

REGRA DA UE · PROTEÇÃO DE DADOS

RGPD: dados pessoais da UE na América do Sul

O Regulamento Geral sobre a Proteção de Dados vale também para empresas sem sede na UE. E com frequência ainda maior ele chega até você pelos seus clientes da UE, assim que você trata dados pessoais para eles.

BASE LEGAL	VALE DESDE	ADEQUAÇÃO	AFETA
Regulamento (UE) 2016/679	25/05/2018	Argentina, Uruguai, Brasil	Quem oferece a pessoas na UE e operadores de dados

Em resumo

O RGPD (Regulamento Geral sobre a Proteção de Dados) define como dados pessoais podem ser tratados: nomes, endereços de e-mail, números de cliente, dados de localização, dados de saúde e tudo o que possa ser associado a uma pessoa. Ele vale diretamente em todos os Estados-Membros desde 25/05/2018.

Para empresas de fora da UE, o RGPD se aplica por dois caminhos. O primeiro é o critério do mercado de destino, no artigo 3.º, n.º 2: quem oferece bens ou serviços a pessoas na UE ou monitora o comportamento delas, por exemplo com rastreamento em um site, está sujeito diretamente ao RGPD. O segundo caminho é mais comum. Uma empresa da UE contrata você para tratar dados em nome dela e só pode fazer isso se houver um contrato nos termos do artigo 28 e se a transferência para o seu país for permitida pelo capítulo V (art. 44 a 50).

O capítulo V prevê várias bases. A mais simples é uma decisão de adequação da Comissão, pelo artigo 45: nesse caso, seu país é considerado seguro e os dados circulam como dentro da UE. Sem ela, o cliente da UE precisa de garantias adequadas pelo artigo 46, na prática quase sempre as cláusulas contratuais-tipo da Comissão (Decisão de Execução (UE) 2021/914).

As autoridades de controle podem aplicar multas de até 20 milhões de euros ou 4 % do faturamento anual mundial, o que for maior (art. 83.º, n.º 5). Contra empresas de fora da UE, a execução é mais difícil; contra o seu cliente da UE, não. Por isso ele verifica com cuidado a quem confia os dados e garante no contrato responsabilidade e direitos de controle. Um vazamento de dados em um prestador de Lima recai juridicamente sobre o contratante em Madri.

Quem é afetado na América do Sul

São afetados diretamente lojas virtuais, fornecedores de SaaS, operadoras de turismo, escolas de idiomas ou empresas de aplicativos que se dirigem de propósito a clientes na UE. Um hotel em Cusco com página de reservas em alemão e preços em euros entra nesse grupo. Essas empresas precisam nomear um representante na UE pelo artigo 27. A única exceção é o tratamento ocasional, sem grande volume de dados sensíveis (art. 27.º, n.º 2).

São afetados indiretamente todos os operadores, chamados no texto da UE de subcontratantes: call centers em Bogotá para uma operadora de telecomunicações espanhola, suporte de TI de Córdoba, processamento de folha de pagamento, desenvolvimento de software com dados reais de clientes, análise de dados, hospedagem em nuvem.

PAÍS	DECISÃO DE ADEQUAÇÃO DA UE	O QUE O CLIENTE DA UE PRECISA
Argentina	Sim, Decisão 2003/490/CE, confirmada no relatório da Comissão de 15/01/2024	Contrato pelo art. 28
Uruguai	Sim, Decisão de Execução 2012/484/UE, confirmada em 15/01/2024	Contrato pelo art. 28
Brasil	Sim, adotada em 26/01/2026	Contrato pelo art. 28
Chile, Colômbia, Peru, Equador, Paraguai, Bolívia	Não	Contrato pelo art. 28, cláusulas contratuais-tipo e avaliação de impacto da transferência

A decisão sobre o Brasil é recíproca: a ANPD, por sua vez, reconheceu a UE como adequada. Ela cobre o setor público e o privado. Para uma software house de Florianópolis, desde a decisão de 26/01/2026 as cláusulas contratuais padrão e a avaliação de impacto da transferência deixam de ser necessárias para dados vindos da UE. Isso elimina boa parte da papelada que antes havia com cada cliente da UE.

A adequação dispensa as cláusulas contratuais-tipo, mas não o contrato do artigo 28 nem as medidas técnicas de proteção. Seu cliente vai continuar exigindo as duas coisas.

Prazos

O RGPD vale sem alterações desde 2018. As novidades dizem respeito sobretudo à região: a decisão de adequação para o Brasil, de 26/01/2026, e novas leis nacionais, por exemplo no [Chile](#) e no

Paraguai, que ainda não são plenamente aplicáveis.

Em novembro de 2025 a Comissão propôs um “Digital Omnibus”, que também deve alterar partes do RGPD. Enquanto a proposta não for aprovada, vale o RGPD na versão conhecida. Por isso, planeje com base no direito em vigor.

No dia a dia, há prazos mesmo assim. O controlador da UE precisa notificar uma violação de dados à autoridade de controle em até 72 horas (art. 33). Como operador, você precisa informá-lo “sem demora injustificada”, e muitos contratos fixam para isso 24 ou 48 horas.

O que os clientes da UE pedem na prática

- Um contrato de tratamento de dados (em inglês, DPA) pelo artigo 28, normalmente no modelo do cliente.
- Para países sem adequação, as cláusulas contratuais-tipo, em geral o Módulo 2 (controlador para operador) ou o Módulo 3 (operador para suboperador).
- Uma avaliação de impacto da transferência (Transfer Impact Assessment), que analisa se autoridades do seu país podem acessar os dados.
- Uma descrição das suas medidas técnicas e organizativas pelo artigo 32.
- Uma lista dos seus suboperadores, como provedores de nuvem e sistemas de chamados.
- Um registro das atividades de tratamento para os dados do cliente.
- Como prova dessas medidas, muitas vezes um certificado [ISO/IEC 27001](#), às vezes complementado pela ISO/IEC 27701 para privacidade.

Quem se dirige diretamente a clientes na UE precisa ainda de uma política de privacidade conforme o RGPD, de uma base legal para cada tratamento, de um processo para pedidos de acesso e de exclusão e, se for o caso, do representante na UE pelo artigo 27.

Primeiros passos

1. Defina se você se dirige diretamente a pessoas na UE ou se só trata dados para empresas da UE. Disso depende se você precisa de um representante na UE.
2. Liste quais dados pessoais você recebe de clientes da UE, onde eles ficam armazenados e quem tem acesso.
3. Verifique a legislação do seu próprio país. A LGPD e as leis da Argentina e do Uruguai são parecidas com o RGPD; em outros países falta bastante coisa. Os detalhes estão nas páginas por país.

4. Prepare uma descrição das medidas técnicas e organizativas que você possa entregar a qualquer cliente.
5. Defina um fluxo para violações de dados, com aviso ao cliente dentro do prazo contratual.
6. Faça o [Diagnóstico UE](#) gratuito para enxergar as lacunas.

Uma plataforma GRC como o [Sightadel](#) ajuda a manter atualizados o registro, as medidas e os contratos de muitos clientes. Para a parte técnica do artigo 32, o [veyrisk](#) verifica de fora o que sua empresa deixa visível na internet, como serviços abertos e certificados, e entrega um relatório que você pode anexar à descrição das medidas.

Relação com certificações

O RGPD prevê certificações próprias pelo artigo 42, que na prática são raras. Por isso os clientes da UE recorrem à [ISO/IEC 27001](#) para comprovar a segurança do tratamento exigida pelo artigo 32. Fornecedores de SaaS com clientes nos EUA costumam ter um [relatório SOC 2](#), que muitos clientes da UE também aceitam. Se você trabalha com IA e dados pessoais, vale olhar o [Regulamento da IA](#). Para prestadores de TI de bancos entra o [DORA](#); para muitos outros, a [NIS2](#).

Um certificado não substitui a análise caso a caso. Mas mostra que direitos de acesso, criptografia, registros de log e o tratamento de incidentes estão organizados e são verificados regularmente por terceiros. São exatamente esses os pontos que o cliente pergunta quando avalia suas medidas. Quem tem o certificado responde com uma referência, em vez de vinte páginas de explicação.

FAQ

O RGPD vale para a minha empresa na América do Sul?

Sim, se você oferece bens ou serviços a pessoas na UE ou monitora o comportamento delas (art. 3.º, n.º 2). Se você só trata dados em nome de uma empresa da UE, as obrigações chegam pelo contrato do art. 28.

O que muda com a decisão de adequação para o Brasil?

Desde 26/01/2026 empresas da UE podem transferir dados pessoais para o Brasil sem cláusulas contratuais-tipo. O contrato do art. 28 e as medidas de segurança continuam necessários. Mais na página sobre o [Brasil](#).

Preciso de um representante na UE?

Se o RGPD vale diretamente para você por causa do art. 3.º, n.º 2, em regra sim (art. 27). Se você atua apenas como operador de um cliente da UE, normalmente não.

O que é uma avaliação de impacto da transferência?

Uma análise de se a legislação do país de destino, por exemplo os poderes de acesso das autoridades, enfraquece a proteção dada pelas cláusulas contratuais-tipo. Ela é comum para países sem decisão de adequação.

Qual ferramenta ajuda a manter a documentação do RGPD em dia?

Uma plataforma GRC em que o registro das atividades de tratamento, as medidas técnicas e organizativas e os contratos ficam no mesmo lugar. O [Sightadel](#) suporta o RGPD como marco regulatório, é desenvolvido e hospedado na Alemanha, e os dados ficam na UE.

Fontes · Atualizado em: 11 de outubro de 2026

Regulamento (UE) 2016/679 (RGPD), EUR-Lex: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

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

Comissão Europeia: declaração conjunta da UE e da ANPD de 28/01/2026: https://commission.europa.eu/news-and-media/news/joint-press-statement-michael-mcgrath-and-waldemar-goncalves-ortunho-junior-director-president-2026-01-28_en

Relatório da Comissão de 15/01/2024 sobre as decisões de adequação existentes: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024DC0007>

Decisão de Execução (UE) 2021/914 (cláusulas contratuais-tipo): https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
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 o GDPR: 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 →](#)

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>