AUTORIDADE BRASILEIRA DE CONTROLE DE DOPAGEM

DIRETRIZES SOBRE A OCORRÊNCIA DE VIOLAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS

#jogolimpo

A presente diretriz tem como objetivo definir os princípios de caracterização, consequências e notificação de uma violação da proteção de dados.

Este documento está em acordo com a Lei Geral de Proteção de Dados (LGPD) brasileira e o Padrão Internacional para Proteção da Privacidade e das Informações Pessoais da Agência Mundial Antidopagem (AMA/WADA).

A forma como a Autoridade Brasileira de Controle de Dopagem (ABCD) faz a gestão das violações, notificações e reclamações segue os procedimentos e normas citados que colaboram para um sistema eficiente de controle das violações à privacidade e proteção de dados pessoais.

1. VIOLAÇÃO DE DADOS PESSOAIS

De acordo com o Padrão Internacional para Proteção da Privacidade e das Informações Pessoais (PIPPIP) da AMA/WADA, violação de dados é definida como um incidente de segurança que resulta na perda, roubo, dano e/ou processamento ilegal de informações pessoais, seja em formato eletrônico, impresso ou outra forma, interferência em sistema de informação que comprometa a privacidade, segurança, confidencialidade, disponibilidade ou integridade das Informações Pessoais.

Existem três tipos de violação de dados pessoais:

- **Confidencialidade** – quando existe uma divulgação ou acesso acidental ou não autorizado a dados pessoais.
- **Disponibilidade** – quando existe uma perda de acesso ou a destruição acidental ou não autorizada de dados pessoais.
- **Integridade** – quando existe uma alteração acidental ou não autorizada dos dados pessoais.

1.1 RESPONSABILIDADES DA ABCD EM CASO DE VIOLAÇÃO DAS REGRAS DE PROTEÇÃO DE DADOS

Em acordo com o art 9.1 – 9.3 do PIPPIP da AMA/WADA a ABCD deve:

- Proteger as Informações Pessoais que processam aplicando todas as salvaguardas de segurança necessárias, incluindo proteção física, organizacional, técnica e ambiental e outras medidas, para evitar uma violação de segurança.
- Aplicar medidas de segurança que levem em conta a sensibilidade das Informações Pessoais que estão sendo processadas.
- Aplicar um nível de segurança às Informações Pessoais Sensíveis que processam, refletindo o risco correspondentemente maior que uma violação de segurança envolvendo tais informações apresenta ao Participante ou Pessoa a quem as Informações Pessoais se referem.
- Garantir que quando compartilhar informações pessoais com agentes terceirizados em conexão com suas Atividades Antidopagem que tais Agentes Terceirizados estejam sujeitos a controles apropriados, incluindo controles contratuais e técnicos, a fim de proteger a confidencialidade e privacidade das Informações Pessoais para garantir que as Informações Pessoais serão processadas apenas em nome da Organização Antidopagem ou dentro do escopo da delegação ou contratação de tal Agente Terceiro, conforme o caso.
- Escolher Agentes Terceirizados que forneçam a quantidade suficiente de informações de garantias que estejam de acordo com a lei aplicável nacional e internacional em relação às medidas técnicas de segurança e organizacionais que regem o tratamento de dados a ser realizado.
- Informar Participantes afetados ou outras Pessoas físicas da violação, onde a violação é suscetível de afetar de maneira significativa os direitos e interesses das Pessoas em questão. A informação deve ser fornecida o

mais rápido possível, uma vez que a Organização Antidopagem se torne ciente dos detalhes da violação de segurança e deve descrever a natureza da violação, as possíveis consequências negativas para as Pessoas em causa e as medidas de reparação tomadas ou a ser tomada pela Organização Antidopagem. Além disso, a ABCD deve manter um registro incluindo os fatos relacionados à violação, seus efeitos e ações corretivas.

- Avaliar regularmente seu Processamento de Informações Pessoais Sensíveis e informações de localização para determinar a proporcionalidade e os riscos de processamento de dados e avaliação de quaisquer medidas, incluindo criar medidas de privacidade que possam ser tomadas para reduzir os riscos para os Participantes em questão.
- Assegurar que qualquer funcionário que processe Informações Pessoais esteja sujeito a um dever contratual e/ou estatutário de confidencialidade totalmente executável.

1.1 AVALIAÇÃO DE RISCO

AVALIAR O RISCO E O RISCO ELEVADO

Sempre que um tipo de tratamento, em especial com recurso a novas tecnologias, e tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento, seja suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deve, antes do processamento, realizar uma avaliação do impacto das operações de processamento previstas na proteção de dados pessoais. Uma única avaliação pode abordar um conjunto de operações de processamento semelhantes que apresentam altos riscos análogos.

A avaliação do impacto da proteção de dados é especialmente exigida no caso de:

- uma avaliação sistemática e exaustiva dos aspetos pessoais relativos às pessoas singulares que se baseia no tratamento automatizado, incluindo a definição de perfis, na qual se baseiam as decisões que produzem efeitos jurídicos relativos à pessoa singular ou que a afetam significativamente;
- tratamento em larga escala de categorias especiais de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para efeitos de identificação unívoca de uma pessoa singular, dados relativos à saúde, dados relativos a uma pessoa singular, a vida sexual/orientação sexual, dados pessoais relativos a condenações penais e infrações de uma pessoa devem ser proibidas ou um monitoramento sistemático de uma área acessível ao público em grande escala.

A avaliação deve conter pelo menos:

- uma descrição sistemática das operações de tratamento previstas e as finalidades do tratamento, incluindo, se for caso, o interesse legítimo prosseguido pelo responsável pelo tratamento;
- uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação às finalidades;
- uma avaliação dos riscos para os direitos e liberdades das pessoas; e
- as medidas previstas para enfrentar os riscos, incluindo salvaguardas, medidas de segurança e mecanismos para garantir a proteção dos dados pessoais e para demonstrar o cumprimento dos regulamentos vigentes tendo em conta os direitos e interesses legítimos dos titulares dos dados e outras pessoas interessadas.

Sempre que necessário, o responsável pelo tratamento procede a uma revisão para avaliar se o tratamento é efetuado de acordo com a avaliação do impacto

na proteção de dados, pelo menos quando se verifica uma alteração do risco representado pelas operações de tratamento.

1.2.1 NOTIFICAÇÕES

As obrigações de notificação de violação de segurança estão se tornando cada vez mais comuns em todo o mundo. De acordo com o Artigo 4 do PIPPIP da AMA/WADA as organizações devem cumprir as obrigações nacionais que vão além do padrão internacional (ou seja, alguns regimes nacionais podem exigir notificação adicional a uma autoridade competente ou outras organizações ou impor prazos específicos para notificação). Uma violação não afeta significativamente um indivíduo quando as Informações Pessoais em questão estiverem sujeitas a procedimentos adequados medidas de proteção tecnológica (por exemplo, criptografia) e não há indicação de que a proteção foi comprometida. A notificação será feita por qualquer meio apropriado, seja por escrito, verbalmente ou de outra forma, levando em consideração as circunstâncias particulares da Violação, incluindo o prejuízo que as Pessoas relevantes possam sofrer com o resultado da Violação das Regras de Proteção de Dados.

No caso de violação de dados pessoais, o responsável pelo tratamento deve, sem demora injustificada e, sempre que possível, após ter tido conhecimento da mesma, notificar a violação de dados pessoais à autoridade de controle competente, salvo se improvável que a violação de dados pessoais resulte em risco para os direitos e liberdades das pessoas físicas.

O processador deve notificar o controlador sem demora injustificada após tomar conhecimento de uma violação de dados pessoais.

A notificação referida deve, pelo menos:

- descrever a natureza da violação de dados pessoais, incluindo, sempre que possível, as categorias e número aproximado de titulares de dados

em causa e as categorias e número aproximado de registos de dados pessoais em causa;

- comunicar o nome e contatos do responsável pela proteção de dados ou outro ponto de contacto onde possam ser obtidas mais informações;
- descrever as prováveis consequências da violação de regras de proteção de dados pessoais;
- descrever as medidas tomadas ou propostas a serem tomadas pelo controlador para lidar com a violação das regras de proteção de dados pessoais, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos adversos.

Sempre que, e na medida em que, não seja possível fornecer as informações ao mesmo tempo, as informações podem ser fornecidas por fases sem atrasos indevidos.

O controlador deve documentar qualquer violação de dados pessoais, incluindo os fatos relacionados à violação das regras de proteção de dados pessoais, seus efeitos e as medidas corretivas tomadas. Essa documentação deve permitir à autoridade supervisora verificar o cumprimento do presente artigo.

1.2.2 POSSÍVEIS CONSEQUÊNCIAS DE UMA VIOLAÇÃO DE DADOS PESSOAIS

Uma violação pode potencialmente ter vários efeitos adversos significativos sobre as pessoas, que podem resultar em danos físicos, materiais ou imateriais, entre eles: perda de controle sobre os seus dados pessoais, limitação dos seus direitos, discriminação, roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação e a perda de confidencialidade de dados pessoais protegidos por sigilo profissional.

AUTORIDADE BRASILEIRA DE CONTROLE DE DOPAGEM

#jogolimpo

DIRETRIZES SOBRE A OCORRÊNCIA DE VIOLAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS

A lei brasileira LGPD artigos 15 (IV), 31 e 42 descreve que é de determinação da autoridade nacional quando houver violação ao disposto na lei. Quando houver infração à LGPD em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

E finalmente no capítulo VIII, seção I a LGPD lista os tipos de sanções administrativas aplicáveis pela autoridade nacional, como a seguir:

I - Advertência, com indicação de prazo para adoção de medidas corretivas;

II - Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - Multa diária, observado o limite total a que se refere o inciso II;

IV - Publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - Eliminação dos dados pessoais a que se refere a infração;

X - Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

1.3 PROCEDIMENTOS PARA APRESENTAR UMA RECLAMAÇÃO

As reclamações e denúncias sobre eventuais violações de privacidade e de proteção a dados pessoais podem ser apresentadas à ABCD através do e-mail denuncia@abcd.gov.br .

Todas as reclamações são encaminhadas e tratadas pelo Gestor responsável pela privacidade e proteçãos aos dados pessoais, que assegurará que a resposta aconteça dentro do prazo e dentro das regras vigentes nacionais e internacionais.

1.3.1 Confidencialidade

O canal é seguro e as informações de má conduta repassadas à ABCD serão mantidas sob sigilo, protegendo a identidade do denunciante e atendendo às normas nacionais e internacionais.

1.3.2 Respostas às reclamações

A ABCD recebe e responde as reclamações em até 5 dias, a contar do recebimento.

A ABCD informa ao reclamante sobre o andamento e o resultado da reclamação, incluindo a possibilidade de recurso administrativo e outros canais de manifestação, caso seja do interesse da parte.