Wasabi Technologies
DORA Statement

The Digital Operational Resilience Act (DORA) is an EU regulation designed to strengthen the cybersecurity and operational resilience of the EU financial sector. It applies to financial entities (e.g. banks, insurers, investment firms) and certain Information and Communication Technology (ICT) third-party service providers ("ICT Providers"). Wasabi welcomes the operational resilience goals that DORA advances, and we want our financial-sector customers to understand clearly how Wasabi supports DORA compliance. The purpose of this statement is to explain Wasabi's position under DORA and to show, requirement by requirement, that the contract provisions that already apply to Wasabi services are sufficient to meet DORA obligations.

DORA's requirements generally fall in two categories: 1) requirements applying to all ICT Providers; 2) additional requirements applying to those ICT Providers supporting "critical or important functions" (Critical Third-Party Providers or "CTPPs").

Wasabi complies with the requirements of DORA Article 30, paragraphs 1 and 2, applicable to all ICT providers (category 1 above), which are already satisfied by the existing Wasabi contract documents that govern our relationship with customers—principally the Customer Agreement and the Data Processing Agreement ("DPA"). Article 30(1) requires that the rights and obligations of the financial entity and the ICT provider be clearly allocated and set out in writing, with service level agreements documented in a durable, accessible format. Wasabi's contract documents do exactly that. The mapping later in this statement identifies, for each Article 30(2) element, the specific existing provision that addresses it. The remaining requirements of DORA (category 2 above) do not apply to Wasabi, as we are neither listed as a critical third-party ICT Provider (current list is attached as Exhibit A), nor do the services we provide fall within the definition of critical or important functions as envisioned by DORA. This is not to downplay the importance of our services—security and compliance are of the utmost importance to Wasabi. Rather, this is to describe Wasabi's role and what DORA requires based on the actual nature of Wasabi's services and what DORA views as "critical" threats to the EU financial system. This position is consistent with the language in DORA itself.

DORA Article 3(22): " 'critical or important function' means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law."

In other words, if Wasabi services were disrupted, would that materially impair our customer's performance? Would it cause a financial customer to cease operations or fail to provide financial services to their customers? Would it affect its authorisation to operate?

> *Applying this definition to Wasabi's service: The typical use case for Wasabi is to provide a backup of a customer's data. Even if we had a temporary service disruption (which is unlikely), the result is a potential delay in a data backup, or a short delay in access to the stored copy of the customer's data. The customer*

still has access to its primary copy—wherever that is stored—which allows the customer to continue to provide services. Our customers typically do not need immediate access to the backed-up data and information they store in order to provide their services. Put another way, a service disruption would not materially impair their services. If our services were unavailable, would it cause our customer to temporarily close its doors and turn away customers because it couldn't access a backup copy of its data? Probably not.

Recital 3 of DORA emphasizes the systemic cyber risk that DORA is trying to address: the high level of interconnectedness across financial entities and financial markets, particularly the interdependencies of information and communication technology systems.

Wasabi and systemic risk: Wasabi is not listed as a critical third-party ICT provider by EU regulators, but that is a good thing. Wasabi is actually the safer choice precisely because we're not on the CTPP list. Providers get designated as CTPPs under DORA because they're huge and deeply interconnected: hard to substitute, and hard to migrate away from. That concentration is exactly what makes them risky: if one goes down, the shock can ripple across dozens of major institutions and threaten the stability of the financial system itself—which is why DORA's own recitals flag "concentration risk" as a real concern. Wasabi doesn't carry that baggage. We're not deeply entangled with a huge share of those on the CTPP list, and our architecture is built for portability rather than lock-in. So in the unlikely case of something going wrong at Wasabi, it stays contained. It's not the kind of single point of failure that can take down a chunk of the financial system with it.

Under DORA, the two additional requirements for "critical" providers that draw the most attention, 1) threat-led penetration testing (DORA Article 30(3)(d)), and 2) the right to monitor performance through access, inspection, and audit (DORA Article 30(3)(e)), do not technically apply to Wasabi. Nonetheless, Wasabi addresses both in a way that should satisfy every customer while also preserving the security of the multi-tenant platform that protects all other customers.

Threat-led penetration testing (Article 30(3)(d)). Article 30(3)(d) requires a provider to "participate and fully cooperate in the financial entity's TLPT as referred to in Articles 26 and 27." Those Articles, and the implementing technical standards on TLPT, scope mandatory TLPT to financial entities identified by the authorities on the basis of impact and systemic-risk criteria, so a financial entity outside that scope has no corresponding TLPT obligation to pass through to its provider. Wasabi's Acceptable Use Policy prohibits customers from conducting their own third-party penetration testing of our platform and network, because testing on shared infrastructure could compromise the security of other customers. Instead, Wasabi maintains rigorous, independent security procedures:

- We conduct our own penetration tests
- We conduct weekly vulnerability scans
- We are ISO 27001 Certified
- We continuously monitor all vaults and storage regions 24/7

Access, inspection, and audit (Article 30(3)(e)). DORA does not require a provider to grant physical or unfettered third-party access to shared infrastructure. Article 30(3)(e)(ii) expressly preserves "the right of the financial entity to agree on alternative assurance levels if other clients' rights are affected." Wasabi's storage cages and servers host many customers, and allowing one customer's third party into that environment would affect the security and privacy rights of the others—precisely the situation Article 30(3)(e)(ii) is designed to accommodate. Wasabi meets a customer's assurance needs through current third-party audit reports and certifications, together with reasonable supporting documentation such as Wasabi certifying in writing its compliance. The data centers have their own SOC 2 Type 2 and ISO 27001 certifications, and a customer may obtain relevant reports under NDA with the data centers. Data Center Links and Security Resources:

Data center documents request: https://info.wasabi.com/dc_report_request

Wasabi third-party compliance documentation: https://wasabi.com/company/trust-center

How Wasabi's Existing Contract Documents Satisfy DORA Article 30(2)

The table below maps each element required by DORA Article 30(2)—the provisions that apply to every ICT third-party service provider—to the specific provision in Wasabi's existing Customer Agreement ("CA") or Data Processing Agreement ("DPA") that addresses it. This demonstrates that a separate DORA-specific amendment is not necessary to bring a Wasabi relationship into line with Article 30(2).

DORA Art. 30(2)	What DORA requires	Existing Wasabi provision
(a)	A clear and complete description of all functions and ICT services to be provided, indicating whether subcontracting of an ICT service supporting a critical or important function is permitted and the conditions applying.	CA §1 describes the Services and links to the Documentation/user guides. DPA §11 and CA §12.2 address sub-processors and the conditions on their use.
(b)	The locations (regions or countries) where the functions and ICT services are provided and where data is processed, including the storage location, and the requirement to notify the financial entity in advance of any change.	DPA §13: the Customer alone selects the storage region, and Wasabi will not transfer Content to another location. The sub-processor list (DPA Schedule C) identifies any regions used for support.
(c)	Provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data.	DPA Schedule B (Technical and Organisational Measures): encryption (AES-256, TLS 1.2/1.3), network security, access

DORA Art. 30(2)	What DORA requires	Existing Wasabi provision
		controls, and physical security backed by SOC 2 and ISO 27001.
(d)	Provisions ensuring access, recovery and return of personal and non-personal data in an easily accessible format in the event of insolvency, resolution or discontinuation of the provider, or termination of the contract.	DPA §16 (recovery period) and CA §4.1: the Customer may modify, remove, or export its Content at any time; Wasabi does not control or restrict that access.
(e)	Service level descriptions, including updates and revisions thereof.	CA §2.2 and the linked Service Level Agreement at wasabi.com/legal/sla.
(f)	The obligation to provide assistance to the financial entity when an ICT incident related to the service occurs.	DPA §10 and DPA Schedule B, paragraph 8 (incident notification and assistance).
(g)	The obligation to fully cooperate with the competent authorities and resolution authorities of the financial entity, including persons appointed by them.	DPA §7 (cooperation with regulators).
(h)	Termination rights and related minimum notice periods, in accordance with the expectations of competent and resolution authorities.	CA §7 and DPA §15 (termination).
(i)	The conditions for the provider's participation in the financial entity's ICT security awareness programmes and digital operational resilience training.	DPA Schedule B, paragraph 10 (training). Wasabi already conducts security training, and DORA Article 13(6) only applies “where appropriate”. Based on the nature of Wasabi’s services, Wasabi’s existing security training is sufficient.

Exhibit A: European Supervisory Authorities List of
Critical Third-Party Providers under DORA (published 18 November 2025)

- Accenture plc
- Amazon web Services EMEA Sar
- Bloomberg L.P.
- Capgemini SE
- Colt Technology Services
- Deutsche Telekom AG
- Equinix (EMEA) B.V.
- Fidelity National Information Services, Inc.
- Google Cloud EMEA Limited
- International Business Machine Corporation
- InterXion HeadQuarters B.V.
- Kyndryl Inc.
- LSEG Data and Risk Limited
- Microsoft Ireland Operations Limited
- NTT DATA Inc.
- Oracle Nederland B.V.
- Orange SA
- SAP SE
- Tata Consultancy Services Limited