

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

DORA Article 30 clause annex

VIDIMUS SASU position on the contractual provisions required by Article 30 of Regulation (EU) 2022/2554

Article 30 lists what the written arrangement between a financial entity and an ICT third-party service provider must contain. This annex states, clause by clause, the position Vidimus proposes and where it is already written down. It is an informational document offered to speed up contracting; the operative wording is the master services agreement.

Article 30(2), every arrangement

Article 30(2)(a)

DOCUMENTED TODAY

REQUIREMENT

A clear and complete description of all functions and ICT services, stating whether subcontracting of an ICT service supporting a critical or important function is permitted and under which conditions.

VIDIMUS POSITION

The order form describes the service as a software-as-a-service control plane for AI agent assurance and lists the subprocessors engaged. Vidimus does not sub-outsource operation of the platform; the conditions for any future subcontracting are set in the MSA and prior notice of subprocessor changes applies.

Already documented in: Data processing addendum, sub-processors (<https://www.vidimus.fr/legal/dpa#subprocessors>); Trust and security (<https://www.vidimus.fr/security>)

Article 30(2)(b)

DOCUMENTED TODAY

REQUIREMENT

The regions or countries where the functions and ICT services are provided and where data is processed and stored, including the storage location, with a requirement to notify in advance of any change.

VIDIMUS POSITION

Data at rest and object storage are in Frankfurt (eu-central-1), EU. Server code executes in Frankfurt (fra1). Language-model processing is in the EU. Vidimus notifies the customer in advance of any change to these locations.

Already documented in: Trust and security (<https://www.vidimus.fr/security>); Data processing addendum, international transfers (<https://www.vidimus.fr/legal/dpa#transfers>)

Article 30(2)(c)

DOCUMENTED TODAY

REQUIREMENT

Provisions on availability, authenticity, integrity and confidentiality, including the protection of personal data.

VIDIMUS POSITION

Tenant isolation is enforced by row-level security, the audit trail is append-only with a per-organisation hash chain, and evidence packs are immutable, hashed and signed. Personal data protection is governed by the data processing addendum, including the Article 32 security measures.

Already documented in: Data processing addendum, security measures (<https://www.vidimus.fr/legal/dpa#security>); Trust and security (<https://www.vidimus.fr/security>)

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

Article 30(2)(d)**DOCUMENTED TODAY****REQUIREMENT**

Provisions ensuring access, recovery and return of personal and non-personal data in an easily accessible format on insolvency, resolution, discontinuation of operations or termination.

VIDIMUS POSITION

Customer data is exportable throughout the term: evidence packs as PDF, the agent inventory as CSV, agent records and the audit trail as JSON. Evidence packs verify after exit without contacting Vidimus because the signing public keys stay published. Return or deletion follows the data processing addendum.

Already documented in: Data processing addendum, return or deletion at end (<https://www.vidimus.fr/legal/dpa#return>)

Article 30(2)(e)**TO AGREE IN THE MSA****REQUIREMENT**

Service level descriptions, including their updates and revisions.

VIDIMUS POSITION

Service levels, support response times and any credits are set in the MSA. Outside an MSA the service is provided as is to the extent French law permits; no service level is claimed by default.

Already documented in: Terms of use, service level and warranty (<https://www.vidimus.fr/legal/terms#warranty>)

Article 30(2)(f)**TO AGREE IN THE MSA****REQUIREMENT**

An obligation to assist at no additional cost, or at a cost determined in advance, when an ICT incident related to the service occurs.

VIDIMUS POSITION

Vidimus assists with incidents affecting the service. Whether that assistance is at no additional cost or at a rate fixed in advance is set in the MSA, so the customer can price it before signature.

Already documented in: Data processing addendum, personal data breach notification (<https://www.vidimus.fr/legal/dpa#breach>)

Article 30(2)(g)**COUNSEL REVIEW PENDING****REQUIREMENT**

An obligation to cooperate fully with the competent authorities and resolution authorities of the financial entity.

VIDIMUS POSITION

Vidimus accepts an obligation to cooperate with the competent and resolution authorities of the customer, including access to information relating to the service.

Article 30(2)(h)**DOCUMENTED TODAY****REQUIREMENT**

Termination rights and the related minimum notice periods, in line with the expectations of competent and resolution authorities.

VIDIMUS POSITION

Absent an MSA, either party may terminate on 30 days notice, and Vidimus may terminate for material breach not cured within 15 days. Supervisory expectations on notice periods for a critical or important function are accommodated in the MSA.

Already documented in: Terms of use, term and termination (<https://www.vidimus.fr/legal/terms#term>)

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

Article 30(2)(i)

TO AGREE IN THE MSA

REQUIREMENT

The conditions for participation of the provider in the financial entity ICT security awareness programmes and digital operational resilience training.

VIDIMUS POSITION

Vidimus staff who operate the service can take part in the customer security awareness programme and resilience training where the arrangement requires it. Scope and frequency are set in the MSA.

Article 30(3), critical or important functions

Article 30(3) adds the following where the ICT service supports a critical or important function. The financial entity makes that determination, not Vidimus.

Article 30(3)(a)

TO AGREE IN THE MSA

REQUIREMENT

Full service level descriptions with precise quantitative and qualitative performance targets, allowing effective monitoring and corrective action without undue delay.

VIDIMUS POSITION

Quantitative targets, including availability and support response, are agreed in the MSA for a service supporting a critical or important function. Vidimus does not publish a default availability figure it has not measured over a full contract year.

Already documented in: Terms of use, service level and warranty (<https://www.vidimus.fr/legal/terms#warranty>)

Article 30(3)(b)

TO AGREE IN THE MSA

REQUIREMENT

Notice periods and reporting obligations, including notification of any development that might materially impact the ability to provide the services.

VIDIMUS POSITION

Vidimus notifies the customer of any development materially affecting its ability to provide the service, including a change of control, a change of hosting region or the loss of a subprocessor. Notice periods are set in the MSA.

Already documented in: Terms of use, change of control (<https://www.vidimus.fr/legal/terms#change-of-control>)

Article 30(3)(c)

COUNSEL REVIEW PENDING

REQUIREMENT

Requirements to implement and test business contingency plans and to have ICT security measures, tools and policies providing an appropriate level of security.

VIDIMUS POSITION

The security measures in place are stated on the trust page and in section 5 of the vendor diligence pack. Business contingency plans exist for the platform; their testing cadence and evidence are agreed with the customer in the MSA.

Already documented in: Trust and security (<https://www.vidimus.fr/security>)

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

Article 30(3)(d)

COUNSEL REVIEW PENDING

REQUIREMENT

An obligation to participate and fully cooperate in the threat-led penetration testing of the financial entity under Articles 26 and 27.

VIDIMUS POSITION

Vidimus cooperates with threat-led penetration testing that covers the service, subject to scoping that protects other tenants of the multi-tenant platform. Pooled testing under Article 26(4) is acceptable where several financial entities are involved.

Article 30(3)(e)

COUNSEL REVIEW PENDING

REQUIREMENT

The right to monitor performance on an ongoing basis, including unrestricted rights of access, inspection and audit by the financial entity, an appointed third party and the competent authority, with agreed audit levels, frequencies and areas.

VIDIMUS POSITION

The data processing addendum already grants audit and inspection rights to the customer and an auditor it mandates. For a critical or important function Vidimus accepts unrestricted access, inspection and audit rights for the customer and its competent authority, with the frequency and areas agreed so that other tenants stay protected.

Already documented in: Data processing addendum, audit rights (<https://www.vidimus.fr/legal/dpa#audit>)

Article 30(3)(f)

TO AGREE IN THE MSA

REQUIREMENT

Exit strategies, in particular a mandatory adequate transition period during which the provider continues to provide the service to reduce the risk of disruption.

VIDIMUS POSITION

Vidimus accepts a transition period during which the service continues on the same terms while the customer migrates, with export of all customer data in the formats listed in the vendor diligence pack. The length is agreed in the MSA.

Already documented in: Data processing addendum, return or deletion at end (<https://www.vidimus.fr/legal/dpa#return>)

Status key

- Documented today: the position is already written down at the reference given.
- To agree in the MSA: Vidimus accepts the requirement; the figures are set in the master services agreement.
- Counsel review pending: the proposed position has not yet been reviewed by counsel.
- Counsel review pending. Informational document, not a contractual document.