

Entenda o Regulamento Geral Europeu de Proteção de Dados

DANIEL

Lei 2016/679 começa a valer a partir de 25 de maio de 2018. Veja como isso afeta seus negócios:



O QUE DIZ A LEI

Prevê a proteção de dados pessoais de pessoas físicas processados por meios automatizados ou integrantes de um sistema de arquivo



O QUE SÃO DADOS PESSOAIS

Qualquer informação relacionada a uma pessoa física identificada ou identificável (titular dos dados). **Exemplo:** nome, email, RG, telefone etc.

DADOS SENSÍVEIS

Dados biométricos, de saúde, genéticos ou que revelam etnia, condenações criminais, religião, opinião política, orientação sexual, dentre outros



CONTROLADOR

Organização ou indivíduo que determina como e por que os dados pessoais do titular serão processados. **Exemplo:** Banco



PROCESSADOR

Organização ou indivíduo que processa os dados pessoais por ordem do controlador. **Exemplo:** Serviço de nuvem contratado



AUTORIDADES SUPERVISORAS

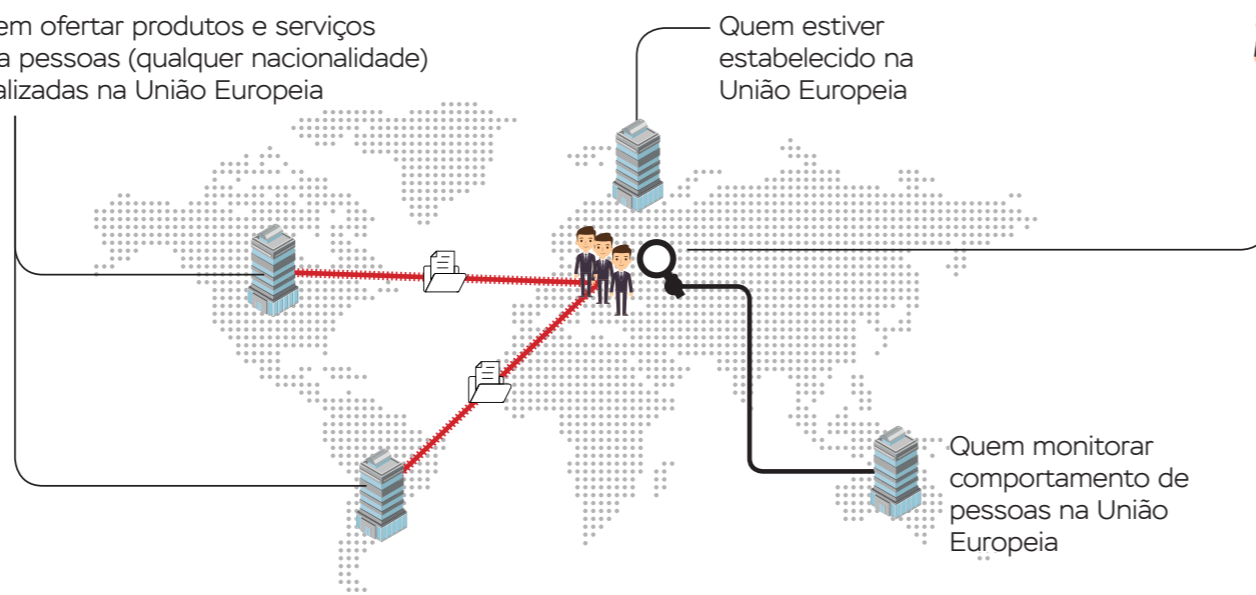
Autoridade que supervisiona o cumprimento e aplica as penalidades previstas no Regulamento. Cada país membro da União Europeia possui a sua autoridade. No Brasil, a criação da autoridade está sendo discutida no projeto de lei sobre proteção de dados pessoais

A QUEM SE APLICA

Quem ofertar produtos e serviços para pessoas (qualquer nacionalidade) localizadas na União Europeia

Quem estiver estabelecido na União Europeia

Quem monitorar comportamento de pessoas na União Europeia



DIREITOS DOS TITULARES DOS DADOS

	Direito de acesso	Obter do controlador a informação de quais dados estão sendo processados
	Direito de retificação	Solicitar a retificação sem atraso de dados incorretos
	Direito de portabilidade	Receber dados pessoais de maneira estruturada e em formato universal
	Direito ao esquecimento	Ter apagados os dados pessoais, assim como links e reproduções desses dados
	Direito à limitação do processamento	Solicitar a limitação do processamento de dados pessoais
	Direito de oposição	Opor-se ao processamento de dados pessoais e a decisões fundamentadas exclusivamente no processamento automatizado de dados

REGRAS QUE DEVEM SER SEGUIDAS POR QUEM PROCESSA DADOS



Legitimidade

O processamento deve obedecer a uma das seguintes bases legais: consentimento; necessidade contratual; obrigação legal; interesse público e vital; legítimo interesse



Qualidade dos dados

Devem ser garantidas a integridade, disponibilidade e confidencialidade dos dados e a resiliência do sistema e serviço



Privacy by design/ Privacy by default

A proteção de dados deve ser observada em todas as etapas de desenvolvimento dos produtos e serviços e sempre na sua forma mais protetiva ao titular dos dados



Accountability

DPIA - Avaliação do impacto na proteção de dados
Deve ser realizada sempre que as operações utilizarem novas tecnologias e representarem alto risco ao titular dos dados

Registro e retenção de dados
Devem ser mantidos documentação e registro das atividades de processamento de dados pessoais e política adequada de retenção

DPO
Indicação de profissional responsável pela política de proteção de dados



Transparência nas informações

Toda comunicação ao titular dos dados deve ser escrita de maneira clara, objetiva e visual



Comunicação em caso de vazamento de dados

CONTROLADOR
Deverá notificar a autoridade supervisora em até 72 horas e comunicar o titular dos dados o mais breve possível nos casos de vazamento de alto risco

PROCESSADOR
Deverá notificar o controlador o mais breve possível



Transferência internacional de dados

Devem ser atendidas regras específicas sempre que os dados processados forem transferidos para países fora da União Europeia ou para organizações internacionais

PENALIDADES



Cada autoridade supervisora poderá aplicar multas administrativas em razão da infração ao regulamento. Cada caso será analisado individualmente



As penalidades poderão chegar até **EUR 20 milhões** ou **4% do faturamento global** da empresa, o que for maior



Direito à **indenização** em face do controlador/processador por danos morais e materiais sofridos pelo titular dos dados

Para que um DPO?

Esta posição é legalmente requerida quando as principais atividades do controlador/processador envolverem:

- monitoramento regular e sistemático dos titulares de dados em larga escala
- processamento de dados pessoais sensíveis em larga escala
- processamento de dados pessoais por autoridade ou órgão público

Para mais informações: www.daniel-ip.com