

COUNTRY · MERCOSUR

Argentina: What EU customers expect

The EU has recognized Argentina as a country with adequate data protection since 2003. The law behind that dates from 2000, and a reform is pending in Congress. There is no cybersecurity law.

DATA PROTECTION	EU ADEQUACY	AGREEMENT WITH THE EU	CYBERSECURITY
Ley 25.326 (2000)	yes, since 2003	EU-Mercosur, provisional since May 1, 2026	no law, sector rules for banks

Overview: trade with the EU

According to the European Commission, roughly two thirds of Argentina's exports to the EU in 2025 were agricultural products, mainly oilseeds and protein crops such as soy and the animal feed made from them. Chemicals accounted for 13.7 %, fuels and mining products for 6.7 %. If you sell soybean meal from Rosario or beef from the Pampas to Europe, the [EUDR](#) is the rule you need to deal with first.

Argentina also has a strong software industry. Development teams in Buenos Aires, Córdoba and Mendoza have worked for clients in Spain, Germany and the Netherlands for years. For them, data protection and IT security come first.

Data protection: Ley 25.326 compared with the GDPR

The legal basis is Ley 25.326 on the protection of personal data, passed in 2000, together with its implementing regulation, Decreto 1558/2001. The AAIP (Agencia de Acceso a la Información Pública) is the supervisory authority. The law covers consent, purpose limitation, rights of access and erasure, and a registry of databases. Much of what the [GDPR](#) later added is missing: data protection impact assessments, a mandatory data protection officer, fines calculated as a percentage of revenue and a statutory deadline for reporting data breaches.

Even so, the EU recognized Argentina as adequate in 2003 (Decision 2003/490/EC) and confirmed this in the Commission's report of January 15, 2024. Argentina has also ratified the Council of Europe's modernized Convention 108+. Your EU customers can therefore transfer personal data to Argentina without standard contractual clauses.

Reform in Congress: bill 3397-D-2026 was introduced in the Chamber of Deputies on July 16, 2026. Among other things, it provides for a breach notification deadline and higher fines. Until it passes, Ley 25.326 applies unchanged.

If you already work to GDPR standards, you will have little to catch up on when the reform arrives. For service providers with EU customers this is the sensible route anyway, because the data processing agreement under Art. 28 GDPR requires these standards regardless of Argentine law.

Cybersecurity compared with NIS2

Argentina has no cybersecurity law. There is a national cybersecurity strategy and a government emergency team, CERT.ar, within the Dirección Nacional de Ciberseguridad. None of this creates obligations for companies of the kind that [NIS2](#) sets in the EU for energy, transport, health or digital services.

Binding requirements exist in the financial sector. Through Comunicación "A" 7724, the central bank BCRA sets minimum standards for IT and information security, and further Comunicaciones govern how banks respond to and report cyber incidents. If you supply software or data center services to Argentine banks, you will know these requirements from their contracts.

For EU customers, what counts in the end is the contract. A software company in Córdoba developing for a German insurer will receive clauses based on [DORA](#). A maker of networked control units has to meet the requirements of the [Cyber Resilience Act](#) if the device is sold in the EU.

Reporting deadlines compared

EVENT	ARGENTINA	EU
Data breach, notice to the authority	no statutory deadline in Ley 25.326	72 hours (Art. 33 GDPR)
Notice to affected individuals	no statutory deadline	without undue delay if the risk is high (Art. 34 GDPR)
Significant cyber incident	no general law; banks report under BCRA rules	24 h early warning, 72 h notification, final report after one month (Art. 23 NIS2)

Since your home law sets no deadline, in practice your EU customer sets it in the contract. Expect 24 to 48 hours and set up your process so you can meet it: who decides, who reports, and what information goes into the first notice.

Authorities, CSIRT, accreditation body

AREA	BODY
Data protection	AAIP, Dirección Nacional de Protección de Datos Personales
CSIRT	CERT.ar, Dirección Nacional de Ciberseguridad
Financial sector	BCRA, Banco Central de la República Argentina
Accreditation	OAA, Organismo Argentino de Acreditación

Certificates for [ISO 27001](#) or [ISO 9001](#) issued by OAA-accredited bodies are generally accepted in the EU. Some large groups insist on a certifier they know. Sort that out before the audit.

What EU customers typically ask for

For the EUDR, agricultural exporters need geolocation data for every plot where the soy or cattle in the EU shipment was produced, plus proof that no deforestation has taken place there since December 31, 2020. Argentina is classified as a standard-risk country. Food manufacturers will also be asked about [IFS](#), [BRCGS](#) or [FSSC 22000](#).

IT service providers receive security questionnaires, a data processing agreement and often a request for an ISO 27001 certificate or a SOC 2 report. You can build an information security management system with a GRC platform such as [Sightadel](#) and document it for the audit.

In practice, Argentine suppliers get a package of several documents: the data processing agreement, an annex listing technical and organizational measures, a list of subprocessors, a nondisclosure agreement and a security questionnaire that often runs to more than a hundred questions. For the questions about vulnerabilities and what is reachable from the internet, an external attack surface check such as [veyrisk](#) provides a report you can attach. Thanks to adequacy, standard contractual clauses are not needed. If you pass data on to service providers outside Argentina yourself, for example a cloud provider in the United States, your EU customer will still ask how that transfer is safeguarded.

A sensible starting point for companies in Argentina:

1. Find out which of your customers are based in the EU and which EU rules apply to them.
2. Bring your data protection program up to GDPR level, even where Ley 25.326 asks for less. This also prepares you for the reform.
3. Set an internal incident reporting deadline that is shorter than any deadline in your contracts.
4. For agricultural exports, collect geolocation data for your own plots and those of your suppliers.

5. Check whether an ISO 27001 certificate or a food safety standard would save you from providing individual evidence again and again.

The free [EU Readiness Check](#) gives you a first overview of your gaps.

Agreement with the EU

The [EU-Mercosur Agreement](#) was signed in Asunción on January 17, 2026. Argentina ratified it in February 2026. Since May 1, 2026, the trade part has been provisionally applied between the EU and Argentina, Brazil, Paraguay and Uruguay. To claim the tariff preference, you need a statement on origin. The broader partnership agreement is still going through ratification.

What this means in practice: for each product, check the tariff rate, the tariff reduction schedule and the rule of origin. You will find both in the European Commission's Access2Markets portal, sorted by tariff code. For processed goods, the rule of origin decides whether enough value was added within Mercosur. Some agricultural products are subject to tariff rate quotas, meaning limited volumes at the preferential rate. Your importer in the EU often knows these rules better than you do and can help you put the statement on origin on the invoice correctly. Keep your proof of origin for several years, because customs can check after the fact.

Tariff benefits do not change EU product law. The EUDR, CBAM and the GDPR still apply in full.

FAQ

Can EU customers transfer data to Argentina without standard contractual clauses?

Yes. Argentina has had an adequacy decision since 2003 (2003/490/EC), confirmed in 2024. If you process data on a customer's behalf, you still need a contract under Art. 28 GDPR.

Is there a duty to report data breaches in Argentina?

Ley 25.326 sets no statutory deadline. Reform bill 3397-D-2026 would change that, but it has not been passed yet. EU customers usually set the deadline in the contract.

Does Argentina have a law like NIS2?

No. Binding security requirements exist mainly in the financial sector, set by the central bank BCRA.

Is the EU-Mercosur Agreement already in force?

The trade part has been provisionally applied since May 1, 2026. Details are on the page about the [agreement](#).

Which tool helps an Argentine IT provider prepare for ISO 27001?

Without a national cybersecurity law, ISO 27001 is the usual reference for EU customers. [Sightadel](#) is a GRC platform developed and hosted in Germany that guides you through the standard with templates, tasks and evidence, and it is available in Spanish. The certificate is issued by an accredited certification body.

Sources · Last updated: October 11, 2026

Ley 25.326, Información Legislativa: <https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790>

AAIP, Agencia de Acceso a la Información Pública: <https://www.argentina.gob.ar/aaip>

European Commission: adequacy decisions: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Honorable Cámara de Diputados: bills (Proyectos): <https://www.hcdn.gob.ar/proyectos/>

BCRA: Comunicaciones: <https://www.bkra.gob.ar/>

European Commission, DG Trade: Argentina: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/argentina_en

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>