ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: BSA – THE SOFTWARE ALLIANCE

CPF/CNPJ: 02.469.832/0001-87

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS	
IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Convém que um incidente de segurança seja considerado relevante para fins de notificação quando o incidente cria um alto risco de roubo de identidade ou fraude financeira.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	É importante que o regulamento deixe claro que apenas incidentes de segurança relevantes devam ser notificados, conforme exige a Lei Geral de Proteção de Dados Pessoais (LGPD). Para isso, o regulamento precisa adotar uma abordagem em duas vertentes: primeiro, é necessário definir um incidente de segurança e, em seguida, oferecer orientação sobre quando o incidente de segurança deve ser considerado relevante para notificação. **Definição de Incidente de Segurança**: Considerando que esta Consulta está relacionada à regulamentação da Lei Geral de Proteção de Dados Pessoais (LGPD), os incidentes no âmbito da próxima regulamentação devem estar relacionados a dados pessoais conforme definido pela LGPD. O regulamento deve deixar claro que os incidentes de segurança que requerem uma análise mais aprofundada para determinar se uma notificação de incidente de segurança será necessária são aqueles que **impactam negativamente a privacidade, disponibilidade ou integridade dos dados pessoais mantidos por uma organização.** **Incidente de segurança relevante**: De acordo com a LGPD, apenas incidentes de segurança relevantes devem ser notificados. A relevância de um incidente de segurança deve ser avaliada com base na probabilidade de apresentar altos riscos de roubo de identidade ou fraude financeira.

	Por exemplo, a violação de dados pessoais que são inutilizáveis, ilegíveis ou indecifráveis para um terceiro não autorizado devido ao uso de métodos como criptografia, redação, controles de acesso e outros mecanismos, não deve necessitar de notificação de segurança. Da mesma forma, os incidentes que afetam dados pessoais que já são de domínio público provavelmente não causarão alto risco de roubo de identidade ou fraude financeira. Por exemplo, se um banco de dados listando apenas os nomes e afiliações profissionais de indivíduos cujos perfis de mídia social publicamente disponíveis incluem essas informações fossem acessados por terceiros não autorizados, este é um incidente que provavelmente não criaria o risco de fraude financeira ou roubo de identidade, razão pela qual o incidente não deve ser considerado relevante para efeitos do presente regulamento.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Para fins de notificação de incidente de segurança, a relevância do incidente deve ser o fator determinante. Um incidente de segurança deve ser considerado relevante, indicando a exigência de notificação, se representar um alto risco de roubo de identidade ou fraude financeira devido ao acesso não autorizado, destruição, uso, modificação ou divulgação de dados pessoais. De acordo com o exemplo referido na resposta à pergunta 2, se um banco de dados listando apenas os nomes de indivíduos e suas afiliações profissionais que refletem informações publicamente disponíveis for acessado por um terceiro não autorizado, o risco de essas informações apresentarem um impacto negativo sobre esses indivíduos devido a fraude financeira ou roubo de identidade é muito baixo, então o incidente não seria considerado relevante. Por outro lado, se o mesmo banco de dados também contivesse números de previdência social dos titulares dos dados, haveria um risco de roubo de identidade e o incidente seria considerado relevante. É importante que o regulamento deixe claro que a notificação só será exigida se houver motivos razoáveis para supor que ocorreu um incidente de segurança relevante. Determinar a ocorrência de um incidente de segurança relevante requer uma investigação por parte do controlador de dados. Portanto, o simples fato de uma empresa ter conhecimento de um potencial incidente de segurança não deve incitar a necessidade de notificação. Por favor, veja detalhes adicionais sobre este problema na pergunta 6.
O que deve ser considerado na avaliação dos riscos do incidente?	Conforme descrito acima, o potencial de fraude financeira ou roubo de identidade deve ser avaliado ao considerar os riscos apresentados por um incidente de segurança. Essa avaliação pode ser feita por meio de uma avaliação do impacto da proteção de dados, por exemplo.

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	As informações exigidas pelo artigo 48, §1 são suficientes. Se não for possível fornecer todas as informações necessárias ao mesmo tempo, as informações podem ser fornecidas em fases, sem atrasos indevidos.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Imediatamente após um incidente de segurança, as empresas devem ser encorajadas - e ter tempo adequado - a concentrar seus recursos na realização de uma investigação completa e na restauração da integridade dos sistemas potencialmente comprometidos. Oferecer às empresas um prazo razoável para tais esforços ajuda a prevenir danos adicionais. A exigência de notificação nas primeiras horas após a empresa ter conhecimento de um potencial incidente de segurança força a empresa a desviar seus recursos da investigação do incidente e da implementação de ações que poderiam mitigar ou eliminar o risco para os titulares dos dados. Para garantir que as empresas ajam rapidamente ao saber de um potencial incidente de segurança, o regulamento deve exigir que as empresas tomem medidas imediatas para estabelecer se há motivos razoáveis para supor que ocorreu um incidente de segurança relevante. Se, após realizar essa avaliação inicial, a empresa concluir que ocorreu um incidente de segurança relevante, ela deve tomar medidas corretivas para eliminar ou reduzir a probabilidade de danos relevantes aos titulares dos dados, bem como notificar a ANPD em até 72 horas. O prazo para notificar a ANPD deve começar a partir do momento em que a empresa estabeleça com um grau razoável de certeza que um incidente de segurança relevante ocorreu e que atende ao limite de notificação, e não quando souber inicialmente que um potencial incidente de segurança pode ter ocorrido. Essa abordagem ajudará a evitar sobrecarregar a ANPD com notificações imateriais e evitará o desvio de recursos da empresa de atividades que promovam a segurança de dados para a preparação de notificações que provavelmente não atingirão o limite de notificações.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	As notificações de incidentes devem conter informações acionáveis suficientes para permitir que os titulares dos dados se protejam de possíveis efeitos negativos de um relevante interesse de segurança, sem conter muitos detalhes que possam tornar as notificações difíceis de entender e ineficazes. A notificação aos titulares dos dados deve incluir os elementos exigidos pela LGPD, art. 48, §1º I, IV e VI, bem como o nome e contatos do responsável pela proteção de dados ou outro ponto de contato onde possam ser obtidas informações adicionais. A empresa notificadora pode optar por acrescentar outras informações que considere relevantes para um determinado caso.

	Quanto ao prazo para notificação, os titulares dos dados devem ser notificados dentro de um prazo razoável, que pode variar dependendo das circunstâncias. No entanto, nos casos em que a notificação de incidente de segurança aos titulares dos dados pode interferir negativamente nas investigações conduzidas pela ANPD e / ou outras autoridades legais, e a notificação aos titulares dos dados pode exacerbar os riscos apresentados pelo incidente de segurança, a notificação aos titulares dos dados deve ser esperada quando a empresa notificadora é autorizada pelas autoridades competentes para fazê-lo.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Os métodos de notificação devem maximizar as chances de que a notificação chegue aos indivíduos afetados pelo incidente de segurança em tempo hábil. A notificação individual via correio, correio eletrônico ou telefone deve ser permitida, nos casos em que essas formas de comunicação sejam viáveis. As empresas também devem ter permissão para se comunicar com os titulares dos dados por meio de suas plataformas se considerarem que este é o melhor método para contatar os titulares dos dados afetados pelo incidente de segurança. Avisos públicos, referidos como "avisos substitutos" por algumas leis estaduais dos EUA, que são entregues por meio da mídia impressa ou anúncios postados de forma destacada no site da empresa notificadora também devem ser permitidos quando a empresa notificadora não tiver informações suficientes ou atualizadas para todos os indivíduos afetados pelo incidente de segurança. Os avisos públicos também devem ser autorizados se a notificação for urgente e a notificação individual causar atrasos que podem tornar a notificação ineficaz.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Conforme apontado na resposta à questão 2 acima, apenas incidentes de segurança relevantes devem gerar a obrigatoriedade de notificação à ANPD. Notificações sobre outros incidentes de segurança não devem ser exigidas.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Quando as empresas estabelecem que há motivos razoáveis para presumir que um incidente de segurança relevante possa ter ocorrido, elas devem tomar medidas corretivas imediatas para mitigar ou evitar o risco de danos ao titular dos dados. Se as ações corretivas tomadas eliminarem com sucesso o risco para o titular dos dados, não deverá ser necessária notificação aos titulares dos dados. Após análise das informações recebidas da empresa notificadora, caso a ANPD não considere que as medidas corretivas foram bem-sucedidas, poderá exigir que os titulares dos dados sejam notificados. Por exemplo, se as informações de crédito sobre vários titulares de dados forem removidas de um banco de dados por um terceiro não autorizado, apresentando riscos às pontuações de crédito dos

	titulares de dados, mas o controlador de dados for capaz de restaurar os dados, o risco representado pelo incidente de segurança teria sido eliminado e não deve ser necessária notificação aos titulares dos dados.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Quanto maior a sensibilidade e a confidencialidade dos dados envolvidos em um incidente de segurança, mais provável que eles possam causar danos mais graves devido ao roubo de identidade ou fraude financeira. Por exemplo, incidentes de segurança que causam o acesso não autorizado de nomes completos, endereços, registro geral (RG) e cadastro de pessoas físicas (CPF) podem desencadear a solicitação de notificação, já que esses dados normalmente não são amplamente compartilhados para evitar fraudes financeiras e roubo de identidade.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	A ANPD poderia usar padrões internacionais de segurança da informação, como os padrões ISO.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Como a segurança perfeita não existe, os riscos de possíveis incidentes de segurança nunca podem ser totalmente eliminados, mas podem ser atenuados e seus efeitos podem ser interrompidos antes que ocorram danos aos titulares dos dados. A ANPD deve adotar uma abordagem baseada em risco e neutra em termos de tecnologia e exigir que as empresas mantenham práticas de segurança de dados que tenham um escopo razoável de acordo com o tamanho e a complexidade de uma organização, a confidencialidade e o volume de dados pessoais em seus sistemas e o custo das ferramentas disponíveis para melhorar a segurança e reduzir vulnerabilidades
SUGESTÃO DE NORMATIVO, SE HOUVER	
O papel dos controladores e operadores de dados As notificações de incidentes de segurança à ANPD e aos titulares dos dados, quando necessárias, devem ser feitas pela empresa com a qual os titulares de dados se relacionam diretamente (controladores de dados). Essa abordagem promove um bom gerenciamento de dados, garantindo que os controladores de dados adotem uma abordagem de ciclo de vida para gerenciar a segurança da informação.	

Os contratos entre controladores de dados e operadores de dados devem permanecer aplicáveis, permitindo uma alocação eficiente de risco. Na verdade, para aumentar a proteção da privacidade, os processadores de dados muitas vezes não têm visibilidade sobre o tipo de dados que processam, nem muitas vezes têm as informações de contato do titular dos dados. Isso evitaria que os processadores de dados determinassem com precisão se o incidente aciona os requisitos de notificação e que contatassem os titulares dos dados para notificá-los sobre o incidente, se necessário.

Se ocorrer um incidente de segurança envolvendo um processador de dados, o processador de dados deve notificar o controlador de dados. O controlador de dados, então, avalia o risco com base nas informações fornecidas pelo processador de dados e faz uma determinação sobre o risco apresentado aos titulares dos dados pelo incidente, emitindo as notificações necessárias se forem justificadas