

The DORA Contract Checklist

DORA (the EU's Digital Operational Resilience Act, Regulation (EU) 2022/2554, in force since January 2025) makes these terms mandatory in every contract a financial firm holds with a third-party provider of information and communication technology (ICT). When a vendor agreement or a DORA addendum lands on your desk, these are the terms to confirm, the article each one comes from, and the weak versions that leave you out of compliance.

✓ **CONFIRM IT'S THERE AND ADEQUATE** ⚠ **WATCH FOR: THE VERSION THAT FAILS DORA**

Scope, Definitions & Interpretation		THE ADDENDUM & MASTER AGREEMENT
Description of services	✓ A clear, complete description of every function and ICT service, in the contract or a referenced schedule (Art. 30(2)(a)).	⚠ No description, or a vague pointer that leaves the scope of the arrangement undefined.
Key definitions	✓ "DORA" and "ICT-related incident" are defined, or tied to the Regulation.	⚠ Terms used but undefined, so the obligations they trigger are unclear.
Order of precedence	✓ The DORA addendum prevails over the master agreement for the ICT services.	⚠ Master agreement controls, or no precedence stated, so the DORA terms get overridden.
Amendments	✓ Changes are made in writing and signed, except where DORA compliance requires otherwise.	⚠ Oral or unilateral amendment allowed.
Data: Access, Location & Protection		ART. 30(2)(B)–(D)
Data location	✓ The regions and countries where services are provided and data is processed and stored are named, with advance notice of any change (Art. 30(2)(b)).	⚠ Location unstated, or the vendor can move data with no notice.
Data protection	✓ Provisions on the availability, authenticity, integrity, and confidentiality of your data, including personal data (Art. 30(2)(c)).	⚠ Generic "reasonable security" with none of the four properties named.
Access & return	✓ Access, recovery, and return of your data in an easily accessible format on termination or the vendor's insolvency (Art. 30(2)(d)).	⚠ No return right; data effectively trapped when the contract ends.
Resilience & Security		ART. 30(2)(I), 30(3)(C)
Business continuity	✓ The vendor implements and tests business contingency plans and can restore the service after a disruption (Art. 30(3)(c)).	⚠ "Reasonable efforts" to keep a plan, with no commitment to test it or restore service.
Security measures	✓ ICT security measures, tools, and policies giving an appropriate level of security, kept current through the term (Art. 30(3)(c)).	⚠ Absent, or frozen at signing with no upkeep obligation.
Resilience training	✓ The contract sets how the vendor's staff take part in your security-awareness and resilience training (Art. 30(2)(i)).	⚠ No participation obligation on the vendor's people.
Incidents, Audit & Testing		ART. 30(2)(F)–(G), 30(3)(B),(D),(E)
Incident assistance	✓ The vendor assists you when an ICT incident related to the service occurs, at no additional cost or a cost set in advance (Art. 30(2)(f)).	⚠ Assistance optional or discretionary, or billed at an open-ended, undefined cost.
Notice & reporting	✓ Notice periods and a duty to report any development that could materially affect delivery of the service (Art. 30(3)(b)).	⚠ No reporting duty, or notice only if you ask.
Right to monitor & audit	✓ Unrestricted access, inspection, and audit for you, an appointee, and the competent authority, not curbed by other clauses (Art. 30(3)(e)).	⚠ Audit capped, fee-gated, or subject to the vendor's prior approval.
Cooperation & testing	✓ Full cooperation with the competent and resolution authorities (Art. 30(2)(g)); participation in threat-led penetration testing where in scope (Art. 30(3)(d); Arts. 26–27).	⚠ Cooperation "commercially reasonable" or approval-gated; testing left unaddressed.
Subcontracting & Service Levels		ART. 30(2)(A),(E), 30(3)(A)
Subcontracting	✓ The contract states whether subcontracting of a critical or important function is permitted and, if so, the conditions that apply (Art. 30(2)(a); RTS (EU) 2025/532).	⚠ Silent on subcontracting, or unconditional subcontracting with no stated conditions.
Service levels	✓ Service level descriptions with updates and revisions; for critical functions, precise quantitative and qualitative targets you can monitor (Art. 30(2)(e), 30(3)(a)).	⚠ Qualitative or "best efforts" service levels; no way to keep them current.
Exit & Termination		ART. 28(7)–(8), 30(3)(F)
Exit strategy	✓ A tested exit plan: the vendor keeps the service running through an adequate transition period so you can migrate to another provider or bring it in-house (Art. 30(3)(f); Art. 28(8)).	⚠ No exit strategy; the service simply stops at termination.
Termination rights	✓ You may terminate on the DORA grounds: significant vendor breach; changes that impair the service; evidenced weaknesses in the vendor's ICT risk management; or the competent authority no longer being able to supervise you (Art. 28(7); Art. 30(2)(h)).	⚠ Termination weighted to the vendor, or the DORA grounds missing.
A clean exit	✓ You can exit without disrupting your business; transition assistance is defined and any termination charges do not trap you (Art. 28(8)).	⚠ Exit penalties or fees steep enough to lock you in.
Two Things to Get Right First		BEFORE YOU REVIEW
✓ Know your critical or important functions. DORA's enhanced Article 30(3) terms (full service-level detail, notice and reporting, tested business-continuity plans, threat-led penetration testing, unrestricted audit, and exit plans) apply to the ICT services supporting those functions. Identify them first; the bar is higher there.		✓ The vendor reads the same list. An ICT provider handed this addendum works the mirror image, confirming each obligation is bounded, funded, and operationally achievable before it signs. Same terms, opposite side of the table.