

PAÍS · MERCOSUL

Brasil: o que os clientes da UE esperam

Desde janeiro de 2026, a UE reconhece o Brasil como país com nível adequado de proteção de dados. Isso facilita o fluxo de dados, mas não substitui as comprovações de segurança da informação, de desmatamento ou de emissões.

PROTEÇÃO DE DADOS LGPD, Lei 13.709/2018	ADEQUAÇÃO DA UE sim, desde 01/2026	ACORDO COM A UE UE-Mercosul, provisório desde 01/05/2026	CIBERSEGURANÇA sem lei geral, PL 4.752/2025 em tramitação
--	---------------------------------------	--	--

Visão geral: comércio com a UE

O Brasil é o maior parceiro comercial da UE na América do Sul. Segundo a Comissão Europeia, cerca de 42 % das exportações brasileiras para a UE em 2025 foram produtos agrícolas e 27 % combustíveis e produtos de mineração, principalmente petróleo bruto e também minério de ferro. Quem embarca soja do Paraná, café de Minas Gerais ou celulose de Mato Grosso do Sul para Roterdã ou Hamburgo esbarra primeiro em regras de cadeia de suprimentos como o [EUDR](#). Exportadores de aço e alumínio são afetados pelo [CBAM](#).

Some-se a isso uma exportação de serviços em crescimento: software houses de São Paulo, Florianópolis ou Recife desenvolvem para bancos, seguradoras e clientes industriais na Europa. Para elas, proteção de dados e segurança da informação pesam mais do que tarifas.

Proteção de dados: a LGPD comparada ao RGPD

A LGPD (Lei nº 13.709/2018) está em vigor desde setembro de 2020, e a ANPD aplica sanções desde agosto de 2021. Ela foi inspirada no [RGPD \(Regulamento Geral sobre a Proteção de Dados\)](#): bases legais para cada tratamento, direitos dos titulares, encarregado, relatórios de impacto e o dever de comunicar incidentes de segurança. Quem implementa bem a LGPD já cumpre boa parte das obrigações do RGPD.

Desde janeiro de 2026 existe também uma decisão de adequação da UE (Decisão de Execução (UE) 2026/179). O reconhecimento é mútuo: com a Resolução CD/ANPD nº 32/2026, a ANPD também reconheceu a UE como adequada. Para os seus clientes na UE, isso significa que dados pessoais podem vir para o Brasil sem cláusulas contratuais padrão e sem avaliação de impacto da transferência. Ficam de fora apenas as transferências para fins de segurança pública e perseguição penal.

A adequação trata apenas da transferência de dados. Se você trata dados por conta de um cliente da UE, continua precisando de um contrato de tratamento de dados nos termos do art. 28 do RGPD e de comprovar suas medidas técnicas e organizacionais.

Dois diferenças aparecem na prática. A LGPD prevê dez bases legais, entre elas a proteção do crédito; o RGPD, seis. E o prazo para comunicar incidentes é contado em dias úteis, não em horas. Quem atende os dois regimes faz melhor em alinhar seus processos ao prazo mais curto.

Cibersegurança comparada à NIS2

Aqui ainda não existe uma lei que, como a [NIS2](#), fixe obrigações para setores inteiros. O Decreto nº 11.856/2023 instituiu a Política Nacional de Cibersegurança (PNCiber) e um comitê (CNCiber), mas não criou uma autoridade de supervisão com poder sobre as empresas. O projeto do Marco Legal da Cibersegurança (PL 4.752/2025) está no Senado. A principal questão em aberto é se a supervisão ficará com uma nova agência ou com a Anatel.

Até agora, as regras obrigatórias são setoriais. Pela Resolução CMN nº 4.893/2021, bancos precisam ter uma política de segurança cibernética, controlar a contratação de serviços em nuvem e comunicar incidentes relevantes ao Banco Central. Para instituições de pagamento vale algo equivalente pela Resolução BCB nº 85/2021.

Para fornecedores de clientes europeus, isso é secundário. Pela NIS2, seu cliente na UE precisa gerenciar a segurança da cadeia de suprimentos e repassa essa obrigação a você por contrato. Quem fornece software para empresas financeiras na UE recebe ainda cláusulas do [DORA](#) no contrato, e fabricantes de produtos conectados se enquadram no [Cyber Resilience Act](#).

Prazos de notificação comparados

SITUAÇÃO	BRASIL	UE
Incidente com dados, comunicação à autoridade	3 dias úteis a partir do conhecimento, se houver risco relevante (Res. CD/ANPD 15/2024); prazo em dobro para agentes de pequeno porte	72 horas (art. 33 do RGPD)
Comunicação aos titulares	também 3 dias úteis	sem demora indevida, se o risco for alto (art. 34 do RGPD)

SITUAÇÃO	BRASIL	UE
Incidente cibernético significativo	sem lei geral; bancos comunicam ao Banco Central	alerta inicial em 24 h, notificação em 72 h, relatório final após um mês (art. 23 da NIS2)

A regra da ANPD também exige que você registre os incidentes e guarde essa documentação por cinco anos. Um cliente da UE normalmente fixa no contrato um prazo próprio, muitas vezes de 24 a 48 horas, para conseguir cumprir as 72 horas dele.

Autoridades, CSIRT, organismo de acreditação

ÁREA	ÓRGÃO
Proteção de dados	ANPD, Autoridade Nacional de Proteção de Dados
Cibersegurança federal	GSI/PR com o CTIR Gov (administração pública federal)
CSIRT para empresas	CERT.br, do NIC.br
Setor financeiro	Banco Central do Brasil, Conselho Monetário Nacional
Acreditação	INMETRO, acreditação pela Cgcre

Certificados de organismos acreditados pela Cgcre costumam ser aceitos na UE, porque a Cgcre participa dos acordos internacionais de reconhecimento entre acreditadores. Mesmo assim, pergunte antes da auditoria se o seu cliente exige um certificador específico.

O que os clientes da UE costumam exigir

Para exportadores do agronegócio e de commodities, o EUDR vem em primeiro lugar. Seu comprador precisa dos dados de geolocalização das suas áreas e da comprovação de que não houve desmatamento ali depois de 31/12/2020. No EUDR, o Brasil está classificado como país de risco padrão. Por isso vale a diligência devida completa; a diligência devida simplificada do art. 13 só existe para países de baixo risco. Na cadeia de alimentos, somam-se certificações [IFS](#), [BRCGS](#) ou [FSSC 22000](#).

Prestadores de serviços de software e TI geralmente recebem um questionário de segurança baseado na NIS2 e na [ISO 27001](#). Perguntas típicas: em quanto tempo você comunica um incidente? Quem tem acesso aos dados de produção? Há testes de intrusão? Um certificado ISO 27001 responde a muitas dessas perguntas de uma vez. Para montar o sistema de gestão até a auditoria, a plataforma

[Sightadel](#) conduz pelos requisitos da norma e guarda as comprovações.

Muitos clientes também verificam de fora o que você expõe na internet: portas abertas, certificados vencidos, versões antigas de servidor. Quem acompanha isso continuamente, por exemplo com o [veyrisk](#), já sabe a resposta antes de o questionário chegar.

No contrato, essas exigências costumam virar anexos: um contrato de tratamento de dados nos termos do art. 28 do RGPD, uma lista das medidas técnicas e organizacionais, prazos de notificação de incidentes, direitos de auditoria do cliente e regras para subcontratados. Como o Brasil é considerado adequado, as cláusulas contratuais padrão deixam de ser necessárias. O restante seu cliente exige mesmo assim, e vai revisar de novo na renovação.

Um bom ponto de partida para empresas brasileiras:

1. Verifique quais regras da UE afetam seus clientes e pergunte ativamente pelas exigências, em vez de esperar o questionário.
2. Coloque sua documentação da LGPD lado a lado com os requisitos do RGPD. Registro das operações de tratamento, bases legais e relatórios de impacto geralmente podem ser aproveitados.
3. Estruture um processo de notificação que cumpra o prazo contratual mais curto e teste esse processo uma vez por ano.
4. Para o EUDR, reúna dados de geolocalização e comprovações dos seus fornecedores antes que o comprador peça.
5. Decida se um certificado ISO 27001 ou uma norma de segurança de alimentos responde aos questionários dos clientes mais rápido do que cada informação avulsa.

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. Sua parte comercial, o acordo comercial interino, é aplicada provisoriamente desde 01/05/2026 entre a UE e Brasil, Argentina, Paraguai e Uruguai. As tarifas caem de forma escalonada, e você precisa de uma declaração de origem para usar a preferência. 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 não dispensa o direito da UE. EUDR, CBAM, RGPD e regulamentos de produto valem para mercadorias brasileiras da mesma forma que para mercadorias de qualquer outro país.

FAQ

Clientes da UE ainda precisam de cláusulas contratuais padrão para transferir dados ao Brasil?

Não. Desde a decisão de adequação (UE) 2026/179, de janeiro de 2026, dados podem ser transferidos ao Brasil sem SCC. Um contrato de tratamento de dados continua necessário se você trata dados por conta do cliente.

O Brasil tem uma lei como a NIS2?

Ainda não. O PL 4.752/2025 está no Senado. Até lá valem regras setoriais, sobretudo para bancos e instituições de pagamento.

Em quanto tempo preciso comunicar um incidente com dados à ANPD?

Em até três dias úteis a partir do conhecimento, se houver risco relevante para os titulares (Resolução CD/ANPD 15/2024). Agentes de pequeno porte têm o prazo em dobro.

O acordo UE-Mercosul reduz minhas obrigações no EUDR?

Não. As vantagens tarifárias dependem da comprovação de origem, e o EUDR continua valendo sem mudanças. Mais detalhes na página sobre o [EUDR](#).

Qual ferramenta ajuda a responder aos questionários de segurança de clientes da UE?

A plataforma de GRC [Sightadel](#) reúne ISO 27001, NIS2 e RGPD em um só sistema e reaproveita as comprovações de uma norma na outra. Ela é desenvolvida e hospedada na Alemanha, e os dados ficam na UE.

Fontes · Atualizado em: 11 de outubro de 2026

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

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

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

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

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

Comissão Europeia, DG Comércio: Brasil: <https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries->

and-regions/brazil_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>