
SANS SECURITY AWARENESS

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

# GDPR

## Visão Geral

Você pode ter ouvido falar de uma nova lei chamada GDPR, ou o Regulamento Geral de Proteção de Dados. Esta lei foi desenvolvida pela União Europeia e entra em vigor em 25 de maio de 2018. Aplica-se a qualquer organização que manipule as informações pessoais de qualquer residente na União Europeia (UE), independentemente de onde no mundo essa organização esteja localizada. O GDPR exige que as organizações mantenham a privacidade e a segurança das informações pessoais de qualquer residente da UE. Para garantir a conformidade com o GDPR, os princípios-chave precisam ser compreendidos e implementados.

As pessoas têm direito à privacidade. As organizações precisam respeitar sua privacidade, restringindo os dados pessoais que coletam e processam sobre eles e salvaguardando esses dados. As obrigações de privacidade aplicam-se a qualquer informação, utilizada isoladamente ou combinada com outras informações, que possa identificar uma pessoa que viva na União Europeia. Essas informações podem ser itens como endereços, números de passaporte, números de carteira de motorista, detalhes financeiros, dados biométricos, associações a sindicatos, histórico médico, dados de localização ou informações relacionadas à orientação sexual, religiosa ou política de uma pessoa. O regulamento aplica-se a uma “pessoa natural”, que significa um indivíduo vivo. Aqui estão alguns dos principais princípios do GDPR que devem ser seguidos:

- **Os dados pessoais dos indivíduos devem ser processados de forma legal, justa e transparente;**
- **As pessoas precisam ser informadas sobre o que está sendo coletado e com que propósito;**
- **Os dados pessoais devem ser coletados para fins específicos, explícitos e legítimos. Não deve ser usado por quaisquer outras razões que conflitem com esses propósitos;**
- **Os dados pessoais só devem ser mantidos e processados pelo tempo que for necessário para esse fim e por não mais que isso;**
- **Dados pessoais devem ser mantidos atualizados e precisos;**

**As pessoas têm o direito de receber uma cópia de seus dados ou solicitar que seus dados pessoais não sejam mais usados ou, em alguns casos, excluídos totalmente;**

**As organizações devem implementar medidas de segurança apropriadas para proteger os dados pessoais contra destruição, perda, alteração ou divulgação acidental ou ilegal;**

**Além disso, as organizações precisam garantir que todos os funcionários que lidam com dados pessoais recebam treinamento adequado sobre como manter de forma segura e proteger esses dados;**

As medidas de proteção que estão em vigor para proteger os dados pessoais devem garantir um nível de proteção adequado à natureza sensível dos dados. À medida que o risco associado aos dados se torna maior, o mesmo acontece com o esforço e a despesa das medidas para proteger os dados. Essas medidas devem ser revisadas e atualizadas regularmente, conforme apropriado. Registros bem documentados sobre decisões e medidas de privacidade e segurança ajudam a mostrar conformidade com os requisitos. Além disso, as organizações são legalmente obrigadas a empregar medidas, como contratos e ações de revisões, para proteger dados pessoais ao transferi-los para terceiros externos ou, particularmente, para as partes fora da União Europeia. Por fim, no caso de uma violação de dados pessoais, as organizações devem comunicar a violação no prazo de 72 horas após tomarem conhecimento dela. A falha das organizações em cumprir com o GDPR pode resultar em multas de até 4% de sua receita global, tornando o GDPR uma das regulamentações globais financeiramente mais dispendiosas do mundo.

## Editor Convidado

***Brian Honan*** *é CEO da BH Consulting, uma empresa independente de consultoria em segurança cibernética e proteção de dados com sede em Dublin, Irlanda. Brian atuou como consultor especial do Centro de Crimes Cibernéticos da Europol (EC3), é fundador da primeira CERT da Irlanda e participa do conselho consultivo de várias empresas inovadoras de segurança. Encontre Brian em* www.linkedin.com/in/brianhonan ou Twitter @brianhonan.

## Recursos

Visão Geral da GDPR Overview para Pessoas e Organizações (em Inglês): http://gdprandyou.ie

A regulamentação GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679

Traduções e Arquivos OUCH!: https://www.sans.org/u/D88