

COUNTRY · MERCOSUR

Uruguay: What EU customers expect

Uruguay has the most developed data protection law in Mercosur and has held an EU adequacy decision since 2012. Critical sectors must report cyber incidents within 24 hours.

DATA PROTECTION	EU ADEQUACY	AGREEMENT WITH THE EU	CYBERSECURITY
Ley 18.331 (2008), Ley 19.670	yes, since 2012	EU-Mercosur, provisional since May 1, 2026	Ley 20.212 Art. 78 et seq., Decreto 66/025

Overview: trade with the EU

According to the European Commission, more than half of EU imports from Uruguay in 2025 were pulp and paper (52 %). Animal products followed (21 %), mainly beef, then vegetable products (11 %). Pulp mills on the Río Uruguay and meat plants in the interior are therefore directly affected by the [EUDR](#), which covers wood and cattle.

At the same time, Montevideo is one of the most important software hubs in Latin America. Many companies there develop for clients in Spain, Germany or Scandinavia and process personal data from the EU along the way.

Data protection: Ley 18.331 compared with the GDPR

Ley 18.331 on the protection of personal data dates from 2008, and its implementing regulation is Decreto 414/009. With Ley 19.670 of 2018 and Decreto 64/020, Uruguay brought its law closer to the [GDPR](#): the law also applies to controllers abroad if they process data of people in Uruguay, there is a duty to report data breaches, and certain organizations must appoint a data protection officer. The supervisory authority is the URCDP (Unidad Reguladora y de Control de Datos Personales) within AGESIC.

The EU recognized Uruguay as adequate in 2012 with Implementing Decision 2012/484/EU and confirmed this in the Commission's report of January 15, 2024. Uruguay has also ratified the Council of Europe's Convention 108+. Your EU customers can therefore transfer data to Uruguay without standard contractual clauses.

For processors, adequacy does little to reduce the paperwork: the contract under Art. 28 GDPR, the list of subprocessors and evidence of technical and organizational measures are still

required.

Cybersecurity compared with NIS2

Uruguay is one of the few countries in the region with statutory cyber obligations outside the financial sector. Under Art. 78 and the following articles of Ley 20.212 (Rendición de Cuentas 2022), public bodies and private operators in critical sectors must report security incidents within 24 hours. Decreto 66/025 sets out how this works: reporting to CERTuy, appointing security officers, retaining logs and applying the Marco de Ciberseguridad, a national framework with controls similar to ISO 27001.

Compared with [NIS2](#), fewer organizations are covered. In the EU, NIS2 also applies to medium-sized companies in 18 sectors, including food production and digital services. In Uruguay, the duty applies to critical sectors. At 24 hours, though, the first notice is just as fast as the NIS2 early warning.

Suppliers to European customers also face contractual requirements: NIS2 supply chain clauses, [DORA](#) for financial clients and the [Cyber Resilience Act](#) for products with digital elements.

Reporting deadlines compared

EVENT	URUGUAY	EU
Data breach, notice to the authority	72 hours from awareness, to the URCDP (Decreto 64/020, Art. 4)	72 hours (Art. 33 GDPR)
First measures after a data breach	start within 24 hours (Decreto 64/020, Art. 3)	no separate deadline
Cyber incident, critical sectors	24 hours, to CERTuy (Ley 20.212, Decreto 66/025)	24 h early warning, 72 h notification, final report after one month (Art. 23 NIS2)

The data breach deadlines are the same in Uruguay and the EU. A process that covers both is therefore easy to set up.

Authorities, CSIRT, accreditation body

AREA	BODY
Data protection	URCDP within AGESIC
Cybersecurity, CSIRT	AGESIC with CERTuy

AREA	BODY
Financial sector	BCU, Banco Central del Uruguay
Accreditation	OUA, Organismo Uruguayo de Acreditación

With certificates, what matters is less where the certification body is located than who accredited it. Before you hire one, ask whether its accreditation by OUA or by a foreign body is covered by the international recognition arrangement of the Global ACI (since January 1, 2026 the successor to IAF and ILAC; existing accreditations remain recognized). If so, EU customers will generally accept the certificate. Some large groups still require a specific certifier. Clarify that before you spend money on an audit.

What EU customers typically ask for

A software company in Montevideo developing for a bank in Madrid will receive a security questionnaire, a contract under Art. 28 GDPR and DORA clauses on audit rights and exit plans. An [ISO 27001](#) certificate is often expected. If you already work under the Marco de Ciberseguridad, you have implemented a good share of the controls. In [Sightadel](#) you can build on them for ISO 27001, with templates, tasks and evidence for each requirement.

Many EU customers also check the externally visible attack surface of their service providers. With [veyrisk](#) you see the same findings yourself and can fix them before the customer asks.

Pulp and timber exporters need geolocation data for their plantations and proof of deforestation-free origin for the EUDR. Meat exporters need the same information for their pastures, plus food safety certificates for [IFS](#), [BRCGS](#) or [FSSC 22000](#).

In the contract, these requirements usually appear as annexes: a data processing agreement, technical and organizational measures, reporting deadlines, audit rights and a list of subprocessors. Thanks to adequacy, standard contractual clauses are not needed. If you use service providers in countries without adequacy yourself, such as a support team in Asia, your EU customer will want to know how that transfer is safeguarded.

A sensible starting point for companies in Uruguay:

1. Check whether you belong to a critical sector under Ley 20.212. If so, the 24-hour reporting duty to CERTuy already applies to you.
2. Compare your documentation under Ley 18.331 and Ley 19.670 with the GDPR requirements. The gaps are usually small.
3. Build one reporting process for the URCDP, CERTuy and your EU customers.

4. Check how far your controls under the Marco de Ciberseguridad already cover the requirements of ISO 27001.
5. For timber, pulp and meat exports, collect the geolocation data for the EUDR.

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

Agreement with the EU

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

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

EU law applies in full despite the agreement, and that includes the EUDR, CBAM and the GDPR.

FAQ

Do EU customers need standard contractual clauses for Uruguay?

No. Uruguay has had an adequacy decision since 2012 (2012/484/EU), confirmed in 2024.

How quickly must a data breach be reported in Uruguay?

Within 72 hours of becoming aware of it, to the URCDP (Decreto 64/020). That matches the GDPR deadline.

Who has to report cyber incidents in Uruguay?

Public bodies and private operators in critical sectors, within 24 hours, to CERTuy (Ley 20.212, Decreto 66/025).

Does the Marco de Ciberseguridad help with ISO 27001?

Yes, the controls overlap heavily. It does not replace a certificate, though. More on the [ISO 27001](#) page.

Which tool helps a software company in Uruguay with ISO 27001 and DORA requests?

Sightadel supports ISO 27001, DORA and the GDPR as frameworks and reuses work from one for the next. It is developed and hosted in Germany. **veyrisk** shows which of your systems are reachable from the internet, with a report you can share with the customer.

Sources · Last updated: October 11, 2026

Ley 18.331, IMPO: <https://www.impo.com.uy/bases/leyes/18331-2008>

Decreto 64/020, IMPO: <https://www.impo.com.uy/bases/decretos/64-2020>

Ley 20.212, Art. 78, IMPO: <https://www.impo.com.uy/bases/leyes/20212-2023/78>

Decreto 66/025, IMPO: <https://www.impo.com.uy/bases/decretos/66-2025>

URCDP: <https://www.gub.uy/unidad-reguladora-control-datos-personales/>

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

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

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

PUT IT INTO PRACTICE WITH TOOLS MADE IN GERMANY



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

[See Sightadel →](#)



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

[See veyrisk →](#)



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

[See Valar →](#)

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

Which of these apply to your company?

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

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