b/luz

ANÁLISE-RESUMO

Regulamento de Comunicação de Incidente de Segurança

No dia 26 de abril, foi publicada a Resolução CD/ANPD nº 15, de 24 de abril de 2024, que estabelece as **regras para a comunicação de incidentes de segurança envolvendo dados pessoais** à ANPD e aos titulares. A resolução prevê aspectos relacionados ao prazo de notificação, estabelece aspectos processuais e providências para a salvaguarda dos direitos dos titulares.

O QUE É CONSIDERADO UM INCIDENTE?

A ANPD define incidente de segurança como um evento adverso que comprometa a **confidencialidade, integridade, disponibilidade e autenticidade da segurança** de dados pessoais, podendo decorrer de ações voluntárias ou acidentais que resultem na divulgação, difusão, alteração, perdas indevidas ou acessos não autorizados a dados pessoais, independentemente do meio em que estão armazenados. Exemplos:

- Envio de informações para o destinatário incorreto
- Furto de um dispositivo de armazenamento de dados
- Invasão de um sistema de armazenamento de informações

QUANDO OS INCIDENTES DEVEM SER COMUNICADOS?

Capítulo III Seção I

Devem ser comunicados à ANPD e aos titulares os incidentes de segurança com dados pessoais que tiverem as seguintes características:

Causar risco ou danos relevantes aos titulares

Entendido como aqueles que têm o potencial de **afetar significativamente interesses e direitos fundamentais dos titulares** ao:

- impedir o exercício de direitos ou a utilização de um serviço

ou

- ocasionar danos materiais ou morais aos titulares

ex: discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

+

Envolver pelo menos um dos seguintes critérios

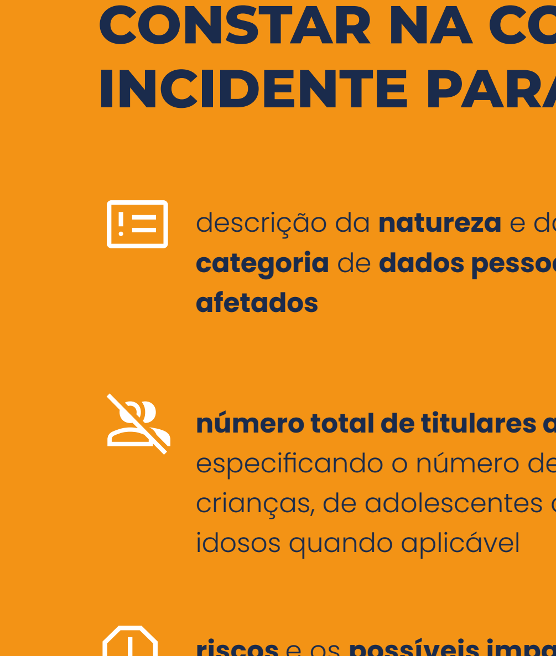
- Dados pessoais sensíveis
- Dados financeiros
- Dados em larga escala

  obs: deve abranger número significativo de titulares, considerando, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica de localização dos titulares.
- Dados de crianças e adolescentes ou idosos
- Dados de autenticação em sistemas
- Dados protegidos por sigilo legal, judicial ou profissional

QUEM É O RESPONSÁVEL PELA COMUNICAÇÃO?

O CONTROLADOR DOS DADOS PESSOAIS

É responsável pela comunicação do incidente de segurança envolvendo dados pessoais tanto para o titular quanto para a ANPD.



QUAL O PRAZO DE COMUNICAÇÃO?

3 dias úteis

obs.: outros prazos também podem ser aplicados conforme previsto em legislação específica.

Para realizar a comunicação à ANPD e/ou aos titulares, contados a partir do conhecimento pelo controlador de que o incidente afetou dados pessoais.

! Para os **agentes de tratamento de pequeno porte** o prazo de comunicação é contado em dobro

As informações poderão ser complementadas, de maneira fundamentada, no prazo de 20 dias úteis, a contar da data da comunicação.

QUAIS INFORMAÇÕES DEVERÃO CONSTAR NA COMUNICAÇÃO DO INCIDENTE PARA A ANPD?

- descrição da **natureza** e da **categoria** de **dados pessoais afetados**
- **número total de titulares afetados**, especificando o número de crianças, de adolescentes ou de idosos quando aplicável
- **riscos** e os **possíveis impactos** aos titulares
- os motivos da demora, no caso de a **comunicação não ter sido realizada no prazo previsto**
- o **número total** de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente
- **medidas técnicas e de segurança** adotadas ou que serão adotadas para **reverter ou mitigar os efeitos do incidente,** observados os segredos comerciais e industriais
- **dados do encarregado** ou de quem represente o controlador
- **a identificação do controlador** e, se for o caso, declaração de que se trata de agente de tratamento de pequeno porte
- informações sobre o **operador**, se houver
- **descrição do incidente**, incluindo a causa principal, caso seja possível identificá-la
- a **data da ocorrência** do incidente, quando possível determiná-la, e a de seu **conhecimento** pelo controlador

QUAIS INFORMAÇÕES DEVERÃO CONSTAR NA COMUNICAÇÃO DO INCIDENTE PARA OS TITULARES?

- **descrição da natureza e da categoria de dados pessoais afetados**
- **riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares**
- **medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, se houver**
- **data do conhecimento do incidente de segurança**
- **contato para obtenção de informações e dados do encarregado, se houver**
- **os motivos da demora, no caso de a comunicação não ter sido feita no prazo previsto**
- **as medidas técnicas e de segurança adotadas para a proteção dos dados, observados os segredos comercial e industrial**

É necessário que a comunicação do incidente para os titulares siga os seguintes critérios:

Uso de linguagem simples e de fácil entendimento

Ocorrer de forma direta e individualizada

pode ser realizada pelos meios usualmente utilizados pelo controlador para contatar o titular, como telefone, e-mail, mensagem eletrônica ou carta.

? E caso não seja possível conduzir a comunicação direta e individualizada para os titulares?

O controlador deverá comunicar o incidente pelos meios de divulgação disponíveis, como no seu sítio eletrônico, aplicativos, suas mídias sociais e canais de atendimento ao titular. A comunicação deverá ser de fácil visualização e ficar disponibilizada pelo período de, no mínimo, três meses.

O controlador deverá juntar ao processo de comunicação de incidente uma declaração de que foi realizada a comunicação aos titulares, constando os meios de comunicação ou divulgação utilizados, em até 3 dias úteis, contados do término do prazo de comunicação ao titular.

O QUE FAZER SE NÃO FOR NECESSÁRIO COMUNICAR O INCIDENTE?

O controlador deverá manter o registro de incidentes de segurança, inclusive daqueles não comunicados à ANPD e aos titulares, pelo prazo mínimo de cinco anos, contados a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

O QUE ACONTECE COM OS INCIDENTES NÃO COMUNICADOS PELO CONTROLADOR QUE A ANPD VENHA A TOMAR CONHECIMENTO?

Caso o incidente possa ocasionar risco ou dano relevante aos titulares, e o controlador não tenha comunicado o incidente, a Autoridade poderá, de ofício, investigar a situação por meio do procedimento de apuração de incidente de segurança.

SANÇÕES

A ANPD poderá fixar multa diária para assegurar a adoção imediata pelo controlador de medidas preventivas necessárias para salvaguardar direitos dos titulares, a fim de prevenir, mitigar ou reverter os efeitos do incidente e evitar a ocorrência de dano grave e irreparável ou de difícil reparação.

O limite da multa diária a ser estabelecida pela ANPD é de **R$ 50.000.000,00 (cinquenta milhões de reais)** conforme disposto no Regulamento de Dosimetria e Aplicação de Sanções Administrativas.

A ANPD poderá instaurar processo administrativo sancionador para apurar o descumprimento da obrigação de comunicação do incidente de segurança, podendo resultar na aplicação das demais sanções previstas na legislação.

APÓS A COMUNICAÇÃO, QUAL SERÁ O PROCEDIMENTO SEGUIDO PELA ANPD?

1 Recebimento da comunicação do incidente pela ANPD

2 Realização de auditorias ou inspeções

A ANPD poderá, **a qualquer momento**, determinar ou realizar auditorias ou inspeções junto aos agentes de tratamento para coletar informações complementares ou validar as informações recebidas.

3 Avaliação da gravidade do incidente

Com as informações fornecidas pelo controlador ou coletadas durante as auditorias e inspeções, a ANPD avaliará a gravidade do incidente.

4 Determinação de providência de salvaguardas

Avaliada a gravidade do incidente, a ANPD poderá determinar ao controlador:

Ampla divulgação do incidente	Medidas de mitigação
Em meios físicos ou digitais, sempre considerando a necessidade de alcançar o maior número possível de titulares afetados, podendo incluir mídia escrita impressa, radiodifusão ou transmissão de informações pela Internet. quando a comunicação realizada pelo controlador se mostrar insuficiente para alcançar os titulares afetados.	Que garantam a confidencialidade, a integridade, a disponibilidade e a autenticidade dos dados pessoais afetados, bem como medidas capazes de minimizar os efeitos do incidente para os titulares de dados.

DIVULGAÇÃO NO SITE DA ANPD

A ANPD poderá divulgar, em seu sítio eletrônico, informações estatísticas agregadas relativas aos incidentes de segurança.

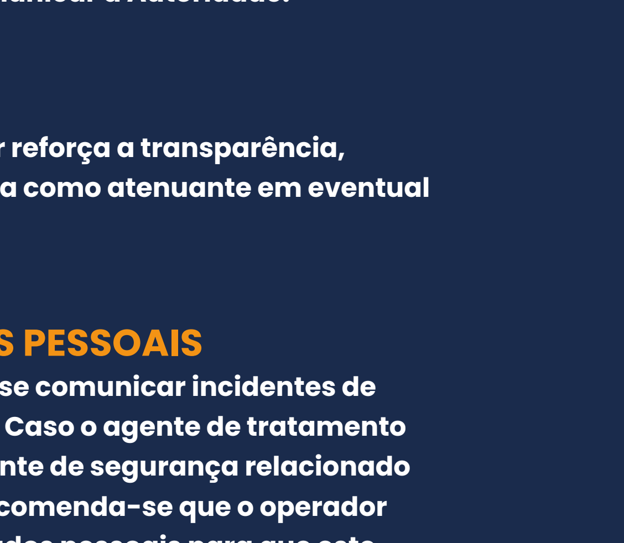
5 Instauração de processo administrativo sancionador

Caso o controlador não adote as medidas solicitadas, a ANPD poderá instaurar processo administrativo sancionador, podendo resultar na aplicação de multas e outras sanções descritas na lei.

6 Fim do processo de comunicação de incidente

Ocorrerá a extinção do processo de comunicação de incidente de segurança, caso:

1) não sejam identificadas evidências suficientes da ocorrência do incidente;
2) a ANPD considere que o incidente não possui potencial para acarretar risco ou dano relevante aos titulares;
3) o incidente não envolva dados pessoais;
4) tenham sido tomadas todas as medidas adicionais para mitigação ou reversão dos efeitos gerados; ou
5) haja a realização da comunicação aos titulares e adoção das providências pertinentes pelo controlador



PONTOS IMPORTANTES SOBRE A COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA

NEM TODO INCIDENTE DEVE SER COMUNICADO À ANPD

Existe a obrigação legal de comunicar à ANPD apenas os incidentes que possam causar riscos ou danos relevantes aos titulares. É papel do controlador dos dados pessoais realizar uma avaliação cuidadosa sobre os riscos e impactos aos titulares decorrentes do incidente, verificando se existe a necessidade de comunicar a Autoridade.

INDICAÇÃO DE BOA-FÉ

A comunicação voluntária do incidente pelo controlador reforça a transparência, cooperação e boa-fé do agente e poderá ser considerada como atenuante em eventual ação fiscalizatória da ANPD.

CASO ATUE COMO OPERADOR DOS DADOS PESSOAIS

O artigo 48 da LGPD determina que a obrigação legal de se comunicar incidentes de segurança à ANPD é do controlador dos dados pessoais. Caso o agente de tratamento atue como operador e tome conhecimento de um incidente de segurança relacionado aos dados tratados sob as ordens de um controlador, recomenda-se que o operador envie as informações necessárias ao controlador dos dados pessoais para que este, caso deseje, realize a devida comunicação.

b/luz