Sapiologie

OFFICIAL DOCUMENT

Personal Data Processing Agreement (DPA)

Referred to in the Order Form · Article 28 of Regulation (EU) 2016/679 (GDPR) · English translation provided for convenience: only the French version is authoritative

Publisher / Processor	SAPIOLOGIE, a French simplified joint-stock company (SAS) with share capital of €64,302.08, registered with the Lille Métropole Trade and Companies Register under number 901 482 356, whose registered office is at 229 rue Solférino, 59000 Lille, France (hereinafter "Sapiologie")
Customer / Controller	The legal entity named in the Order Form that refers to this agreement (hereinafter "the Customer")
Version	1.6
Date of adoption	17 November 2026
Scope	This agreement is referred to in the Order Form signed by the duly authorised representatives of both Parties and forms an integral part of it. It is entered into by signature of the Order Form, with no separate signature required. It applies to any processing of personal data carried out by Sapiologie on behalf of the Customer, and prevails over any other contractual document for such processing only.
Data protection contact	Data protection lead: Selim Youssry. Requests relating to personal data: contact@sapiologie.com
Applicable version	The applicable version is the one referred to in the signed Order Form. It remains binding for the initial term and for each renewal period. Any change requires a written amendment signed by the duly authorised representatives of both Parties, in accordance with the General Terms and Conditions of Sale.

Preamble

Sapiologie publishes and hosts a SaaS platform for life cycle assessment and ecodesign (hereinafter "the Platform"). To provide the Platform, Sapiologie processes personal data on behalf of the Customer. Within the meaning of the GDPR, the Customer acts as **controller** and Sapiologie as **processor**, subject to article 4 bis.

This agreement sets out the conditions under which Sapiologie undertakes to carry out, on behalf of the Customer, the processing operations defined in Annex 1, in accordance with article 28 of the GDPR. It forms an integral part of the Contract between Sapiologie and the Customer, and is referred to through the Order Form under article 3.1 of the General Terms and Conditions of Sale. In the event of any conflict between this agreement and any other contractual provision relating to the protection of personal data, this agreement prevails.

Article 1: Definitions

The terms "personal data", "processing", "controller", "processor", "data subject" and "personal data breach" have the meaning given to them in article 4 of the GDPR. "Customer Data" means the personal data processed by Sapiologie on behalf of the Customer in connection with the services.

Article 2: Subject matter and duration

This agreement governs the processing of Customer Data by Sapiologie for the term of the main contract. It remains applicable until the actual deletion of the Customer Data under the conditions of article 10. The nature and purpose of the processing and the categories of data and data subjects are described in **Annex 1**.

For its own purposes (management of the contractual and commercial relationship, invoicing, support by email, compliance with its legal obligations), Sapiologie acts as controller.

Article 3: Sapiologie's obligations

Sapiologie undertakes to:

- **Documented instructions.** Process Customer Data only on documented instructions from the Customer, including with regard to transfers to a third country. The Order Form, the General Terms and Conditions of Sale, this agreement and the Customer's configuration of the Platform constitute the Customer's initial instructions; any additional instruction is given in writing. If Sapiologie considers that an instruction infringes the GDPR or another applicable data protection provision, it immediately informs the Customer. If European Union or French law requires Sapiologie to carry out processing, it informs the Customer before the processing, unless prohibited by law.
- **Exclusive purpose.** Process Customer Data only to provide the services to the Customer, never on its own account. Sapiologie may produce usage statistics in aggregated form, anonymised within the meaning of the GDPR, allowing no direct or indirect re-identification.
- **Staff confidentiality.** Ensure that the persons authorised to process Customer Data have committed to confidentiality (non-disclosure agreement signed on hiring and acceptance of the internal security policy) and receive information security awareness training at least once a year.
- **Security.** Implement the technical and organisational measures described in **Annex 2**, in accordance with article 32 of the GDPR, and maintain them at a level at least equivalent throughout the term of the contract.
- **Record.** Keep the record of the categories of processing activities carried out on behalf of the Customer, in accordance with article 30.2 of the GDPR.
- **Cooperation.** Cooperate with the competent supervisory authority (in France, the CNIL) at its request, and make available to the Customer the information necessary to demonstrate compliance with the obligations laid down in article 28 of the GDPR.
- **Authorised staff.** Restrict access to Customer Data to those members of its staff who need it to perform the services, on the principle of least privilege.

Article 4: Customer's obligations

The Customer, as controller, undertakes to: document in writing any additional instruction concerning the processing of Customer Data; ensure that it has a legal basis for the processing it carries out through the Platform and inform the data subjects; not submit to the Platform any data falling within the special categories of article 9 of the GDPR, nor any data relating to criminal convictions and offences referred to in article 10 of the GDPR; supervise the processing, including the use of the user accounts it administers.

Article 4 bis: Consultancy configuration and processing chain

Where the Customer uses the Platform to carry out analyses for the benefit of its own clients within the meaning of article 13 of the General Terms and Conditions of Sale, and acts in that capacity as processor for one of its clients acting as controller, this agreement applies between the Parties as a **sub-processing agreement within the meaning of article 28.4 of the GDPR**: Sapiologie acts as sub-processor of the Customer and its obligations are owed to the Customer alone.

In this configuration, the Customer represents and warrants: (i) that it holds the written authorisation, general or specific, of each controller concerned to engage Sapiologie as sub-processor, as well as the right to enter into this agreement; (ii) that the instructions it gives Sapiologie comply with those received from the controller and do not exceed the purposes authorised by the controller; (iii) that it is responsible, towards the controller, for informing data subjects, handling the exercise of their rights and making the notifications provided for in articles 33 and 34 of the GDPR; (iv) **that the obligations undertaken by Sapiologie under this agreement satisfy those that the Customer has itself undertaken towards each controller concerned**.

The Customer informs Sapiologie in writing, before the corresponding Data is uploaded, of any requirement of a controller that exceeds the obligations of this agreement, in particular a shorter notification period, a higher audit frequency or a location constraint. Such a measure requires a written amendment signed by both Parties; failing prior notice, these requirements are not enforceable against Sapiologie.

Sapiologie takes instructions only from the Customer, as sole point of contact: any request from a controller or from an end client of the Customer is forwarded without undue delay to the Customer, who responds to it, unless otherwise required by law or instructed in writing by the Customer; requests from a data subject follow article 7.

The Customer indemnifies Sapiologie against any claim by a controller or a data subject resulting from a breach of the warranties in this article, under the terms of article 13.2 of the General Terms and Conditions of Sale.

Audits by the ultimate controller. Requests for audit or inspection from a controller of the Customer, or based on the audit right that such controller holds over the whole sub-processing chain, are exercised through the Customer, under the conditions and within the same audit allowance provided for in article 11, regardless of the number of controllers concerned.

End of the relationship between the Customer and one of its clients. Where the Customer stops working for one of its clients while keeping its subscription, the fate of the corresponding Data is governed by **article 13.3 of the General Terms and Conditions of Sale**: the export is sent to the entity designated for that purpose in the Order Form, and deletion is carried out only on the instruction of the person authorised to give it.

Article 5: Sub-processing

The Customer gives Sapiologie a general authorisation to engage sub-processors to perform the services. Sapiologie uses a single sub-processor: **OVHcloud (OVH SAS)**, a company governed by French law, which hosts the Platform, files and backups in France.

Sapiologie informs the Customer in writing of any intended addition or replacement of a sub-processor at least **30 days** before it takes effect. The Customer may raise reasoned and legitimate objections within that period. If an objection cannot reasonably be resolved, either party may terminate the service concerned, without compensation on either side on that ground alone; Sapiologie then refunds the Customer, pro rata temporis, the prepaid amounts corresponding to the period after the effective date of termination.

Sapiologie contractually imposes on each sub-processor data protection obligations at least equivalent to those of this agreement, and remains fully liable to the Customer for the performance of their obligations.

Where the Customer declares its own application programming interface keys to power the built-in conversational agent (article 17 of the General Terms and Conditions of Sale) or connects its external agent through the MCP connector (same article), the relationship with the model provider is the Customer's alone, under the conditions of those articles.

The service providers that Sapiologie uses for its own processing as controller, in particular its email, its customer relationship management tool, its invoicing tool and its approved electronic invoicing platform, are described in Sapiologie's privacy policy.

ecoinvent Association acts as an independent controller, under the conditions of article 6 bis.

Article 6: Data location and transfers

The Platform and the Customer Data, backups included, are hosted **exclusively in France**, with OVHcloud, on **dedicated servers and an object storage service located exclusively on French territory**; they are encrypted at rest, backups included, and each client's Data is logically segregated. Customer Data is processed **exclusively in the European Union and the European Economic Area**. Any transfer that might become necessary, including on account of an already authorised sub-processor, would be notified in writing to the Customer at least 30 days in advance, subject to the right of objection under article 5, and conditional on the prior implementation of the appropriate safeguards provided for in Chapter V of the GDPR.

Article 6 bis: Third-party recipient acting on its own account

The ecoinvent database is published by **ecoinvent Association**, governed by Swiss law, and is subject to its own named-user licence. Where a User takes out, through Sapiologie, a licence to access this database, Sapiologie provides ecoinvent Association with the data needed to issue and monitor that licence: **the User's first and last name, business email address, country, company identification, licence start and end dates, licence type and volume of datasets consulted**. This information is transmitted **at the end of each quarter**.

ecoinvent Association alone determines the purposes and means of the processing it carries out on this data, for the management of its licences and compliance with its own obligations. In this respect it acts as an **independent controller**, and not as a sub-processor of Sapiologie: article 5 of this agreement does not apply to it. Sapiologie acts as a **transmitting recipient** and carries out no other processing of this data on behalf of ecoinvent Association.

This communication is **necessary for the performance** of the licence order placed by the Customer: without it, the named-user licence cannot be issued in the name of the designated User. It takes place only for Users for whom a licence is taken out through Sapiologie. Switzerland is covered by an adequacy decision of the European Commission; no additional transfer safeguard is required on that account.

The Customer informs the Users concerned of this communication and of its recipient, under articles 13 and 14 of the GDPR. Sapiologie provides it on request with the information needed for that purpose.

Article 7: Assistance to the Customer

Taking into account the nature of the processing, Sapiologie assists the Customer through appropriate technical and organisational measures:

- in responding, insofar as possible, to requests from data subjects exercising their **rights** (access, rectification, erasure, restriction, portability, objection). If such a request is sent directly to Sapiologie, Sapiologie forwards it to the Customer without undue delay; the response is the Customer's responsibility, unless the Customer instructs otherwise or the law requires otherwise;
- in ensuring compliance with the obligations under **articles 32 to 36 of the GDPR** (security of processing, notification of breaches, data protection impact assessments and prior consultation of the supervisory authority), taking into account the information available to Sapiologie.

Article 8: Personal data breaches

Sapiologie notifies the Customer of any personal data breach affecting Customer Data **without undue delay and no later than 24 hours** after qualifying the event as a personal data breach, at the contact address designated by the Customer or, failing such designation, to the administrators of the Customer account. The notification includes, insofar as the information is available: the nature of the breach, the categories and approximate number of data subjects and records concerned, the point of contact at Sapiologie, the likely consequences of the breach and the measures taken or proposed to remedy it or mitigate its effects. Information may be provided in phases if it is not all available at the same time.

Sapiologie documents the breach and the measures taken. The Customer, as controller, makes the notifications provided for in articles 33 and 34 of the GDPR where applicable; any notification made by Sapiologie on behalf of the Customer requires the Customer's prior agreement, except where Sapiologie is itself subject to a legal obligation to notify.

Article 9: Requests from public authorities

If a public authority or a third party asks Sapiologie for access to Customer Data, Sapiologie informs the Customer without delay before any disclosure, unless prohibited by law. Sapiologie verifies the lawfulness of the request, challenges through the available legal remedies any request it considers unlawful or excessive, and discloses only the data strictly necessary to respond to it. It documents each request and the action taken.

Article 10: Data at the end of the contract

At the end of the contract, for whatever reason, the Customer benefits from the **reversibility window** provided for in article 27 of the General Terms and Conditions of Sale, during which Customer Data is kept solely for the purposes of its return and of read and export access.

At the Customer's choice, Sapiologie either **returns** all Customer Data to it in usable standard formats and then **deletes** it, or **deletes** it without prior return; deletion covers all existing copies, backups included. The Customer states this choice in writing within 30 days of the end of the contract; failing that, Sapiologie deletes the data at the end of the reversibility window, after notifying the date in writing at least 15 days in advance. Deletion periods, the purge of backups and the deletion certificate are governed by **articles 27 and 28 of the General Terms and Conditions of Sale**, which apply to all Customer Data.

By way of exception, Sapiologie keeps after deletion: the data it is legally required to keep, in particular accounting records, for the statutory period; the signed Contract and the evidence of its signature, for five years from its end; connection logs, for the period provided for in article 14.2 of the General Terms and Conditions of Sale. This data is processed only for the corresponding purposes.

Article 11: Audits and demonstration of compliance

Sapiologie makes available to the Customer the information necessary to demonstrate compliance with this agreement, in particular: the current **ISO 27001:2022** certificate, issued by an independent third-party body, the available certificates of security audits and tests, and relevant extracts of its security policy under a non-disclosure agreement.

If these elements are not reasonably sufficient to demonstrate compliance, such sufficiency being assessed in good faith, the Customer may have an audit carried out, **including an on-site inspection**, under the conditions of frequency, notice, appointment of the auditor, conduct, scope and costs provided for in **articles 22.2 and 22.3 of the General Terms and Conditions of Sale**. The audit findings are confidential and communicated to Sapiologie. In the event of persistent disagreement on the sufficiency of the documentary evidence after a written exchange, the Customer retains the right to have the audit carried out under the conditions of this article.

By way of exception, the frequency and notice limitations of articles 22.2 and 22.3 of the General Terms and Conditions of Sale do not apply where the audit follows a personal data breach affecting Customer Data or is requested by a competent supervisory authority; the notice period is then reduced to 5 business days.

Article 12: Liability

Each party's liability under this agreement is governed by article 82 of the GDPR and by the main contract.

Article 13: Governing law

This agreement is governed by French law. Any dispute relating to its validity, interpretation or performance falls within the jurisdiction designated by the General Terms and Conditions of Sale.

Annex 1: Description of the processing

Item	Description
Nature and purpose of the processing	Provision of the Sapiologie Platform (life cycle assessment and ecodesign): creation and management of user accounts, user authentication (password or OpenID Connect identity federation), provision of collaborative features, technical and security logging.
Categories of data subjects	Platform Users designated by the Customer, whether or not they belong to its staff: employees of the Customer, service providers working on its behalf, and Guest Users to whom the Customer grants a right to consult or collect data, in particular staff of its suppliers and, in the consultancy configuration, staff of its own clients; contacts of the Customer for contractual and invoicing purposes; where applicable, business contacts of third parties that the Customer enters in the Platform.
Categories of data	Identification data and business contact details (last name, first name, business email address, job title, business telephone number where applicable); connection and usage data (identifiers, connection and activity logs).
Duration of the processing	Term of the main contract, plus the return and deletion periods provided for in article 10. Connection and activity logs are kept for twelve months from the recording of each entry, in accordance with article 14.2 of the General Terms and Conditions of Sale.

Annex 2: Technical and organisational measures (article 32 GDPR)

Security governance

- Information security management system **certified ISO 27001:2022**, audited by an independent third-party body; documented internal security policy, reviewed at least once a year.
- Designated information security officer (chief technology officer).

Access control

- Individual named accounts; role-based authorisation management on the principle of least privilege; access reviews at least once a year, and every six months for production systems.

- Documented process for granting and revoking access when staff join, change roles and leave.
- Mandatory multi-factor authentication for administrator accounts, in particular those of the hosting infrastructure.
- Server administration using personal keys protected by a passphrase, through an encrypted virtual private network; a hardened and encrypted fallback access is maintained in case that network is unavailable; other administration interfaces are not exposed to the internet.
- Multi-factor authentication available to all users of the Platform.
- Access to backups restricted to the systems administration team.

Encryption

- Encryption of exchanges between users and the Platform (TLS 1.2 minimum, TLS 1.3 supported) and between servers on separate hosts.
- Encryption of data at rest: server data partition, storage and backups.
- Encrypted administration flows (virtual private network or hardened fallback access).
- Staff workstations: encrypted disk, automatic session lock, antivirus.

Segregation

- Logical segregation of data between clients: each client accesses only its own content.
- Separation of test and production environments; production data is never used for development or testing. By way of exception, with the Customer's agreement, a file it has sent may be copied, for the time needed to resolve an anomaly only, to the encrypted workstation of an authorised staff member; this copy is limited to what the anomaly requires, is never placed in a code repository or shared space, and is deleted once the anomaly is fixed. A file kept as a permanent test case is anonymised first.

Logging and monitoring

- Logging of sign-ins and sign-outs, privileged actions and security events (failed sign-ins, privilege escalation attempts), with each technical identifier linked to a natural person.
- Native application audit log: time-stamped traceability of changes, available to the Customer's administrators.
- Continuous monitoring of the Platform, automatic alerts (detection of malicious code, service unavailability) and a documented escalation procedure.

Protection against malware and vulnerability management

- Anti-malware protection deployed, with documented detection and response procedures; files uploaded to the Platform are scanned by an antivirus before processing.
- Vulnerability management: static code analysis on every change, blocking on failure; weekly analysis of software dependencies and third-party components; automatic security updates of server operating systems; monitoring of published vulnerabilities; remediation according to severity and exposure; patches applied to pre-production then production, under a documented change management process.
- External penetration test carried out every year by an independent provider.

Backups and business continuity

- Daily automatic backup of the production database, encrypted, stored in two geographically distinct regions in France, 30-day retention, with daily execution checks. Files uploaded by the Customer are kept on encrypted object storage whose durability is ensured by the hosting provider; they are not backed up separately.
- Formalised disaster recovery plan: recovery time objective (RTO) of 2 hours and recovery point objective (RPO) of 24 hours, tested at least once a year, each test being documented.

Incident management and physical security

- Documented procedure for the detection, classification and handling of security incidents; notification of breaches in accordance with article 8 of this agreement.
- Hosting in data centres operated by OVHcloud, whose compliance certificates are provided on request under the conditions of article 22.1 of the General Terms and Conditions of Sale.

Staff

- Confidentiality undertaking signed by all staff on hiring, which survives their departure; acceptance of the security policy and of the acceptable use charter.
- Information security awareness training at least once a year.