WWF
Política Interna

WWF Network

Violação de Dados Pessoais – Protocolos de Rede

Versão 1 – Novembro 2018

Para mais informação, por favor contacte Escritório do Conselho Geral.

I. O que é este protocolo?

O WWF da uma grande importância à proteção de dados pessoais que obtemos, mantemos e processamos. Os dados incluem informações de:

- Funcionários,
- Doadores,
- Apoiadores on-line,
- Consultores,
- Membros do conselho e muito mais.

Normalmente só devem ser acessíveis à aqueles autorizados a acessá-los em virtude de suas responsabilidades no WWF.

No entanto, os dados pessoais podem ser perdidos, roubados ou mal utilizados, criando riscos legais, financeiros e de reputação e, principalmente, danos à pessoa a quem os dados se referem.

Usamos o termo “Violação de dados” se ocorrer uma violação na segurança de dados pessoais que leve à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais transmitidos, armazenados ou processados de outra forma.

O objetivo deste Protocolo de Rede é ter um processo comum para encaminhar informações de graves violações de dados pessoais para um nível de Rede. O escalonamento garante que estamos lidando com quaisquer riscos legais ou de reputação além do compromisso do escritório “violado”, bem como para fornecer, conforme a capacidade permitir, suporte adicional ao escritório que sofreu uma violação.

II. O que devo fazer em caso de violação de dados no meu escritório?

1) Primeiro, foque na prevenção! Todos os escritórios devem tomar cuidado para:

- Ser informado de qualquer legislação de dados pessoais a que deve obedecer. Os regulamentos podem diferir de país para país. IMPORTANTE: O Regulamento Geral de Proteção de Dados da UE (GDPR) se aplica a qualquer organização, incorporada e localizada na UE ou não, que obtenha, mantenha e processe dados pessoais de cidadãos da UE. O GDPR determina os requisitos de relatório relacionados a violações de dados.
- Compreender e cumprir todos os requisitos para denunciar violações de dados a autoridades locais e, como no caso do GDPR, a outras autoridades.
- Ter políticas e procedimentos de segurança de dados pessoais e informações em vigor e monitorar sua eficácia, bem como a conscientização dos funcionários sobre eles.
- Implementar um protocolo de violação de nível de escritório.
- Procure orientação na Rede e com a assessoria jurídica local para ajudar com qualquer uma das etapas acima.

2) Escale! Se houver uma suspeita ou violação real de dados pessoais, os escritórios devem seguir qualquer legislação que possa se aplicar a eles, bem como informar à WWF International, Chief Operating Officer da violação dentro de 24 horas da descoberta da violação.

Apêndice: Definições

Termo	Definição
Dados Pessoais	Qualquer informação relativa a uma pessoa singular identificada ou identificável, que possa ser identificada, direta ou indiretamente, em particular por referência a um identificador como nome, número de identificação, dados de localização, identificador on-line ou factores específicos de natureza física, psicológica e genética, identidade mental, económica, cultural ou social dessa pessoa. Isso significa que as informações são diretamente sobre alguém ou podem ser rastreadas, como, por exemplo: um nome, possivelmente em combinação com um endereço e uma data de nascimento. O fato de estar relacionado a uma pessoa natural significa que os dados relacionados às organizações não são dados pessoais. Um item de informação não é um dado pessoal se medidas técnicas ou organizacionais foram tomadas para criptografar ou remover informações pessoalmente identificáveis dos conjuntos de dados, para que as pessoas que os dados descrevam permaneçam anônimas (anonimização). Exemplos de dados pessoais: exemplos óbvios são o nome, endereço, local de residência, números de telefone de alguém. Informações mais confidenciais incluem detalhes salariais e de pagamento, nomes de usuário, senhas e outros detalhes de login e dados que podem ser usados para fraudes (de identidade), como cópias de documentos de identidade, dados financeiros sobre doações e legados.
Categorias Especiais de Dados Pessoais	Um subconjunto de dados pessoais revelando origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação a sindicatos, processamento de dados genéticos ou biométricos para identificar de forma única uma pessoa ou dados relativos à saúde, vida sexual ou orientação sexual.
Violação de Dados	Ocorreu uma violação da segurança dos dados pessoais ("incidente de segurança") em que dados pessoais foram perdidos ou violados, ou se o processamento ilegal dos dados pessoais não puder ser razoavelmente excluído. Uma violação de dados pode levar a sérias consequências para a privacidade das pessoas cujos dados estão contidos no arquivo violado, bem como para o controlador de dados. Exemplos de incidentes que podem levar a violações de dados (não exaustivas): • O roubo ou perda de um stick USB ou outra unidade removível; • O roubo ou perda de um telefone celular; laptop ou outro aparelho de computador; • O uma violação e / ou acesso não autorizado à rede e / ou infra-estrutura do WWF (incluindo roteador, servidor, firewall, etc.) Por terceiros; • O uma avaria da rede, causada por uma parte não autorizada; • O envio de um email não criptografado com uma lista de dados pessoais para um destinatário (não autorizado); • O a transferência de arquivos contendo informações (potenciais) do doador por meio de um ambiente desprotegido; • O roubo ou perda de materiais impressos com dados pessoais; • O a descoberta de recibos de salários de funcionários do WWF em um contêiner de lixo público; • O roubo dentro das instalações do WWF, onde um ou mais dos materiais acima são roubados; • O Todas as situações em que dados pessoais são perdidos ou o processamento ilegal desses dados não pode ser excluído. Em um caso em que estamos falando apenas de um ponto fraco na segurança, onde nenhum dado pessoal foi realmente perdido e o processamento ilegal de dados pessoais pode ser excluído, isso é uma violação de segurança e não uma violação de dados. Nesse caso, obviamente, medidas são tomadas para selar esta violação de segurança. Exemplo de uma situação que não é uma violação de dados: Um banco de dados contendo dados pessoais é excluído devido a erro humano por parte do operador do sistema. Um backup completo e atualizado do banco de dados está disponível, com base no qual o banco de dados pode ser imediatamente reconstruído. Este não é um caso de violação de dados.