

## EU RULE · CYBERSECURITY

# NIS2: cybersecurity your EU customers pass on to you

NIS2 requires companies in the EU to check the security of their suppliers as well. That is why questionnaires, incident reporting clauses and audit rights end up with you, even if the law never mentions you.

| LEGAL BASIS              | APPLIES SINCE                | REPORTING DEADLINES | AFFECTS                               |
|--------------------------|------------------------------|---------------------|---------------------------------------|
| Directive (EU) 2022/2555 | Oct 18, 2024 (national laws) | 24 h, 72 h, 1 month | IT, software and industrial suppliers |

## In brief

NIS2 is an EU directive on cybersecurity. It applies to “essential” and “important” entities in 18 sectors, including energy, transport, health, digital infrastructure, ICT service management, food, chemicals and the manufacture of certain goods such as machinery, vehicles or electronics. Because it is a directive, each member state has passed its own law. The core obligations are the same everywhere, though.

Two articles matter for you. Article 21 requires information security risk management, and that explicitly includes supply chain security (para. 2(d)). The entity has to take into account the vulnerabilities of each direct supplier, the quality of its products and its security practices, including secure development (para. 3). Article 23 governs the reporting of significant incidents to the authorities: an early warning within 24 hours, an incident notification within 72 hours and a final report after one month.

An EU company can only meet these deadlines if its service providers also alert it quickly. That is why they now appear in many supply contracts, often in a stricter form.

## Who it affects in South America

Most companies in the region are affected by NIS2 indirectly. Your customer in Germany, Spain or the Netherlands carries the obligation and passes it on by contract. Typical cases:

- Nearshore development teams in Buenos Aires, Montevideo, Medellín or Lima building software for a utility or a hospital in the EU.
- IT support and call centers with access to customer systems.

- Manufacturers of controllers, sensors or industrial equipment, for example from São Paulo or Córdoba, supplying water utilities, manufacturers or logistics companies.
- Food processors whose buyers are themselves covered by NIS2 and therefore also ask about IT security in production.

You are directly affected if you offer certain digital services in the EU: cloud computing, data centers, content delivery networks, managed services and managed security services, DNS services, domain registration, online marketplaces, search engines and social networks. Under Article 26, these providers fall under the jurisdiction of the member state where they have their main establishment. If you have no establishment in the EU but offer services there, you must designate a representative in the EU (Art. 26(3)). If you do not, any member state in which the services are provided can take action (Art. 26(4)). A managed service provider from Porto Alegre with customers in Portugal should get legal advice on this.

Even without a direct obligation, it is worth reading the law. Almost every clause an EU customer puts in front of you can be traced back to Article 21 or 23. Knowing that makes negotiating easier.

## Deadlines

Member states had to transpose NIS2 by October 17, 2024, and the national rules have applied since October 18, 2024. Several countries were late. In practice the work is done in all major markets today, and purchasing departments are applying the new requirements.

In January 2026, the Commission proposed a targeted amendment to NIS2, together with a new legal framework for ICT supply chain security. Until that is adopted, the directive applies in its current form. For suppliers, it is already clear that the supply chain will become more important, not less. If you start building your program today, you will have little to redo later, because the obligations under Articles 21 and 23 already apply and form the basis of every customer request. Newly negotiated framework agreements with EU customers already contain the clauses anyway.

| REPORT UNDER ART. 23  | DEADLINE FOR THE EU ENTITY   | WHAT IT MEANS FOR YOU                                  |
|-----------------------|------------------------------|--------------------------------------------------------|
| Early warning         | 24 hours from becoming aware | Customers often require your notice within a few hours |
| Incident notification | 72 hours                     | Initial assessment, affected systems, indicators       |
| Final report          | 1 month                      | Root cause, measures taken, cross-border impact        |

## What EU customers actually ask for

The requirements are very similar from customer to customer. Expect the following:

- A security questionnaire, often based on ISO/IEC 27001 Annex A.
- An [ISO/IEC 27001](#) certificate, or for SaaS providers with US customers, a [SOC 2 Type II report](#) as an alternative.
- Contract clauses on reporting security incidents, often within 24 hours or sooner.
- Audit rights, on site or remote.
- Evidence of vulnerability management and penetration testing.
- For software, a software bill of materials (SBOM) and information on secure development.
- An incident response and business continuity plan.

A certificate answers a large part of the questionnaire in one go. Without one, you have to back up every answer separately, and do it again for every customer.

Watch out for contradictions. If your questionnaire says two-factor login is enforced on all accounts and the audit then turns up exceptions for legacy systems, you lose trust. An honest answer with a date for closing the gap works better. Keep your answers in one place so that sales and IT give the same information to every new customer. A GRC platform such as [Sightadel](#) can hold those answers together with the evidence behind them. In tenders run by large EU groups, the security assessment often decides whether you make the shortlist at all.

## First steps

1. Check whether you offer any of the services listed in Article 26 in the EU. If you do, get legal advice on the EU representative.
2. Make a list of your EU customers and their sectors. A customer in energy or health will ask for more than a retailer.
3. Decide who in the company assesses security incidents and informs the customer, with a deputy and a phone number.
4. Check your key systems from the outside: which servers, logins and services can be reached from the internet? Tools such as [veyrisk](#) show this on an ongoing basis.
5. Answer a real customer questionnaire honestly and mark the gaps. That becomes your action plan.
6. Plan ISO/IEC 27001 certification early, because building the management system and getting through the audit take time.

The free [EU Readiness Check](#) shows you in ten minutes how far along you already are.

## How it relates to certifications

NIS2 does not require any certificate. EU customers do accept recognized evidence, though, because it lets them document their own due diligence. [ISO/IEC 27001](#) covers most questions, as long as the certification body is accredited, in the region for example through Cgcre in [Brazil](#), OAA in [Argentina](#) or ONAC in [Colombia](#). Automotive suppliers also need [TISAX](#). If you work for banks or insurers, [DORA](#) comes on top, and for connected products, the [Cyber Resilience Act](#).

It also helps to look at your own country. [Chile](#) has the Ley Marco de Ciberseguridad, a law that resembles NIS2 in many respects; in [Uruguay](#), critical sectors are subject to reporting obligations. If you already have obligations there, part of the work is done.

## FAQ

### Does NIS2 apply to my company in South America?

Directly, only if you offer certain digital services in the EU, such as cloud, data center, managed services or DNS. In all other cases your EU customer passes the obligations on to you by contract.

### Do I need an ISO 27001 certificate for NIS2?

Not by law. Many EU customers ask for it anyway, because it makes their supply chain review under Article 21 easier. More on the [ISO/IEC 27001](#) page.

### How quickly do I have to report an incident to my EU customer?

That is set out in your contract. Because the customer itself has to submit an early warning within 24 hours, many contracts require you to report within a few hours.

### What is a representative in the EU?

A person or company established in the EU that acts as the authorities' point of contact for certain digital service providers without an EU establishment (Art. 26(3)).

### Which tools help with NIS2 requests from EU customers?

[Sightadel](#) supports NIS2 and ISO/IEC 27001 as frameworks and keeps policies, tasks and evidence in one place, hosted in Germany. [veyrisk](#) checks what is reachable from the internet and delivers a report you can attach to a security questionnaire.

---

**Sources** · Last updated: October 11, 2026

Directive (EU) 2022/2555 (NIS2), EUR-Lex: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

European Commission: NIS2 Directive: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

ENISA: NIS2 Directive: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

General information, not legal advice. The official texts are authoritative.

#### PUT IT INTO PRACTICE WITH TOOLS MADE IN GERMANY



Sightadel walks your team through NIS2: templates, tasks, evidence and audit preparation in one place. Built and hosted in Germany, with an optional consultant package.

[See Sightadel →](#)



veyrisk shows what attackers can see of your company from the outside: open services, certificates, known vulnerabilities. You can hand the report to EU customers and auditors.

[See veyrisk →](#)



Valar is a hardware firewall running neonotu software. It protects offices and sites and produces the logs NIS2 and ISO 27001 ask for.

[See Valar →](#)

Sightadel, veyrisk and Valar are products of neonotu GmbH, which operates MercoEU.

#### Which of these apply to your company?

The free EU Readiness Check shows you by industry and country in 10 minutes.

<https://www.mercoeu.com/en/eu-readiness-check>