

WHITE PAPER

EU requirements for suppliers from South America

Exporting, agreements, EU rules and certifications: what companies from Mercosur, Chile, Colombia, Peru and Ecuador need to know.

OCTOBER 16, 2026 · [HTTPS://WWW.MERCOEU.COM](https://www.mercoeu.com)

Contents

1. Exporting to the EU: What you need to know before you start
2. The EU-Mercosur Agreement
3. NIS2: cybersecurity your EU customers pass on to you
4. DORA: when your customer is a bank in the EU
5. GDPR: personal data from the EU in South America
6. AI Act: AI products for the EU market
7. Cyber Resilience Act: security for connected products
8. EUDR: deforestation-free supply chains
9. CBAM: the carbon price at the EU border
10. CSDDD and CSRD: your customers' due diligence and reporting duties
11. Forced Labour Regulation: no market access for products made with forced labor
12. Certifications EU customers ask for
13. Your country next to EU law

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

GUIDE · FIRST STEPS

Exporting to the EU: What you need to know before you start

Seven steps from your first tariff code to your first order. Written for companies in Mercosur, Chile, Colombia, Peru and Ecuador that are shipping to the EU for the first time or want to grow their EU business.

This page gives a general overview. It does not replace legal, customs or tax advice for your specific case. The legal texts and the answers of the competent authorities are binding.

Step 1: Check market access

It all starts with a number: your product's tariff code. The first six digits follow the Harmonized System (HS), which is the same worldwide. The EU extends them to the eight-digit Combined Nomenclature and, for imports, to the ten-digit TARIC code. Your home tariff code in Mercosur (NCM) or in the Andean countries matches the HS in the first six digits. After that, the systems diverge.

Take that number to [Access2Markets](#), the European Commission's free portal. In "My Trade Assistant" you enter the product code, country of origin and EU destination country. You then see the standard duty rate, the preferential rate under the agreement, import VAT in the destination country, product requirements and the rules of origin. The ROSA tool walks you step by step through whether your product meets the rules of origin. The Commission's TARIC database also shows quotas, anti-dumping duties and import restrictions.

Which agreement applies depends on your country:

COUNTRY	LEGAL BASIS	IN EFFECT SINCE
Argentina, Brazil, Paraguay, Uruguay	EU-Mercosur Interim Trade Agreement, provisionally applied	May 1, 2026
Chile	EU-Chile Interim Trade Agreement (ITA)	Feb 1, 2025
Peru	EU-Colombia/Peru Trade Agreement	Mar 1, 2013
Colombia	EU-Colombia/Peru Trade Agreement	Aug 1, 2013
Ecuador	Accession to the Trade Agreement	Jan 1, 2017

COUNTRY	LEGAL BASIS	IN EFFECT SINCE
Bolivia	Generalised Scheme of Preferences, special arrangement GSP+	2014

You will find details on the agreements on the page [EU-Mercosur Agreement](#). For Bolivia: in June 2026 the EU published a new GSP regulation that applies for ten years from January 1, 2027. Before signing contracts for 2027, check which preferences will then apply to your product.

The preferential rate only applies to goods originating in the partner country, and only with the right proof. The agreements differ a good deal here:

- Mercosur: the exporter makes a statement on origin with fixed wording, on the invoice or another commercial document. Exporters from Argentina, Brazil and Uruguay add their national tax or registration number (CUIT, CNPJ, RUT). For a transition period of three years, which can be extended by two, the EU also accepts official certificates of origin.
- Chile: a statement on origin by the exporter, including the RUT, or the importer's knowledge of the origin. The old EUR.1 has not been accepted since February 1, 2025.
- Colombia, Peru, Ecuador: EUR.1 movement certificate or an origin declaration on the invoice. An approved exporter may make the declaration; for consignments up to €6,000, any exporter may.
- Bolivia (GSP): statement on origin. If the originating goods in a consignment are worth more than €6,000, the exporter must be listed in the Registered Exporter system REX; you register with the competent authority in your own country.

Work through the rule of origin once for each product before you price with the preferential rate. Packing, simple mixing or simple assembly are not enough. A furniture maker in Misiones using fittings from Asia, or a food producer with imported ingredients, should check the bill of materials against the rule in the agreement.

Step 2: Meet the product requirements

An agreement lowers the duty. The requirements for the product stay the same as for a manufacturer in Germany or Spain.

Industrial goods

Many product groups are covered by EU harmonization legislation: machinery, electrical equipment, radio equipment, toys, pressure equipment, construction products, medical devices. If yours falls under it, you need a conformity assessment, technical documentation, an EU declaration of conformity and the CE marking. Harmonized standards referenced in the Official Journal of the EU

give a presumption that the product meets the requirements. For connected devices and software, the [Cyber Resilience Act](#) adds its own rules from December 11, 2027.

Consumer products without a specific rule of their own fall under the General Product Safety Regulation (EU) 2023/988, in application since December 13, 2024. Two points affect exporters directly. First, a product may only be placed on the market if an economic operator established in the EU is responsible for it (Art. 16 in conjunction with Art. 4 of Regulation (EU) 2019/1020). That is usually your importer or an authorized representative. Second, instructions and safety information must be in a language set by each member state. If you sell through an online marketplace, the listing has to name the manufacturer and the responsible person.

In practice, labeling means the manufacturer's name and address, a type or batch number, the CE mark where required, and warnings in the local language. Plan the label for each destination country before you print packaging.

Food, animals and plants

Here the hurdles are higher and the lead time longer. Regulation (EU) 2017/625 governs official controls at the border. Products of animal origin follow a listing principle: your country must be approved for the product category, often with an approved residue monitoring plan, and your establishment must appear on the list of approved establishments. Beef from Uruguay, honey from Argentina or shrimp from Ecuador can only enter the EU from listed establishments. The listing is requested by the competent authority in your country, such as SENASA, MAPA, SAG, ICA, SENASA Perú or Agrocalidad.

Every consignment of animals, animal products and many plants needs an official certificate issued or recorded in the EU's TRACES system. The consignment is checked at a border control post: documents, identity and, depending on risk, sampling. Pesticide maximum residue levels are set by Regulation (EC) No 396/2005. They are often stricter than in South America, and for active substances without EU approval a very low default value usually applies. An avocado exporter in Antioquia should build the spraying schedule around these limits rather than around the home market.

EU buyers take a HACCP-based food safety system for granted. Retailers usually also ask for IFS, BRCGS or FSSC 22000. More on this on the page [Food safety](#).

Step 3: Organize customs and import

Ask your buyer the most important question early: who declares the goods in the EU? EU customs law does not use the term "importer of record" as such. It speaks of the declarant. Under Art. 170 of the Union Customs Code (UCC), the declarant must be established in the EU. There are exceptions, for

example for transit, temporary admission and occasional declarations. Normally, then, your EU customer or its freight forwarder handles the import.

The declarant needs an EORI number for this. As an exporter without an establishment in the EU, you need one yourself if you lodge customs declarations or entry summary declarations, apply for a customs decision, or act as a carrier. In that case you apply for the EORI in the member state where you first carry out such an activity.

The delivery term sets out who bears what. The usual choice is the International Chamber of Commerce's Incoterms 2020. Under FCA, FOB or CIF your responsibility ends before the EU border, and the buyer takes care of import, duty and taxes. Under DDP you owe the duty and import VAT in the destination country yourself. That usually means an indirect customs representative in the EU, an EORI number and often a VAT registration in the member state. Only agree to DDP once you have that setup in place.

On import, import VAT and possibly excise duties (on wine or spirits, for example) are due on top of the customs duty. Each member state sets its own rates; Access2Markets shows them by country. An importer entitled to deduct input VAT can usually reclaim the import VAT. For the tax treatment of your business model, especially for sales to consumers or warehousing in the EU, bring in a tax advisor in the destination country.

Before the goods arrive, the EU requires safety and security data in the Import Control System ICS2. The entry summary declaration is usually lodged by the carrier. To do so, the carrier needs precise information from you: a meaningful description of the goods, the HS code, the consignor and the consignee. "Various goods" or "spare parts" will not do and lead to queries and delays.

The usual documents include the commercial invoice, packing list, waybill or bill of lading, the proof of origin and, for food, the health certificate. If quantities, weights and descriptions do not match across the documents, customs will often hold the consignment.

Step 4: Sort out contracts and payment

EU buyers work with framework agreements and purchasing terms that often run to twenty pages or more. Expect these elements:

- a supplier code of conduct on human rights, working conditions, the environment and corruption, often with the obligation to pass it on to your own suppliers;
- a data processing agreement under Art. 28 GDPR as soon as you process personal data for the customer, plus standard contractual clauses where needed;
- an information security annex with minimum measures, reporting deadlines for security incidents and rules for subcontractors;

- audit and information rights: the customer or an auditor it appoints may review your processes, on site or by questionnaire;
- liability, warranty, recalls and proof of insurance;
- choice of law and place of jurisdiction or arbitration.

Go through these clauses with your legal counsel before you sign. Many obligations are negotiable, such as audit frequency, reporting deadlines or liability caps. Whatever you sign, you will have to prove later.

A contract for the sale of goods is often automatically governed by the UN Convention on Contracts for the International Sale of Goods (CISG) if both countries are parties and the contract does not exclude it. Decide deliberately whether you want that.

On payment: with new business relationships, many exporters protect themselves with a documentary letter of credit under the ICC rules ERA 600 (UCP 600) or with documentary collection. Established EU customers, on the other hand, usually insist on payment on open account with a payment term. The EU Late Payment Directive 2011/7/EU generally limits payment terms between businesses to 60 days, unless the contract expressly provides otherwise and this is not grossly unfair to the creditor. For outstanding receivables, export credit insurers and factoring companies in your country offer cover.

Step 5: Answer your customers' compliance questions

The questionnaire arrives at supplier onboarding at the latest. It contains the obligations your EU customer has to meet itself and passes on to you. Which rules affect your business depends on your product or service:

IF YOU SUPPLY ...	EXPECT QUESTIONS ON
IT services, software, data processing	GDPR , NIS2 , DORA for banks and insurers, the AI Act for AI features
Connected devices, software as a product	Cyber Resilience Act
Soy, beef and leather, coffee, cocoa, wood, rubber, palm oil	EUDR
Steel, aluminum, cement, fertilizers, hydrogen	CBAM
All goods, especially agriculture, mining, textiles	Forced Labour Regulation , CSDDD and CSRD

A recognized certificate is often the fastest way to answer many of these questions. Depending on the industry, EU buyers ask for [ISO 9001](#) for quality, [ISO 14001](#) for the environment, [ISO/IEC 27001](#)

for information security, [food safety](#) standards and, in the automotive industry, [TISAX](#). A certificate will not replace a questionnaire, though it makes it a lot shorter.

In practice, the same questions come back from every new customer. If policies, evidence and earlier answers sit in one place, such as a GRC platform like [Sightadel](#), the next questionnaire takes days instead of weeks. Security questionnaires often also ask how you find vulnerabilities in systems reachable from the internet. An external attack surface check such as [veyrisk](#) provides a report you can attach.

The free [EU Readiness Check](#) shows in about ten minutes which of these rules apply to you and where the gaps are.

Step 6: Find customers and use the support available

You do not have to go it alone for your first contacts. Several networks can help, most of them free or for a small fee.

The European Commission's Enterprise Europe Network (EEN) connects small and medium-sized companies with business partners, technology cooperation and advice. It has partner organizations in Argentina, Brazil, Chile and Peru. In its partnering database you can post cooperation offers and search requests from European companies.

The EU delegations in your country know the agreements, organize business forums and refer you to the trade sections of the member states. The member states' embassies have their own trade promotion staff. The German Chambers of Commerce Abroad (AHK) have offices in Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Paraguay, Peru and Uruguay. They offer market studies, partner searches and business delegations to Germany. Other member states, such as France, Italy or Spain, also run bilateral chambers in most countries.

The national export promotion agencies know the funding available at home and organize joint stands at trade fairs:

- Brazil: ApexBrasil
- Chile: ProChile
- Colombia: ProColombia
- Peru: PROMPERÚ
- Ecuador: Pro Ecuador
- Uruguay: Uruguay XXI
- Paraguay: REDIEX at the Ministry of Industry and Commerce

In Argentina and Bolivia, state export and investment promotion has been restructured in recent years. Your foreign ministry can tell you who to contact today.

Trade fairs are still the fastest way to meet many buyers at once. For food, Anuga in Cologne and SIAL in Paris are the big meeting points, for fruit and vegetables Fruit Logistica in Berlin, for industrial goods Hannover Messe. A joint stand run by your export agency usually costs less than a stand of your own and brings visitors with it.

Step 7: A plan for the first 90 days

The plan below assumes a company that has an exportable product and wants to win its first EU customer. For food of animal origin, establishment approval usually takes longer, so file that application right away.

WEEK	TASK	OUTCOME
1 to 2	Determine the tariff code, run Access2Markets for two or three destination countries	Duty rate, preferential rate, taxes and product requirements per country
2 to 3	Check the rule of origin with ROSA, compare against the bill of materials	Decision on whether the preferential rate is within reach; form of proof of origin settled
3 to 5	Clarify product law: CE, product safety, labeling or SPS requirements, establishment listing	List of missing tests, documents and labels
4 to 6	Complete the EU Readiness Check, collect certificates and evidence	Gap list for data protection, security and supply chain; folder with certificates
5 to 7	Contact your export agency, the EEN and chambers, choose trade fairs	Partner search meetings, trade fair plan for 12 months
6 to 8	Prepare model contracts: supplier code of conduct, data processing agreement, security annex	Your own positions on liability, audits and reporting deadlines
8 to 10	Set the Incoterm and payment method, choose a freight forwarder and customs representative	Pricing delivered to the EU border and to the customer, import process settled
10 to 13	First quotes, sample shipment, answer the supplier questionnaire	Quote with the customer, onboarding underway

Keep the results in one file: tariff code, origin calculation, conformity documents, certificates, contract templates. You will need that file again for your second customer, and customs can check proofs of origin years later.

<https://www.mercoeu.com/en/exporting-to-the-eu>

PUT IT INTO PRACTICE WITH TOOLS MADE IN GERMANY



Sightadel walks your team through your EU requirements: 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 →](#)

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

TRADE · AGREEMENTS

The EU-Mercosur Agreement

Since May 1, 2026, the EU has been provisionally applying the trade part of the agreement with Argentina, Brazil, Paraguay and Uruguay. Tariffs are coming down and public tenders are opening up. The EU's product and supply chain rules, however, still apply in full.

In brief

The agreement between the EU and Mercosur was negotiated for more than 25 years. Negotiations were politically concluded on December 6, 2024 in Montevideo. The agreement consists of two legal instruments:

- The EU-Mercosur Partnership Agreement (EMPA) covers political dialogue, cooperation and trade. It is a mixed agreement and has to be ratified by all 27 member states.
- The Interim Trade Agreement (iTA) contains only the trade part, which falls under the EU's exclusive competence: tariffs, rules of origin, customs procedures, services and public procurement. It expires as soon as the EMPA enters into force.

For companies, the Interim Trade Agreement is what counts right now. The Council of the EU authorized its signature and provisional application on January 9, 2026. It was signed on January 17, 2026 in Asunción. Since May 1, 2026, it has been provisionally applied between the EU and Argentina, Brazil, Paraguay and Uruguay.

Provisional application means the rules already apply even though ratification on the EU side is not yet complete. Customs authorities apply the preferential rates, and companies can rely on them. The political debate in some member states continues, but for now it does not change how the agreement is applied.

What applies since May 1, 2026

According to the European Commission, provisional application brings, among other things:

- the immediate removal or a sharp reduction of tariffs on key industrial goods, for example cars and pharmaceuticals;
- a first tariff cut for most agricultural and food products;
- access to the first volumes of the tariff-rate quotas for sensitive agricultural products;

- access to public tenders on both sides;
- protection for 344 EU geographical indications;
- safeguard mechanisms and tighter controls for sensitive agricultural sectors.

Many tariff cuts are phased in over several years. The rate for your product is set out in the agreement's tariff schedules. If you export soy from Paraná, beef from Uruguay, wine from Mendoza or honey from Paraguay, it pays to check both the schedule and the quotas.

Service providers will also see changes. The agreement contains rules on licensing procedures, non-discriminatory treatment and the temporary stay of skilled professionals. An engineering firm from Porto Alegre running a project in Portugal, or a software company from Montevideo with teams on site at a customer, can benefit. Access to public procurement works both ways: EU companies can bid for contracts in Mercosur and Mercosur companies for contracts in the EU, in each case within the lists agreed in the agreement.

Preferential tariffs only apply to goods originating in one of the parties. The exporter certifies origin with a statement on origin; on the EU side this runs through the REX registration system. Check the rules of origin for your product before you calculate with the preferential rate. For processed goods that use inputs from third countries, qualifying is not a given.

Timeline and open questions

DATE	STEP
Dec 6, 2024	Political conclusion in Montevideo
Jan 9, 2026	Council authorizes signature and provisional application
Jan 17, 2026	Signature in Asunción
Jan 21, 2026	European Parliament requests an opinion from the Court of Justice of the EU, by 334 votes to 324
May 1, 2026	Provisional application of the Interim Trade Agreement with AR, BR, PY, UY

The Court of Justice's opinion under Article 218(11) TFEU is still pending. Until it is delivered, the European Parliament cannot give its consent to the agreement. Provisional application continues regardless. The Partnership Agreement also needs ratification by every member state; there is no way to tell yet when it will enter into force.

[Bolivia](#) has been a full member of Mercosur since 2024 (instrument of ratification deposited in July 2024), with a transition period for adopting Mercosur law. It is not a party to the agreement with the EU.

Chile, Colombia, Peru and Ecuador

The associated states have their own agreements with the EU, which have been in place for some time.

COUNTRY	AGREEMENT	IN FORCE SINCE
Chile	Interim Trade Agreement (ITA), signed on Dec 13, 2023 together with the Advanced Framework Agreement	Feb 1, 2025
Peru	EU-Colombia/Peru Trade Agreement	Mar 1, 2013
Colombia	EU-Colombia/Peru Trade Agreement	Aug 1, 2013
Ecuador	Accession to the Trade Agreement by protocol	Jan 1, 2017

The agreement with Chile replaces the trade part of the 2002 Association Agreement and includes chapters on energy and raw materials and on sustainable food systems, among others. The agreement with Colombia, Peru and Ecuador contains a title on trade and sustainable development that refers to the ILO core labor standards and to international environmental agreements.

For exporters from these countries, the same applies as for Mercosur: the agreements cover tariffs and origin. A copper producer in Antofagasta, a banana exporter in Guayaquil or a coffee house in Huila still has to meet the EU's rules on products, data and supply chains in full.

What the agreement does not change

A trade agreement lowers tariffs and simplifies procedures. It does not exempt anyone from the EU's product, data protection and supply chain rules. All [EU rules](#) apply to goods and services from Mercosur exactly as they do to those from any other country:

- From December 30, 2026, soy, beef, coffee and wood need the evidence required by the [EUDR](#).
- Since January 1, 2026, steel, aluminum and fertilizers have been subject to the [Carbon Border Adjustment Mechanism](#).
- From December 11, 2027, connected products must conform to the [Cyber Resilience Act](#).
- From December 14, 2027, products made with forced labor are banned under the [Forced Labour Regulation](#).

- Food must meet EU standards; the sanitary and phytosanitary chapters speed up procedures but do not lower any requirements.

In the trade and sustainable development chapter, the parties commit to the ILO core labor standards and the Paris Agreement. The chapter on technical barriers to trade follows international standards and makes conformity assessment easier, but it does not replace CE marking.

First steps for exporters

1. Check the preferential tariff rate and the phase-in schedule for each product.
2. Find out whether your product meets the rules of origin, and set up your statement on origin.
3. For agricultural products, check whether quotas apply and how they are allocated.
4. Work out which EU rules apply to your product. The tariff advantage is worth nothing if the buyer cannot purchase because evidence is missing. Ask your most important buyers directly which documents they will expect from 2027.
5. Prepare the certificates that EU customers in your industry expect, such as [ISO 9001](#), [food safety](#) or [ISO/IEC 27001](#).

Buyers rarely ask for one document only. Certificates, supplier self-assessments and evidence for individual EU rules tend to arrive at the same time. A GRC platform such as [Sightadel](#) keeps the tasks, evidence and supplier assessments for this in one place.

The free [EU Readiness Check](#) shows how well prepared you are for EU customers. You will find country-specific details on the pages for [Argentina](#), [Brazil](#), [Paraguay](#) and [Uruguay](#).

<https://www.mercoeu.com/en/eu-mercosur-agreement>

PUT IT INTO PRACTICE WITH TOOLS MADE IN GERMANY



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

[See Sightadel →](#)

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

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.

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.

<https://www.mercoeu.com/en/eu-rules/nis2>

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.

EU RULE · FINANCIAL SECTOR

DORA: when your customer is a bank in the EU

Since January 17, 2025, banks, insurers and other financial entities in the EU have had to select, contract and monitor their IT service providers according to fixed rules. If you supply them with software, data center services or IT support, you will feel it directly.

In brief

The Digital Operational Resilience Act, DORA for short, is an EU regulation. It applies directly in every member state, with no national implementing law needed. It is addressed to financial entities: banks, insurers, payment and e-money institutions, investment firms, fund managers, crypto-asset service providers and others. They have to set up their IT so that they can withstand disruptions, attacks and outages.

A large part of the regulation deals with ICT third-party service providers, meaning the external providers of IT services. Article 28 requires the financial entity to assess a provider's risks before signing a contract, to record all contracts in a register of information and to have an exit strategy for important services. Article 29 deals with concentration risk and explicitly mentions providers in third countries: insolvency law and data protection in the provider's country have to be taken into account. Article 30 sets out what every contract must contain.

For a provider from South America, this means your customer may only hire you if the contract contains these minimum terms and you supply the information required.

Who it affects in South America

Only providers that the European Supervisory Authorities (EBA, EIOPA and ESMA) designate as critical ICT third-party service providers have direct obligations under DORA. The first list was published on November 18, 2025 and named 19 providers, mostly large cloud, data center, network and financial software companies. Under Article 31(12), a critical provider from a third country may only be used if it sets up a subsidiary in the EU within twelve months of its designation.

The usual case is indirect. This includes:

- Fintechs and software companies, for example from São Paulo, Buenos Aires or Bogotá, that develop or run payment, lending or insurance software for EU customers.

- Nearshore teams that code, test or maintain systems for European banks.
- Data centers and hosting providers with European financial customers.
- Call centers and BPO providers working with access to customer systems.
- Providers of market, credit or fraud data.

All of them are recorded in the customer's register of information and have to accept the contract clauses under Article 30. According to an EBA answer in its Q&A process (Q&A 2024_7096), intra-group service providers are excluded from designation as critical providers. That exemption does not extend to the contractual obligations.

An example: a software company in Montevideo runs the claims portal for a Spanish insurer. Before renewing the contract, the insurer has to check where the data is stored, who has access, how quickly the portal is back up after an outage and what happens if the software company stops operating. The answers go into its register and its risk assessment. If the software company cannot back them up, the insurer has to cover the risk in some other way or switch providers.

Deadlines

DORA has applied since January 17, 2025. Financial entities had to update existing contracts and build their registers. If you negotiate with an EU bank today, the DORA addendum comes along with the framework agreement. Older contracts without these clauses are brought up to date at the next renewal, often at short notice.

DATE	WHAT HAPPENED
Jan 17, 2025	DORA applies in all member states
Nov 18, 2025	First list of critical ICT third-party service providers (19 providers)
12 months after designation	Critical providers from third countries need an EU subsidiary (Art. 31(12))

Oversight of critical providers is strict. Under Article 35(6), periodic penalty payments of up to 1% of average daily worldwide turnover are possible.

What EU customers actually ask for

Article 30 sets out what a contract for ICT services must contain. This includes a clear description of the services, the locations where data is processed, rules on access, inspection and audit, termination rights, support during security incidents and, for important services, participation in the customer's tests and exercises. In practice, expect the following:

- A DORA contract addendum covering these points. Many banks have their own templates.
- Data for the register of information: your LEI (Legal Entity Identifier), data processing locations and the subcontractors you use.
- An [ISO/IEC 27001](#) certificate or a [SOC 2 report](#).
- Evidence of business continuity management, often based on ISO 22301.
- Willingness to host the customer's and the supervisors' auditors on site.
- An exit plan describing how the customer can bring the service back in-house or transfer it in an orderly way.

The LEI catches many providers by surprise. You apply for it through accredited issuing organizations, and it has to be renewed every year. Without it, your customer cannot record you correctly in its register.

For important or critical functions, participation in testing comes on top. Large financial entities must regularly carry out threat-led penetration tests, and a provider running such a function can be brought in. Agree in the contract how this works, who bears the costs and how your other customers are protected.

Your own providers come under scrutiny too. If you work for an EU bank on a cloud platform or hand parts of the work to freelancers, the customer will want to know and may need to approve it.

First steps

1. Check which of your EU customers are financial entities. A leasing company or a payment service provider can fall under DORA too.
2. Apply for an LEI if you do not have one yet.
3. List every location where you store or process customer data, and all your subcontractors.
4. Go through your most important customer's DORA addendum point by point and mark what you do not meet today.
5. Write an incident response and recovery plan for the services you provide to financial customers, and test it.
6. Keep evidence, policies and audit reports ready in one place. A GRC platform such as [Sightadel](#) helps you maintain this for several customers at once.

The [EU Readiness Check](#) gives you an initial assessment.

How it relates to certifications

DORA does not name a mandatory certificate. EU banks do assess their providers against fixed criteria, though, and a recognized certificate shortens that review considerably. For information security that means [ISO/IEC 27001](#), often supplemented by [SOC 2](#) for providers with US customers. If you supply AI models for credit decisions or fraud detection, you should also know the [AI Act](#) and [ISO/IEC 42001](#). Whenever personal data is processed, the [GDPR](#) applies as well. For providers from [Brazil](#), [Argentina](#) and [Uruguay](#), data transfers are simpler thanks to an adequacy decision.

DORA and [NIS2](#) overlap. For financial entities, DORA takes precedence as the more specific rule, but the requirements for suppliers are similar. If you work for both groups of customers, one management system can serve both.

<https://www.mercoeu.com/en/eu-rules/dora>

PUT IT INTO PRACTICE WITH TOOLS MADE IN GERMANY



Sightadel walks your team through DORA: 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 →](#)

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

EU RULE · DATA PROTECTION

GDPR: personal data from the EU in South America

The General Data Protection Regulation also applies to companies with no establishment in the EU. Even more often, it reaches you through your EU customers as soon as you process personal data on their behalf.

In brief

The GDPR governs how personal data may be processed: names, email addresses, customer numbers, location data, health data and anything else that can be linked to a person. It has applied directly in all member states since May 25, 2018.

For companies outside the EU, there are two ways the GDPR can apply. The first is the targeting principle in Article 3(2): if you offer goods or services to people in the EU or monitor their behavior, for example through tracking on a website, you are directly subject to the GDPR. The second is more common. An EU company hires you to process data on its behalf, and it may only do so if there is a contract under Article 28 and the transfer to your country is permitted under Chapter V (Art. 44 to 50).

Chapter V offers several legal bases. The simplest is a Commission adequacy decision under Article 45: your country is then considered safe, and data flows as it would within the EU. Without one, the EU customer needs appropriate safeguards under Article 46, in practice almost always the Commission's standard contractual clauses (Implementing Decision (EU) 2021/914).

Supervisory authorities can impose fines of up to 20 million euros or 4% of worldwide annual turnover, whichever is higher (Art. 83(5)). Enforcement is harder against companies outside the EU, but not against your EU customer. That is why your customer checks carefully whom it entrusts with data and has liability and audit rights written into the contract. A data breach at a service provider in Lima falls back legally on the client in Madrid.

Who it affects in South America

Online stores, SaaS providers, tour operators, language schools and app developers that specifically target customers in the EU are directly affected. A hotel in Cusco with a German-language booking page and prices in euros is one of them. Under Article 27, these companies must designate a representative in the EU. The only exception is occasional processing that does not involve large-

scale sensitive data (Art. 27(2)).

All processors are indirectly affected: call centers in Bogotá working for a Spanish telecom operator, IT support from Córdoba, payroll, software development with real customer data, data analytics, cloud hosting.

COUNTRY	EU ADEQUACY DECISION	WHAT THE EU CUSTOMER NEEDS
Argentina	Yes, Decision 2003/490/EC, confirmed in the Commission report of Jan 15, 2024	Contract under Art. 28
Uruguay	Yes, Implementing Decision 2012/484/EU, confirmed on Jan 15, 2024	Contract under Art. 28
Brazil	Yes, adopted on Jan 26, 2026	Contract under Art. 28
Chile , Colombia , Peru , Ecuador , Paraguay , Bolivia	No	Contract under Art. 28, standard contractual clauses and a transfer impact assessment

The decision for Brazil is mutual: Brazil's data protection authority, ANPD, has in turn recognized the EU as adequate. It covers both the public and the private sector. For a software company in Florianópolis, since the decision of January 26, 2026, transfers from the EU no longer need standard contractual clauses or a transfer impact assessment. That removes much of the paperwork it used to have with every EU customer.

Adequacy saves you the standard contractual clauses. It does not replace the Article 28 contract or the technical safeguards, and your customer will keep asking for both.

Deadlines

The GDPR has applied unchanged since 2018. New dates mainly concern the region: the adequacy decision for Brazil of January 26, 2026, and new national laws, for example in [Chile](#) and [Paraguay](#), that are not yet fully applicable.

In November 2025, the Commission proposed a “Digital Omnibus” that would also amend parts of the GDPR. Until the proposal is adopted, the GDPR applies in its familiar form. Plan on the basis of the law as it stands.

There are still deadlines in day-to-day work. The EU controller has to report a data breach to the supervisory authority within 72 hours (Art. 33). As a processor, you must inform the controller “without undue delay”, and many contracts set 24 or 48 hours for this.

What EU customers actually ask for

- A data processing agreement (DPA) under Article 28, usually on the customer's template.
- For countries without adequacy, the standard contractual clauses, usually Module 2 (controller to processor) or Module 3 (processor to sub-processor).
- A transfer impact assessment that evaluates whether authorities in your country can access the data.
- A description of your technical and organizational measures (TOMs) under Article 32.
- A list of your sub-processors, such as cloud providers and ticketing systems.
- A record of processing activities for the customer's data.
- As evidence of the TOMs, often an [ISO/IEC 27001](#) certificate, sometimes supplemented by ISO/IEC 27701 for privacy.

If you target customers in the EU directly, you also need a GDPR-compliant privacy notice, a legal basis for every processing activity, a process for access and deletion requests and, where required, the EU representative under Article 27.

First steps

1. Establish whether you target people in the EU directly or only process data for EU companies. That determines whether you need an EU representative.
2. List which personal data you receive from EU customers, where it is stored and who has access.
3. Check the law in your own country. Brazil's LGPD and the laws in Argentina and Uruguay are similar to the GDPR; in other countries, quite a lot is missing. The country pages have the details.
4. Prepare a TOM description that you can hand to any customer.
5. Set up a data breach procedure, with notice to the customer within the contractual deadline.
6. Take the free [EU Readiness Check](#) to see where the gaps are.

A GRC platform such as [Sightadel](#) helps you keep records, TOMs and contracts up to date for many customers.

How it relates to certifications

The GDPR has its own certification mechanisms under Article 42, but they are rarely used in practice. EU customers therefore rely on [ISO/IEC 27001](#) as evidence of security of processing under Article 32. SaaS providers with US customers often have a [SOC 2 report](#), which many EU customers also accept. If you work with AI and personal data, take a look at the [AI Act](#). For IT service providers to banks, [DORA](#) comes on top, and for many others [NIS2](#).

A certificate does not replace a case-by-case review. It does show that access rights, encryption, logging and incident handling are in place and are regularly checked by outsiders. Those are exactly the points the customer asks about in its TOM review. With the certificate, you answer with a reference instead of twenty pages of explanation.

<https://www.mercoeu.com/en/eu-rules/gdpr>

PUT IT INTO PRACTICE WITH TOOLS MADE IN GERMANY



Sightadel walks your team through the GDPR: 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 →](#)

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

EU RULE · ARTIFICIAL INTELLIGENCE

AI Act: AI products for the EU market

The AI Act applies wherever the provider is based, as soon as an AI system is offered in the EU or its output is used there. The obligations phase in step by step; the dates for high-risk systems were pushed back in July 2026.

In brief

The AI Act classifies AI systems by risk. Certain practices are prohibited, such as social scoring or manipulative techniques that cause harm (Art. 5). High-risk systems are allowed but tightly regulated. They include systems for recruitment, creditworthiness assessment, education and exams, critical infrastructure, and AI used as a safety component in products such as machinery or medical devices (Art. 6 with Annexes I and III). Chatbots and AI-generated content are subject to transparency obligations (Art. 50). General-purpose AI models, meaning large language and image models, have rules of their own (Art. 53 et seq.).

Most AI applications in companies, such as suggested replies in customer service or inventory forecasts, fall into none of these groups or only under the transparency obligations. The real effort is concentrated on high-risk systems.

Violations are expensive. For prohibited practices, Article 99 provides for fines of up to 35 million euros or 7% of worldwide annual turnover; for most other obligations, up to 15 million euros or 3%. For small and medium-sized enterprises, the lower of the two amounts applies in each case.

In July 2026, the EU used Regulation (EU) 2026/1744, the “Digital Omnibus on AI”, to postpone several deadlines and adjust individual obligations. It was published in the Official Journal on July 24, 2026 and entered into force three days later.

Who it affects in South America

Under Article 2(1)(a), the regulation applies to providers that place AI systems on the market or put them into service in the EU, regardless of where they are based. Under point (c), it also applies to providers and deployers in third countries if the output of the system is used in the EU. A startup in Buenos Aires that sells candidate screening software to HR departments in Germany is therefore the provider of a high-risk system within the meaning of the regulation.

Providers of high-risk systems and of general-purpose AI models that have no establishment in the EU must appoint an authorized representative in the EU (Art. 22 and Art. 54).

Even if you only use AI, you can have obligations. The regulation calls this a “deployer”. A logistics company in Montevideo that uses an AI tool to evaluate staff at its Spanish branch is the deployer of a high-risk system in the EU. It must use the system according to the instructions, monitor it and keep logs.

Development service providers are indirectly affected. A team in Medellín that trains a fraud detection model for a French provider has no provider obligations of its own. The client, however, needs documentation on the data, training and testing to pass its conformity assessment. Article 25 governs responsibilities along the value chain and requires suppliers of components to provide the information needed for this.

Typical high-risk cases from the region: scoring software from fintechs in São Paulo or Bogotá for EU lenders, HR tools from Santiago, learning platforms with automated grading from Montevideo, image analysis for medical devices.

Deadlines

The regulation has been in force since August 1, 2024. Its obligations apply in stages. The overview below reflects the changes made by Regulation (EU) 2026/1744.

FROM	WHAT APPLIES
Feb 2, 2025	Prohibited practices (Art. 5) and the AI literacy requirement for staff (Art. 4)
Aug 2, 2025	Obligations for general-purpose AI models, governance, penalties
Aug 2, 2026	Transparency obligations under Art. 50
Dec 2, 2026	End of the transition period for marking AI-generated content (Art. 50(2)) for systems placed on the market before Aug 2, 2026
Dec 2, 2027	High-risk systems under Annex III, e.g. HR, credit, education (originally Aug 2, 2026)
Aug 2, 2028	High-risk AI in products under Annex I, e.g. machinery, medical devices

The postponement buys time, but the requirements themselves are unchanged. If you are developing a high-risk system for the EU market, you need risk management, data quality, logging and human

oversight from the start. Retrofitting them later is hardly possible.

What EU customers actually ask for

EU customers now buy AI with their own list of questions. Expect the following:

- A classification of your system as prohibited, high-risk, subject to transparency obligations or without special obligations, with the reasoning.
- For high-risk systems, the technical documentation under Annex IV, the conformity assessment, the EU declaration of conformity and registration in the EU database.
- Information on training data: origin, rights, quality and how bias is handled.
- Instructions for use for the deployer, so your customer can meet its own obligations as a deployer.
- Logging and the ability to provide human oversight.
- Marking of AI-generated text, images, audio and video where Art. 50 requires it.
- The name of your EU authorized representative, if you need one.
- Often an [ISO/IEC 42001](#) certificate as evidence of an AI management system.

If your system processes personal data, the [GDPR](#) applies as well. Many of the questions overlap, for example on data origin and purpose limitation.

AI clauses are showing up more and more in contracts: a commitment that customer data will not be used for training, notice of significant model changes, cooperation with audits. The law does not always require them, but they reflect your customer's due diligence obligations.

First steps

1. Record every AI feature in your products and services, including embedded third-party models.
2. Assign each feature to a risk group. Check Annex III carefully, because the list of high-risk areas is specific.
3. Clarify your role: are you a provider, a deployer or a supplier to an EU provider?
4. Train your team. The AI literacy requirement has applied to all providers and deployers since February 2, 2025.
5. For high-risk systems, start on documentation and risk management now so that you are ready before December 2, 2027.
6. Check whether an ISO/IEC 42001 management system would make a difference to your customers.

Put the results in writing. A short list with the system, its purpose, the risk group and the person responsible is enough to start with, and it answers the first question every EU customer asks. If the list grows, a GRC platform such as [Sightadel](#), which supports the EU AI Act as a framework, can hold the inventory, the tasks and the evidence for each system.

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

How it relates to certifications

[ISO/IEC 42001](#) describes a management system for AI: roles, risk assessment, life cycle and data handling. It is not required by law, but it covers many of the regulation's organizational obligations and EU customers are asking for it more and more. For the security of systems and data, [ISO/IEC 27001](#) remains the standard; the two can be built up together. In [Sightadel](#), work already done for ISO/IEC 27001 can be reused for ISO/IEC 42001. If you supply AI software to banks, you should also know [DORA](#). AI in connected products also falls under the [Cyber Resilience Act](#).

<https://www.mercoeu.com/en/eu-rules/ai-act>

PUT IT INTO PRACTICE WITH TOOLS MADE IN GERMANY



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

[See Sightadel →](#)

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

EU RULE · PRODUCT SECURITY

Cyber Resilience Act: security for connected products

If you sell hardware or software with digital elements in the EU, the Cyber Resilience Act treats you as a manufacturer, even without an establishment in Europe. The reporting obligations for exploited vulnerabilities have applied since September 11, 2026.

In brief

The Cyber Resilience Act, CRA for short, is an EU regulation on cybersecurity requirements for “products with digital elements”. This means hardware and software that can connect directly or indirectly to a device or network: routers, cameras, controllers, industrial sensors, smart home devices, but also commercial software such as apps, operating systems or firmware. Areas with their own rules are excluded, for example medical devices, vehicles and aviation.

The CRA covers the entire life cycle. When it ships, a product must meet the essential requirements in Annex I: no known exploitable vulnerabilities, secure default settings, protection against unauthorized access and the ability to receive security updates. After that, the manufacturer must handle vulnerabilities and deliver updates for a support period that is generally at least five years (Art. 13). At the end of this comes the CE marking, which will also cover cybersecurity.

For most products, a self-assessment by the manufacturer is enough. For certain important and critical products, such as firewalls, network devices or smart cards, a harmonized standard or a notified body is needed, depending on the class.

Who it affects in South America

A manufacturer outside the EU counts as a manufacturer under the CRA as soon as its product is made available on the EU market. A company in Manaus that supplies control electronics to a machine builder in Italy therefore carries the manufacturer's obligations, provided it places the product on the market under its own name. It can appoint an authorized representative in the EU (Art. 18) to take on certain tasks.

Software companies with commercial products are affected in the same way: an accounting app from Santiago, security software from Buenos Aires, firmware for agricultural sensors from Rosario. With pure contract development, where the EU customer sells the product under its own name, the customer becomes the manufacturer. It will then pass the requirements on to you by contract.

Then there is the route through the importer. Under Article 19, an importer may only place products on the market that comply with the requirements. It therefore checks whether the conformity assessment, technical documentation, CE marking and the manufacturer's contact details are in place. If they are missing, it will not buy.

Under Article 20, distributors have similar but somewhat lighter checking obligations. If an importer or distributor learns of a vulnerability, it must inform the manufacturer. Where there is a serious risk, market surveillance can require products to be recalled or withdrawn from the market. For an exporter, this means a problem with one product can hold up an entire shipment in an EU warehouse.

Free open source software outside of a commercial activity is not covered by the CRA. As soon as you build it into a product you sell, you are responsible for the security of those components.

Deadlines

FROM	WHAT APPLIES
Jun 11, 2026	Rules on conformity assessment bodies
Sep 11, 2026	Reporting obligations under Art. 14 for actively exploited vulnerabilities and severe security incidents, including for products already on the market
Dec 11, 2027	All remaining obligations, including the requirements in Annex I, conformity assessment and CE marking

The reporting obligations are already running. If a manufacturer becomes aware of an actively exploited vulnerability in its product, it must submit an early warning within 24 hours, a notification within 72 hours and a final report no later than 14 days after a corrective measure is available. For severe security incidents, the final report is due within one month. Reports go through ENISA's single reporting platform (Art. 16), which has been in operation since September 11, 2026.

The reporting obligation also covers products you sold years ago, as long as they are on the market in the EU. If you do not have a vulnerability reporting process, now is the time to set one up.

What EU customers actually ask for

- An EU declaration of conformity, for all products with digital elements from December 11, 2027.
- The technical documentation, with a risk assessment and a description of the security measures.

- A software bill of materials (SBOM) listing all components and libraries.
- A coordinated vulnerability disclosure (CVD) policy with a contact address for reports.
- A stated support period and proof of how updates are delivered.
- For important or critical products, the result of the required conformity assessment, where applicable a certificate from a notified body.
- For industrial products, often evidence based on the IEC 62443 series of standards.

Many importers and distributors are already asking for this today, even though most obligations do not apply until the end of 2027. They do not want stock in their warehouse that they will no longer be allowed to sell.

Large buyers are also writing the requirements into their purchasing terms: assurance of CRA conformity from a set date, reporting of vulnerabilities to the customer, provision of updates for an agreed minimum period, and liability for recalls. Read these clauses carefully before you sign supply contracts that run beyond 2027.

First steps

1. Make a list of all products you supply to the EU that contain software or can be connected.
2. Check for each product whether it falls into the classes of important or critical products (Annexes III and IV).
3. Set up a reporting process right away: who takes in reports of vulnerabilities, who assesses them, who reports within 24 hours?
4. Generate an SBOM for each product version. Many build tools can do this automatically.
5. Check which of your systems can be reached from the internet, such as update servers and remote maintenance access. Tools such as [veyrisk](#) show this from the outside.
6. Plan the conformity assessment and documentation so they are finished before December 11, 2027.

The free [EU Readiness Check](#) gives you an initial picture.

How it relates to certifications

The CRA does not require any management system certification. An [ISO/IEC 27001](#) certificate does show, however, that your development, your build environment and your incident handling are under control, and it helps with the process requirements. For industrial products, IEC 62443 is widely used. Automotive suppliers usually need [TISAX](#), even though vehicles themselves are not covered by the CRA. Quality management under [ISO 9001](#) makes the documentation easier. For the organizational

work around it, a GRC tool such as [Sightadel](#) keeps tasks, evidence and document versions together. If you supply products to operators of critical services, [NIS2](#) comes on top, and AI features in products also fall under the [AI Act](#).

For manufacturers from [Brazil](#), where a lot of electronics and automation equipment is made, the CRA is one of the most important new EU rules. The requirements are the same whether the goods go through an importer or straight to an industrial customer.

<https://www.mercoeu.com/en/eu-rules/cyber-resilience-act>

PUT IT INTO PRACTICE WITH TOOLS MADE IN GERMANY



Sightadel walks your team through ISO 27001: 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 →](#)

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

EU RULE · SUPPLY CHAIN

EUDR: deforestation-free supply chains

From December 30, 2026, large and medium-sized companies may only sell seven commodities and the products made from them in the EU if they are deforestation-free and legally produced. Your EU buyer can only prove that with your data.

In brief

The EU Deforestation Regulation, EUDR for short, covers seven commodities: cattle, cocoa, coffee, oil palm, rubber, soy and wood. It also covers many products made from them, listed in Annex I, such as leather, chocolate, furniture, paper or soybean meal. These goods may only be placed on the EU market or exported from it if three conditions are met (Art. 3):

- They are deforestation-free, meaning the land was not deforested after December 31, 2020 (Art. 2(13)).
- They were produced legally under the law of the country of production, for example in terms of land rights, environmental law, labor law and tax law.
- A due diligence statement for them has been filed in the EU information system.

The due diligence statement is filed by the EU operator, which is usually the importer. To do so, the operator must collect information (Art. 9), assess the risk (Art. 10) and mitigate it where necessary (Art. 11). The core of the information is the geolocation of every plot of land on which the goods were produced (Art. 9(1)(d)). For plots larger than four hectares, a polygon is required instead of a single point, except for cattle.

The regulation has been amended twice: by Regulation (EU) 2024/3234, which pushed the start date back by a year, and by Regulation (EU) 2025/2650, which postponed it again and introduced simplifications, among them fewer reporting obligations for downstream companies and traders.

Who it affects in South America

The legal obligation sits with the operator in the EU. In practice, every producer and exporter whose goods go there is affected, because without geolocation data and proof of legality the buyer cannot file a due diligence statement and cannot sell the goods.

COMMODITY	MAIN COUNTRIES OF ORIGIN IN THE REGION
Soy	Brazil , Argentina , Paraguay , Uruguay

COMMODITY	MAIN COUNTRIES OF ORIGIN IN THE REGION
Cattle and leather	Brazil, Argentina, Paraguay, Uruguay
Coffee	Brazil, Colombia , Peru , Ecuador
Cocoa	Ecuador, Peru, Brazil
Wood and pulp	Brazil, Chile , Uruguay
Rubber	Brazil
Palm oil	Colombia, Ecuador

The Commission classifies countries by risk (Art. 29, Implementing Regulation (EU) 2025/1093). Chile and Uruguay are rated low risk. Argentina, Bolivia, Brazil, Colombia, Ecuador, Paraguay and Peru are standard risk. No country in South America is rated high risk.

How much work you face depends heavily on your supply chain. A large farm in Mato Grosso that works its own land knows its polygons. A coffee exporter in Huila that buys from hundreds of smallholders through intermediaries first has to map every single plot. With cattle the chain is often long, because animals pass through several farms before slaughter. The regulation requires the geolocation of every establishment where the animals were kept.

Low risk does not mean there is nothing to do. Geolocation and the due diligence statement remain mandatory for wood from Chile or beef from Uruguay as well. Only the risk assessment and risk mitigation are dropped (Art. 13), as long as there is no sign of mixing with goods from other countries.

Deadlines

DATE	WHAT APPLIES
Dec 31, 2020	Cut-off date: land deforested after this date is excluded
Dec 30, 2026	Obligations for large and medium-sized operators and traders
Jun 30, 2027	Obligations for micro and small enterprises established as such by Dec 31, 2024 (Art. 38(3) as amended)

On May 4, 2026, the Commission presented its simplification report and did not propose any further postponement. Plan on December 30, 2026. A harvest of coffee from Huila or soy from Paraná that arrives in Hamburg or Rotterdam in the first half of 2027 needs the data today.

Member states enforce the rules. Article 25 provides, among other things, for fines with a maximum of at least 4% of the company's annual turnover in the EU, as well as confiscation of the goods and the revenue from them, and temporary exclusion from public contracts. Your buyer bears these risks, and it will pass them on to you in its contracts, for example through warranties and withdrawal rights.

What EU customers actually ask for

- Geographic coordinates of every production plot, as a polygon for plots larger than four hectares.
- Harvest period or production date, quantity and tariff code (HS code).
- Names and addresses of the suppliers in the chain back to the producer.
- Proof of legality: land titles, environmental permits, in Brazil for example registration in the CAR environmental registry, and evidence of compliance with labor and tax law.
- A check against the cut-off date, usually based on satellite imagery.
- Evidence that product flows are kept separate, so verified goods are not mixed with unverified ones.
- For resale, the reference number of a due diligence statement that has already been filed.

Certifications such as RTRS or ProTerra for soy, FSC or PEFC for wood, Rainforest Alliance for coffee and cocoa or RSPO for palm oil help with data collection. They do not replace the due diligence obligation, though, and the EU buyer will still ask for the geolocation data.

First steps

1. Use the customs tariff to check for each product whether it falls under Annex I.
2. Map the plots of every producer you buy from. With cooperatives that have many smallholders, this is the biggest effort, so start early.
3. Check the plots against the December 31, 2020 cut-off date. Public satellite data and specialized services can help.
4. Collect proof of legality for each producer and keep it up to date.
5. Set up your logistics so that verified goods stay separate.
6. Agree with your EU buyers on the format in which they need the data.

Decide who in the company is responsible for the data. Buyers ask at short notice, often for individual containers, and a supplier that can answer within hours stays the supplier of choice. Land titles,

permits and supplier declarations each have an expiry date. A GRC tool such as [Sightadel](#) can hold them as evidence per supplier, assign renewal tasks and keep the supplier assessment in one place. The geolocation and satellite checks themselves need a specialized service.

The free [EU Readiness Check](#) gives you an assessment of where you stand.

How it relates to certifications

The EUDR does not require a certificate. Environmental management under [ISO 14001](#) does show that you manage environmental risks systematically, and it makes the documentation easier. For food exporters, the [food safety](#) standards such as IFS, BRCGS or FSSC 22000 remain in place alongside it, because food retailers require them regardless of the EUDR. Many of your buyers' questions overlap with the due diligence obligations under the [CSDDD and CSRD](#) and, from December 14, 2027, with the [Forced Labour Regulation](#), which also requires traceability back to the producer. If you map your supply chain properly once, you can use the data for all three. That saves collecting the same data twice from the same producers.

The [EU-Mercosur Agreement](#) does not change anything about the EUDR. Tariff advantages only apply to goods that also meet the EU's product rules.

<https://www.mercoeu.com/en/eu-rules/eudr-deforestation>

PUT IT INTO PRACTICE WITH TOOLS MADE IN GERMANY



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

[See Sightadel →](#)

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

EU RULE · CLIMATE AND CUSTOMS

CBAM: the carbon price at the EU border

Since January 1, 2026, EU importers have had to pay for the emissions embedded in steel, aluminum, cement, fertilizers and hydrogen. How much depends on the data you supply as the manufacturer.

In brief

The Carbon Border Adjustment Mechanism (CBAM) is meant to stop production from moving to countries with weaker climate rules. Anyone importing certain carbon-intensive goods into the EU has to buy and surrender CBAM certificates for the emissions released in making them. The price is based on the EU Emissions Trading System. A carbon price actually paid in the country of origin is deducted (Art. 9).

Annex I covers these groups of goods:

- Iron and steel, including certain downstream products such as pipes, screws and structural parts.
- Aluminum and certain aluminum products.
- Cement.
- Fertilizers, such as ammonia and nitrates.
- Hydrogen.
- Electricity.

Embedded emissions are the greenhouse gases released in producing a good. Direct emissions come from your own installation, for example from the blast furnace or electrolysis. Indirect emissions come from the electricity the installation consumes. For complex goods, the emissions of the precursors also count. For a steel screw, this means the manufacturer needs data on the wire it buys, and the wire supplier needs data on its pig iron.

The regulation was simplified in October 2025 by Regulation (EU) 2025/2083. Since then, a volume threshold has replaced the earlier value limit, and many small importers are exempt altogether.

Who it affects in South America

The obligation to buy and surrender certificates falls on the importer in the EU. Only an authorized CBAM declarant may import the goods (Art. 5 and 17). It has to file a CBAM declaration every year (Art. 6) stating the embedded emissions of the goods it imported.

Only the manufacturer knows those emissions. If it does not supply actual values for each installation, the importer has to use the Commission's default values, and those include mark-ups. That makes the goods more expensive and the manufacturer less attractive than a competitor with good data. This is why CBAM is a data obligation for manufacturers in South America, even though the law does not name them directly.

Those most affected include:

- Steel and pig iron producers in [Brazil](#), a major supplier to the EU.
- Aluminum smelters in Brazil and [Argentina](#).
- Fertilizer producers and green hydrogen and ammonia projects in [Chile](#), [Uruguay](#) and Brazil.
- Manufacturers of steel components, screws or pipes that fall under the covered downstream products.

Copper is not covered. An exporter of copper cathodes from Antofagasta has nothing to do with CBAM, unless the Commission extends the scope.

Chile, Colombia and Argentina levy carbon taxes, and Brazil is building an emissions trading system. Whether such a price can be deducted depends on whether it was actually paid on the emissions of the goods in question and not refunded. This has to be checked and documented case by case.

Operators of installations outside the EU can register in the CBAM Registry for third-country operators and store their verified emissions data there. Their customers in the EU can then access it instead of asking for new spreadsheets every time.

Deadlines

PERIOD	WHAT APPLIES
Oct 1, 2023 to Dec 31, 2025	Transitional period: quarterly reports only, no payment
since Jan 1, 2026	Definitive period: imports only by authorized CBAM declarants
Feb 1, 2027	Sale of CBAM certificates begins
Sep 30, 2027	First annual declaration and surrender of certificates for 2026

The threshold is 50 tonnes per importer per year, counted across all CBAM goods except hydrogen and electricity. Importers below it have no obligations. Once it is exceeded, the obligation applies to the entire annual volume. A trader that occasionally imports a few tonnes of screws is therefore exempt. A steel trader with regular shipments from Brazil is not, and it will ask you for data.

Emissions for 2026 are not settled until 2027, but they are being generated now. If you do not give your customer verified data for 2026, its bill in September 2027 will be calculated with default values.

What EU customers actually ask for

- Emissions data per installation and per product, direct and, where required, indirect, calculated using the methods in Annex IV and the implementing acts.
- The Commission's template for passing data from operator to importer.
- For actual values, a verification report from an accredited verifier.
- Information on precursors, such as the pig iron or primary aluminum you buy in.
- Proof of any carbon price paid in the country of origin, if it is to be deducted.
- Production route, installation name and location, so the data can be assigned without ambiguity.

Many buyers now write into their contracts the date by which verified data must be available and who bears the extra cost if default values have to be used.

If you supply several EU customers, collect and verify the data properly once and give every customer the same values. Inconsistent figures for the same installation will come to light at the latest when the authorities check. An aluminum smelter in Puerto Madryn with customers in Germany, Italy and Spain saves itself three times the work this way.

Keeping track of which customer has asked for what, and by when, is a task of its own. A general GRC platform such as [Sightadel](#) can hold the customer requests, deadlines and the documents prepared for the verifier in one place. The emissions calculation itself follows the Commission's method and is done outside it.

First steps

1. Use the tariff codes to check which of your products fall under Annex I.
2. Ask your EU customers whether they are above the 50-tonne threshold and which data they need in which format.
3. Set up an emissions calculation for each installation using the Commission's method. Metered data on energy and raw material consumption is the basis.
4. Hire an accredited verifier in good time, so the 2026 data is verified before the first surrender.
5. Register your installations in the CBAM Registry for third-country operators.

6. Find out whether a carbon price is paid in your country that can be deducted, and how you will document it.

The free [EU Readiness Check](#) gives you an initial overview of all EU requirements.

How it relates to certifications

CBAM requires verification of emissions data, not a management system. Environmental management under [ISO 14001](#), often supplemented by ISO 50001 for energy and a greenhouse gas inventory under ISO 14064, does create the data and processes a verifier can build on. Quality management under [ISO 9001](#) helps keep the documentation clean. Customers ask for the same data for their sustainability reports under the [CSRD](#).

The [EU-Mercosur Agreement](#) lowers tariffs but does not exempt anyone from CBAM. The border adjustment applies to goods from all third countries, regardless of trade agreements and preferential tariffs.

<https://www.mercoeu.com/en/eu-rules/cbam>

EU RULE · SUSTAINABILITY

CSDDD and CSRD: your customers' due diligence and reporting duties

Large EU companies have to report on sustainability and examine human rights and environmental risks in their supply chain. Since Omnibus I in February 2026, far fewer companies are covered, and smaller suppliers are better protected.

In brief

Two EU directives determine what large customers in Europe want to know about sustainability. The Corporate Sustainability Reporting Directive (CSRD, Directive (EU) 2022/2464) requires sustainability reports under the European Sustainability Reporting Standards (ESRS), including information on the value chain. The Corporate Sustainability Due Diligence Directive (CSDDD, Directive (EU) 2024/1760) requires very large companies to identify, prevent and bring to an end adverse impacts on human rights and the environment in their chain of activities.

Both directives were cut back sharply in 2025 and 2026. First, the “stop-the-clock” Directive (EU) 2025/794 postponed the deadlines. Then the Omnibus I package, Directive (EU) 2026/470, changed their scope and content. It was published in the Official Journal on February 26, 2026 and entered into force 20 days later.

Neither directive applies directly to suppliers in South America unless they are very large themselves and generate a lot of revenue in the EU. The requirements reach them through customers' questionnaires, codes of conduct and contract clauses.

Who it affects in South America

	CSRD (REPORTING)	CSDDD (DUE DILIGENCE)
EU companies	more than 1,000 employees and more than €450 million net turnover	more than 5,000 employees and more than €1.5 billion worldwide net turnover
Companies outside the EU	more than €450 million turnover in the EU in two consecutive years, plus an EU subsidiary or branch with more than €200 million turnover	more than €1.5 billion net turnover in the EU

Only large groups from the region with substantial EU business are directly affected, for example in agricultural trading, mining or the food industry. For them, the CSDDD applies from 2029; the CSRD applies as soon as the EU turnover thresholds are reached.

The usual case is indirect. An auto parts maker in Córdoba, a winery in Mendoza or a coffee exporter in Huila gets requests from customers that have to report or meet due diligence obligations themselves. They ask about working conditions, wages, occupational safety, environmental impact and the emissions data the customer needs for its own greenhouse gas inventory.

National laws continue to apply alongside the EU directives, such as the German Supply Chain Due Diligence Act (Lieferkettensorgfaltspflichtengesetz) and the French duty of vigilance law (“Loi de vigilance”). Customers from these countries therefore often ask detailed questions already today.

In practice, the requests land with sales, not with management. Decide who answers them and who signs off on the answers. Contradictory information given to different customers does more harm than an open gap that you name, together with a plan and a date.

Deadlines

DATE	WHAT APPLIES
Feb 26, 2026	Omnibus I, Directive (EU) 2026/470, published in the Official Journal
Mar 19, 2027	Transposition of the CSRD amendments into national law
Jul 26, 2028	Transposition of the CSDDD into national law
Jul 26, 2029	CSDDD applies to all companies in scope

The largest listed companies in the EU have been reporting under the CSRD since financial year 2024. Many of your customers have therefore already published a report and know what data they need. The financial year from which a particular company reports under the new CSRD depends on its size and on the national implementing law. Ask your customer directly when it will need your data.

Omnibus I removed the obligation to adopt a climate transition plan from the CSDDD and set a uniform cap on fines of 3% of worldwide net turnover.

What EU customers actually ask for

One change matters especially to suppliers: the value chain cap on information requests. Companies with an average of no more than 1,000 employees are protected. A customer that has to report may not ask them, for its CSRD report, for more information than the voluntary standard for such

companies provides. If it asks for more, it must point out that you are not required to supply the additional information.

The cap only applies to reporting. Requirements arising from quality agreements, food law, the [EUDR](#) or the [Forced Labour Regulation](#) are not affected.

For due diligence under the CSDDD, the cap does not apply in the same form. A large customer has to identify risks in its chain of activities and can require contractual assurances from direct business partners for this purpose, such as compliance with its code of conduct. The directive provides that it should support small and medium-sized business partners and not impose disproportionate costs on them. If there is a specific suspicion, for example reports of child labor at supplier farms, it will ask more detailed questions and demand remediation. Under the directive, ending the business relationship is a last resort.

Typical requests:

- A signed supplier code of conduct.
- A questionnaire or a rating through platforms such as EcoVadis, Sedex or IntegrityNext.
- A sustainability report under the voluntary standard for SMEs (VSME).
- A greenhouse gas inventory for Scope 1 and 2 under the GHG Protocol or ISO 14064.
- Social audits, such as SMETA, amfori BSCI or SA8000.
- A grievance mechanism through which employees and local residents can report abuses.
- ISO 14001 and ISO 45001 certificates.

First steps

1. Count your employees. Below 1,000, you are protected against CSRD requests and can politely limit excessive questionnaires.
2. Gather your EU customers' requests and look for the overlaps. The same metrics usually come up again and again.
3. Prepare a greenhouse gas inventory once and update it every year.
4. Write a short report under the VSME standard. It answers many questions in one go.
5. Set up a simple grievance channel and document how you handle reports.
6. Check your own upstream suppliers for labor and environmental risks, especially where seasonal work, subcontractors or raw materials from high-risk areas play a role.

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

How it relates to certifications

Neither directive requires a certificate. [ISO 14001](#) demonstrates orderly environmental management and supplies data for your customers' reports. [ISO 9001](#) shows documented processes, which auditors like to see. For food exporters, the [food safety](#) standards come on top. If you supply carbon-intensive industries, you will also need the emissions data for [CBAM](#).

The due diligence obligations of the CSDDD overlap with the [EUDR](#) and the [Forced Labour Regulation](#). Once you know your supply chain, you can serve all three. A tool such as [Sightadel](#) helps you keep evidence and answers for many customers in one place.

<https://www.mercoeu.com/en/eu-rules/csddd-csrd>

EU RULE · HUMAN RIGHTS

Forced Labour Regulation: no market access for products made with forced labor

From December 14, 2027, products made wholly or partly with forced labor may neither be sold in the EU nor exported from it. This applies to every product, every company size and every country of origin.

In brief

Regulation (EU) 2024/3015 prohibits placing products made with forced labor on the EU market, making them available there or exporting them from the EU (Art. 3). Unlike many other EU rules, it has no thresholds. It applies to raw materials, intermediate goods and finished products, to large groups and small businesses alike, and to goods from every country, including the EU itself. Online sales are included.

Under the definition of the International Labour Organization (ILO), forced labor means any work that is exacted under the menace of a penalty and for which the person has not offered themselves voluntarily. Typical indicators are withheld identity documents, debt bondage, withheld wages, restrictions on freedom of movement and threats.

The regulation does not create a due diligence obligation for every company. It relies on investigations by the authorities. These follow a risk-based approach and draw on tip-offs, publicly available information and a Commission database of risk areas and risk products (Art. 8). If they find forced labor, they order the products to be withdrawn from the market and donated, recycled or destroyed. The companies concerned bear the costs.

The procedure has two stages. First, the authority carries out a preliminary review and can request information from the company, for example on upstream suppliers and on the measures taken against forced labor. Only if a substantiated concern remains after that does it open a formal investigation. If the risk lies outside the EU, for example on a farm in South America, the Commission leads the investigation. The company can comment and submit evidence at every stage. Good documentation can end a case at the first stage, before a formal investigation begins.

Who it affects in South America

The obligation falls on the economic operator that places the product on the market in the EU. But because the goods themselves are banned, every exporter is indirectly affected. The EU buyer carries the risk of an entire shipment being recalled or stopped at the border, and it wants to rule that out in advance.

Buyers will look especially closely at sectors where cases have been documented, past or present:

- Cattle ranching and charcoal, for example in remote regions of Brazil.
- Harvest work in coffee, sugarcane, fruit and other crops that rely on many seasonal workers.
- Mining, including small-scale and informal mines.
- Textiles and apparel involving home-based work and subcontractors.
- Fishing and fish processing.

That does not mean every business in these sectors is under suspicion. It means buyers will ask for more evidence the longer and less transparent the chain is. A coffee exporter from Minas Gerais that buys from many small farms has to be able to explain how it checks working conditions at those farms.

The region has its own instruments that buyers know about. In [Brazil](#), the Ministry of Labor publishes a list of employers found to have used labor analogous to slavery, known as the “Lista Suja”. EU buyers are increasingly checking whether suppliers or their upstream suppliers appear on it.

Deadlines

DATE	WHAT APPLIES
Dec 13, 2024	Regulation enters into force
Jun 30, 2026	Commission launches the Single Portal with guidelines and information to help companies prepare (legal deadline for the guidelines under Art. 11: Jun 14, 2026)
Dec 14, 2027	The ban applies; authorities can investigate and take decisions

There is a little over a year left until December 2027. That sounds like a long time, but it is tight for building traceability back to the raw material. Many buyers will adjust their supply contracts during 2027 so that goods they sell after the deadline are already documented. Goods produced and put into storage today may still be on the market after December 14, 2027, and will then fall under the

ban.

What EU customers actually ask for

- Transparency about the supply chain back to the raw material: names, locations and roles of upstream suppliers.
- Social audits under recognized standards such as SMETA, amfori BSCI or SA8000.
- Employment contracts, payroll records and working time records, including for seasonal workers and subcontractors' employees.
- Proof that neither you nor your upstream suppliers appear on national blacklists.
- A policy against forced labor, signed and communicated throughout the company.
- A grievance channel that workers can use without fear.
- Rules for labor recruiters, in particular a ban on recruitment fees paid by the workers themselves.

Also expect new contract clauses: a warranty that there is no forced labor in the supply chain, audit rights for the buyer that extend to your upstream suppliers, liability for recall costs and the right to reject shipments. Before you sign, check whether you can actually give these assurances for your own chain.

Much of this evidence matches what buyers ask for under the [CSDDD](#) or national supply chain laws. Agricultural exporters already know traceability down to the plot from the [EUDR](#).

First steps

1. Map your supply chain, at least to the first processing stage, and for agricultural and mining products back to the producer.
2. Mark the points with higher risk: seasonal work, subcontractors, labor recruiters, remote sites.
3. Check your upstream suppliers against national lists such as the Lista Suja.
4. Carry out a social audit or have one carried out, starting with the high-risk points.
5. Set up a confidential grievance channel that your subcontractors' workers can also use.
6. Read the Commission's guidelines on the Single Portal and compare your practices with them.

Document every step with a date. If an authority asks questions, the only thing that counts is what you can back up with records. Keep audit reports, corrective action plans and evidence of their implementation for at least as long as your goods are sold in the EU. A GRC tool such as [Sightadel](#) can hold this evidence per supplier, track corrective actions as tasks and keep the supplier assessment current.

The free [EU Readiness Check](#) gives you an overview of all EU requirements.

How it relates to certifications

The regulation does not accept any certificate as a free pass. Social audits and sustainability certifications are still strong evidence for your buyers. In agriculture, Rainforest Alliance, Fairtrade or Bonsucro also cover working conditions. A management system under [ISO 9001](#) takes care of documentation, and ISO 45001 of occupational health and safety. Food exporters can often combine [food safety](#) audits with social audits to save on audit days. Environmental management under [ISO 14001](#) is often audited in the same package.

The [EU-Mercosur Agreement](#) commits the parties to the ILO core labor standards, which include the prohibition of forced labor. The Forced Labour Regulation applies independently of that, to every single product.

<https://www.mercoeu.com/en/eu-rules/forced-labour>

CERTIFICATIONS · OVERVIEW

Certifications EU customers ask for

Hardly any certification is required by law in the EU. Even so, it often decides whether you make it onto the supplier list.

Why EU customers ask for certifications

Many EU rules oblige your customer to check its supply chain: [NIS2](#) for cybersecurity, [DORA](#) for IT providers to banks, the [GDPR](#) for personal data, [CSRD](#) and [CSDDD](#) for the environment and human rights. For a purchasing department, a certificate from an independent body is the easiest evidence there is. It will not replace every questionnaire, but it shortens it considerably and often saves you a separate supplier audit.

Which certification for which industry

INDUSTRY	TYPICAL PROOF
Software, IT services, BPO, data centers	ISO/IEC 27001 , plus SOC 2 for US customers
Manufacturing, components, packaging	ISO 9001
Mining, chemicals, agro-processing, logistics	ISO 14001
Food and beverages	HACCP, plus IFS Food , BRCGS or FSSC 22000
Automotive suppliers	TISAX
Providers of AI systems	ISO/IEC 42001

A software company in Montevideo working for an insurer in Madrid will usually get further with ISO/IEC 27001 than with any other proof. A meat exporter from Paysandú, on the other hand, needs HACCP and, as a rule, one of the GFSI-recognized food safety standards.

Accreditation: the only thing that makes the paper count

EU buyers recognize a certificate when the certification body is accredited by an accreditation body that has signed the international recognition arrangement. Until the end of 2025 that was the IAF MLA. Since January 1, 2026, the Global Accreditation Cooperation Incorporated (Global ACI) has carried on the IAF and ILAC arrangements, and existing accreditations remain recognized. All nine

countries on MercoEU have an accreditation body listed there as a signatory: Cgcre at INMETRO in [Brazil](#), OAA in [Argentina](#), INN in [Chile](#), ONAC in [Colombia](#), INACAL in [Peru](#), SAE in [Ecuador](#), OUA in [Uruguay](#), ONA in [Paraguay](#) and DTA-IBMETRO in [Bolivia](#). Whether a body is recognized for the specific standard is stated in the scope of its accreditation.

Where to start

Start by asking your most important EU customers which proof they expect. If the contract does not say, the [EU Readiness Check](#) can help: it shows, by industry and country, which certifications will do the most for you.

Once the decision is made, preparation is mostly organized work: policies, risks, tasks and evidence for each requirement. For ISO/IEC 27001, ISO 9001, ISO/IEC 42001, SOC 2 or HACCP, a GRC platform such as [Sightadel](#) sets up the requirements of the standard and shows what is still open. The certificate itself is issued by an accredited certification body after the audit.

<https://www.mercoeu.com/en/certifications>

PUT IT INTO PRACTICE WITH TOOLS MADE IN GERMANY



Sightadel

Sightadel walks your team through your EU requirements: 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 →](#)

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

COUNTRIES · OVERVIEW

Your country next to EU law

For each of the nine countries, we show where local law stands, how it differs from the GDPR and NIS2, and which agreement with the EU applies.

The nine countries at a glance

COUNTRY	DATA PROTECTION LAW	CYBERSECURITY LAW	EU ADEQUACY	TRADE AGREEMENT WITH THE EU
Argentina	Ley 25.326 (2000), reform in Congress	none	yes (2003)	EU-Mercosur, provisional since May 1, 2026
Brazil	LGPD, Lei 13.709/2018	none, bill PL 4.752/2025	yes (since Jan 2026)	EU-Mercosur, provisional since May 1, 2026
Paraguay	Ley 7593/2025, fully applicable from late Nov 2027	none	no	EU-Mercosur, provisional since May 1, 2026
Uruguay	Ley 18.331 (2008), Ley 19.670	Ley 20.212 Art. 78 ff., Decreto 66/025	yes (2012)	EU-Mercosur, provisional since May 1, 2026
Bolivia	none	none	no	none; tariff preferences under GSP+
Chile	Ley 21.719, in force from Dec 1, 2026 (postponement requested)	Ley 21.663 (2024)	no	Interim Trade Agreement since Feb 1, 2025
Colombia	Ley 1581 de 2012	none, Decreto 338/2022	no	Trade Agreement since 2013
Peru	Ley 29733, DS 016-2024-JUS	framework under DU 007-2020 and DS 126-2025-PCM	no	Trade Agreement since 2013

COUNTRY	DATA PROTECTION LAW	CYBERSECURITY LAW	EU ADEQUACY	TRADE AGREEMENT WITH THE EU
Ecuador	LOPDP (2021)	Ley Orgánica para el Fortalecimiento de la Ciberseguridad (2026)	no	Trade Agreement since 2017

What adequacy changes for you

For Argentina, Uruguay and, since January 2026, Brazil, the EU has found that data protection is equivalent. Your EU customers can transfer data there without signing standard contractual clauses. For the other six countries, they need those clauses plus a transfer impact assessment. You need a data processing agreement under the [GDPR](#) in all nine countries.

Cybersecurity: few laws, many contracts

Chile comes closest to [NIS2](#), with an early warning due after just three hours. Uruguay requires critical sectors to report within 24 hours. Ecuador has had its own law since May 2026, and Peru regulates reporting for digital services by decree. In the remaining countries, the main rules come from banking supervisors.

For suppliers, local law is only part of the picture anyway. EU customers pass their obligations under NIS2, [DORA](#) and the [Cyber Resilience Act](#) down to you by contract, whatever country you are based in. A GRC platform such as [Sightadel](#) lets you keep the policies and evidence for these clauses in one place and reuse them for each customer.

Agreements and the supply chain

The [EU-Mercosur agreement](#) has applied provisionally with Argentina, Brazil, Paraguay and Uruguay since May 1, 2026. Bolivia is a Mercosur member but not a party. Chile, Colombia, Peru and Ecuador have their own agreements. None of them exempts you from the [EUDR](#) or [CBAM](#).

The free [EU readiness check](#) shows where your company stands.

<https://www.mercoeu.com/en/countries>