees and authorized users.

Annex B — Technical and Organizational Measures

B.1 Encryption

- Data at rest: AES-256-GCM encryption via AWS KMS with hardware security modules (HSM)
- Data in transit: TLS 1.3 for all connections
- Automatic key rotation on a regular schedule

B.2 Access Controls

- Role-based access control (RBAC) across all systems
- Multi-factor authentication (MFA) required for all employee access
- API key scopes and granular permissions for Controller access
- Just-in-time access provisioning for support personnel
- Quarterly access reviews and recertification

B.3 Network Security

- Private VPCs with network segmentation
- Web Application Firewall (WAF) via Cloudflare
- DDoS protection and rate limiting
- Intrusion detection and prevention systems

B.4 Monitoring and Logging

- 24/7 security monitoring and alerting
- SIEM (Security Information and Event Management) with log aggregation
- Anomaly detection for unusual access patterns
- Audit logs retained for a minimum of 90 days

B.5 Personnel Measures

- Background checks for all employees with access to Personal Data
- Confidentiality agreements for all personnel
- Regular security awareness training
- Principle of least privilege enforced

B.6 Business Continuity

- Multi-availability zone deployment
- Automated backups with geographic redundancy
- Documented disaster recovery plan with regular testing
- Recovery Time Objective (RTO): 4 hours; Recovery Point Objective (RPO): 1 hour

B.7 Certifications and Auditing

- Annual SOC 2 Type II audit
- Regular penetration testing by independent third parties
- Continuous vulnerability scanning
- Responsible disclosure and bug bounty program

Annex C — Authorized Sub-processors

The following Sub-processors are authorized by the Controller as of the effective date of this DPA. The Processor shall notify the Controller at least 30 days before engaging any new Sub-processor.

Sub-processor	Purpose	Location	Data Types
Amazon Web Services (AWS)	Cloud infrastructure, file storage, databases	US (default); EU available for Enterprise	All customer files and account data
Cloudflare	CDN, DDoS protection, DNS, WAF	Global (edge locations)	Request metadata, cached content
Stripe	Payment processing and billing	United States	Billing information only
Postmark	Transactional email delivery	United States	Email addresses, notification content
Plausible Analytics	Privacy-focused website analytics	European Union (Germany)	Anonymous, aggregated usage data only

Annex D — Standard Contractual Clauses

The parties agree that the Standard Contractual Clauses (Module 2: Controller to Processor) as set out in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 are hereby incorporated by reference into this DPA.

The following selections apply to the SCCs:

SCC Clause	Selection
Module	Module 2 (Controller to Processor)
Clause 7 (Docking clause)	Included
Clause 9(a) (Sub-processor authorization)	Option 2: General written authorization with 30-day notice
Clause 11(a) (Redress)	Optional clause not included
Clause 13(a) (Supervision)	The supervisory authority of the EU Member State in which the Controller is established
Clause 17 (Governing law)	Laws of Ireland
Clause 18(b) (Forum)	Courts of Ireland

End of Data Processing Agreement — Metricall (a parent organization of Uplint) — uplint.dev