MANUAL LGPD – Lei Geral de proteção de dados

1. Apresentação.

A Lei Geral de Proteção de Dados Pessoais é a legislação brasileira que regula as atividades de tratamento de dados pessoais, que alterou os artigos 7º e 16 do Marco Civil da Internet e iniciou a sua vigência em 18/09/2020. A LGPD estabelece regras sobre o tratamento de dados pessoais, com objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural, impondo mais proteção aos dados pessoais e penalidades pelo seu descumprimento

2. Principais Conceitos

- Autoridade Nacional - Órgão da administração pública responsável por fiscalizar o cumprimento da LGPD no território brasileiro.
- Controlador - Pessoa física, ou entidade do setor público ou privado, que determina a finalidade e a forma de tratamento dos dados pessoais, dentre outros fatores relacionados ao processamento.
- Dados anonimizados - Informações que se referem a pessoas físicas, mas que não podem ser ligados a nenhuma pessoa física específica nem direta, nem indiretamente, considerando-se os meios técnicos disponíveis.
- Dados pessoais - Informações relacionadas a pessoas físicas que podem ser identificadas direta ou indiretamente, por meio de um conjunto de informações.
- Dados pessoais sensíveis - Dentro da categoria de dados pessoais, os dados pessoais sensíveis são exclusivamente as informações relacionadas à 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 vinculadas a uma pessoa física.
- Encarregado - Também chamado de Data Protection Officer (DPO), o Encarregado pela Proteção de Dados é uma pessoa indicada pelo Controlador/Operador para agir como canal de comunicação entre o Controlador e os titulares de dados, e entre o Controlador e a Autoridade Nacional de Proteção de Dados (ANPD). O DPO pode tanto ser interno à organização como externo, em regime de contratação de prestação de serviços (também conhecido como “DPO as a service”).
- Operador - Pessoa física, ou entidade do setor público ou privado, que realiza o tratamento dos dados pessoais em nome do Controlador.
- Tratamento - Toda e qualquer operação com dados pessoais. Alguns exemplos: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
- Titular de dados - Pessoa física a quem os dados se referem.

3. Espécies de Dados Pessoais

Dado Pessoal é toda e qualquer informação que possa levar a identificação, direta ou indireta, de uma pessoa; qualquer dado que possa ser associado a um indivíduo, fazendo com que a aplicação da norma se concentre sobre o poder que este indivíduo tem sobre seus dados.

A definição de dado pessoal pode influenciar no equilíbrio de poder entre o cidadão e aquele que coleta e utiliza os dados, sendo subdivididos nas seguintes categorias:

- Dados Pessoais Comuns: Diretos, ou seja, informações de pessoas físicas identificadas ou identificáveis: nome completo, e-mail, telefone, registro geral (RG), cadastro pessoa física (CPF) e endereço; Indiretos: endereços de IP, geolocalização e identificadores eletrônicos;
- Dados Sensíveis: são dados que merecem especial atenção e cujo tratamento pode ensejar a discriminação de seu titular, ou seja, origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organizações religiosas, filosóficas e políticas, dados sobre saúde, vida sexual, dados genéticos e biométricos.
- Dados Anônimos: são dados que se referem a pessoas que não podem ser identificadas – como dados estatísticos, por exemplo. Um dado anônimo, ainda que seja referente a uma pessoa (ou grupos de pessoas), não permite a identificação do titular, são os denominados dados anonimizados.

4. Princípios gerais para tratamento de dados pessoais

A Lei define que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem tratamento posterior.

Livre acesso: garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento.

Não discriminação: impossibilidade de realização do tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos.

Necessidade: limitação do tratamento ao necessário para a realização de suas finalidades.

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Qualidade dos dados: garantia aos titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Responsabilização e prestação de contas: demonstração pelo agente da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e da eficácia dessas medidas

Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Transparência: garantia aos titulares de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os agentes de tratamento, observados os segredos comercial e industrial.

5. Por Que a segurança da informação é tão importante?

Segurança da Informação é um dos principais desafios dos dias de hoje. No nosso ambiente de trabalho as informações estão expostas a uma variedade de ameaças internas e externas que não existiam há pouco tempo. Estas ameaças podem impactar os clientes do Grupo Cronológica, possibilitar a violação de regulamentos e leis, como a Lei Geral de Proteção de Dados Pessoais (LGPD), e afetar negativamente a reputação e a estabilidade financeira da empresa. A cronológica assume todas as precauções técnicas para se prevenir destas ameaças e conta com o comprometimento dos colaboradores no dia-a-dia de trabalho.

O colaborador da Cronológica é a base para a proteção da empresa e assume um papel importante nessa tarefa, seja por meio do gerenciamento correto das senhas, seja mantendo a segurança de documentos e dados

pessoais, ou ainda atentando-se a quem está solicitando as informações. São práticas importantes tanto quanto todas as proteções técnicas implementadas em nossos sistemas. A maioria dos incidentes de segurança e proteção não são causados por falhas em tecnologia, mas sim por falhas humanas, ou seja, você é a chave para manter a nossa informação protegida.

6. Bases de tratamento de dados pessoais

A Lei Geral de Proteção de Dados prevê que tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I) Consentimento do titular;
II) Cumprimento de obrigação legal ou regulatória pelo regulador;
III) Pela administração pública para execução de política pública;
IV) Realização de estudo por órgão de pesquisa;
V) Quando necessário para execução do contrato;
VI) Exercício regular do direito em processo judicial, administrativo ou arbitral;
VII) Proteção da vida ou incolumidade física do titular ou terceiro;
VIII) Tutela da saúde em procedimento realizado por profissionais de saúde/serviços de saúde/agência sanitária;
IX) 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;
X) Proteção do crédito.

7. Consentimento

O consentimento deverá referir-se a finalidades determinadas e ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado.

8. Direito dos titulares dos dados

- Os titulares poderão solicitar, a qualquer momento:
- Confirmação - Confirmar se existem dados.
- Acesso - Acesso aos dados que são tratados.
- Correção - Corrigir os dados.
- Anonimização, Bloqueio, Eliminação - Solicitar anonimização, bloqueio, ou eliminação dos dados. Portabilidade - Portabilidade de dados para congênere ou outro produto.
- Revogação de Consentimento - Revogar o consentimento concedido anteriormente.
- Informação sobre compartilhamento - Qual entidade pública ou privada os dados poderão ser compartilhados.

9. Tratamento de dados pessoais sensíveis

O tratamento de dados pessoais sensíveis deverá ter o consentimento do titular ou responsável legal de forma específica ou destacada para finalidades específicas.

Entretanto, poderá ser tratado sem o consentimento quando for indispensável para:

a) Cumprimento de obrigação legal ou regulatória pelo controlador;
b) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou
regulamentos;
c) Realização de estudos por órgão de pesquisa, garantida;
d) Exercício regular de direitos, inclusive em contrato e em processo
judicial, administrativo e arbitral;
e) Proteção da vida ou da incolumidade física do titular ou de terceiros;
f) Tutela da saúde;
g) Garantia da prevenção à fraude e à segurança do titular.

Poderá ser objeto de vedação ou regulamentação pela ANPD, a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados, quando consentido pelo titular

- **Término do tratamento de dados pessoais -** O término deverá ocorrer nas seguintes hipóteses:
    a. Quando a finalidade foi alcançada ou os dados deixem de ser necessários ou pertinentes ao alcance da finalidade específica;
    b. No fim do período de tratamento;
    c. Quando o consentimento for revogado pelo titular do dado;
    d. Por determinação da autoridade nacional, quando houver violação ao disposto na Lei;

- **Eliminação dos dados** - os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
    a. Cumprimento de obrigação legal ou regulatória;
    b. Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.
    c. Estudo por órgão de pesquisa;
    d. Transferência a terceiro.

10. **Principais papéis e responsabilidades**

Além das Boas Práticas e Governança, os papéis e responsabilidades são:

Controlador: Tratar e proteger os dados pessoais dos titulares de dados de acordo com a LGPD; elaborar relatório de impacto à proteção de dados; comunicar à Autoridade Nacional e ao titular a ocorrência de incidente de segurança da informação que possa acarretar risco ou dano relevante aos titulares.

ATENÇÃO: A lei não prevê prazo específico, apenas menciona que a comunicação deverá ocorrer em prazo razoável, a ser definido pela Autoridade Nacional de Proteção de Dados - ANPD.

Operador: O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Autoridade Nacional de Proteção de Dados: A Autoridade Nacional de Proteção de Dados – ANPD é um órgão da administração pública direta federal do Brasil que faz parte da Presidência da República e possui atribuições relacionadas à proteção de dados pessoais, determinando as diretrizes da aplicação e fiscalização do cumprimento da LGPD.

Encarregado pelo tratamento de dados - Dpo – Data Protection Officer: Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da autoridade nacional e adotar providências; orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

11. Segurança e sigilo de dados

As empresas que tratam dados pessoais devem adotar medidas de segurança aptas à proteção dos dados desde a coleta até a sua exclusão, inclusive em caso de incidente de segurança.

12. Responsabilidade e indenização de danos

A empresa será obrigada à reparação de danos causados e comprovados no exercício da atividade de tratamento de dados sempre que um incidente de segurança ocorrer e causar danos aos titulares dos dados envolvidos.

Os agentes não serão responsabilizados quando provarem não terem realizado o tratamento de dados, não terem violado a LGPD ou quando o dano for decorrente de culpa exclusiva do titular dos dados.

13. RESPONSABILIDADES DOS AGENTES DE TRATAMENTO DE DADOS

Os Agentes de Tratamento são o Controlador e o Operador de dados, e a eles recaem responsabilidades.

Os Agentes de Tratamento de dados devem realizar o Tratamento de forma lícita e com a segurança que o Titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

(i) o modo pelo qual é realizado;

(ii) o resultado e os riscos que razoavelmente dele se esperam;

(iii) as técnicas de Tratamento de Dados Pessoais disponíveis à época em que foi realizado.

Nos termos da LGPD, a Gestora ou o Operador que, em razão do exercício de atividade de Tratamento de Dados Pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de Dados Pessoais, obrigado a repará-lo, ressalvadas as exceções legais.

A Gestora, no âmbito de suas responsabilidades e nos termos aqui descritos, providência de forma diligente o adequado Tratamento dos Dados Pessoais que tenha acesso, adotando medidas de segurança, técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de Tratamento inadequado ou ilícito.

Por fim, caso a Gestora, na qualidade de Controlador, venha a se utilizar de Operador terceiro para o Tratamento de Dados Pessoais, será este o responsável pelo referido Tratamento, em nome da Gestora.

Desta forma, e nos termos da LGPD, o Operador será responsável solidário (pela totalidade da obrigação) por evento danoso quando desobedecer aos comandos lícitos do Controlador ou descumprir as determinações da LGPD, salvo nos casos de exclusão previstos na lei, acima citados.

14. Segurança e Sigilo dos Dados

Segurança da Informação - A segurança da informação prevista na LGPD, em relação aos Dados Pessoais, mesmo após seu término, é responsabilidade dos Agentes de Tratamento de Dados Pessoais ou qualquer outra pessoa que intervenha no Tratamento.

A Gestora possui Política de Segurança da Informação que abrange também os Dados Pessoais que sejam tratados pela Gestora, e trazem as medidas estabelecidas para a proteção dos dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de Tratamento inadequado ou ilícito. Tais medidas são observadas desde a fase de concepção do produto ou do serviço, até sua execução.

A ANPD poderá dispor sobre padrões mínimos para proteção dos dados, consideradas a natureza das informações tratadas, as características específicas do Tratamento e o estado atual da tecnologia.

Incidentes de dados - Cabe à Gestora (na qualidade de Controlador) comunicar à ANPD e ao Titular de Dados Pessoais quaisquer incidentes de segurança que possa acarretar risco ou dano relevante ao Titular e essa comunicação deve ser realizada em prazo razoável (a ser definido pela ANPD).

Por sua vez, na comunicação à ANPD será mencionada a descrição da natureza dos Dados Pessoais afetados, as informações sobre os Titulares envolvidos, a indicação das medidas técnicas e de segurança utilizadas para a proteção dos Dados Pessoais, observados os segredos comercial e industrial, os riscos relacionados ao incidente, os motivos da demora, no caso de a comunicação não ter sido imediata, e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

A ANPD poderá determinar à Gestora que divulgue o fato em meios de comunicação e que adote medidas para reverter ou mitigar os efeitos do incidente.

A adoção de políticas de boas práticas e governança de dados aqui definidas, bem como as demais estabelecidas na Política de Segurança da Informação, auxilia a Gestora a cumprir suas obrigações perante a legislação de proteção de dados e reforça os esforços nesse sentido.

Com a introdução das regras da LGPD, qualquer sistema ou solução deve ser pensada observando a proteção dos Dados Pessoais dos Titulares, desde o início, ou seja, desde a concepção do produto: sempre levando em conta os princípios da proatividade e não reatividade, privacidade como padrão, privacidade incorporada ao projeto, funcionalidade total, segurança, visibilidade e transparência e por fim, respeito pela privacidade do usuário.

Controle dos Dados Pessoais - A Gestora (na qualidade de Controlador) é responsável pela guarda dos Dados Pessoais coletados e armazenados em seus sistemas, sendo que os Dados Pessoais devem ser tratados com base nas hipóteses permitidas na legislação.

Nas hipóteses em que o Tratamento de dados não tiver sido previamente mapeado pela Gestora, o Encarregado deverá ser acionado para definir as providências a serem tomadas para garantir o correto Tratamento dos Dados Pessoais.

Normas de segurança e padrões técnicos - De acordo com a LGPD, é obrigação legal da Gestora adotar medidas de segurança, técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de Tratamento inadequado ou ilícito.

As medidas de segurança devem ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. As normas de segurança e padrões técnicos para o gerenciamento de riscos de segurança cibernética e para mitigação de riscos estão previstos na Política de Segurança da Informação da Gestora.

15. Fiscalizações e sanções

A LGPD estabelece que as sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios, dentre outros:

- a gravidade e a natureza das infrações e dos direitos pessoais afetados;
- boa-fé´do infrator;
- grau do dano;
- cooperação do infrator;
- existência de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao Tratamento seguro e adequado de dados;
- adoção de política de boas práticas e governança.

A ANPD (Autoridade Nacional de Proteção de Dados) é um órgão da administração pública federal, dotada de autonomia técnica e decisória, com jurisdição no território nacional e com sede e foro no Distrito Federal, tem o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural.

As sanções administrativas previstas são, dentre outras:

a) Advertência, com indicação de prazo para adoção de medidas corretivas;
b) Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
c) multa diária limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
d) publicização da infração;
e) bloqueio dos Dados Pessoais; e
f) eliminação dos Dados Pessoais.