Counsel review pending. Informational document, not a contractual document.

Vendor diligence pack

VIDIMUS SASU as an ICT third-party service provider under Regulation (EU) 2022/2554 (DORA)

1. Provider identity

VIDIMUS SASU operates the Vidimus agent assurance platform. This pack answers the diligence a financial entity performs before entering or renewing a contractual arrangement for the use of ICT services, and gives the values its register of information needs.

Legal name	VIDIMUS SASU
Trading name	Vidimus
Registration	RCS Nanterre 106 772 619
Registered office	11bis rue du 8 mai 1945, 92700 Colombes, France
Country of incorporation	France
Legal entity identifier (LEI)	Not assigned Use the SIREN above where the template allows an alternative identifier.
Website	https://www.vidimus.fr
General contact	hello@vidimus.fr
Data protection contact	dpo@vidimus.fr
Security contact	security@vidimus.fr

2. Service description

Vidimus is a software-as-a-service control plane for approving, testing, monitoring and auditing AI agents. Customers register an agent, the platform classifies it against the EU AI Act, runs adversarial probes against the agent endpoint the customer configures, evaluates control checklists, and produces immutable, signed evidence packs.

Delivery model	Software as a service, multi-tenant, browser-based
Type of ICT service	Software as a service supporting AI governance and assurance The customer classifies the service against its own register taxonomy.
Function supported	Determined by the customer Vidimus does not execute the customer business function itself.
Access to customer systems	Only the agent endpoint the customer configures Reached over HTTPS with credentials the customer supplies, held in the platform vault.
Annual cost	Provided on request Per contract; needed for the register of information.

Counsel review pending. Informational document, not a contractual document.

3. Hosting, data location and transfers

Where the data rests, where the code runs and who is incorporated where are three different facts. All three are stated below because a diligence review deserves all three.

Data at rest	Supabase, Frankfurt (eu-central-1), EU
Object storage	Supabase, Frankfurt (eu-central-1), EU Evidence packs and uploaded documents.
Application hosting	Vercel, Frankfurt (fra1) Every server function is pinned to fra1 in configuration, and a test in the repository fails if the pin is removed.
Hosting provider incorporation	United States Transfers covered by Standard Contractual Clauses.
Language-model processing	Mistral AI, EU
LLM observability	Langfuse, EU region
Transactional email	Resend Messages never contain tenant agent data.
Transfer mechanism	Standard Contractual Clauses Data processing addendum, international transfers

4. Subprocessors

Processing by subprocessors is governed by the data processing addendum, and customers are notified before subprocessor changes.

Supabase	database, authentication, file storage (Frankfurt, EU) Holds all tenant data at rest: agents, test runs, reviews, evidence packs, audit logs.
Vercel	application hosting and content delivery (Frankfurt, EU) US-incorporated, executing our server code in its Frankfurt region. Transfers are covered by Standard Contractual Clauses.
Mistral AI	language-model processing (EU) Probe generation, judging, document verification and risk narratives.
Langfuse	LLM observability (EU region) Stores the prompts and completions of platform LLM calls, which include probe text and the responses of the agent under test.
Resend	transactional email (Provided on request) Messages never contain tenant agent data.
Google Cloud Vertex AI	language-model processing for customer-connected Vertex agents (EU region) Engaged only where a customer connects a Vertex-based agent.

Sentry	error monitoring (EU region) Request bodies, headers, cookies and personal data are stripped before sending.

5. Security controls

The controls below are implemented in the running system. No certification is claimed.

Tenant isolation	Every tenant-scoped table carries an organisation id enforced by Postgres row-level security, child tables are bound to their parent organisation by composite foreign keys, and evidence-pack files are stored under tenant-prefixed paths with the same membership check on read.
Append-only audit trail	Approval decisions, control overrides, membership changes and evidence-pack exports are written to an append-only audit log. Database triggers refuse updates and deletes for every role including our own service role, and each entry is linked to the previous one by a SHA-256 hash chain per organisation, verified nightly.
Evidence integrity	Evidence packs are immutable numbered versions. Each records the SHA-256 of the stored file, carries a content fingerprint on every page and is signed with an Ed25519 key held in our vault; the public keys are published so a pack verifies without contacting us.
Staff access	Vidimus staff hold no standing access to tenant data. Support access is granted by the customer from Settings as a time-boxed grant that expires automatically, every use is consumed and logged, and the grants are visible to the customer in the dashboard.
Credentials and secrets	Credentials supplied to reach an agent endpoint are stored in Supabase Vault and application tables persist only opaque secret identifiers. Application logs carry identifiers such as tenant, agent and run id, never prompts, agent responses or secrets.
Authentication	Passwords are at least 12 characters and checked against known breach corpora. Any member can enrol a TOTP authenticator and an organisation can require it for every member, with no product page rendering without a verified second factor. Sign-in through Google Workspace or Microsoft Entra ID is available and an SSO sign-in can only join an organisation that lists its email domain.
Application security	Every response carries a Content Security Policy whose script sources are limited to a per-request nonce, plus HSTS, frame denial and a restrictive Permissions-Policy. Inputs crossing a trust boundary are validated with typed schemas, rate limits on sign-in and public forms are enforced in the database, and machine-to-machine secrets are compared in constant time.
Encryption	Data in transit is protected by TLS on every public endpoint, with HSTS enforced. Data at rest is encrypted by the managed platform, and endpoint credentials are additionally encrypted in Supabase Vault.

6. Incident management and notification

Counsel review pending. Informational document, not a contractual document.

Incidents affecting the platform are handled by the provider incident process; incidents involving personal data carry the contractual notification below. DORA incident classification and supervisory reporting remain the financial entity obligation.

Personal data breach notification	Vidimus notifies the customer without undue delay and in any event within 72 hours of becoming aware of a personal data breach, with the information required by Article 33(3) GDPR. Data processing addendum, personal data breach notification
ICT incident assistance	Assistance is provided for incidents affecting the service Cost and response targets are set in the master services agreement; see clause 30(2)(f) in the annex.
Notification of material developments	To be agreed in the master services agreement DORA Article 30(3)(b) for services supporting a critical or important function.

7. Continuity, exit and data return

Exit is a data question first: what comes back, in what format, and when the copies are gone.

Return and deletion of data	At the customer choice, data is returned or deleted after the end of the services, with deletion completed within 30 days of termination unless a longer period is required by law. Data processing addendum, return or deletion at end
Export formats	Evidence packs as PDF, agent inventory as CSV, audit trail and agent records as JSON Exports are available to the customer throughout the term, not only at exit.
Verification after exit	Evidence packs verify without contacting Vidimus Each pack carries a SHA-256 and an Ed25519 signature; the public keys stay published after a key is retired.
Business continuity and recovery objectives	Provided on request Recovery objectives are agreed per contract.
Transition period on exit	To be agreed in the master services agreement DORA Article 30(3)(f); see the annex.

8. Audit and access rights

Audit and inspection	Vidimus makes available the information necessary to demonstrate compliance and allows for and contributes to audits and inspections by the customer or an auditor it mandates, no more than once per year unless a regulator requires otherwise, on reasonable notice and subject to confidentiality. Data processing addendum, audit rights
Access for competent authorities	Vidimus cooperates with competent and resolution authorities Scope and mechanics are set in the master services agreement; see clause 30(2)(g) in the annex.

Counsel review pending. Informational document, not a contractual document.

Independent attestations	None today Vidimus holds no security certifications today and does not claim otherwise. ISO/IEC 27001 preparation is on the roadmap, and vendor security questionnaires are answered in the meantime.

9. Sub-outsourcing

The subprocessors in section 4 are the full set engaged in delivering the service. Vidimus does not sub-outsource the operation of the platform itself.

Subprocessor approval	Prior notice of changes Data processing addendum, sub-processors
Chain outsourcing conditions	To be agreed in the master services agreement DORA Article 30(2)(a) requires the conditions for subcontracting an ICT service supporting a critical or important function.

10. Insurance

Professional and cyber insurance	Provided on request Certificate available to a customer under evaluation.

11. Register of information values

The values a financial entity copies into its register of information for this contractual arrangement. Fields the customer determines are marked as such.

Provider legal name	VIDIMUS SASU
Provider identification code	SIREN 106 772 619 No LEI assigned.
Country of the provider	France
Provider registered office	11bis rue du 8 mai 1945, 92700 Colombes, France
Parent undertaking of the provider	Provided on request
Type of ICT service	Software as a service supporting AI governance and assurance
Function supported and its criticality	Determined by the customer
Storage of data	Yes
Location of data at rest	Frankfurt (eu-central-1), EU
Location of data processing	EU

Counsel review pending. Informational document, not a contractual document.

Location of management of the data	France, EU
Sensitiveness of the data stored	Determined by the customer
Reliance level on the ICT service	Determined by the customer
Governing law of the arrangement	Law of France
Notice period for the provider	30 days absent a master services agreement Terms of use, term and termination
Annual expense or cost	Provided on request

12. Legal notice

Company	VIDIMUS SASU, RCS Nanterre 106 772 619
Share capital	1 €
Registered office	11bis rue du 8 mai 1945, 92700 Colombes, France
Publication director	Président The legal notice names the role and the company.

- Document version 1.0, generated 2026-09-06.
- Counsel review pending. Informational document, not a contractual document.