

REGRA DA UE · SETOR FINANCEIRO

DORA: quando seu cliente é um banco na UE

Desde 17/01/2025, bancos, seguradoras e outras entidades financeiras da UE precisam escolher, contratar e monitorar seus prestadores de TI seguindo regras fixas. Quem fornece software, serviços de data center ou suporte de TI para eles sente isso diretamente.

BASE LEGAL	VALE DESDE	NÚCLEO PARA FORNECEDORES	AFETA
Regulamento (UE) 2022/2554	17/01/2025	Art. 28 a 30	Prestadores de TI de entidades financeiras da UE

Em resumo

O Digital Operational Resilience Act, conhecido como DORA, é um regulamento da UE. Ele vale diretamente em todos os Estados-Membros, sem lei de transposição. Os destinatários são entidades financeiras: bancos, seguradoras, instituições de pagamento e de moeda eletrônica, empresas de investimento, gestoras de fundos, prestadores de serviços de criptoativos e outras. Elas precisam organizar sua TI de forma a suportar falhas, ataques e interrupções.

Boa parte do regulamento trata dos terceiros prestadores de serviços de TIC, ou seja, os fornecedores externos de serviços de TI. O artigo 28 exige que a entidade financeira avalie os riscos de um fornecedor antes de fechar contrato, registre todos os contratos em um registro de informações e tenha uma estratégia de saída para serviços importantes. O artigo 29 trata do risco de concentração e menciona expressamente fornecedores em países terceiros: a legislação de falências e a de proteção de dados do país do prestador precisam ser levadas em conta. O artigo 30 define o que todo contrato precisa conter.

Para um fornecedor da América do Sul, isso significa que seu cliente só pode contratar você se o contrato tiver esse conteúdo mínimo e se você fornecer as informações exigidas.

Quem é afetado na América do Sul

Obrigações diretas pelo DORA só têm os fornecedores classificados como terceiros prestadores críticos de serviços de TIC pelas autoridades europeias de supervisão EBA, EIOPA e ESMA. A primeira lista saiu em 18/11/2025, com 19 fornecedores, sobretudo grandes provedores de nuvem, data

center, rede e software financeiro. Pelo artigo 31, n.º 12, um fornecedor crítico de país terceiro só pode ser usado se abrir uma subsidiária na UE em até doze meses após a classificação.

O caso comum é ser afetado de forma indireta. Isso inclui:

- Fintechs e software houses, por exemplo de São Paulo, Buenos Aires ou Bogotá, que desenvolvem ou operam software de pagamentos, crédito ou seguros para clientes da UE.
- Equipes nearshore que programam, testam ou dão suporte a sistemas de bancos europeus.
- Data centers e provedores de hospedagem com clientes financeiros europeus.
- Call centers e prestadores de BPO que trabalham com acesso aos sistemas do cliente.
- Fornecedores de dados de mercado, de crédito ou de prevenção a fraudes.

Todos eles entram no registro de informações do cliente e precisam aceitar as cláusulas contratuais do artigo 30. Segundo uma resposta da EBA no procedimento de perguntas e respostas (Q&A 2024_7096), prestadores intragrupo ficam fora da classificação como fornecedor crítico. Isso não vale para as obrigações contratuais.

Um exemplo: uma software house de Montevideu opera o portal de sinistros de uma seguradora espanhola. Antes de renovar o contrato, a seguradora precisa verificar onde ficam os dados, quem tem acesso, em quanto tempo o portal volta a funcionar após uma falha e o que acontece se a software house encerrar as atividades. As respostas vão para o registro e para a avaliação de riscos da seguradora. Se a software house não conseguir comprová-las, a seguradora precisa cobrir o risco de outra forma ou trocar de fornecedor.

Prazos

O DORA vale desde 17/01/2025. As entidades financeiras tiveram de adaptar os contratos existentes e montar seus registros. Quem negocia hoje com um banco da UE recebe o anexo DORA junto com o contrato-quadro. Contratos mais antigos sem essas cláusulas são ajustados na renovação seguinte, muitas vezes com prazo curto.

DATA	O QUE ACONTECEU
17/01/2025	O DORA passa a valer em todos os Estados-Membros
18/11/2025	Primeira lista de terceiros prestadores críticos de serviços de TIC (19 fornecedores)
12 meses após a classificação	Fornecedores críticos de países terceiros precisam de uma subsidiária na UE (art. 31, n.º 12)

A supervisão dos fornecedores críticos é rigorosa. Pelo artigo 35, n.º 6, são possíveis sanções pecuniárias compulsórias de até 1 % do faturamento diário médio mundial.

O que os clientes da UE pedem na prática

O artigo 30 define o que um contrato de serviços de TIC precisa conter. Entre os itens estão uma descrição clara do serviço, os locais de tratamento dos dados, regras de acesso, inspeção e auditoria, direitos de rescisão, o apoio em incidentes de segurança e, para serviços importantes, a participação em testes e exercícios do cliente. Na prática, espere o seguinte:

- Um anexo contratual DORA que reflita esses pontos. Muitos bancos têm modelos próprios.
- Dados para o registro de informações: seu código LEI (Legal Entity Identifier), locais de tratamento dos dados e subcontratados utilizados.
- Um certificado [ISO/IEC 27001](#) ou um [relatório SOC 2](#).
- Comprovações de gestão de continuidade, muitas vezes segundo a ISO 22301.
- Disposição para receber no local os auditores do cliente e da autoridade de supervisão.
- Um plano de saída que descreva como o cliente pode retomar ou transferir o serviço de forma ordenada.

O código LEI pega muitos fornecedores de surpresa. Ele é solicitado a entidades emissoras credenciadas e precisa ser renovado todo ano. Sem ele, seu cliente não consegue registrar sua empresa corretamente.

Em funções importantes ou críticas, entra ainda a participação em testes. Grandes entidades financeiras precisam fazer regularmente testes de intrusão orientados por ameaças, e um prestador que opera uma função desse tipo pode ser incluído. Defina no contrato como isso funciona, quem paga os custos e como seus outros clientes ficam protegidos.

Seus próprios fornecedores também entram no radar. Se você trabalha para um banco da UE usando uma plataforma de nuvem ou repassa partes do trabalho a freelancers, o cliente vai querer saber e, se for o caso, aprovar.

Primeiros passos

1. Verifique quais dos seus clientes da UE são entidades financeiras. Uma empresa de leasing ou um prestador de serviços de pagamento também pode se enquadrar.
2. Solicite um código LEI, se ainda não tiver.

3. Faça uma lista de todos os locais onde você armazena ou trata dados de clientes e de todos os subcontratados.
4. Leia o anexo DORA do seu cliente mais importante item por item e marque o que você ainda não cumpre.
5. Escreva um plano de continuidade e recuperação para os serviços que presta a clientes financeiros, e teste esse plano.
6. Mantenha comprovações, políticas e relatórios de auditoria em um só lugar. Uma plataforma GRC como o [Sightadel](#) ajuda a manter isso para vários clientes ao mesmo tempo.

O [Diagnóstico UE](#) dá uma primeira avaliação.

Relação com certificações

O DORA não exige nenhum certificado. Mas os bancos da UE avaliam seus prestadores por critérios fixos, e um certificado reconhecido encurta bastante essa avaliação. Para segurança da informação, esse certificado é a [ISO/IEC 27001](#), muitas vezes complementada pelo [SOC 2](#) no caso de fornecedores com clientes nos EUA. Quem fornece modelos de IA para decisões de crédito ou detecção de fraudes deve conhecer também o [Regulamento da IA](#) e a [ISO/IEC 42001](#). Se houver tratamento de dados pessoais, vale sempre também o [RGPD](#). Para fornecedores do [Brasil](#), da [Argentina](#) e do [Uruguai](#), a transferência de dados é mais simples graças à decisão de adequação.

DORA e [NIS2](#) se sobrepõem. Para entidades financeiras, o DORA prevalece como regra mais específica, mas as exigências para fornecedores são parecidas. Quem trabalha para os dois grupos de clientes pode atender a ambos com um único sistema de gestão. No [Sightadel](#), DORA e NIS2 estão disponíveis como marcos próprios, e o que você documenta para um deles pode ser reaproveitado no outro.

FAQ

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

Diretamente, só se sua empresa for classificada como terceiro prestador crítico de serviços de TIC. Caso contrário, as obrigações chegam pelo contrato com seu cliente financeiro da UE.

O que é um registro de informações?

Uma lista em que cada entidade financeira da UE mantém todos os contratos de serviços de TIC, com dados sobre fornecedor, serviço, locais dos dados e subcontratados (art. 28, n.º 3). Você fornece os dados para ela.

Preciso abrir uma empresa na UE?

Só se sua empresa for classificada como fornecedor crítico. Nesse caso, o artigo 31, n.º 12, exige uma subsidiária na UE em até doze meses.

Um relatório SOC 2 basta para o DORA?

Muitos bancos aceitam. Na Europa, porém, o certificado ISO/IEC 27001 é mais difundido. A comparação está em [SOC 2 ou ISO 27001](#).

Qual ferramenta ajuda a responder às exigências DORA de vários clientes?

Uma plataforma GRC com DORA como marco. O [Sightadel](#) reúne políticas, comprovações e tarefas por requisito e é desenvolvido e hospedado na Alemanha. Para perguntas sobre vulnerabilidades em sistemas acessíveis pela internet, o [veyrisk](#) fornece um relatório da sua superfície de ataque externa.

Fontes · Atualizado em: 11 de outubro de 2026

Regulamento (UE) 2022/2554 (DORA), EUR-Lex: <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>

ESMA: designação dos terceiros prestadores críticos de serviços de TIC: <https://www.esma.europa.eu/press-news/esma-news/european-supervisory-authorities-designate-critical-ict-third-party-providers>

EBA: supervisão no âmbito do DORA: <https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act/dora-oversight>

EBA Q&A 2024_7096: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2024_7096

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 DORA: 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>