

COUNTRY · MERCOSUR ASSOCIATE

Ecuador: What EU customers expect

Ecuador has had a data protection law modeled on European rules since 2021, and since May 2026 a law to strengthen cybersecurity. A trade agreement has linked the country with the EU since 2017.

DATA PROTECTION	EU ADEQUACY	AGREEMENT WITH THE EU	CYBERSECURITY
LOPDP (2021)	no	Trade Agreement, since Jan 1, 2017	Ley Orgánica para el Fortalecimiento de la Ciberseguridad (2026)

Overview: trade with the EU

Ecuador mainly ships food to Europe: bananas from El Oro and Los Ríos, shrimp from the Gulf of Guayaquil, canned tuna from Manta, cocoa and cut flowers from the highlands. The Commission publishes figures only for the Andean countries as a group. In 2025, 48.7% of that trade was agricultural products, 27.1% mineral products and 13.5% fisheries, an area where Ecuador is particularly strong.

Cocoa and palm oil exporters are covered by the [EUDR](#). Fishing and food companies also need EU approval for food of animal origin and reliable food safety certificates.

Data protection: LOPDP compared with the GDPR

The Ley Orgánica de Protección de Datos Personales (LOPDP) was published in the Registro Oficial in May 2021. After a two-year transition period, the sanctions have also applied since May 2023. The implementing regulation is Decreto Ejecutivo 904 of 2023. The regulator is the Superintendencia de Protección de Datos Personales (SPDP).

The LOPDP closely follows the [GDPR](#): legal bases, data subject rights, data protection officers, impact assessments, obligations for processors and rules for international transfers. If you know the GDPR, you will find your way around quickly.

The deadline for reporting data breaches is different: Art. 43 LOPDP requires notification to the SPDP no later than five days after the breach. Processors must inform the controller within two days. Reports are filed through an electronic system run by the SPDP.

Ecuador does not have an EU adequacy decision. Your EU customers need standard contractual clauses and a transfer impact assessment for transfers.

Cybersecurity compared with NIS2

Since May 22, 2026, the Ley Orgánica para el Fortalecimiento de la Ciberseguridad has been in force, published in the Registro Oficial. Its stated aim is to protect critical infrastructure and keep essential services running. It creates a Sistema Nacional de Ciberseguridad and amends seven existing laws, including the LOPDP and the telecommunications law. Its main focus is on public bodies and operators of critical infrastructure.

The approach is similar to [NIS2](#), which targets essential and important entities in 18 sectors. Whether your company is covered, which risk management obligations apply and how quickly incidents must be reported are things you should check against the text of the law in the Registro Oficial and the implementing rules. A company that already works to [ISO 27001](#) will cover most of the requirements.

For suppliers to European customers, the contractual requirements apply regardless: NIS2 supply chain clauses, [DORA](#) for financial customers, and the [Cyber Resilience Act](#) for connected products.

Reporting deadlines compared

TRIGGER	ECUADOR	EU
Data breach to the authority	no later than 5 days after the breach, to the SPDP (Art. 43 LOPDP)	72 hours (Art. 33 GDPR)
Processor to controller	2 days	without undue delay (Art. 33(2) GDPR)
Significant cyber incident	law in force since May 22, 2026; check deadline and reporting body in the text in the Registro Oficial	24 h early warning, 72 h notification, final report after one month (Art. 23 NIS2)

If you process data for an EU customer, the deadline in your contract applies, usually 24 to 48 hours. The two days the LOPDP gives processors are usually not enough for that.

Authorities, CSIRT, accreditation body

AREA	BODY
Data protection	SPDP, Superintendencia de Protección de Datos Personales

AREA	BODY
CSIRT	EcuCERT at ARCOTEL
Financial sector	Superintendencia de Bancos
Accreditation	SAE, Servicio de Acreditación Ecuatoriano

For certificates, where the certification body is located matters less than who accredited it. Before you sign the contract, ask whether the accreditation by SAE or a foreign body falls under the international recognition arrangement of the Global ACI (since January 1, 2026 the successor to IAF and ILAC; existing accreditations remain recognized). If it does, EU customers will usually accept the certificate. Some large groups still insist on a specific certifier. Settle that before you spend money on an audit.

Which body receives reports under the new cybersecurity law is best checked directly in the text of the law or with your sector regulator.

What EU customers typically require

A shrimp farmer from El Oro supplying a wholesaler in Spain needs EU market approval for the facility, traceability back to the pond and usually a certificate under [IFS](#), [BRCGS](#) or [FSSC 22000](#). Banana and flower exporters are asked about GLOBALG.A.P. For the EUDR, cocoa exporters must supply geolocation data for the plots and proof of deforestation-free production after December 31, 2020. Ecuador is classified as a standard-risk country.

IT service providers receive standard contractual clauses, security questionnaires and the question about [ISO 27001](#). If you are setting up a management system under ISO 27001, you can manage policies, risks and evidence in a GRC platform such as [Sightadel](#).

In the contract, these points usually sit in annexes: standard contractual clauses, a data processing agreement, technical and organizational measures, reporting deadlines and audit rights. For the transfer impact assessment, your EU customer will ask about storage locations, access and encryption. The LOPDP gives you a good basis here, because it adopts many of the GDPR's terms and obligations.

A sensible starting point for Ecuadorian companies:

1. Check whether you fall under the 2026 cybersecurity law.
2. Compare your documentation under the LOPDP with GDPR requirements. The gaps are usually small.
3. Set your internal incident reporting deadline well below the LOPDP's five days.

4. For cocoa and palm oil, collect the geolocation data for all plots, including those of your suppliers.
5. Keep approvals, traceability records and food safety certificates for shrimp, tuna and bananas up to date.

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

Agreement with the EU

Ecuador is associated with Mercosur but is not part of the EU-Mercosur agreement. It acceded to the EU's Trade Agreement with Colombia and Peru, which has applied to Ecuador since January 1, 2017. To claim the tariff preference, you need proof of origin. The agreement contains a chapter on trade and sustainable development that refers to the ILO core labor standards and international environmental agreements.

In practice, this means you should look up the tariff rate and the rule of origin for each product in the European Commission's Access2Markets portal, searchable by HS code. Many agricultural and industrial products have been duty-free for years, while some goods are subject to quotas or transition rules. For processed goods, the rule of origin decides whether enough value was added in the country. Your importer in the EU can help you issue the proof of origin correctly. Keep the supporting documents for several years, because customs can check after the fact.

The EUDR, CBAM and GDPR apply to Ecuadorian goods and services regardless of the agreement.

FAQ

How quickly must a data breach be reported in Ecuador?

No later than five days after the breach, to the SPDP (Art. 43 LOPDP). Processors inform the controller within two days.

Does Ecuador have a cybersecurity law?

Yes. The Ley Orgánica para el Fortalecimiento de la Ciberseguridad has been in force since May 22, 2026. It aims to protect critical infrastructure and essential services.

Do EU customers need standard contractual clauses for Ecuador?

Yes. Ecuador does not have an EU adequacy decision.

Does the EU-Mercosur agreement apply to Ecuador?

No. Since 2017, Ecuador has been a party to the trade agreement with Colombia and Peru.

Which tool helps with security questionnaires from EU customers?

Policies, risks and evidence for ISO 27001 or NIS2 can be managed in [Sightadel](#), which is developed and hosted in Germany. For questions about your internet-facing systems, [veyrisk](#) checks them from the outside and documents the findings for ISO 27001 and NIS2.

Sources · Last updated: October 11, 2026

Registro Oficial del Ecuador: <https://www.registroficial.gob.ec/>

Asamblea Nacional: Ley Orgánica para el Fortalecimiento de la Ciberseguridad:
<https://www.asambleanacional.gob.ec/es/node/115246>

EcuCERT: <https://www.ecucert.gob.ec/>

European Commission, DG Trade: Andean Community: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/andean-community_en

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

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

PUT IT INTO PRACTICE WITH TOOLS MADE IN GERMANY



Sightadel

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

[See Sightadel →](#)



veyrisk

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

[See veyrisk →](#)



valar

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

[See Valar →](#)

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

Which of these apply to your company?

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

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