

Data Processing Agreement (DPA)

Last updated: 20 June 2026 · enrow.io/en/legal/dpa

CONTENTS

Clause 1 — Purpose	Clause 9 — Right of Audit
Clause 2 — Definitions	Clause 10 — International Compliance
Clause 3 — Roles of the Parties	Clause 11 — Liability
Clause 4 — Description of the Processing	Clause 12 — Term and Termination
Clause 5 — Obligations of ENROW as Data Processor	Clause 13 — Final Provisions
Clause 6 — Obligations of the Client	Annex 1 — Description of the Processing
Clause 7 — Sub-Processors	Annex 2 — Technical and Organisational Measures (TOMs)
Clause 8 — Transfers Outside the EEA	Annex 3 — List of Sub-Processors

This Data Processing Agreement (hereinafter the "DPA") is entered into between:

SCHRUTE FARMS, a French limited liability company (SARL) with a share capital of five hundred euros (€500), having its registered office at 123 Rue De Rome, 75017 Paris, registered with the Paris Trade and Companies Register (RCS Paris) under number 981 316 300, represented by its joint managers Thomas LUCY and Louis CONGARD, operating the "ENROW" service (hereinafter "ENROW" or the "Provider"),

and

The Client, being the legal entity which has subscribed to the Service and accepted ENROW's General Terms and Conditions of Sale and Use (the "Terms") (hereinafter the "Client"),

hereinafter referred to individually as a "Party" and collectively as the "Parties".

This DPA is entered into pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR) and Loi n°78-17 of 6 January 1978, as amended (Loi Informatique et Libertés). It forms an integral part of the Contract between the Parties, as defined in the contractual hierarchy set out in Clause 1 of the Terms.

The Data Protection Officer (DPO) of ENROW is Mr Louis CONGARD, contactable at dpo@enrow.io.

Clause 1 — Purpose

The purpose of this DPA is to set out the conditions under which ENROW processes Personal Data on behalf of the Client in connection with the provision of the B2B professional data enrichment Service, and to specify the obligations of each Party with respect to data protection.

Clause 2 — Definitions

Terms used in this DPA shall bear the same meaning as in the Terms, save for the specific definitions set out below:

- **"Personal Data"**: any information relating to an identified or identifiable natural person within the meaning of Article 4(1) of the GDPR.
- **"Data Controller"**: the natural or legal person which determines the purposes and means of the processing of Personal Data (Article 4(7) GDPR).
- **"Data Processor"**: the natural or legal person which processes Personal Data on behalf of the Data Controller (Article 4(8) GDPR).

- **"Sub-Processor"**: any sub-processor engaged by ENROW to process Personal Data on behalf of the Client.
- **"Data Breach"**: any breach of security leading, whether accidentally or unlawfully, to the destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data (Article 4(12) GDPR).
- **"Data Subject"**: any identified or identifiable natural person whose Personal Data is processed.
- **"Supervisory Authority"**: any independent public authority responsible for monitoring the application of data protection regulations (in France: the CNIL).

Clause 3 — Roles of the Parties

3.1 — Dual Capacity of ENROW

The Parties acknowledge that ENROW acts in two distinct capacities:

(a) Independent Data Controller: ENROW acts as Data Controller in respect of the Personal Data which it collects, aggregates and maintains in its own enrichment database (professional emails, telephone numbers, LinkedIn profiles, company information). Such processing is predicated upon ENROW's legitimate interest (Article 6(1)(f) GDPR), as documented in a LIA reviewed on an annual basis.

(b) Data Processor: ENROW acts as Data Processor within the meaning of Article 28 of the GDPR when it processes Client Data (data transmitted by the Client for enrichment) on behalf of and on the instructions of the Client.

3.2 — The Client as Data Controller

The Client acts as Data Controller in respect of:

- The Client Data which it transmits to ENROW for enrichment;
- Its use of the Enriched Data returned by the Service.

The Client shall determine alone the purposes and means of its use of the Enriched Data downstream of the Service and shall be solely responsible for compliance with its obligations under the GDPR and the French Data Protection Act (Loi Informatique et Libertés) in that regard.

Clause 4 — Description of the Processing

The details of the processing are described in Annex 1 to this DPA. They include, in particular:

- **Purpose of processing:** Enrichment of B2B professional data on behalf of the Client.
- **Categories of Data Subjects:** Professional contacts (prospects, potential clients) of the Client: employees, directors, partners of legal entities.
- **Categories of Personal Data processed:** Surname, first name, professional email address, professional and/or personal telephone number, job title, company name, LinkedIn profile URL, company information (sector, size, location).
- **Sensitive data:** No sensitive data within the meaning of Article 9 of the GDPR shall be processed.
- **Duration of processing:** Duration of the Subscription. Client Data shall be retained for a maximum of 90 days and thereafter automatically deleted. Technical cache: 48 hours.
- **Location of processing:** European Union — AWS Paris (eu-west-3).

Clause 5 — Obligations of ENROW as Data Processor

5.1 — Client's Instructions

ENROW shall process Client Data only on the documented instructions of the Client. These Terms and this DPA constitute the Client's initial instructions. Any additional instructions shall be transmitted in writing (by email to dpo@enrow.io).

If ENROW considers that an instruction constitutes a violation of the GDPR or any other applicable regulation, it shall inform the Client forthwith in writing.

5.2 – Confidentiality

ENROW warrants that persons authorised to process Personal Data have committed themselves to confidentiality or are subject to an appropriate statutory obligation of confidentiality. Only those persons whose access is strictly necessary for the performance of the Service shall have access.

5.3 – Security of Processing

ENROW shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the GDPR. Such measures are described in Annex 2 to this DPA. ENROW shall carry out regular reviews of the effectiveness of such measures.

5.4 – Data Breach Notification

In the event of a Data Breach affecting Client Data, ENROW undertakes to:

- Notify the Client without undue delay and in any event within seventy-two (72) hours of becoming aware thereof;
- Provide the following information: a description of the nature of the breach (categories and approximate number of Data Subjects and records affected), likely consequences, measures taken or proposed to be taken to remedy the breach, and contact details of the DPO;
- Document the breach in an internal register and cooperate with the Client to enable it to comply with its own notification obligations (Articles 33 and 34 GDPR);
- Notify the CNIL within 72 hours in its capacity as Data Controller in respect of data held in its own enrichment database.

5.5 – Assistance to the Client

ENROW shall assist the Client, insofar as is reasonably practicable having regard to the nature of the processing, in:

- Responding to requests by Data Subjects to exercise their rights (access, rectification, erasure, objection, portability, restriction);
- Complying with its obligations under Articles 32 to 36 of the GDPR (security, breach notification, data protection impact assessment);
- Responding to requests from and audits by any Supervisory Authority.

If ENROW receives a request directly from a Data Subject in respect of Client Data, it shall inform the Client without undue delay and shall not respond directly save on the Client's instructions.

5.6 – Fate of Data upon Termination

In accordance with Clause 14.3 of the Terms, upon termination of the Contract:

- **Export:** the Client shall have thirty (30) days in which to export its Client Data in CSV and/or JSON format via the Software, the API or upon request to support@enrow.io;
- **Deletion:** after such period, ENROW shall permanently delete all Client Data, including copies and backups, within a further period of thirty (30) days;
- **Certification:** ENROW shall provide the Client, upon request, with a written certificate of deletion.

The deletion of Client Data shall not affect anonymised and aggregated data used in accordance with Clause 9.6 of the Terms.

Clause 6 – Obligations of the Client

The Client, in its capacity as Data Controller, undertakes to:

- Have a valid legal basis for transmitting Client Data to ENROW and for using the Enriched Data (Clause 8.2 of the Terms);
- Inform Data Subjects in accordance with Articles 13 and 14 of the GDPR;
- Ensure that its instructions to ENROW are compliant with applicable regulations;
- Not transmit any sensitive data within the meaning of Article 9 of the GDPR;
- Cooperate with ENROW in the event of a Data Breach, an audit or a request from a Supervisory Authority.

Clause 7 — Sub-Processors

7.1 — General Authorisation

The Client hereby grants ENROW a general authorisation to engage Sub-Processors for the provision of the Service (including without limitation Third-Party enrichment Providers and hosting providers). The list of Sub-Processors currently engaged is set out in Annex 3 to this DPA and is also available upon request from the DPO.

7.2 — Notification and Right of Objection

In accordance with Clause 12.2 of the Terms, ENROW shall notify the Client of any change to the Sub-Processors (whether by addition or replacement) no fewer than fifteen (15) days prior to the effective date of such change. The Client may object in writing within fifteen (15) days. Failing agreement, the objection shall be deemed to constitute notice of termination of the Contract in accordance with Clause 12.2 of the Terms.

7.3 — Obligations Imposed on Sub-Processors

ENROW shall contractually impose on each Sub-Processor data protection obligations substantially equivalent to those contained in this DPA, in particular as regards confidentiality, security, purpose limitation and data deletion.

7.4 — Liability

ENROW shall remain fully liable to the Client for the performance by its Sub-Processors of their data protection obligations.

Clause 8 — Transfers Outside the EEA

All data is hosted within the European Economic Area (EEA), on AWS servers in Paris (eu-west-3).

In the event that a transfer of Personal Data to a third country becomes necessary, in particular in connection with the engagement of a Sub-Processor established outside the EEA, ENROW shall ensure in advance that appropriate safeguards are in place in accordance with Chapter V of the GDPR:

- **Adequacy decision** of the European Commission (Article 45 GDPR);
- **Standard Contractual Clauses (SCCs)** adopted by the European Commission (Implementing Decision 2021/914), supplemented where necessary by additional measures (Article 46(2)(c) GDPR);
- **Any other recognised transfer mechanism** under the GDPR (binding corporate rules, derogations under Article 49).

The Client shall be informed of any transfer outside the EEA via the list of Sub-Processors (Annex 3), which specifies, for each Sub-Processor, its location and the applicable transfer mechanism.

Where SCCs are required, they shall be deemed to have been entered into between ENROW and the relevant Sub-Processor. The Client may obtain a copy upon request from the DPO.

Clause 9 — Right of Audit

In accordance with Article 28(3)(h) of the GDPR, the Client may request an audit of ENROW's practices with respect to the processing and security of Personal Data, subject to the following conditions:

- **30 days' prior written notice** to dpo@enrow.io;
- **Maximum of 1 audit per annum**, save in the event of an established breach or a request from a Supervisory Authority;
- **Scope:** GDPR and DPA compliance only. The source code, proprietary algorithms and trade secrets shall be excluded;
- **Conduct:** by the Client or an independent third party bound by a confidentiality obligation. ENROW may object to any auditor which is a competitor;
- **Costs borne by the Client**, save in the event of a material breach by ENROW.

Alternative: ENROW may satisfy the audit request by providing the Client with one or more of the following documents, dated no more than 12 months prior: an independent third-party penetration test report, a completed CSA CAIQ (Consensus Assessments Initiative Questionnaire) security questionnaire, or any other recognised security certification or audit report as applicable. The provision of such documents shall discharge ENROW from the obligation to accept an on-site audit for the period covered, save in the event of an established breach or a request from a Supervisory Authority.

ENROW shall make available to the Client all information necessary to demonstrate compliance with its obligations under Article 28 of the GDPR.

Clause 10 — International Compliance

This DPA shall apply in the framework of the following regulations, to the extent that they are applicable to the processing:

- **GDPR** (Regulation (EU) 2016/679) and the French Data Protection Act (Loi n°78-17);
- **UK GDPR** and the Data Protection Act 2018 (in respect of Data Subjects in the United Kingdom);
- **nFADP** (the new Swiss Federal Act on Data Protection);
- **CCPA / CPRA:** ENROW acts as a "service provider" within the meaning of the CCPA/CPRA. ENROW does not sell or share Personal Data within the meaning of such regulations.

Clause 11 — Liability

The liability of each Party under this DPA shall be subject to the limitations and exclusions set out in Clause 16 of the Terms, save for the applicable exceptions (gross negligence, wilful misconduct, breach of data protection obligations).

Each Party shall be responsible for compliance with its own obligations under applicable data protection regulations. The Client shall remain solely responsible for its use of the Enriched Data downstream of the Service.

Clause 12 — Term and Termination

This DPA shall enter into force on the date of acceptance of the Terms by the Client and shall remain in force for so long as the Contract is in effect. ENROW's obligations with respect to the deletion of Client Data (Clause 5.6) and confidentiality shall survive the termination of the Contract.

Clause 13 — Final Provisions

13.1 — Hierarchy

This DPA forms an integral part of the Contract. In the event of any inconsistency between this DPA and the Terms, this DPA shall prevail in respect of any matter relating to the processing of Personal Data. In all other respects, the Terms shall prevail.

13.2 — Amendment

ENROW may amend this DPA in order to comply with changes in applicable regulations. Any material amendment shall be notified to the Client thirty (30) days prior to its coming into effect.

13.3 — Governing Law

This DPA shall be governed by French law. The courts of Paris shall have exclusive jurisdiction.

Annex 1 — Description of the Processing

- **Data Controller (Client Data):** The Client.
- **Data Processor:** SCHRUTE FARMS / ENROW.
- **DPO of the Processor:** Louis CONGARD — dpo@enrow.io.
- **Purposes of processing:** B2B professional data enrichment (search for emails, phone numbers, LinkedIn profiles, company information) from Client Data transmitted by the Client.
- **Nature of processing:** Collection, consultation, matching, structuring, temporary storage, return, deletion.
- **Categories of Data Subjects:** Professional contacts (employees, directors, partners, self-employed persons) of legal entities targeted by the Client in the course of its B2B prospecting.
- **Categories of Personal Data:** Surname, first name, professional email address, professional telephone number, personal telephone number (where applicable), job title, company name and information (sector, size, location, website), LinkedIn profile URL.
- **Sensitive data (Art. 9 GDPR):** None.
- **Legal basis (processing by ENROW as Controller):** Legitimate interest (Article 6(1)(f) GDPR) — documented LIA.
- **Frequency of processing:** Continuous, on the Client's request via the Software, the API or the Extension.
- **Client Data retention period:** Maximum 90 days after transmission, followed by automatic deletion.
- **Technical cache:** 48 hours (justified by performance and verification requirements; purged within 24 hours in the event of an objection request).
- **Location:** EU — AWS Paris (eu-west-3).

Annex 2 — Technical and Organisational Measures (TOMs)

In accordance with Article 32 of the GDPR, ENROW implements the following measures:

A. Encryption

- **In transit:** all communications are encrypted via TLS 1.2 or higher (HTTPS). Unencrypted connections are rejected.
- **At rest:** stored data is encrypted via AES-256 (native AWS encryption).
- **Passwords:** irreversible hashing using the bcrypt algorithm with individual salting.

B. Access Control

- **Authentication:** identification by email and password, with multi-factor authentication (MFA) available and recommended.
- **Access management:** strict RBAC (Role-Based Access Control) model. Each access right is limited to what is strictly necessary (principle of least privilege).
- **Sessions:** signed JWT tokens with automatic expiry.

C. Infrastructure and Hosting

- **Hosting provider:** Amazon Web Services (AWS), region eu-west-3 (Paris). AWS holds ISO 27001, SOC 1/2/3 certifications and is GDPR-compliant.
- **Network isolation:** databases and internal services are isolated within a Virtual Private Cloud (VPC) with no direct public access.
- **Backups:** automatic daily backups, encrypted, with configured retention.

D. Logging and Monitoring

- **Access logs:** traceability of user actions (identifier, action, timestamp, IP address). Logs encrypted at rest.
- **Monitoring:** continuous infrastructure monitoring with automated alerts in the event of anomalies.

E. Minimisation and Retention

- Only data strictly necessary for the provision of the Service shall be collected and processed;
- Client Data: maximum 90 days, followed by automatic deletion;
- Technical cache: 48 hours;
- Effective and irreversible deletion at the end of the retention period.

F. Organisational Security

- Data protection awareness training for all staff;
- Robust password policy for internal access;
- Principle of least privilege applied across all teams;
- Confidentiality undertaking signed by each member of staff with access to Personal Data.

G. Incident Management

- Internal security incident management procedure;
- Notification to the Client within 72 hours (Clause 5.4 of this DPA);
- Register of breaches maintained and kept up to date.

These measures are reviewed and updated on a regular basis to take account of the state of the art, implementation costs and the nature of the risks.

Annex 3 — List of Sub-Processors

Part A — Published Sub-Processors (list in force as at 20 June 2026)

Sub-Processor	Purpose	Categories of Personal Data	Location	Transfer mechanism
Amazon Web Services (AWS)	Hosting, infrastructure, databases, storage	All Personal Data processed by the Service	EU (Paris, eu-west-3)	No transfer outside EEA

Sub-Processor	Purpose	Categories of Personal Data	Location	Transfer mechanism
Stripe, Inc.	Payment processing and billing	Name, email, Client payment data	EU (Ireland)	No transfer outside EEA
SigNoz	Logging, monitoring and observability	Technical identifiers, IP addresses, usage logs	EU (European instance)	No transfer outside EEA
HubSpot, Inc.	CRM — client and prospect relationship management	Name, first name, email, company, interaction history	EU (France / Germany, European instance)	No transfer outside EEA
Brevo (ex-Sendinblue)	Email marketing and transactional communications	Name, first name, Client/User email	France / EU	No transfer outside EEA
Intercom, Inc.	Client support (chat, tickets, knowledge base)	Name, first name, email, content of support exchanges	EU (Ireland)	No transfer outside EEA
Anthropic, Inc. (Claude.ai)	AI assistance for data processing and analysis. No data is used for model training.	Data processed on an ad hoc basis without persistence	USA	Adequacy decision (EU-US DPF) + SCCs. Contractual no-training clause.
Partnero	Affiliate programme and commission management	Name, email, affiliate referral data	EU (Estonia)	No transfer outside EEA
Google Workspace	Internal communication (email, documents)	Internal data, potentially Client Personal Data in exchanges	EU (France servers)	No transfer outside EEA (France region configured)
Slack Technologies (Salesforce)	Internal communication between teams	Internal data, potentially Client Personal Data in exchanges	EU (European instance)	No transfer outside EEA

Part B — Data Enrichment Providers (Confidential List)

In connection with the provision of the enrichment Service, ENROW engages specialist providers in the following categories:

Category	Purpose	Types of Personal Data
SERP data providers	Extraction of publicly available data via search engines	Name, first name, company, publicly available professional data
Professional contact data providers	Supplementary enrichment of professional emails and telephone numbers	Professional email, professional and/or personal telephone number
Firmographic data providers	Company information enrichment (sector, size, revenue, location, legal structure)	Company name, registration number, sector, headcount, revenue, registered office address
Business signals providers	Detection of business signals (fundraising, hiring, job changes, technologies used, news)	Company data, names and roles of directors and staff, publicly available professional events

Confidentiality of the nominative list: the complete nominative list of enrichment providers, including their identity, location and the applicable transfer mechanism, constitutes a trade secret of ENROW within the meaning of Directive (EU) 2016/943 on the protection of undisclosed know-how and business information, and of Loi n°2018-670 of 30 July 2018 transposing such Directive into French law.

Communication to the Client: such list shall be communicated upon written request to the DPO (dpo@enrow.io), subject to the prior execution of a non-disclosure agreement (NDA) by the Client. The Client undertakes not to

disclose such list or the information contained therein to any third party, and to use it solely for the purposes of verifying ENROW's compliance with the GDPR.

Right of objection: the notification and right of objection mechanism provided for in Clause 7.2 of this DPA and Clause 12.2 of the Terms shall apply in full to enrichment providers. The Client shall be notified of any change no fewer than fifteen (15) days prior to the effective date, even where the name of the new provider is communicated under NDA.

Common safeguards: ENROW warrants that each enrichment provider (a) is contractually bound by data protection obligations substantially equivalent to those contained in this DPA, (b) is located within the EEA or covered by a transfer mechanism compliant with Chapter V of the GDPR, and (c) processes Personal Data solely within the strict scope of ENROW's instructions and solely for the purposes of enrichment.