WWF
Política Interna

WWF INTERNACIONAL

Protocolo de Violação de Dados – Responsabilidade do Staff

Version 1 – Julho 2018

Esta política é um extrato dos Protocolos Internacionais de Violação de Dados do WWF Versão 1 - Julho de 2018

Para mais informações, entre em contato com o escritório do Conselho Geral.

I. Geral

Os dados pessoais compreendem todos os itens de informação sobre uma pessoa natural identificada ou identificável, por exemplo, do trabalhador, um doador, um apoiante, um consultor, um membro do conselho.

O WWF atribui uma grande importância à proteção de dados pessoais guardados e processados no WWF: os dados pessoais normalmente só devem ser acessíveis àqueles autorizados a acessá-los em virtude de suas funções dentro do WWF - e os procedimentos operacionais visam alcançar isso. No entanto, os dados pessoais podem ser perdidos ou roubados, levando-os a estar disponíveis para terceiros não autorizados. Isso cria riscos legais, financeiros e de reputação e, principalmente, prejudica a pessoa a quem os dados se referem (o titular dos dados).

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 é pôr fim a uma violação de dados, para evitar ou limitar danos, e para satisfazer, conforme aplicável, quaisquer requisitos para notificar a Autoridade de Supervisão competente como deve ser identificado, os titulares de dados afetados (com base Artigo 33 Regulamento Geral de Proteção de Dados (GDPR) e outra legislação que possa ser aplicada) e, se necessário, um representante da WWF International à União Europeia para garantir a conformidade com o GDPR. Todos os envolvidos são obrigados a respeitar a confidencialidade de todas as informações obtidas em relação a uma violação de dados suspeita ou real.

A Equipa de Violação de Dados - conforme explicado abaixo - coordenará todas as actividades e medidas requeridas sob este Protocolo.

II. Responsabilidades do Trabalhador

Um funcionário 1) que perde dados pessoais, ou 2) que percebe que dados pessoais foram perdidos ou adulterados (por exemplo, *hackeados*), ou 3) que percebe, por qualquer motivo, que o processamento ilegal de dados pessoais pode ter ocorrido deve tomar as seguintes ações **imediatamente**:

1. Determine com precisão quais informações podem ter sido perdidas, adulteradas ou processadas ilegalmente:

- O que está em falta precisamente (papel, suporte de dados móvel, laptop, pendrive, etc.)?
- Que informação / dados?
- Quanta informação / dados?
- A informação é pública, confidencial, particularmente sensível?

2. Informe toda a equipa imediatamente (veja o Apêndice A). É importante que o relatório seja feito imediatamente após a descoberta, porque uma grave violação de dados deve ser informada à Autoridade de Supervisão competente dentro de 72 horas após sua descoberta.

Se dados pessoais sensíveis foram perdidos - por exemplo, dados financeiros pessoais, salário, benefícios, fotografias ou informações sobre raça, religião ou saúde - o funcionário deve entrar imediatamente em contato com um membro da equipe por telefone.

3. Informe o gestor de linha se ele / ela perdeu pessoalmente os dados (por exemplo, perda de laptop ou telefone);

4. Se aplicável, após consulta à Equipa, informe a polícia;

5. Fique disponível para mais consultas com a equipe.

6. Todos os funcionários são obrigados a respeitar a confidencialidade de todas as informações obtidas em relação a uma possível violação de dados.

III. Data Breach Team members and contact details

Versão Data1 Julho 2018. Actualizações desta lista serão enviadas a todo staff do WWF Internacional

Nome, Posição	Telefone	Email	Contacto Alternativo
Karianne Sturms, General Counsel	+ 31 (0)30 6937848	ksturms@wwfint.org	Paola Boniello pboniello@wwfint.org
Donna Lusti, Manager, Governance Ethics & Compliance	+ 41 (0)22 3649215	dlusti@wwfint.org	
Linda Humphrey, Director, Global ICT Services	+44 7768 721170	lhumphrey@wwfint.org	Kah Leng Ng klng@wwfint.org
Rebecca Clear, Head, Media Relations	+44 7909 936 628	rclear@wwfint.org	

IV. 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 fatores 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.

Categoria Especial 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.
Assunto dos Dados	Aquele que pode ser identificado, direta ou indiretamente, em particular por referência a um identificador, como nome, número de identificação, dados de localização, identificador on-line ou um ou mais fatores específicos de natureza física, psicológica, genética, mental, econômica, cultural ou identidade social dessa pessoa.
Controlador de Dados	Pessoa singular ou colectiva, autoridade pública, agência ou qualquer outro organismo que, individualmente ou em conjunto com outros, determina os fins e os meios do tratamento de dados pessoais. Na maioria dos casos, para nossos propósitos, o WWF será considerado o controlador de dados.
Processador de Dados	Pessoa singular ou colectiva, autoridade pública, agência ou qualquer outro organismo que processe dados pessoais em nome do responsável pelo tratamento.
Processamento de Dados	Qualquer operação ou conjunto de operações que sejam realizadas mediante dados pessoais ou conjuntos de dados pessoais, seja ou não por meios automatizados, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão , divulgação ou disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição.
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): • roubo ou perda de um stick USB ou outra unidade removível; • roubo ou perda de um telefone celular; laptop ou outro aparelho de computador; • uma violação e / ou acesso não autorizado à rede e / ou infraestrutura do WWF (incluindo roteador, servidor, firewall, etc.) por terceiros; • uma avaria da rede, causada por uma parte não autorizada; • envio de um email não criptografado com uma lista de dados pessoais para um destinatário (não autorizado); • a transferência de arquivos contendo informações (potenciais) do doador por meio de um ambiente desprotegido; • roubo ou perda de materiais impressos com dados pessoais; • a descoberta de recibos de salários de funcionários do WWF em um contêiner de lixo público; • roubo dentro das instalações do WWF, onde um ou mais dos materiais acima são roubados; • 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 da 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.

Equipa de Violação de Dados	A equipa do WWF que coordena os assuntos após a ocorrência de uma violação de dados, com base neste protocolo. Veja o Apêndice A para nomes da equipe atual.
Impacto	As violações de dados são classificadas em vários níveis de impacto para o WWF ou as pessoas envolvidas. Os vários níveis de impacto e as características associadas de uma violação de dados estão incluídos no Anexo D - Níveis de impacto das violações de dados. O foco principal do Protocolo está em lidar com violações de Dados do Impacto 1, em que é necessário apresentar um relatório tanto para a Autoridade Supervisora competente quanto para os envolvidos. Naturalmente impacto 2 e 3 Violações de dados também serão tratadas adequadamente e analisaremos a questão de quais medidas estruturais de segurança são necessárias para evitar violações de dados semelhantes no futuro, com base na análise anual de todos os relatórios, procurando em tendências de causas.

IV. Processo de Respostá de Violação

Uma violação é encontrada e reportada	A quem	Acções
1. Recebimento de entrada Relatório de violação de dados	Trabalhador ou terceiro (Relator)	O relatório para a equipa é feito imediatamente após a descoberta, via e-mail. Relatórios extremamente urgentes também devem ser feitos verbalmente ou por telefone.
The Report is Reviewed		
2. Contacte o relator e preencha uma Lista de Verificação da Avaliação de Violação de Dados (Apêndice C).	Equipa	Discuta o relatório com o repórter, solicite informações adicionais. Uma lista de verificação de avaliação de violação de dados é preenchida para cada relatório. Informe o COO sobre o relatório e outras medidas processuais tomadas.
3. Registo dos relatórios	Equipa	Os relatórios são registrados em um Logbook.
4. Informar o Gestor	Relator	Se o empregado perdeu dados pessoais, o relatório é discutido com o seu gerente.
5. Avaliar se ocorreu uma violação de dados	Equipa	A equipe estabelece se uma violação de dados ocorreu com base na lista de verificação de avaliação de violação de dados preenchida.
5a. Estabeleceu que nenhuma violação de dados ocorreu	Equipa	Decisão registrada no Logbook. O relatório está concluído. Prossiga para o ponto 12.
5b. Estabeleceu que a violação de dados ocorreu.	Equipa	Decisão registrada no Logbook. Estabelecer o nível de impacto com base nos níveis de impacto de violações de dados - apêndice C.
6. Informar o SMT, (no caso de um impacto 1 (grave) violação de dados)	Equipa	Informe a SMT nesta etapa no caso de: • Relatório externo de uma violação de dados; • Grave segurança de TI violação de dados; • Violação de dados sensível à média.
7. Avaliar a necessidade de comunicação (no caso de um impacto 1 (grave) violação de dados)	Equipa	Analise a necessidade de comunicações internas / externas em caso de: • relatório externo de uma violação de dados; • grave violação de dados de segurança de TI; • violação de dados sensível à mídia.
Response to Breach		

8. Tome medidas urgentes, se necessário	Equipa	Em situações urgentes, as medidas são tomadas imediatamente, se necessário.
9. Avaliar a violação de dados à luz dos requisitos de notificação	Equipa	Realize os testes 1 e 2, veja o ponto 9a) e 9b) abaixo Teste 1) Estabeleça se os dados perdidos são de natureza sensível, ou existe um risco significativo de consequências adversas sérias Teste 2) Estabelecer se a violação de dados tem consequências adversas para os titulares dos dados
10. Notificação à autoridade de supervisão competente	Equipa	Nos casos em que o ponto 9a) seja aplicável, notifique a SMT e as Comunicações imediatamente, e as Autoridades, incluindo o Representante da UE (conforme definido pelo GDPR) da WWF Internacional, se aplicável, dentro de 72 horas após a descoberta! A notificação é feita de acordo com as instruções fornecidas pela Autoridade de Supervisão
11. Notificação aos titulares de dados envolvidos	Equipa	**Informar imediatamente** os titulares de dados afetados nos casos em que o ponto 9b) é aplicável.
12. Documentação	Equipa	Manter documentos em arquivos bem organizados: • Logbook • Listas de verificação de avaliação de violação de dados; • Notificações para Autoridade; • Notificações aos sujeitos de dados envolvidos; • Qualquer evidência.
Revisão Anual		
Analise relatórios, tendências	Equipa e SMT	Análise anual de tendências em causas. Se as tendências observadas em causas recorrentes de violações de dados, investigar se as medidas de segurança estruturais são necessárias para evitar essas causas no futuro.