DIRECTIVE (EU) 2022/2555 · REGULATION (EU) 2022/2554

NIS 2 and DORA note for regulated customers

What REVIEWIT SAS provides to customers subject to the NIS 2 Directive or the DORA Regulation to help them meet their obligations towards their providers (incident notification, register of information, audit, exit, testing). The authoritative text is Annex 5 of the data processing agreement.

VERSION
1.0 · November 2026

SCOPE
REVIEWIT SAS · REVIEWIT SaaS solution, all regions

DISTRIBUTION
Public

CONTENTS

01 When Annex 5 applies
02 Incident notification
03 Supply chain security
04 Register of information (DORA, Art. 28)
05 Access, audit and cooperation with authorities
06 Termination and exit strategy
07 Continuity, service levels and testing

PURPOSE

This note is for information only and creates no commitment. REVIEWIT's commitments are set out in Annex 5 of the data processing agreement (DPA), "Security of services and digital operational resilience", whose articles are cited in brackets, and, for exit, in Annex 6. In case of discrepancy, the text of these annexes prevails. This is a translation: the French version prevails.

SECTION 01 When Annex 5 applies

PART	CUSTOMER CONCERNED	CONTENT
Part A	Essential or important entity under NIS 2, or financial entity under DORA, as declared in the special terms (Art. 1.2).	Supply chain security (NIS 2, Art. 21 and 23): measures, incidents, vulnerabilities, ICT providers, authorities.

PART	CUSTOMER CONCERNED	CONTENT
Section B1	Any financial entity under DORA (Art. 1.3).	Clauses of DORA Art. 30(2): description, locations, data protection, return of data, service levels, assistance, cooperation, termination, training, register.
Section B2	Financial entity that designates in writing the Service as supporting a critical or important function (Art. 1.3).	Clauses of DORA Art. 30(3): quantified service levels, reports, continuity, TLPT, subcontracting, unrestricted audit, exit strategy.

Qualifying the supported function is for the Customer alone; REVIEWIT cannot refuse it. A designation made during the contract is recorded in an amendment (Art. 1.3). The annex is a contractual obligation towards the Customer: it does not amount to an acknowledgement that REVIEWIT is itself an entity subject to NIS 2 (Art. 1.5).

SECTION 02 Incident notification

For your own notifications to the authorities (NIS 2, Art. 23; DORA, Art. 19), REVIEWIT informs you of any notifiable incident: unavailability or severe degradation of the Service for more than sixty consecutive minutes, harm to your data, your audit trail or the evidence produced, unauthorised access to production systems, or an imminent threat of any of these. When in doubt, the incident is notified (Art. 5.1).

STEP	MAXIMUM TIMEFRAME	CONTENT
Early warning	24 hours after awareness (Art. 5.2)	Nature, dates, functions and data affected, presumed malicious cause, impact on other customers or cross-border, first measures, follow-up contact.
Update	72 hours after awareness (Art. 5.3)	Initial assessment, severity, impact, available indicators of compromise.
Status report	On request, in particular from an authority (Art. 5.4)	State of the incident and of its handling.
Final report	One month after the early warning (Art. 5.5)	Likely root cause, mitigation measures, cross-border impact; progress report if the incident is still ongoing.

A personal data breach is notified to you no later than 24 hours after awareness (DPA, Art. 8); a single communication may serve both regimes (Art. 3.2). Communications are sent from **security@we-reviewit.com** to the security contact you designate in the special terms and are duplicated in the support area (Art. 5.6, 9.2). REVIEWIT assists you with analysis, containment, recovery and your notifications (Art. 5.8, 15).

SECTION 03 Supply chain security

- **Measures.** Annex 1 of the DPA describes the technical and organisational measures and states, measure by measure, whether it is in place, partial or planned, so that you can assess REVIEWIT's cybersecurity practices (NIS 2, Art. 21(3)). The level of security is not reduced during the contract (Art. 4.1).
- **Development and release.** Static analysis at every build, automated tests, container images with immutable tags scanned on push and deployed by digest, sealed release manifest for the stable channel (Art. 4.2).

- **Vulnerabilities.** Fix or mitigation within fourteen days for a critical vulnerability and thirty days for a high one, from triage; the Customer is informed when an exploitable vulnerability cannot be fixed within that time (Art. 6.1, 6.2). REVIEWIT's vulnerability disclosure policy describes how reports are received (Art. 6.3).
- **Information on request.** Annex 1 in force and changes in the status of its measures, status of the certification programme, answer to your security questionnaire once per twelve-month period (Art. 4.3).
- **ICT providers.** List of REVIEWIT's ICT service providers, including those that process no Customer data, published in the customer area of the Trust Center; their security is assessed before selection and then every year (Art. 7.2, 7.3).

SECTION 04 Register of information (DORA, Art. 28)

REVIEWIT provides the information you need for your register of information on ICT third-party service providers: name, identifiers, country of establishment, services provided, locations and subcontracting chain (Art. 19).

- REVIEWIT SAS is your direct provider; its own providers are listed, with their identification, the service provided, the data location, transfers and their criticality, in "REVIEWIT ICT service providers" (customer area of the Trust Center).
- The Service is provided in the hosting region you choose, Paris, European Union, by default; it is not changed without your instruction. Any change of country of a provider is announced to you thirty days in advance, or as soon as REVIEWIT becomes aware of it if the provider decides with shorter notice (Art. 11).
- It is for you to qualify the function REVIEWIT supports (critical or important function within the meaning of DORA) and to record it as such.

SECTION 05 Access, audit and cooperation with authorities

- **All customers.** Documentary or on-site audit once a year, with thirty days' notice; for infrastructure sub-processors, verification through their independent reports and certifications (DPA, Art. 10).
- **Critical or important function (B2).** Unrestricted right of access, inspection and audit for you, the third party you appoint and the competent authority, including taking copies on site; ten business days' notice except in an emergency or at the request of an authority; pooled audit or independent third-party report where the rights of other customers are at stake (Art. 25).
- **Authorities.** Cooperation with the competent authorities, resolution authorities and CSIRTs you report to; the Customer is informed of any request from an authority that concerns it, unless prohibited by law (Art. 8, 16).

SECTION 06 Termination and exit strategy

- **Termination without penalty** in the cases of DORA Art. 28(7): significant breach, circumstances identified when monitoring the risk, evidenced weaknesses in ICT risk management, impossibility of supervision by the authority (Art. 17.1). Minimum notice when REVIEWIT ends the contract: three months, six months for a critical or important function (Art. 17.3).
- **Exit (Annex 6).** Transition period during which the Service continues to be provided; return package (ZIP archive of documented CSV and JSON files, with a SHA-256 digest manifest); extraction period of at least thirty days; erasure and certificate. For a financial entity, in case of insolvency, resolution or discontinuation of business of REVIEWIT, the package is made available free of charge (Art. 13.2).

- **Critical or important function.** Transition period extended, on notice, up to six months; information useful to your exit plan and testing of that plan with you, under agreed conditions (Art. 26); return package delivered every quarter (Art. 13.2).

SECTION 07 Continuity, service levels and testing

- **Service levels (B2).** Monthly availability of 99.5% measured by the public status page, framed scheduled maintenance, support response times, maximum data loss of twenty-four hours and recovery time of forty-eight hours, notification timeframes; quarterly service report (Art. 20, 21).
- **Continuity.** Automatic database backups and subscription export verified by an actual restore are in place (Annex 1). The continuity plan and the timed restoration test required for section B2 (Art. 22) are at the "planned" status of Annex 1.
- **Penetration test.** Annex 5 provides for an annual penetration test of the Service by an independent third party, whose summary is provided to you on request and in confidence (Art. 6.4). At the date of this note, no penetration test has yet been carried out.
- **TLPT.** When you are required to carry out threat-led penetration testing (DORA, Art. 26 and 27), REVIEWIT takes part at your request, under rules agreed in writing, with the option of a pooled test (Art. 23).
- **Awareness.** Participation in your ICT security awareness and digital operational resilience training programmes, one remote session per year free of charge (Art. 18).

REVIEWIT SAS · Security and incidents: **security@we-reviewit.com** · Data protection officer: **dpo@we-reviewit.com**. Annex 5 is concluded with the DPA; Annex 1 and the list of ICT service providers are available in the customer area of the Trust Center. Version 1.0 · November 2026 · the French version prevails.