Data Processing Agreement (DPA)

Version 1 — 21 May 2026

Pursuant to Article 28 of Regulation (EU) 2016/679 ("GDPR").

Preamble

This Data Processing Agreement ("DPA") governs the processing of personal data carried out by the Processor on behalf of the Controller in connection with the use of the conv2pdf service (file conversion to PDF, accessible via web interface and REST API on the domains `conv2pdf.com` and `api.conv2pdf.com`).

It supplements the Terms of Service and the subscription contract entered into by the Controller. In the event of a conflict between this DPA and the Terms of Service, this DPA prevails with respect to the processing of personal data.

1. Identification of the parties

1.1 The Processor

- **Trade name:** Iris Digital
- **Representative:** Jamal Tantaoui
- **Legal form:** French sole proprietorship (*entreprise individuelle*, *micro-entrepreneur* regime)
- **SIREN:** 524 317 872
- **Registered address:** 8 chemin dou Sarpout, 33610 Cestas, France
- **Contact:** contact@conv2pdf.com

Hereinafter referred to as "**conv2pdf**" or the "Processor".

1.2 The Controller

Any natural or legal person who has subscribed to a paid conv2pdf API plan (Starter, Growth, Business, Enterprise plans) or who uses the service in B2B mode under an authenticated account. Identified at the time of signature of this DPA by:

- corporate name or full name
- legal form
- registration number
- registered address
- name and function of the signatory
- professional email contact

Hereinafter referred to as the "Controller" or the "Client".

2. Definitions

Capitalised terms not defined below have the meaning given to them in the GDPR.

- **Personal Data:** any information relating to an identified or identifiable natural person, as defined in Article 4 of the GDPR.
- **Processing:** any operation performed on Personal Data, within the meaning of Article 4 of the GDPR.
- **Controller:** the Client, who determines the purposes and means of the Processing.
- **Processor:** conv2pdf, which processes the Data on behalf of the Controller.
- **Sub-processors:** the providers used by conv2pdf to deliver the service (see Annex 2).
- **Data Subject:** the natural person whose Data is processed.
- **Personal Data Breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Data.

3. Subject matter, nature and purpose of the Processing

3.1 Subject matter

The Processor processes, on behalf of the Controller, the Data contained in files uploaded via the conv2pdf API or web interface, solely for the purpose of conversion to PDF (and related operations: merge, split, compress, password-protect, public sharing).

3.2 Nature of the Processing

The operations covered by this DPA are:

- the receipt and temporary storage of the input file;
- automated conversion to PDF format using the open-source tools LibreOffice, Ghostscript, qpdf, sharp and pdf-lib;
- making the output file available to the Controller;
- automatic deletion of input and output files within one hour at the latest of their creation;
- technical logging (timestamp, size, processing duration) for statistical and billing purposes.

3.3 Purpose

Performance of the PDF conversion service contract subscribed to by the Controller (GDPR Article 6.1.b).

3.4 Duration

This DPA takes effect on the date of acceptance by the Controller and remains in force throughout the duration of the conv2pdf API subscription. It terminates automatically upon termination of the subscription, without prejudice to the obligations that survive termination (in particular the deletion of the Data).

3.5 Categories of Data processed and Data Subjects concerned

See **Annex 3**.

4. Obligations of the Processor

4.1 Processing on documented instructions

The Processor processes the Data only on documented instructions from the Controller, including with regard to transfers to a third country, unless required to do so by law. Documented instructions arise from

this DPA, the Terms of Service and the explicit parameters passed to the API endpoints.

4.2 Confidentiality

The Processor ensures that persons authorised to process the Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.3 Security measures

The Processor implements the technical and organisational measures described in **Annex 1**, in accordance with Article 32 of the GDPR.

4.4 Sub-processors

The Controller authorises the Processor to engage the sub-processors listed in **Annex 2**. Any modification of this list (addition, replacement) will be notified to the Controller by email with at least thirty days' notice, during which the Controller may raise a reasoned objection. Failing any objection within this period, the modification is deemed accepted.

The Processor imposes on each sub-processor the same data protection obligations as those set out in this DPA, by written contract.

4.5 Assistance to the Controller

The Processor assists the Controller, through appropriate technical and organisational measures and insofar as possible, in:

- responding to requests from Data Subjects exercising their rights (access, rectification, erasure, objection, portability, restriction);
- ensuring compliance with the obligations laid down in Articles 32 to 36 of the GDPR (security, notification, impact assessment, prior consultation).

4.6 Notification of a Personal Data Breach

In the event of a Personal Data Breach affecting the Data processed on behalf of the Controller, the Processor notifies the Controller without undue delay and in any event within seventy-two hours of becoming aware of it, by email to the contact address registered on the customer account.

The notification states at a minimum:

- the nature of the Breach, including the categories and approximate number of Data Subjects and Data records concerned;
- the likely consequences;
- the measures taken or proposed to remedy the Breach and mitigate its effects.

4.7 Deletion or return of Data

At the end of this DPA, and at the Controller's option formulated in writing within thirty days following termination, the Processor shall:

- either permanently delete all Data processed on behalf of the Controller, including backup copies, within a maximum period of sixty days;
- or return such Data to the Controller in a standard machine-readable format, then delete it.

In the absence of a request within the thirty-day period, the Processor proceeds automatically with deletion. The compression and erasure of backups may take up to an additional sixty days due to the natural backup rotation cycle (see Annex 1).

4.8 Audit

The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA. It allows for audits to be conducted by the Controller or by an independent auditor mandated by the Controller, limited to one audit per calendar year, by appointment scheduled at least thirty days in advance, without prejudice to the rights of the CNIL or any other competent supervisory authority.

5. Obligations of the Controller

The Controller:

- ensures it has an appropriate legal basis for the Processing of the Data submitted to the Processor;
- informs the Data Subjects of the use of the Processor and of the nature of the Processing;
- guarantees that the Data submitted is lawful, accurate and limited to what is necessary for the intended purpose;
- does not submit, via the service, special categories of Data (GDPR Article 9) or Data relating to criminal convictions and offences (Article 10) without having previously informed the Processor and obtained its written consent.

6. Transfers outside the European Union

The Processor warrants that **no transfer** of Data to a third country or international organisation outside the European Union takes place in the context of the conv2pdf service. The entire infrastructure (servers, databases, backups, transactional email) is located in France or within the European Union (see Annex 2).

Stripe Payments Europe Ltd, based in Ireland, is the only sub-processor that may use, for fraud prevention purposes, technical components located outside the EU — however, no Data contained in the converted files is transmitted to Stripe (Stripe only receives payment information and the billing email).

7. Duration, termination and survival

This DPA follows the fate of the subscription contract. The obligations relating to confidentiality (Section 4.2), to the deletion of Data (Section 4.7) and to the retroactive notification of a prior Personal Data Breach (Section 4.6) survive termination for the duration necessary for their execution.

8. Governing law and jurisdiction

This DPA is governed by French law. Any dispute relating to its interpretation or execution falls under the exclusive jurisdiction of the courts of the place of the Processor's registered office, subject to mandatory legal provisions to the contrary.

9. Signatures

The Processor	The Controller
Jamal Tantaoui	*Signatory name*
Representative of Iris Digital	*Function*
Date: _____	Date: _____
Signature:	Signature:

Annex 1 — Technical and Organisational Measures (TOMs)

In accordance with Article 32 of the GDPR, the Processor implements the following measures.

A1.1 Transport security

- Minimum TLS 1.2 encryption (TLS 1.3 supported) on all HTTPS connections, Let's Encrypt certificates renewed automatically.
- Automatic HTTP-to-HTTPS redirection, HSTS header valid one year with subdomain inclusion.

A1.2 Storage security

- Input and output files deleted within one hour at the latest of creation (automated deletion by internal cron running every five minutes).
- No result caching: two conversions of the same file produce two strictly independent PDFs, stored and purged separately.
- Passwords (where applicable) hashed with Argon2id, never stored in clear.
- API keys hashed in SHA-256, never stored in clear, displayed only once upon creation.
- Session cookies HMAC-signed, HttpOnly attribute, SameSite Lax, lifetime of thirty days.

A1.3 Network security

- L3/L4 anti-DDoS protection included by the hosting provider OVH.
- Application-level rate limiting per IP address (Nginx + rate-limit module).
- UFW firewall configured to deny by default, openings limited to 80/443 and a custom SSH port.
- Automatic banning by fail2ban in case of repeated attempts (login, access to password-protected files).
- Port surveillance by portsentry, intrusion detection by rkhunter.

A1.4 Administrative access security

- SSH restricted to whitelisted IP addresses, on a non-standard port.

- Ed25519 key authentication only, password disabled.
- Application account separate from the administration account, with no inbound SSH access.
- Application service launched under systemd with security constraints (NoNewPrivileges, ProtectHome, ProtectSystem strict, restricted namespaces).

A1.5 Logging and traceability

- Nginx server logs kept seven days for security.
- Conversion technical metadata (tool used, size, duration) kept thirty days for statistical purposes.
- When the public sharing feature is used, the contributor's IP address, source port and user-agent are kept one year in a dedicated audit log, in accordance with Article 6 II of the French law for confidence in the digital economy (*LCEN*) and decree n° 2021-1363. This data is only disclosed to judicial authorities upon formal legal request.

A1.6 Backups

- Automatic database backups every six hours, encrypted in transit (TLS) to an OVH object storage located in France (Strasbourg).
- Retention of fourteen days locally and thirty days in object storage, automated deletion of older backups.

A1.7 Updates and maintenance

- Debian stable operating system, security updates installed within a maximum of thirty days of publication by the vendor.
- Application dependencies tracked via Dependabot with automatic minor and security version updates, manual review for major changes.

A1.8 Personnel confidentiality

- The Processor is a sole proprietorship; no employee has access to the Data. The legal representative is himself subject to a confidentiality obligation under this DPA.
- In the event of future engagement of collaborators or contractors, they will be contractually subject to an equivalent confidentiality obligation before any access to the Data.

Annex 2 — Authorised sub-processors

Sub-processor	Country	Role	Data transmitted
OVH SAS	France (Roubaix HQ, Gravelines datacenter)	Infrastructure hosting	All Data, in encrypted environment

Sub-processor	Country	Role	Data transmitted
Brevo	France	Transactional emails (magic-link sign-in, email change verification, contact form message forwarding)	Recipient email, email content
Stripe Payments Europe Ltd	Ireland	Payment processing (paid Premium and API subscriptions)	Client professional email, Stripe customer ID, amounts. **Stripe does not receive any Data contained in the converted files.**

None of these sub-processors is located outside the European Union within the meaning of the GDPR.

Annex 3 — Categories of Data and of Data Subjects

A3.1 Data processed

The Processor processes the following Personal Data:

- content of files uploaded by the Client or by the Client's end users, where these files contain Personal Data (the content is never inspected, indexed or analysed);
- email address of the Client's API account;
- IP addresses of API requests and web interface accesses;
- Stripe customer ID (for billing);
- conversion technical metadata (timestamp, size, duration, tool used).

A3.2 Data Subjects

- the API Client (natural person subscribing to the plan, or natural person representing the legal entity Client);
- the Client's end users when they indirectly interact with conv2pdf via the Client's integration;
- the persons whose Data appears in the converted files, the nature of which depends on the use the Client makes of the service.

A3.3 Retention periods

Data	Period	Reason
Input and output files	1 hour maximum	Service performance
Job metadata (size, duration, tool)	30 days	Internal statistics and billing

Data	Period	Reason
Client account (email, plan, hashed API keys)	Duration of the subscription	Contract performance
Stripe customer ID	10 years	Legal accounting obligation
Nginx server logs	7 days	Security
Public sharing audit log (IP, port, user-agent)	1 year	French legal obligation (*LCEN*)
Database backups	14 days local / 30 days object storage	Service continuity

---

In case of any discrepancy between this English translation and the French version, the French version prevails as the legally binding document.