Clearlane

Supplier addendum to help you meet DORA Article 30(2) and NIS2 supply-chain requirements

Version 1.0 · 4 November 2026 · Translations: French, German (the English version prevails) · Maxime Ragionieri EI (brand: Clearlane Apps), 40 rue Bourges, 72000 Le Mans, France

1. Purpose and order of documents

This addendum helps financial entities (Regulation (EU) 2022/2554, "DORA") and essential or important entities under Directive (EU) 2022/2555 ("NIS2") and the national laws transposing it document their use of Clearlane apps. It sets out Clearlane's commitments against each point of DORA Article 30(2) to help you meet your own obligations. It does not state that your arrangement with Clearlane complies with DORA, NIS2 or the national laws transposing NIS2; that assessment is yours.

This addendum forms part of the Clearlane licence terms and applies to every Clearlane licence bought on the Atlassian Marketplace without signature. On written request, Clearlane countersigns a dated PDF copy by electronic signature. If documents conflict, the DPA prevails on personal data, then this addendum, then the licence terms. The limitations and exclusions of liability in the licence terms apply to this addendum. A change to this addendum that reduces a Clearlane commitment takes effect no earlier than 30 days after written notice to customers. This addendum does not change the Atlassian Marketplace terms between you and Atlassian.

2. Description of the service (DORA Art. 30(2)(a))

Clearlane provides apps for Jira and Confluence Cloud built on Atlassian Forge. The apps run on Atlassian's infrastructure. Clearlane operates no servers and has no access to your content. No part of the service that handles your app data is subcontracted to anyone other than Atlassian (hosting, Marketplace billing, help center). For support e-mails, Clearlane uses the providers in its sub-processor list (clearlaneapps.com/trust/); none of them receives app data. Clearlane will give 30 days' written notice before adding any other subcontractor that could access your app data; if you object, you may stop using the app under section 9.

3. Data location (Art. 30(2)(b))

Clearlane provides development and support from France. Your app data is stored in Forge hosted storage within Atlassian's infrastructure. If your site's data is pinned to a data residency location, the app data follows that location; if not, Atlassian chooses the location and may change it. Atlassian may run app processing from another location for reliability. No app data is sent outside Atlassian. Clearlane will give 30 days' written notice before any change that would store or process your app data outside Atlassian, or move its own service location outside France.

4. Security of data (Art. 30(2)(c))

Availability, authenticity, integrity and confidentiality rely on Atlassian's platform controls (encryption at rest and in transit) and on the app controls described in the Clearlane security policy (clearlaneapps.com/security/), including salted hashing of signing passwords and SHA-256 fingerprints of signed content.

5. Access, recovery and return of data (Art. 30(2)(d))

Your app data is stored in your Atlassian site, not by Clearlane, and the apps do not depend on a Clearlane server to run. You can export your data at any time with the apps' built-in exports (CSV, PDF evidence), which remain usable without Clearlane. If Clearlane decides to stop an app or its activity, it will give at least 90 days' written notice and keep the app and its exports available during that period, as far as Atlassian's platform and any insolvency proceedings allow. Atlassian deletes app data under its retention rules after uninstall, so export first.

6. Service levels (Art. 30(2)(e))

Clearlane makes no availability commitment. The apps run on Atlassian Forge with no Clearlane server, so their availability depends on Atlassian's platform; any Atlassian service-level commitment on your plan covers Atlassian's products, not Clearlane apps. Status: clearlaneapps.com/status/. Support: written answer within two business days. Security fixes: within the deadlines of Atlassian's Security Bug Fix Policy for Marketplace apps. Clearlane gives 30 days' written notice before reducing any of these service levels.

7. ICT incidents (Art. 30(2)(f); NIS2 Art. 21(2)(b) and (d))

Clearlane notifies affected customers in writing of any ICT incident caused by a Clearlane app or affecting your app data, whether security-related or operational, without undue delay and no later than 72 hours after becoming aware of it, and gives you the information it has to help you meet your own reporting obligations. Outages of Atlassian's platform are shown on clearlaneapps.com/status/ and Atlassian's status pages. Reporting to authorities (for example under NIS2 Article 23 or DORA Article 19) remains your obligation. Clearlane's 72-hour maximum may be later than your own deadlines (for example the NIS2 24-hour early warning or the DORA initial notification); plan for this in your incident procedure. Clearlane provides this written assistance at no additional cost.

8. Cooperation with authorities (Art. 30(2)(g))

Clearlane fully cooperates with your competent authorities and resolution authorities, and with persons they appoint, including by answering their requests for information and documents about the apps. As Clearlane hosts nothing and cannot access your content, this

cooperation is provided in writing.

9. Termination (Art. 30(2)(h))

You can stop using an app at any time by cancelling its Marketplace licence and uninstalling it. Clearlane will not end your access to an app before your paid licence period ends, except for your material breach of the licence terms, and gives the notice set out in section 5.

10. Security awareness and training (Art. 30(2)(i))

Clearlane takes part in your ICT security awareness and digital operational resilience training in writing: it reads the material you send and confirms in writing that it has done so and how it applies to a supplier with no access to your content. It does not attend live, video or on-site sessions.

10a. Material changes

Clearlane notifies customers in writing, without undue delay, of any development that could materially affect its ability to provide the apps, such as stopping an app, a change of owner, or an Atlassian platform change that removes a function the apps rely on.

11. Information requests (NIS2 Art. 21(2)(d))

Clearlane answers in writing your questionnaires, document requests and follow-up questions, and those of your auditors and competent authorities: acknowledgement within two business days, full answer within ten business days. Published evidence: CAIQ-Lite, security policy, SBOM for each release, OQ test scripts (clearlaneapps.com/trust/ and /validation/). Clearlane does not offer on-site, video or call-based audits or inspections. It therefore cannot accept the additional terms DORA Article 30(3) requires for ICT services supporting critical or important functions (including unrestricted on-site access and audit rights, participation in threat-led penetration testing, quantitative service-level targets, tested business contingency plans and a mandatory exit transition period). If you classify a function supported by a Clearlane app as critical or important, Clearlane apps are not suitable for it.

12. Secure development and vulnerabilities (NIS2 Art. 21(2)(d) and (e))

Dependency audit and SBOM (CycloneDX) for each release; vulnerability reports acknowledged within two business days; coordinated disclosure through clearlaneapps.com/.well-known/security.txt.

13. Limits

Clearlane holds no ISO 27001 or SOC 2 certification and no insurance, offers no availability SLA and no tested business contingency plan, and is run by one person. The counterweight is that the apps do not depend on any Clearlane server, your data stays in your site, the exports work without Clearlane, and section 5 gives notice before any stop. Whether an app supports a critical or important function is your assessment. Liability follows the licence terms.

Contact: hello@clearlaneapps.com