

COUNTRY · MERCOSUR

Brazil: What EU customers expect

Since January 2026, the EU has recognized Brazil as a country with adequate data protection. That makes data flows easier, but it does not replace evidence on IT security, deforestation or emissions.

DATA PROTECTION	EU ADEQUACY	AGREEMENT WITH THE EU	CYBERSECURITY
LGPD, Lei 13.709/2018	yes, since Jan 2026	EU-Mercosur, provisional since May 1, 2026	no cross-sector law, PL 4.752/2025 pending

Overview: trade with the EU

Brazil is the EU's largest trading partner in South America. According to the European Commission, about 42 % of Brazil's exports to the EU in 2025 were agricultural products and 27 % were fuels and mining products, mainly crude oil, followed by iron ore. If you ship soy from Paraná, coffee from Minas Gerais or pulp from Mato Grosso do Sul to Rotterdam or Hamburg, supply chain rules such as the [EUDR](#) are the first thing you run into. Steel and aluminum exporters are affected by [CBAM](#).

On top of that, service exports are growing: software companies in São Paulo, Florianópolis and Recife develop for banks, insurers and industrial clients in Europe. For them, data protection and IT security matter more than tariffs.

Data protection: the LGPD compared with the GDPR

The LGPD (Lei nº 13.709/2018) has applied since September 2020, and the ANPD has been imposing sanctions since August 2021. It is modeled on the [GDPR](#): a legal basis for every processing activity, data subject rights, a data protection officer (encarregado), impact assessments and duties to report security incidents. If you implement the LGPD properly, you have already covered a large share of your GDPR obligations.

Since January 2026 there has also been an EU adequacy decision (Implementing Decision (EU) 2026/179). The recognition is mutual: through Resolução CD/ANPD nº 32/2026, the ANPD has likewise found the EU to be adequate. For your EU customers, this means personal data can flow to Brazil without standard contractual clauses and without a transfer impact assessment. The only exception is transfers for public security and law enforcement purposes.

Adequacy only covers the data transfer. If you process data on behalf of an EU customer, you still need a data processing agreement under Art. 28 GDPR and must document your technical and organizational measures.

Two differences stand out in practice. The LGPD has ten legal bases, including credit protection, while the GDPR has six. And the deadline for reporting data breaches is counted in business days, not hours. If you work under both regimes, it is best to align your processes with the shorter deadline.

Cybersecurity compared with NIS2

Brazil does not yet have a law that sets obligations for entire sectors the way [NIS2](#) does. Decreto nº 11.856/2023 establishes the national cybersecurity policy (PNCiber) and a committee (CNCiber), but it does not create a supervisory authority with direct powers over companies. A draft Marco Legal da Cibersegurança (PL 4.752/2025) is in the Senate. The main open question is whether a new agency or Anatel will take on supervision.

So far, binding requirements exist sector by sector. Under Resolução CMN nº 4.893/2021, banks must have a cybersecurity policy, manage cloud outsourcing and report relevant incidents to the Banco Central. Payment institutions are subject to equivalent rules under Resolução BCB nº 85/2021.

For suppliers to European customers, this is a secondary issue. Under NIS2, your EU customer has to manage security in its supply chain and passes that duty on to you by contract. If you supply software to financial companies in the EU, your contract will also include clauses based on [DORA](#), and makers of connected products fall under the [Cyber Resilience Act](#).

Reporting deadlines compared

EVENT	BRAZIL	EU
Data breach, notice to the authority	3 business days from awareness if there is relevant risk (Res. CD/ANPD 15/2024); double the time for small businesses	72 hours (Art. 33 GDPR)
Notice to affected individuals	also 3 business days	without undue delay if the risk is high (Art. 34 GDPR)
Significant cyber incident	no general law; banks report to the Banco Central	24 h early warning, 72 h notification, final report after one month (Art. 23 NIS2)

The ANPD rule also requires you to document incidents and keep those records for five years. An EU customer will usually set its own deadline in your contract, often 24 to 48 hours, so that it can meet its own 72 hours.

Authorities, CSIRT, accreditation body

AREA	BODY
Data protection	ANPD, Autoridade Nacional de Proteção de Dados
Federal cybersecurity	GSI/PR with CTIR Gov (federal administration)
CSIRT for the private sector	CERT.br at NIC.br
Financial sector	Banco Central do Brasil, Conselho Monetário Nacional
Accreditation	INMETRO, accreditation by Cgcre

Certificates from bodies accredited by Cgcre are generally accepted in the EU, because Cgcre is a member of the international mutual recognition arrangements among accreditation bodies. Still, ask before the audit whether your customer requires a specific certifier.

What EU customers typically ask for

For agricultural and commodity exporters, the EUDR comes first. Your buyer needs the geolocation data for your plots and proof that no deforestation took place there after December 31, 2020. Brazil is classified as a standard-risk country under the EUDR, so the full due diligence obligation applies. Simplified due diligence under Art. 13 is only available for low-risk countries. In the food chain, certificates for [IFS](#), [BRCGS](#) or [FSSC 22000](#) are added on top.

Software and IT service providers are usually handed a security questionnaire based on NIS2 and [ISO 27001](#). Typical questions: How quickly do you report an incident? Who has access to production data? Do you run penetration tests? An ISO 27001 certificate answers many of these questions at once. On a GRC platform such as [Sightadel](#), you can work through the standard step by step and reuse the answers for the next questionnaire.

Many customers also check from the outside what you expose on the internet: open ports, expired certificates, outdated server versions. If you monitor this yourself on an ongoing basis, for example with [veyrisk](#), you know the answer before the questionnaire arrives.

In the contract, these requirements usually end up as annexes: a data processing agreement under Art. 28 GDPR, a list of technical and organizational measures, incident reporting deadlines, the

customer's audit rights and rules for subprocessors. Because Brazil is considered adequate, standard contractual clauses are not needed. Your customer will still ask for everything else, and will review it again at renewal.

A sensible starting point for Brazilian companies:

1. Check which EU rules affect your customers, and ask about their requirements proactively instead of waiting for the questionnaire.
2. Put your LGPD documentation side by side with the GDPR requirements. Records of processing, legal bases and impact assessments can usually be reused.
3. Set up a reporting process that meets the shortest contractual deadline, and rehearse it once a year.
4. Collect geolocation data and evidence from your suppliers for the EUDR before your buyer asks for it.
5. Decide whether an ISO 27001 certificate or a food safety standard would answer your customers' questionnaires faster than any one-off response.

The free [EU Readiness Check](#) shows you where you stand today.

Agreement with the EU

The [EU-Mercosur Agreement](#) was signed in Asunción on January 17, 2026. Its trade part, the interim trade agreement, has been provisionally applied between the EU and Brazil, Argentina, Paraguay and Uruguay since May 1, 2026. Tariffs come down in stages, and you need a statement on origin to use the preference. 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.

The agreement does not exempt you from EU law. The EUDR, CBAM, the GDPR and product regulations apply to Brazilian goods exactly as they do to goods from any other country.

FAQ

Do EU customers still need standard contractual clauses for data transfers to Brazil?

No. Since adequacy decision (EU) 2026/179 of January 2026, data can be transferred to Brazil without SCCs. You still need a data processing agreement if you process data on a customer's behalf.

Does Brazil have a law like NIS2?

Not yet. Draft bill PL 4.752/2025 is in the Senate. Until it passes, sector rules apply, mainly for banks and payment institutions.

How quickly do I have to report a data breach to the ANPD?

Within three business days of becoming aware of it, if there is a relevant risk to the people affected (Resolução CD/ANPD 15/2024). Small businesses get twice as long.

Does the EU-Mercosur Agreement reduce my EUDR obligations?

No. Tariff benefits require proof of origin, and the EUDR applies unchanged. More on the [EUDR](#) page.

Which tool helps a Brazilian IT provider with ISO 27001 and the GDPR?

[Sightadel](#) is a GRC platform developed and hosted in Germany that supports ISO 27001 and the GDPR as frameworks, with templates, tasks and evidence. It is available in Brazilian Portuguese. The certificate itself is issued by an accredited certification body.

Sources · Last updated: October 11, 2026

Lei nº 13.709/2018 (LGPD), Planalto: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

ANPD, Autoridade Nacional de Proteção de Dados: <https://www.gov.br/anpd>

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

Decreto nº 11.856/2023 (PNCiber), Planalto: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11856.htm

CERT.br: <https://cert.br/>

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

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

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>