



▶ BOAS PRÁTICAS E GOVERNANÇA EM PROTEÇÃO DE DADOS

NORMA REGULAMENTADORA SETORIAL

ABEETRANS

ASSOCIAÇÃO BRASILEIRA
DAS EMPRESAS DE ENGENHARIA
DE TRÂNSITO



Considerando a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018);

Considerando que esta nova legislação impacta as atividades de todas as associadas da **ABEETRANS**;

Considerando que o art. 50 da Lei nº 13.709/2018, permite que associações formulem regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais;

Considerando que os associados da **ABEETRANS** poderão ser considerados agentes de tratamento de dados, na forma de legislação incidente;

A **ABEETRANS** resolver editar a presente norma, para auxiliar seus associados na implantação de seus programas de proteção de dados pessoais (compliance), na forma da legislação em vigor.

Art. 1º. Esta norma estabelece recomendações sobre o tratamento de dados pessoais, as boas práticas de segurança de dados e de governança a todos os associados da **ABEE-TRANS**, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

§1º Esta norma não substitui a legislação e jurisprudência brasileira a respeito da proteção de dados pessoais.

§2º Os associados da ABEETRANS, a partir desta norma e da legislação incidente, deverão criar e implementar seus programas de proteção de dados, que deverão considerar as peculiaridades de suas atividades.

Art. 2º. A presente norma tem como fundamentos:

- I. o respeito à privacidade;
- II. a autodeterminação informativa;
- III. a boa-fé;
- IV. a transparência;
- V. o tratamento de dados de acordo com a finalidade e necessidade previamente anunciadas;
- VI. a proteção de dados obtidos dentro e fora do ambiente on-line (internet);
- VII. a qualidade dos dados;
- VIII. a segurança das informações;
- IX. a prevenção de incidentes de privacidade;
- X. a defesa do consumidor e colaborador;
- XI. a não discriminação do titular de dados.



Art. 3º. Para fins desta norma, tal como estabelece a Lei nº 13.709/2018, considera-se:

- I. **agentes de tratamento:** o controlador e operador;
- II. **controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- III. **dado pessoal:** informação relacionada a pessoa natural identificada ou identificável;
- IV. **dado pessoal sensível:** 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; imagens capturadas pelas câmeras/radares operados pela empresa e geolocalização contemplados nas multas.
- V. **compartilhamento de dados:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
- VI. **consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- VII. **encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- VIII. **operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- IX. **titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;



X. **tratamento de dados**: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Art. 4º. O tratamento de dados pessoais pelos associados se dará nas hipóteses previstas no artigo 7º da Lei 13.709/18, em especial:

- I. mediante o fornecimento de consentimento pelo titular;
- II. para o cumprimento de obrigação legal ou regulatória pelo controlador;
- III. quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- IV. para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
- V. para a proteção da vida ou da incolumidade física do titular ou de terceiros;
- VI. quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
- VII. quando o associado receber ou obter dados decorrentes da execução de contrato administrativo celebrado com o Poder Público (art. 26, §1º, IV, Lei nº 13.709/2018).

Parágrafo único.: Sempre que o associado obtiver dados do titular mediante consentimento, deverá considerar:

- I. o consentimento deve ser livre, informado, expresso, prévio, por escrito ou por outro meio eletrônico comprovável;
- II. o silêncio não pode ser considerado consentimento;
- III. o consentimento deverá referir-se a finalidades determinadas e as autorizações genéricas para o tratamento de dados pessoais serão nulas.



Art. 5º. São direitos dos titulares de dados e que devem ser integralmente respeitados pelos associados na condição de agentes de tratamento:

- I. direito à informação: confirmação da existência de tratamento e acesso aos dados pessoais
- II. direito à portabilidade dos dados a outro fornecedor de serviço ou produto.
- III. direito à obtenção de informação das instituições, públicas e privadas, com as quais o controlador realizou o uso compartilhado de dados;
- IV. direito à correção de dados incompletos, desatualizados e inexatos;
- V. direito à informação sobre a possibilidade de não fornecer consentimento;
- VI. direito à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados ilicitamente;
- VII. direito à revogação do consentimento;
- VIII. direito a apresentar reclamação à Autoridade Nacional de Proteção de Dados (ANPD);
- IX. direito à eliminação dos dados pessoais
- X. direito à oposição ao tratamento de dados, se irregular.

Parágrafo único.: Os associados deverão criar canais de comunicação próprios (v.g.: e-mail, telefone, whatsapp) para receber as reclamações e pedidos dos titulares de dados.

Art. 6º. Os associados que se enquadrarem como agentes de tratamento de dados possuem as seguintes obrigações:

I. Obrigações do associado controlador:

- a) provar que obteve consentimento do titular de dados;
- b) manter registro das operações de tratamento de dados;
- c) emitir relatório de impacto à proteção de dados;
- d) informar o titular de dados se houver alteração da finalidade da coleta de dados;
- e) responder solidariamente com o operador;
- f) confirmar a existência e permitir o acesso a dados pessoais de seu titular;
- g) indicar a metodologia da coleta de dados;
- h) indicar como garante a segurança das informações;
- i) indicar publicamente a identidade do encarregado pelo tratamento de dados pessoais;
- j) comunicar a Autoridade Nacional de Proteção de Dados (ANPD) em caso de incidente de segurança;
- k) Manter o sigilo dos dados obtidos.

II. Obrigações do associado operador:

- a) cumprir todas as determinações da Lei nº 13.709/2018;
- b) seguir estritamente as ordens lícitas do controlador;
- c) responder solidariamente com o controlador.

III. Obrigações do encarregado:

- a) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adota providências;
- b) receber comunicações dos titulares, prestar esclarecimentos e adotar providências;
- c) orientar funcionários e os contratados do associado a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- d) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares;
- e) intermediar o contato com a Autoridade Nacional de Proteção de Dados.



Art. 7º. Os associados devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de coleta, destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Art. 8º. Para a adequada adesão do associado à Lei nº 13.709/18, será preciso realizar um diagnóstico inicial e adotar medidas jurídicas, administrativas e tecnológicas.

§1º O diagnóstico deverá conter, pelo menos, os seguintes pontos:

- I. classificação jurídica dos dados coletados;
- II. duração da manutenção dos dados (ciclo de vida);
- III. avaliação da finalidade do uso de dados coletados ou obtidos;
- IV. avaliação da política de proteção de dados de terceiros;
- V. avaliação do controle de gestão de consentimentos;
- VI. elaboração de mapa de riscos.

§2º Após o diagnóstico, as medidas mínimas a serem implementadas pelos associados são as seguintes:

- I. elaboração de políticas internas de segurança e governança de dados, com a participação efetiva da alta diretoria;
- II. elaboração de política de privacidade disponibilizada ao titular de dados, em seu sítio na internet;
- III. implantação de mecanismos de supervisão internos e externos;

- IV. imposição de termos de privacidade e sigilo aos colaboradores que tenham acesso a dados;
- V. treinamento periódico de equipe para mudança na cultura de proteção de dados dentro da empresa, com a adoção de ações educativas;
- VI. avaliar e adequar todos os contratos em que há compartilhamento de dados pessoais;
- VII. estabelecer medidas de segurança de dados de Recursos Humanos;
- VIII. estabelecer controle de acessos físicos e digitais a dados da empresa, colaboradores e de terceiros;
- IX. implementar a segurança física dos ambientes e cibersegurança;
- X. avaliar e implementar a segurança de suas operações à luz da Lei de Proteção de Dados;
- XI. avaliar e implementar a segurança de suas comunicações à luz da Lei de Proteção de Dados;
- XII. estabelecer plano de gestão de incidentes de segurança da informação;
- XIII. indicar o seu Encarregado de Dados.

§3º. As medidas a serem adotadas, sempre com o auxílio de profissionais especializados, deverão levar em conta o porte do associado, a natureza e sensibilidade dos dados coletados e tratados, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios de tratamento de dados do titular.

§4º. Caso a associada colete dados de terceiros pela internet, deverá ater-se às peculiaridades de segurança próprias do ambiente virtual.

Art. 9º. Todas as medidas adotadas pelos associados para se adequar à legislação de proteção de dados deverá ser devidamente documentada (atas, lista de presença, vídeos, etc.), sob pena das autoridades competentes não as considerar válidas.

Art. 10. Esta norma deverá ser anualmente revisada e suas alterações serão comunicadas a cada associado.

Art. 11. Esta norma entra em vigor no dia 01/04/2021.



