RESOLUÇÃO IBA Nº 07/2020

Publicada em 24 de julho de 2020

Dispõe sobre a criação do Pronunciamento Atuarial CPA-O Nº 018 – LGPD.

O **INSTITUTO BRASILEIRO DE ATUÁRIA - IBA**, no exercício de suas atribuições legais e regimentais,

CONSIDERANDO o desenvolvimento da profissão atuarial no Brasil e a maior abrangência de atuação do profissional atuário em suas atividades técnicas,

CONSIDERANDO a necessidade de prover fundamentação apropriada para interpretação e aplicação do disposto na legislação vigente,

RESOLVE:

Art. 1º - Nos termos do artigo 1º do Decreto-Lei nº 806, de 04.09.1969, que dispõe sobre o exercício da profissão de atuário e regulamentação estabelecida pelo Decreto nº 66.408, de 03.04.1970, esta resolução tem por objetivo apresentar procedimentos e diretrizes aos trabalhos referente a Lei Geral de Proteção de Dados.

Art. 2º - O CPA-O 018 é parte anexa desta Resolução e poderá ser alterado com o objetivo de adaptar-se à evolução do trabalho do atuário e/ou de sua atividade profissional, em conformidade com as normas emanadas pelo IBA a respeito.

Art. 3º - Esta Resolução entra em vigor na data da sua publicação.

Rio de Janeiro, 24 de julho de 2020.

LETICIA DE OLIVEIRA DOHERTY
Presidente do Instituto Brasileiro de Atuária

COMITÊ DE PRONUNCIAMENTOS ATUARIAIS (CPA-O)
ORIENTAÇÃO

CPA-O Nº 018 – Lei de Proteção de Dados

(Versão Agosto de 2019)

Sede-RuadaAssembleia,10-S/1304-5-RiodeJaneiro-RJ-Cep.:20011-901
Tel.:+5521 2531-0267/+5521 2531-2865
www.atuarios.org.br

I. INTRODUÇÃO

1. O presente Pronunciamento Técnico destina-se a divulgar sugestões e procedimentos a serem adotados com base na Lei Geral de Proteção de Dados do Brasil - LGPD, cujo conteúdo deve ser observado por todos atuários que exercem a atividade no Brasil ou tratam dados pessoais, mesmo fora do país quando a atividade de tratamento tenha por objetivo a oferta ou fornecimento de bens ou serviços.

2. O presente documento foi desenvolvido com base nos conceitos e definições mínimas acerca do tema LGPD - Lei 13.709/2018 / MP 869/2018 e suas modificações, que tem início de vigência prevista para agosto de 2020.

II. OBJETIVO

3. O objetivo deste Pronunciamento é orientar aos atuários que trabalham com dados relacionados à pessoa natural identificada ou identificável e tem como propósito final proteger as empresas de atuária e atuários contra possíveis penalizações por conta do manuseio incorreto ou vazamento dos dados pessoais.

III. DEFINIÇÕES E COMPETÊNCIAS

4. **Lei Federal 13.709/2018:** É a Lei Geral de Proteção de Dados, é o marco regulador da proteção e transferência de dados pessoais no Brasil, abreviada como LGPD nesse documento.

5. **MP 869/2018**: É a Medida Provisória 869, que altera a Lei 13.709, cria a Agência Nacional de Proteção de Dados e dá outras providências.

6. **Autoridade Nacional de Proteção de Dados (ANPD):** será responsável por garantir o cumprimento da lei, editar normas e procedimentos complementares, aplicar sanções, dentre outras competências que ajudam a sociedade a manter a ética e o compromisso com a segurança de dados.

7. **Dado Pessoal**: corresponde à informação relacionada à pessoa natural identificada ou identificável.

8. **Dado de pessoa identificável**: dados que ao serem tratados, com sua combinação, permitam identificar pessoa natural.

9. **Dados Pessoais Sensíveis**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

10. **Tratamento de Dados Pessoais:** todo ato abaixo relacionado, quando relacionar-se a um dado pessoal, é considerado tratamento de dados pessoais:

a) Produção;
b) Acesso;
c) Coleta;
d) Extração;
e) Recepção;
f) Reprodução;
g) Distribuição;
h) Difusão;
i) Classificação;
j) Processamento;
k) Avaliação;
l) Utilização;
m) Transmissão;
n) Modificação;
o) Arquivamento;
p) Armazenamento;
q) Controle da Informação;
r) Eliminação;
s) Comunicação;
t) Transferência.

11. **Banco de Dados**: conjunto estruturado de dados pessoais, localizado em um ou vários locais, por meio de suporte eletrônico ou físico.

12. **Titular**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

13. **Agentes de tratamento:** são as pessoas ou empresas que desempenham o papel de **controlador** e **operador**.

14. **Controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

15. **Operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

16. **Encarregado:** é o profissional responsável pelo tratamento de dados pessoais e deve ser indicado pelo controlador. O encarregado representa o canal de comunicação entre o controlador, titulares de dados e ANPD.

17. **Anonimização:** corresponde a um processo realizado sobre dados pessoais que transforma o dado em formato e conteúdo que não possa ser identificado por meio de técnicas razoáveis e disponíveis na ocasião de seu tratamento.

18. **Pseudonimização**: perde possibilidade de associação direta ou indireta, senão

mediante informação adicional, mantida separadamente pelo controlador, em ambiente seguro e controlado.

19. **Bloqueio de dado pessoal:** ocorre quando há suspensão temporária de tratamento.

20. **Término do tratamento de dados:** ocorre quando é atingido uma das condições a seguir:

a) Finalidade alcançada ou os dados deixaram de ser necessários (ex. contrato venceu);
b) Fim do período de tratamento (ex. fim do prazo prescricional);
c) Revogação de consentimento, a não ser que por interesse público tenha que ser mantida a informação (ex. o titular do dado contratou seguro, mas a seguradora tem a obrigação legal de armazenar informações por período maior. Essa combinação faz com que se mantenha o dado por mais tempo);
d) Por determinação da ANPD.

21. **Eliminação de dado pessoal:** é necessária quando do término do tratamento de dados e deve respeitar os seguintes critérios:

a) Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
b) Não passível de recuperação;
c) Excetua-se a necessidade de eliminação de dados quando houver:
- Cumprimento de obrigação legal ou regulatória;
- Estudo por órgão de pesquisa, desde que de forma anonimizada;
-Transferência a terceiro, respeitados os requisitos de tratamentos de dados dispostos na Lei da LGPD; ou
- Uso exclusivo do controlador com dados anonimizados (veda acesso por terceiros).

22. **Consentimento:** ocorre quando há concordância do titular dos dados com o tratamento de dados para finalidade determinada e é considerado legítimo quando ocorrer por meio de manifestação livre, informada de forma clara e inequívoca:

a) Se por escrito, deverá ser por cláusula destacada das demais;
b) O ônus da prova de consentimento recai sobre o controlador;
c) Deve ser passível de revogação a qualquer tempo (forma gratuita e facilitada);
d) Aplica-se a uma finalidade determinada;
e) Não deve haver vício de consentimento, autorização genérica, conteúdo enganoso ou abusivo ou ainda ausência de transparência na comunicação.

23. **Princípios:**

a) Boa fé;
b) Finalidade e adequação: propósito legítimo, explícito, informado ao titular;
c) Necessidade: mínimo necessário para a finalidade, não excessivo;
d) Livre acesso e transparência consulta facilitada e gratuita sobre:

- Forma e duração do tratamento;
- Integralidade dos dados pessoais;
- Agentes de tratamento (segredo comercial e industrial).

e) Qualidade dos Dados: exatidão e clareza, relevância e atualização de dados;
f) Não discriminação;
g) Segurança e Prevenção:

- Proteger os dados de acessos não autorizados;
- Prevenir a ocorrência de danos em razão do tratamento.

24. **Livre Acesso:** garantia de consulta facilitada e gratuita sobre a forma e a duração do tratamento, garantindo a integralidade dos dados pessoais do titular, tendo em observância os segredos comercial e industrial.

25. **Transparência:** garantia ao titular de informações claras e precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

26.**Órgão de Pesquisa** trata-se de:

a) Órgão ou entidade da Administração Pública direta ou indireta; ou
b) Pessoa jurídica de direito privado sem fins lucrativos, com sede no país, que inclua em sua missão institucional pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

27. **Estudos de Saúde Pública terão finalidade legitimada:**

a) Acesso a Base de dados pessoais;
b) Dados pessoais serão analisados exclusivamente dentro do órgão;
c) Finalidade estrita para realização de estudos e pesquisas;
d) Mantidos em ambiente controlado e seguro;
e) Práticas de segurança previstas em regulamento específico;
f) Respeitados padrões éticos;
g) Anonimizados ou pseudonimizados (única situação em que dados pseudonimizados são admitidos na LGPD).

28. **Autodeterminação informativa:** direito do titular dos dados ter acesso a:

a) Confirmação da existência de tratamento;
b) Acesso aos seus dados pessoais;
c) Correção de dados incompletos, inexatos ou desatualizados;
d) Portabilidade, por requisição do titular;
e) Requerer a eliminação do dado pessoal, quando oferecido mediante consentimento;
f) Relação de entidades públicas com as quais os dados foram compartilhados;
g) Revogação de consentimento.

IV. ABRANGÊNCIA

29. Todos atuários independentes e atuários responsáveis técnicos das Sociedades que exercem a atividade atuarial no Brasil, ou ainda recebem e têm acesso a dados nacionais,

podendo ser:

a) Seguros, resseguros, previdência aberta, previdência fechada, inclusive regimes próprios, previdência social, capitalização ou saúde suplementar;

b) Sociedades e entidades que operam seguros, resseguros, previdência aberta, previdência fechada, inclusive regimes próprios, previdência social, capitalização ou saúde suplementar.

30. A transferência de dados para outros países ou organismos é permitida, desde que proporcione a mesma proteção da Lei brasileira, sendo de responsabilidade do controlador essa garantia. Cabe ao atuário se certificar do cumprimento de todos requisitos da LGPD quando ele estiver envolvido em transferência de dados para outros países.

V. RESPONSABILIDADE

31. Relacionamos a seguir as principais responsabilidades dos agentes de tratamento e encarregado:

32**. Controlador**

a) Indicar e divulgar publicamente, encarregado pelo tratamento de dados;
Manter registro das operações de tratamento;
b) Indicar razões que impedem adoção de imediata providência em demanda relacionada aos direitos do titular;
c) Informar a pedido do titular, os critérios e os procedimentos utilizados para a decisão automatizada;
d) Informar os agentes de tratamento quando houver: correção, eliminação, anonimização ou bloqueio de dados, para que esses repitam o procedimento;
e) Confirmar a existência ou acesso a dados pessoais do titular em formato simplificado e de forma imediata;
f) Comunicar a ANPD e o titular de eventual ocorrência de incidente de segurança que possa acarretar risco ou dano ao titular;
g) Desenvolver relatório de impacto a proteção de dados pessoais referente ao tratamento de dados.

33. Os controladores respondem solidariamente quando estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados. Nessas situações caberá ao controlador assegurar indenização ao titular, na medida da sua participação no dano causado.

34. **Operador**

a) Respeitar instruções lícitas do controlador;
b) Manter registro das operações de tratamento.

35. O operador responde solidariamente pelos danos causados no tratamento de dados quando descumprir as obrigações da LGPD ou quando não tiver seguido as instruções lícitas do controlador, equiparando-se ao controlador. Nessas situações caberá ao operador assegurar indenização ao titular, na medida de sua participação no dano causado.

36. Encarregado

a) Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
b) Receber comunicações da ANPD e adotar providências;
c) Orientar funcionários e contratados pela entidade;
d) Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

VI. PROCEDIMENTOS GERAIS DE PROTEÇÃO

37. É necessário que as organizações e atuários autônomos implantem um conjunto de medidas internas no qual todas as áreas estejam ligadas com objetivo de atender a nova legislação.

38. Isso determina uma atualização nas políticas de governança corporativa e alteração nas regras de "compliance", incorporando padrões de segurança e mecanismos de proteção de dados.

39. É necessário rever o ciclo completo de vida dos dados dentro das organizações, a forma de recebimento, manuseio, tratamento, armazenamento, compartilhamento e exclusão.

40. Inclusive a exclusão dos dados armazenados após o término dos trabalhos, assim como eliminação de dados obtidos anteriormente à vigência da LGPD.

41. Será necessário indicar um profissional responsável, denominado encarregado, para servir de canal de comunicação entre o público/usuários e a instituição, assim como, futuramente, com a autoridade reguladora e fiscalizadora.

42. Merece destaque que todos os dados anonimizados estão fora do alcance da LGPD, logo, sem prejudicar o resultado dos cálculos atuariais, é recomendado que a área receptora dos dados colha as informações mantendo os dados anonimizados, o tanto quanto possível. Lembrando que, quando o dado é individualizado, porém a combinação de mais de um campo do conjunto de dados permita identificar a pessoa natural, então esses dados não são considerados anonimizados, mas sim pseudonimizados.

43. Portanto, todo e qualquer dado solicitado tem que ter uma finalidade específica ou atender a uma das bases legais previstas na LGPD, não podendo haver casualidade na solicitação que poderá ser questionada pelo titular ou pela ANPD, com eventual

penalização pelo descumprimento da Lei.

VII. BOAS PRÁTICAS DO MANUSEIO DOS DADOS

44. Destacamos a seguir, algumas boas práticas a serem seguidas com o objetivo de mitigar a utilização inadequada, vazamento dos dados e penalização.

Sempre que possível receber os dados anonimizados

45. A anonimização ou ainda pseudonimização, quando possível, deverá ser determinada nas regras de "compliance" envolvendo as áreas jurídica, técnica e comercial. A implantação deverá ter como objetivo determinar que os dados devam ser solicitados sem as características que identifiquem o indivíduo e, quando necessário, apenas uma área designada dentro da empresa deverá ser responsável pelo recebimento e anonimização.

Limitar o acesso à base de dados

46. Definir regras de acesso à base de dados e, quando possível, ocultar as informações sensíveis e que definem a característica do titular do dado, inclusive limitando o acesso remoto aos dados e/ou fora do horário comercial.

Identificar os dados sensíveis e os dados críticos

47. Realizar o mapeamento e análise de risco com objetivo de evitar ataque e vazamento dos dados e definir plano de ação em caso de eventual vazamento. Sendo necessário, determinar o que cada área poderá e deverá acessar, inclusive identificando os dados sensíveis destacados na LGPD.

Utilização Consciente das Bases

48. As bases deverão ser utilizadas no escopo de legitimidade previsto na LGPD ou mediante anonimização para testes e estudos não contratados ou ainda, ter autorização do titular de dados, mitigando o vazamento de informação.

Monitorar os acessos às Base de Dados

49. Registrar, monitorar e bloquear o acesso à base de dados, sendo necessário o monitoramento do ciclo de vida dos dados, da recepção até a exclusão dos dados, no qual será obrigatório o registro de todo acesso às bases e comprovação da exclusão dos dados.

Revisão dos Contratos e Documentos

50. A Revisão dos contratos e documentos é um dos itens importantes destacados na LGPD. É necessário enquadrá-los atendendo às normas de confidencialidade e transparência. Com base na LGPD é necessário deixar claro para quais finalidades os dados pessoais serão utilizados, assim como o tratamento e duração da utilização. O compartilhamento ou utilização após o contrato fica proibido e só poderá ser utilizado conforme as exceções do parágrafo 21.

Eliminação de Dados Pessoais

51. Estabelecer procedimentos relacionados a eliminação dos dados, assim que o objetivo de seu tratamento for atingido, mantendo comprovação da eliminação dos dados.

Importante destacar que, a base de dados não se limita ao registro eletrônico, é extensiva ao registro físico, se houver. Logo, é primordial conhecer a extensão desta base e estabelecer procedimento para cada tipo de registro.

Relatório de Impacto à Proteção de Dados Pessoais

52. Ao atuário, seja ele controlador ou operador de dados pessoais, é recomendado participar da revisão ou elaboração desse documento, interagindo com o encarregado responsável indicando com precisão os dados necessários para o desempenho de suas funções e tarefas, com a respectiva justificativa para cada dado tratado.

VIII. EXCEÇÕES PARA UTILIZAÇÃO E MANUTENÇÃO DOS DADOS

Tratamento dos dados

53. Os dados somente poderão ser tratados para cumprimento de contrato de prestação de serviços, que deu origem a coleta ou poderão ser utilizados para:

a) Estudos por órgão de pesquisa, exigida anonimização;
b) Processo Judicial ou administrativo;
c) Proteção à vida ou incolumidade física;
d) Tutela da saúde, por profissionais da saúde;
e) Proteção ao crédito;
f) Prevenção à fraude e segurança do titular;
g) Independentemente de consentimento, observada isenção quando cedidos pelo controlador por obrigação legal ou tratamento compartilhado de dados pela administração pública, o órgão deve dar publicidade da dispensa de consentimento.
h) Também independe de consentimento:

- No caso de “exercício regular de direitos”;
- Para a proteção da vida ou da incolumidade física do titular.

Conservação dos Dados

54. Com o término do tratamento haverá eliminação dos dados das bases de dados, autorizada a conservação de dados para os seguintes casos:

a) Cumprimento de obrigação legal ou regulatória pelo controlador;
b) Estudo por órgãos de pesquisa;
c) Transferência a terceiro, porém tem que haver uma situação que justifique a transferência de dados a terceiro (ex.: contrato terminou, mas tem que fazer a portabilidade de dados para outro);
d) Uso exclusivo do controlador, desde que anonimizados.

IX. DADOS SENSÍVEIS DE CRIANÇAS E ADOLESCENTES

Dados Sensíveis

55. Para tratamento de dados sensíveis, relacionados à criança ou adolescente, é

necessário consentimento do pais ou seu responsável legal, de forma específica e destacada, para finalidades específicas, logo é de extrema importância um tratamento diferenciado para esse tipo de dado.

Dados Pessoais de Criança

56. O acesso a dados relativos a criança está sujeito a normas específicas:

a) Depende de consentimento específico;
b) Certificar-se que o consentimento é originado dos pais/responsável legal;
c) Exceção: se a finalidade for contatar os pais ou responsável legal uma única vez;
d) Informações disponíveis de forma acessível de acordo com condições físico motora, perceptivas, sensoriais, intelectuais e mentais do usuário.

X. PENALIZAÇÃO

57. A aplicação das sanções compete exclusivamente à ANPD, que articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais, e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. As penalidades poderão ser de multa por incidente de até 2% do faturamento do último exercício do grupo econômico ao qual a empresa faz parte, limitado a R$ 50 milhões, além de outras sanções administrativas, civis e penais aplicadas pela **ANPD**. Não se aplicam esses limites à reparação de danos.

XI. CONCLUSÃO

58. Há de se destacar que este trabalho é uma orientação para a comunidade atuarial e que outros procedimentos podem ser aplicados com objetivo de proteger e tratar os dados pessoais.

59. O Trabalho foi baseado na **Lei Federal 13.709/2018 e na MP 869/2018** que foi interpretada pelos membros deste comitê, porém cabe à ANPD editar normas e procedimentos sobre a proteção de dados pessoais e deliberar, na esfera administrativa, sobre a interpretação da Lei 13.709/2018.