

Regulamento de Comunicação de Incidente de Segurança Em Consulta Pública

Maio de 2023

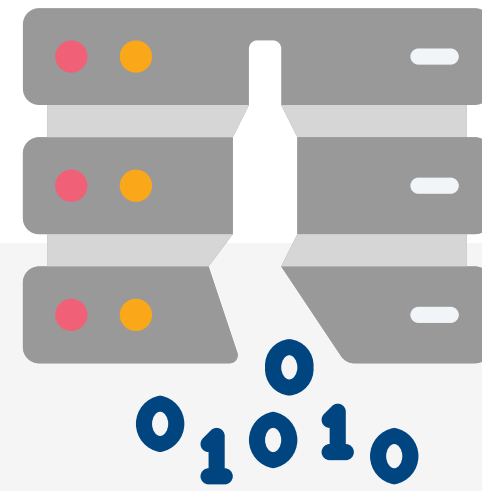
TAUIL | CHEQUER
MAYER | BROWN

A Autoridade Nacional de Proteção de Dados (ANPD) publicou Consulta Pública sobre a minuta da resolução acerca do processo de comunicação de incidentes de segurança da informação à ANPD e aos titulares, conforme exige o art. 48 da Lei nº 13.709/2018 (LGPD).

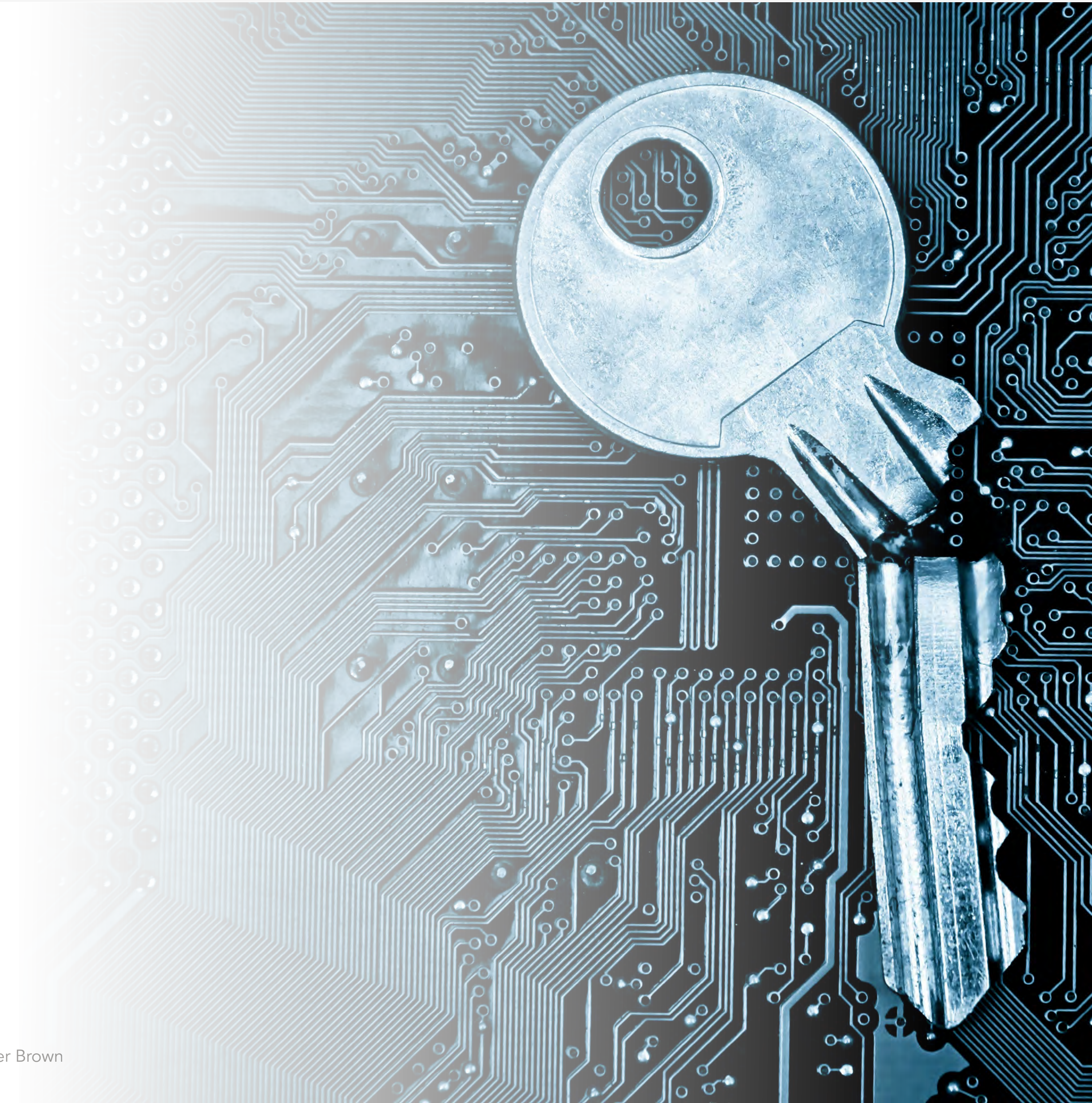
A minuta ficará disponível para contribuições até 31 de maio de 2023 e, a princípio, se aplicará aos processos de comunicação à ANPD em curso.

Os principais pontos da proposta de regulamento são:

- Incidente
- Gatilhos para comunicação
- Decisão pela não comunicação à ANPD
- Prazo para comunicação à ANPD e aos titulares
- Principais informações a serem obrigatoriamente comunicadas à ANPD
- Principais informações a serem obrigatoriamente comunicadas aos titulares
- Atuação da ANPD após a comunicação
- Representação perante a ANPD
- Sigilo sobre as informações prestadas à ANPD
- Registro de incidentes de segurança



Qualquer evento adverso **confirmado** que afete a confidencialidade, integridade, disponibilidade e/ou a autenticidade de dados pessoais.



Quando um incidente **acarretar ou puder acarretar** risco ou dano relevante aos titulares (art. 48 da LGPD). Fatores que indicariam esse risco ou dano:

Afetar **significativamente** interesses e direitos fundamentais dos titulares, a exemplo de:

- Impedir ou limitar o exercício de direitos ou a utilização de um serviço
- Ocasionar danos materiais ou morais aos titulares:

 Discriminação	 Violação à integridade física	 Roubo de identidade
 Violação à imagem e a reputação dos titulares	 Fraudes financeiras	

- Quando o incidente envolver, pelo menos:

 Dados sensíveis	 Dados de crianças e/ou de adolescentes (< 18 anos) ou idosos (> 60 anos)	 Dados financeiros
 Dados de autenticação em sistemas	 Dados em larga escala	

Caso a ANPD tome conhecimento do incidente por outro meio que não o comunicado formal pelo Controlador), ela poderá determinar que o controlador apresente informações acerca do evento e, se entender aplicável, requerer que seja enviada comunicação formal à ANPD.



A ANPD poderá fixar multa diária caso não seja enviada a comunicação no prazo fixado por ela.



A ANPD poderá, ainda, instaurar procedimento paralelo para apurar a falha em não comunicar, que constituiria violação à LGPD.



03 dias úteis, contados do momento em que se toma conhecimento do incidente ou 06 dias úteis para agentes de tratamento de pequeno porte, conforme Resolução CD/ANPD nº 02/2022.

Não ficou claro se o referido prazo seria contado a partir do momento em que o controlador tem essa ciência ou qualquer terceiro.

Pode haver complementação das informações inicialmente prestadas em até 20 dias úteis, a contar do momento em que o controlador tomou conhecimento do incidente (essa complementação acaba ocorrendo 17 dias úteis da primeira comunicação, portanto)

Se necessário, o prazo pode se estender para 40 dias úteis, desde que mediante solicitação fundamentada à ANPD.

O prazo é de 06 dias úteis para agentes de tratamento de pequeno porte, conforme definidos na Resolução CD/ANPD nº 02/2022.

PRINCIPAIS INFORMAÇÕES A SEREM OBRIGATORIAMENTE COMUNICADAS À ANPD

1	Data e hora em que tomou conhecimento do incidente	Número de titulares afetados, indicando, se houver, crianças, adolescentes e/ou idosos	6
2	Descrição do incidente, incluindo causa principal se for possível identificá-la	Medidas de segurança adotadas antes e após o incidente, em especial aquelas para reverter ou mitigar os efeitos do incidente sobre os titulares	7
3	Descrição da natureza e das categorias de dados afetados	Riscos oriundos do incidente, identificando possíveis impactos aos titulares	8
4	Número total de titulares cujos dados são tratados pelo controlador	Motivos da comunicação não ter sido realizada dentro de 03 dias úteis, quando for o caso	9
5	Número total de titulares cujos dados são tratados em cada atividade de tratamento afetada pelo incidente	Declaração de que foi realizada a comunicação aos titulares	10



Data em que tomou conhecimento do incidente

Descrição da natureza e das categorias de dados afetados

Riscos e impactos para os titulares

Medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do incidente

Contato para obtenção de informações

Dados do(a) encarregado(a) (DPO)

Recomendações aos titulares para redução dos efeitos do incidente (item não obrigatório)

A comunicação aos titulares deve ser de forma direta e individualizada (telefone, e-mail, carta ou mensagem eletrônica), quando for possível identificá-los.

Caso não seja possível identificar os titulares, deve ser feita comunicação pública (website, aplicativos, mídias sociais, canais de atendimento aos titulares), que seja de fácil visualização por, no mínimo, 06 meses.

1

Solicitar qualquer informação pertinente ao incidente, fixando prazo para entrega, entre as quais:

- Registro de operações de tratamento dos dados pessoais (ROPA) afetados pelo incidente
- Relatório de impacto à proteção de dados pessoais (RIPD)

Não há clareza se seria o RIPD já realizado para os tratamentos então afetados ou se a ANPD entende que haveria a necessidade de realização de um RIPD específico para o incidente, o que não parece ser aplicável, considerando, principalmente, as Perguntas e Respostas acerca do RIPD recentemente publicadas pela ANPD

- Relatório de tratamento do incidente, que foi definido por essa proposta de regulamento como aquele que contenha “cópias de documentos, dados e informações relevantes para descrever o incidente e as ações adotadas para o seu tratamento, tais como evidências e cronologia do incidente, metodologia de investigação e ferramentas utilizadas, e medidas de segurança adotadas”

Após a comunicação pelo controlador, a ANPD poderá:

Determinar que sejam adotadas medidas urgentes para mitigar efeitos do incidente ou salvaguardar direitos dos titulares, mesmo sem ouvir antes o controlador

2

Realizar auditorias ou inspeções ou determinar a sua realização

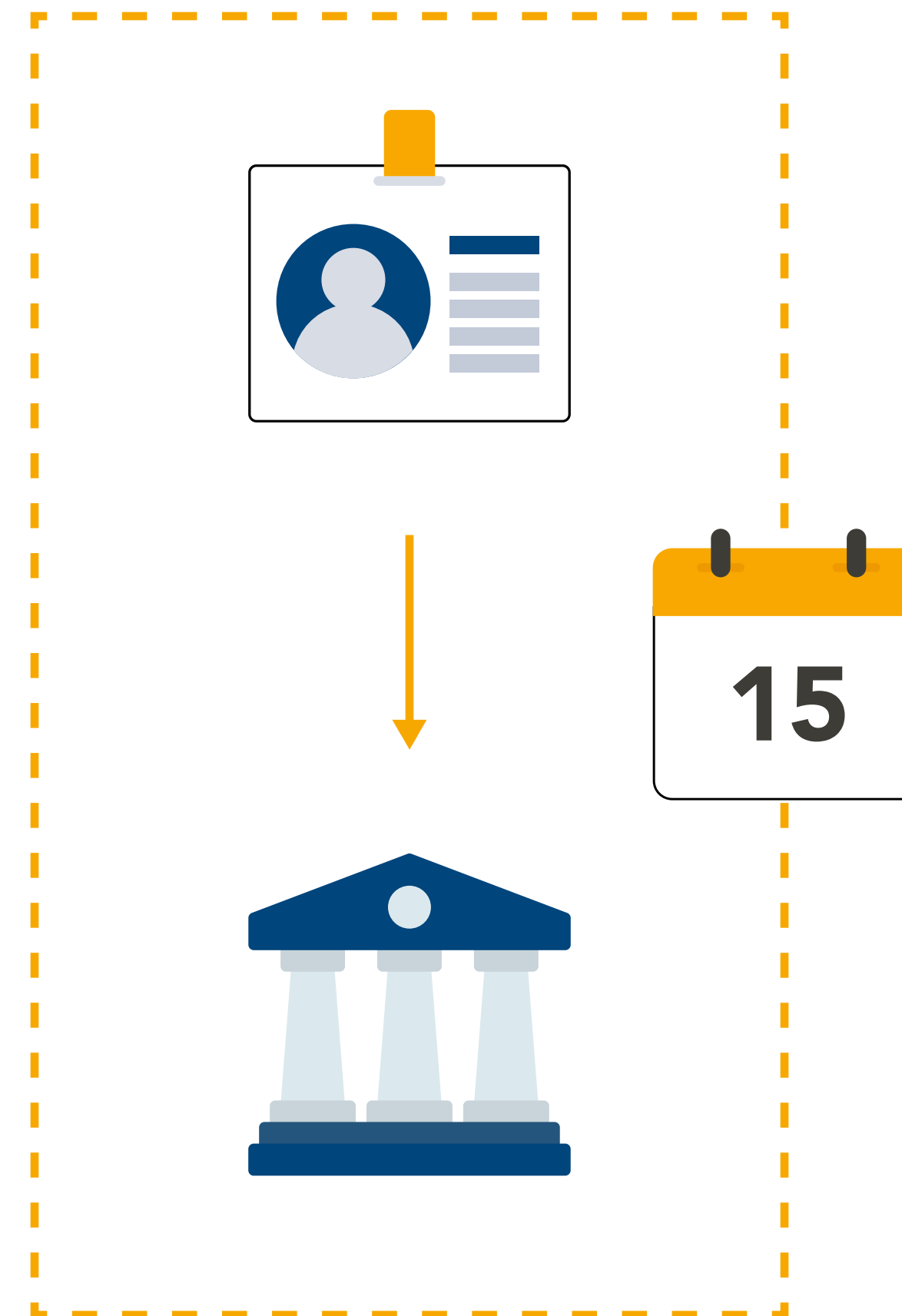
Não ficou claro se a ANPD poderia determinar que terceiros realizem as auditorias ou inspeções, exigindo que o controlador arque com os custos

3

Determinar que o controlador divulgue o incidente em website, redes sociais, mídia impressa, rádio, televisão ou em outros meios de grande alcance, a depender da abrangência de atuação do controlador.

4


Devem ser comunicados os dados do(a) encarregado(a) (DPO) ou do comunicante se for terceiro, devendo neste último caso apresentar procuração em até 15 dias úteis, a contar da primeira comunicação.



Deverá ser solicitado expressamente pelo controlador, de maneira fundamentada.



Como medida de accountability a ser obrigatoriamente implementada (ainda que não expressamente prevista na LGPD), todo controlador deve manter um registro de todos os incidentes, inclusive aqueles não comunicados à ANPD e aos titulares, por, no mínimo, 05 anos, indicando:

- 
- Datas em que tomou conhecimento dos incidentes
 - Descrição geral das circunstâncias em que os incidentes ocorreram
 - Natureza e as categorias dos dados afetados
 - Número de titulares afetados
 - Avaliações dos respectivos riscos e possíveis danos aos titulares
 - Medidas adotadas para correção e mitigação dos efeitos dos incidentes
 - Forma e o conteúdo da comunicação à ANPD e aos titulares, quando aplicável
 - Motivos da ausência de comunicação, conforme o caso



Américas | Asia | Europa | Oriente Médio

O objetivo deste material é meramente informativo, não representando opinião legal para qualquer negócio ou caso específico.