

PAÍS · MERCOSUL

Paraguai: o que os clientes da UE esperam

Desde novembro de 2025, o Paraguai tem uma lei geral de proteção de dados, que passa a ser plenamente aplicável no fim de novembro de 2027, após um período de transição. Uma lei de cibersegurança ainda não existe.

PROTEÇÃO DE DADOS	ADEQUAÇÃO DA UE	ACORDO COM A UE	CIBERSEGURANÇA
Ley 7593/2025, plena a partir do fim de 11/2027	não	UE-Mercosul, provisório desde 01/05/2026	sem lei, estratégia 2025 a 2028

Visão geral: comércio com a UE

As importações da UE vindas do Paraguai são quase só produtos agrícolas: segundo a Comissão Europeia, 82 % em 2025. Soja do leste do país e carne bovina do Chaco são os exemplos mais conhecidos. Ambas se enquadram no [EUDR](#), e é por aí que começam as perguntas dos compradores europeus.

Para o Paraguai, o acordo UE-Mercosul é o maior passo de política comercial em anos. Assunção foi o local da assinatura, em 17/01/2026.

Proteção de dados: a Ley 7593/2025 comparada ao RGPD

Até 2025, o Paraguai não tinha uma lei geral de proteção de dados; havia regras sobretudo para dados de crédito (Ley 6534/2020). A Ley Nº 7593/2025 de Protección de Datos Personales foi promulgada em 27/11/2025. Ela prevê um período de transição de 24 meses e, com isso, passa a ser plenamente aplicável no fim de novembro de 2027. O regulamento ainda não foi editado.

A lei adota muitas das ideias centrais do [RGPD \(Regulamento Geral sobre a Proteção de Dados\)](#): bases legais, direitos dos titulares, obrigações para controladores e operadores, regras para transferências ao exterior. A supervisão ficará com uma Agencia Nacional de Protección de Datos Personales, vinculada ao Ministério de Tecnologias da Informação e Comunicação (MITIC), com autonomia funcional. As multas vão de 20 a 10.000 diárias de salário mínimo.

O Paraguai não tem decisão de adequação da UE. Seus clientes na UE precisam, para cada transferência de dados pessoais ao Paraguai, de cláusulas contratuais padrão (Decisão de Execução (UE) 2021/914) e de uma avaliação de impacto da transferência. Isso vale também para casos simples, por exemplo quando sua equipe comercial em Assunção consulta dados de clientes no CRM de um distribuidor alemão.

Você não precisa esperar até 2027. Quem cria agora um registro das operações de tratamento, controla os acessos e monta um processo para comunicar incidentes com dados atende às expectativas dos clientes da UE e fica preparado para a nova lei.

Cibersegurança comparada à NIS2

O Paraguai não tem lei de cibersegurança. Vários projetos tramitam no Congresso, entre eles uma “Ley de Ciberseguridad de la República del Paraguay”, apresentada em junho de 2025. Por enquanto, a base é a Estrategia Nacional de Ciberseguridad 2025 a 2028 (Decreto Nº 3900/2025). A equipe nacional de resposta a incidentes, o CERT-PY, faz parte da Dirección General de Ciberseguridad do MITIC.

Obrigações como as da [NIS2](#), ou seja, gestão de riscos, segurança da cadeia de suprimentos e prazos fixos de notificação para setores inteiros, não decorrem disso para as empresas. Para bancos, o banco central tem regras próprias de segurança da informação.

Para fornecedores do Paraguai, isso significa que as exigências chegam pelo contrato com o cliente da UE. Uma trading agrícola com software logístico próprio recebe perguntas sobre controle de acesso, backups e planos de contingência; um fabricante de equipamentos conectados, sobre o [Cyber Resilience Act](#).

Prazos de notificação comparados

SITUAÇÃO	PARAGUAI	UE
Incidente com dados, aviso à autoridade	hoje sem prazo vigente; Ley 7593/2025 a partir do fim de 11/2027, detalhes por regulamento	72 horas (art. 33 do RGPD)
Aviso aos titulares	hoje sem prazo vigente	sem demora indevida, se o risco for alto (art. 34 do RGPD)
Incidente cibernético significativo	sem lei	alerta inicial em 24 h, notificação em 72 h, relatório final após um mês (art. 23 da NIS2)

Na prática, o cliente da UE fixa o prazo no contrato, geralmente de 24 a 48 horas. Defina com antecedência quem notifica na sua empresa e quem fica de plantão caso algo aconteça no fim de semana.

Autoridades, CSIRT, organismo de acreditação

ÁREA	ÓRGÃO
Proteção de dados	Agencia Nacional de Protección de Datos Personales (MITIC, em estruturação)
Cibersegurança, CSIRT	MITIC, Dirección General de Ciberseguridad com o CERT-PY
Setor financeiro	BCP, Banco Central del Paraguay
Acreditação	ONA, Organismo Nacional de Acreditación (no CONACYT)

Para certificados, importa menos onde está o organismo certificador e mais quem o acreditou. Pergunte antes da contratação se a acreditação pelo ONA ou por um órgão estrangeiro está coberta pelo acordo internacional de reconhecimento da Global ACI (desde 01/01/2026 sucessora do IAF e do ILAC; as creditações existentes continuam reconhecidas). Nesse caso, o certificado costuma ser aceito por clientes da UE. Alguns grupos empresariais ainda assim exigem um certificador específico. Esclareça isso antes de gastar dinheiro com uma auditoria.

O que os clientes da UE costumam exigir

Para exportadores de soja e carne, o EUDR vem em primeiro lugar: dados de geolocalização de todas as áreas, comprovação de origem livre de desmatamento após 31/12/2020 e comprovação de produção legal segundo o direito paraguaio. No EUDR, o Paraguai está classificado como país de risco padrão. Justamente no Chaco, onde muita floresta foi derrubada nas últimas décadas, os compradores perguntam com detalhe.

Fabricantes de alimentos geralmente precisam de uma certificação [IFS](#), [BRCGS](#) ou [FSSC 22000](#), indústrias muitas vezes de [ISO 9001](#). Quem trata dados de clientes europeus recebe cláusulas contratuais padrão e um questionário de segurança. Muitos desses questionários perguntam por sistemas acessíveis pela internet; o [veyrisk](#) verifica essa superfície de ataque de fora e entrega um relatório.

No contrato, essas exigências costumam aparecer em vários anexos: cláusulas contratuais padrão, contrato de tratamento de dados, medidas técnicas e organizacionais, prazos de notificação e direitos de auditoria. Além disso, seu cliente da UE precisa elaborar uma avaliação de impacto da transferência para o Paraguai. Para isso, ele precisa de informações suas sobre acessos, criptografia e possíveis solicitações de autoridades. Quanto mais precisas forem suas respostas, mais rápido o contrato é assinado.

Um bom ponto de partida para empresas do Paraguai:

1. Identifique quais dados você recebe de clientes da UE e onde eles ficam armazenados.
2. Crie um registro das operações de tratamento e nomeie uma pessoa responsável pela proteção de dados. Você vai precisar das duas coisas, no máximo, com a Ley 7593/2025.
3. Monte um processo de notificação de incidentes que cumpra os prazos dos seus contratos.
4. Para exportações de soja e carne, reúna os dados de geolocalização das suas áreas e das áreas dos seus fornecedores.
5. Veja qual certificado seus clientes pedem com mais frequência e planeje a auditoria com antecedência.

O [Diagnóstico UE](#) gratuito mostra onde sua empresa está hoje.

Acordo com a UE

O [acordo UE-Mercosul](#) foi assinado em 17/01/2026 em Assunção. Desde 01/05/2026, a parte comercial é aplicada provisoriamente entre a UE e Paraguai, Argentina, Brasil e Uruguai. Para obter a preferência tarifária, você precisa de uma declaração de origem. O acordo de parceria mais amplo ainda está em ratificação.

Na prática, isso significa: verifique para cada mercadoria a alíquota, o cronograma de redução tarifária e a regra de origem. Você encontra essas informações no portal Access2Markets da Comissão Europeia, organizadas por código de mercadoria. No caso de produtos processados, a regra de origem define se houve agregação de valor suficiente no Mercosul. Para alguns produtos agrícolas valem cotas tarifárias, ou seja, quantidades limitadas com tarifa preferencial. Seu importador na UE muitas vezes conhece essas regras melhor do que você e pode ajudar a colocar a declaração de origem corretamente na fatura. Guarde as comprovações de origem por vários anos, porque a alfândega pode verificar depois.

O acordo reduz tarifas, não exigências. EUDR, CBAM e RGPD valem integralmente para mercadorias paraguaias.

FAQ

A partir de quando vale a nova lei de proteção de dados do Paraguai?

A Ley 7593/2025 foi promulgada em 27/11/2025 e, após 24 meses de transição, passa a ser plenamente aplicável no fim de novembro de 2027.

Clientes da UE precisam de cláusulas contratuais padrão para o Paraguai?

Sim. O Paraguai não tem decisão de adequação da UE. São necessárias SCC e uma avaliação de impacto da transferência.

O Paraguai tem lei de cibersegurança?

Não. Há projetos no Congresso. Por enquanto, a base é a estratégia nacional 2025 a 2028.

Qual ferramenta ajuda a se preparar para a Ley 7593/2025 e para o RGPD?

Uma plataforma GRC como o [Sightadel](#) conduz você pelos requisitos do RGPD com modelos, tarefas e comprovações, por exemplo para o registro das operações de tratamento. Como a lei paraguaia adota muitas ideias do RGPD, boa parte desse trabalho serve para as duas. O Sightadel é desenvolvido e hospedado na Alemanha.

O que o EUDR exige de exportadores de soja do Paraguai?

Dados de geolocalização das áreas de cultivo e a comprovação de que não houve desmatamento ali após 31/12/2020. Mais na página sobre o [EUDR](#).

Fontes · Atualizado em: 11 de outubro de 2026

Gaceta Oficial de la República del Paraguay: <https://www.gacetaoficial.gov.py/>

MITIC: <https://www.mitic.gov.py/>

CERT-PY: <https://www.cert.gov.py/>

Comissão Europeia: decisões de adequação: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Comissão Europeia, DG Comércio: Paraguai: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/paraguay_en

Informações gerais, sem caráter de consultoria jurídica. Valem os textos oficiais.

COLOQUE EM PRÁTICA COM FERRAMENTAS FEITAS NA ALEMANHA



O Sightadel conduz sua equipe por a NIS2: modelos, tarefas, evidências e preparação para auditoria em um só lugar. Desenvolvido e hospedado na Alemanha, com pacote de consultoria opcional.

[Conhecer o Sightadel →](#)



O veyrisk mostra o que um atacante enxerga da sua empresa por fora: serviços abertos, certificados, vulnerabilidades conhecidas. Você pode apresentar o relatório a clientes europeus e auditores.

[Conhecer o veyrisk →](#)



Valar é um firewall de hardware com software da neonotu. Protege escritórios e unidades e gera os registros exigidos pela NIS2 e pela ISO 27001.

[Conhecer o Valar →](#)

Sightadel, veyrisk e Valar são produtos da neonotu GmbH, empresa que opera o MercoEU.

O que disso se aplica à sua empresa?

O Diagnóstico UE gratuito mostra isso por setor e país em 10 minutos.

<https://www.mercoeu.com/pt/diagnostico-ue>