Hospital das Clínicas Fmusp

FUNDAÇÃO FACULDADE DE MEDICINA

FUNDAÇÃO ZERBINI

LGPD

CARTILHA DE CONSCIENTIZAÇÃO SOBRE A LGPD

CARTILHA
DE CONSCIENTIZAÇÃO SOBRE A LGPD

• LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

A Lei 13.709/2018, conhecida como LGPD, entrou em vigor em 18 de setembro de 2020. Nos termos do artigo 1º da LGPD, a referida lei *"dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".*

Nesse cenário, a organização também deverá estar em conformidade com a LGPD, uma vez que mantém constante contato com dados pessoais de seus colaboradores, parceiros, representantes de fornecedores e clientes.

É importante lembrar que esta lei é pautada em diversas legislações de proteção de dados pessoais, tendo como principal referência o Regulamento Geral de Proteção de Dados (GDPR), que é um conjunto de regulações do direito europeu no âmbito da privacidade e proteção de dados pessoais.

Por isso, pensando na promoção da cultura da transparência e da proteção dos dados pessoais dos seus titulares, essa cartilha foi elaborada como parte do projeto de adequação da organização à LGPD, com o objetivo de repassar informações importantes sobre a lei protetora de dados pessoais a todos que compõem e realizam tratamento destas informações em nome da organização.

• CONCEITOS E DEFINIÇÕES

Para melhor compreensão da LGPD, são apresentados abaixo os principais conceitos e definições relacionadas à Lei:

TITULAR

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art. 5, V). Observação: a LGPD fornece proteção apenas às pessoas físicas, não incluindo dados de pessoas jurídicas. **Ex:** dados pessoais de cliente pessoa natural; representantes de empresas; colaboradores terceirizados; colaboradores internos.

OPERADOR

Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII). **Ex:** empresas terceirizadas que realizam o tratamento de dados pessoais em nome da organização.

CONTROLADOR

Pessoa natural ou jurídica a quem compete as decisões referentes ao tratamento de dados pessoais (art. 5º, VI). **Ex:** o própria organização.

Observação: De acordo com a Autoridade Nacional de Proteção de Dados (ANPD), *"não são considerados controladores (autônomos ou conjuntos) ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento".*

ENCARREGADO

Pessoa indicada pelo controlador que atua como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD).

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

É o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD, além de possuir atribuições relacionadas a proteção de dados pessoais e a privacidade em todo o território nacional (art. 5º, XIX).

DADOS PESSOAIS

A LGPD trouxe também a definição de dado pessoal em seu artigo 5º, I, como sendo *"informação relacionada a pessoa natural identificada ou identificável"*. Ex.: nome, CPF, RG, dados bancários, profissão, nacionalidade, endereço, localização etc.

Programa de Conscientização sobre Privacidade

DADOS PESSOAIS SENSÍVEIS

Ainda no artigo 5º, inciso II, a LGPD qualificou dado pessoal sensível como *"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".*

Em outras palavras, quando há a coleta desta espécie de dados, por exemplo, de atestados médicos, há repasse de informação sensível. Neste caso, para que a o tratamento seja feito de forma correta, é necessário que haja a adoção de mecanismos de segurança ainda maiores.

TRATAMENTO DE DADOS PESSOAIS

Interessante lembrar também a definição de tratamento apresentada pela LGPD (art. 5º, X), em que dispõe que tratamento será *"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"*.

Ou seja, o simples acesso a um dado pessoal em uma tela de computador, por exemplo, já caracteriza o tratamento.

• IMPORTÂNCIA DA PROTEÇÃO DE DADOS

Para que uma organização mantenha sua integridade e possa se desenvolver de forma saudável, a segurança de dados pessoais deve ser elevada à condição de prioridade.

A ausência de conformidade com a LGPD pode acarretar prejuízos que vão desde a perda de confiança devido à publicização de incidentes com dados pessoais até multas exorbitantes.

Sendo assim, a sobrevivência organizacional está diretamente relacionada ao compromisso com privacidade e proteção de dados pessoais.

• EXERCÍCIO DE DIREITOS PELOS TITULARES

Os titulares de dados pessoais têm direitos em relação às suas informações, sendo garantidos os direitos fundamentais à liberdade, à intimidade e à privacidade, nos termos do art. 17 da LGPD.

Pensando nisso, a LGPD trouxe no artigo 18, diversos direitos que podem ser exercidos pelo titular de dados pessoais. São eles:

I. **Confirmação** da existência de tratamento;

II. **Acesso** aos dados;

III. **Correção** de dados incompletos, inexatos ou desatualizados;

IV. **Anonimização**, **bloqueio ou eliminação** de dados desnecessários, excessivos ou tratados em desconformidade com a lei;

V. **Portabilidade** dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.

VI. **Eliminação** dos dados pessoais tratados com o consentimento do titular, **exceto** nas hipóteses previstas no art. 16:

Art . 16. 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:

I - cumprimento de obrigação legal ou regulatória pelo controlador;
II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

VII. **Informação** das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII. **Informação** sobre a possibilidade de **não fornecer consentimento** e sobre as consequências da negativa;
IX. **Revogação do consentimento**, quando os dados estivem sendo tratados com base nesse fundamento.

Para que o titular possa exercer esses direitos, o titular pode formalizar a solicitação pelos meios de comunicação fornecidos pela organização, seja de forma presencial ou remota através da Ouvidoria ou Portal Fale Conosco.

O prazo máximo para atendimento à solicitação do titular é de 15 dias corridos, a contar da data do requerimento do titular, nos termos do art. 19, inciso II da LGPD.

• DEFINIÇÃO DE PAPÉIS

O **controlador** é responsável pela tomada de decisões acerca do tratamento de dados pessoais. É quem direciona os operadores acerca da manutenção, uso e guarda das informações.

A função do operador pode ser exercida por fontes externas à organização, as quais ficam responsáveis por executar as atividades conforme orientações do controlador. Ex.: empresas terceirizadas.

Tais definições aplicam-se a todos os prestadores de serviços externos que realizem tratamento de dados pessoais em nome da organização, visto que caracterizam como operadores e têm papel substancial na conformidade da Organização com a LGPD.

• RESPONSABILIDADE DOS AGENTES

Tanto o controlador como o operador podem ser responsabilizados pelo tratamento indevido dos dados pessoais que causem danos patrimoniais, morais, individuais ou coletivos aos titulares (art. 42).

Caso haja envolvimento de diversos controladores, por exemplo, a própria organização e outra empresa ou membro do Poder Público que esteja igualmente responsável pela tomada de decisões referente ao tratamento dos dados pessoais (Controladoria Conjunta), respondem solidariamente entre si, ou seja, ambos podem ser obrigados a pagar integralmente a multa imposta, por exemplo.

Além disso, o operador que atuar diretamente no tratamento do dado pessoal e ocasionar o referido dano será equiparado ao controlador.

Dessa forma, o operador responde também de maneira solidária pelos danos causados quando descumprir as obrigações da legislação de proteção de dados ou

Quando não tiver seguido as instruções lícitas do controlador, hipótese em que este responderá conjuntamente com o controlador (art. 42, §1º, I e II).

Pode-se elencar como exemplos de fatos que podem acarretar a responsabilidade civil:

- Vazamentos (*data leaks*);
- Não atendimento aos direitos do titular;
- Tratamento em desconformidade com a LGPD.

Para mitigar a ocorrência destes riscos, é importante que a organização e todos que possuem vínculo com o tratamento de dados pessoais auxiliem nas informações de incidentes e controle de acesso aos dados a fim de manter a cultura de privacidade.

• BASES LEGAIS E HIPÓTESES DE TRATAMENTO

A LGPD também traz diferentes bases legais e hipóteses de tratamento que justificam o tratamento de dados pessoais.

Destaca-se que a lei separou as hipóteses de tratamento de dados pessoais em: “tratamento de dados pessoais” (art. 7º) e “tratamento de dados pessoais sensíveis” (art. 11º).

O tratamento de **dados pessoais** poderá ser realizado apenas nas seguintes hipóteses:

I- Mediante o fornecimento de consentimento pelo titular;

• Quando não há outra base legal que legitime o tratamento dos dados, no qual é exigida a autorização expressa para a coleta e uso dos dados pessoais.

II- Para o cumprimento de **obrigação legal** ou regulatória pelo controlador;

III- Pela **administração pública**, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV- Para a realização de **estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais;

V- 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;

• Para a execução do contrato de trabalho ou de compra e venda, por exemplo.

VI- para o **exercício regular de direitos** em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII- Para a **proteção da vida** ou da incolumidade física do titular ou de terceiros;

VIII- Para a **tutela da saúde,** exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX- 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

X- Para a **proteção do crédito**, inclusive quanto ao disposto na legislação pertinente.

Ao passo que o tratamento de **dados pessoais sensíveis** poderá ser realizado

somente na ocorrência das seguintes hipóteses:

I- Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II- Sem fornecimento de consentimento do titular, nas hipóteses em que 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, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) **exercício regular de direitos**, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) **proteção da vida** ou da incolumidade física do titular ou de terceiros;

• Coleta de atestados médicos, realização de exames admissionais, uso de EPI, por exemplo.

f) **tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da **prevenção à fraude** e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Destaque: O importante é, principalmente, que a organização fundamente o tratamento e que haja proteção dessas informações.

• PRIVACIDADE DESDE A CONCEPÇÃO E POR PADRÃO

Um dos pontos importantes é a manutenção da privacidade de ponta a ponta, desde a concepção do tratamento (coleta dos dados pessoais) e a continuidade da proteção até o final da tratativa.

A privacidade desde a concepção *(privacy by design)* tem o objetivo de analisar possíveis problemas na tratativa dos dados pessoais e atuar de forma preventiva, antes que incidentes aconteçam. A ideia é que a organização incorpore esta metodologia de forma a incluí-la entre seus valores e conduta ética.

Esta metodologia possui 7 pilares, quais sejam:

1. Ser proativo e não reativo – Prevenir e não remediar

Deve haver o monitoramento constante das atividades, análise de riscos e desenvolvimento de correções sempre que uma vulnerabilidade for identificada.

2. Privacidade por padrão

Proporcionar a máxima proteção ao usuário de forma contínua.

3. Privacidade incorporada ao *design*

A privacidade não deve ser vista como um complemento ao projeto, pois ela é parte intrínseca e indissociável.

4. Funcionalidade completa – Soma positiva, ao invés de soma zero

A proteção dos dados pessoais deve trazer benefício a todas as partes envolvidas no tratamento.

5. Segurança de ponta a ponta

Os dados devem seguir seu fluxo de forma segura, desde o início até a sua destinação final, de forma que não sejam esquecidos e arquivados de maneira indiscriminada.

6. Visibilidade e transparência

Os agentes de tratamento devem prezar pelo completo atendimento dos direitos dos titulares, oferecendo meios de comunicação para possíveis solicitações.

7. Respeito pela privacidade do titular

As atividades devem sempre ser centradas na privacidade do usuário, pensando na proteção completa dos dados pessoais.

• SANÇÕES ADMINISTRATIVAS

A Lei Geral de Proteção de Dados Pessoais entrou em vigor em setembro de 2020 e suas sanções administrativas podem ser aplicadas desde agosto de 2021 (art. 52).

As organizações que violarem a lei ou causarem incidentes de segurança poderão sofrer as penalidades previstas na Lei que variam de acordo com a gravidade, inclusive a organização. Sendo assim, as possíveis sanções são:

- **Advertência;**
- **Multa simples**, de até 2 % do faturamento da pessoa jurídica, limitado a R$ 50.000.000,00 (cinquenta milhões) por infração;
- **Multa diária**;
- **Publicização da infração;**
- **Bloqueio dos dados pessoais**;
- **Eliminação dos dados pessoais**;
- **Suspensão** parcial do funcionamento do banco de dados pelo período máximo de 6 meses, prorrogáveis por igual período;
- **Suspensão** do exercício da atividade de tratamento dos dados pessoais pelo período máximo de 6 meses, prorrogáveis por igual período;
- **Proibição parcial ou total** do exercício de atividades relacionadas a tratamento de dados.

Destaca-se que aquele que não contribuir com as diretrizes estabelecidas pela organização em relação à privacidade e proteção de dados poderá sofrer penalidades administrativas, civis e criminais.

Sua ajuda é muito importante para a organização se adequar à LGPD!

• DOCUMENTAÇÃO E A LGPD

TODOS os processos que envolvem dados pessoais devem estar documentados. O Encarregado de Dados é o ponto focal nessa atividade, o qual torna-se responsável por gerenciar os registros, zelar e manter atualizadas as documentações relativas ao tratamento de dados pessoais.

• REGISTRO DAS OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS

Consiste no Registro das Operações de Tratamento dos Dados Pessoais realizados pela organização (art. 37). Este registo permite que a organização tenha uma visão completa de todos os dados pessoais que são tratados e, consequentemente, a identificação de quais processos estes dados estão utilizados, bem como o seu respectivo ciclo de vida. Trata-se de um documento vivo com necessidade de revisão periódica.

Neste documento é possível identificar:

- Quem são os **agentes** de tratamento;
- **Descrição** do tratamento;
- Qual a **finalidade** do tratamento;
- Quais **espécies** de dados pessoais são tratadas;
- Quais **categorias** de titulares e sua relação com o controlador;
- Se há o **compartilhamento** de dados pessoais na própria organização e com terceiros; e
- As **bases legais** que legitimam o tratamento dos dados pessoais.

• RELATÓRIO DE IMPACTO À PRIVACIDADE DE DADOS (RIPD)

O RIPD tem a função de identificar, analisar e minimizar potenciais riscos de incidentes envolvendo dados pessoais, bem como indicar se a operação de tratamento de dados pessoais possui, ou não, respaldo legal para a sua realização (art. 5º, XVII).

Neste documento há a descrição dos processos de tratamento de dados pessoais (ciclo de vida) bem como medidas, salvaguardas e mecanismos de mitigação de riscos.

A utilização deste Relatório aumenta a conscientização sobre questões de privacidade e proteção de dados na organização

Este documento poderá ser solicitado pela ANPD durante uma investigação em que seja identificado um alto risco aos titulares. Entre os critérios que possivelmente serão utilizados pela ANPD para identificar esse alto risco estão os seguintes:

- Fundamentados no legítimo interesse do controlador;
- Realização de tratamento automatizado, incluindo a definição de perfis;
- Tratamento de dados pessoais sensíveis em larga escala;

• GESTÃO DE CONTRATOS E A LGPD

A organização trata diversos dados pessoais ao longo da gestão de cada documento contratual.

É possível que, a depender da natureza do contrato, por exemplo os contratos de trabalho e aqueles firmados com os nossos clientes, haja a coleta de dados pessoais sensíveis por exigência legal, como é o caso de atestados médicos para admissão de novos colaboradores, ou ainda, para justificativa de faltas, por exemplo.

Em razão disso, é fundamental que nos contratos haja cláusulas sobre o respectivo tratamento e aos riscos envolvidos nessa relação à luz da privacidade de dados pessoais.

• SIGILO E PROTEÇÃO DE DADOS PESSOAIS NA TERCEIRIZAÇÃO

Nos casos de compartilhamento ou contratação de terceirizadas, é importante zelar pela **CONFIDENCIALIDADE** e **PRIVACIDADE** dos dados pessoais compartilhados entre as empresas.

O compartilhamento dos dados somente deve ocorrer em casos imprescindíveis e inerentes à execução do contrato, de forma a zelar sempre pela proteção e sigilo dos dados (art. 5º, XVI).

• TRATAMENTO DE DADOS PESSOAIS DE TERCEIROS NA GESTÃO DE CONTRATOS

Em virtude da relação contratual da organização com outras empresas, imprescindível manter a conformidade com a proteção dos dados pessoais tratados. Para tanto, é preciso que:

- Haja **adequação contratual**, para assegurar que ambas as partes do contrato compreendem a importância do devido tratamento de dados pessoais;
- Sejam atendidos os princípios da **finalidade** (propósitos legítimos) e **coleta**

mínima;

- Possíveis incidentes sejam imediatamente **notificados** para ambas as partes do contrato e ao Encarregado.

• MEDIDAS TÉCNICAS E ADMINISTRATIVAS DE SEGURANÇA

Com o propósito de se preservar a segurança dos dados pessoais, os agentes de tratamento devem adotar medidas técnicas e administrativas de segurança aptas a proteger os dados pessoais (art. 6º, inciso VII da LGPD).

Para tanto, sugere-se a implementação de controles físicos e lógicos nos sistemas. Ex.: Armazenamento de documentos físicos em locais com segurança, bem como controle de acesso às pastas digitais inseridas em um servidor de arquivos etc.

• INCIDENTES DE SEGURANÇA SEGUNDO A LGPD

Incidentes de segurança são eventos indesejados ou inesperados que têm grande probabilidade de comprometer as operações e ameaçar a segurança da informação.

Estes podem representar violações de dados pessoais e assim deverão ser tratados não só pela equipe de segurança da informação, mas também por todos os colaboradores, os quais têm a responsabilidade de prezar pela segurança dos dados e comunicar quaisquer possíveis incidentes.

• NOTIFICAÇÃO E RESPOSTA ÀS VIOLAÇÕES DE DADOS

- **Incidente de segurança:** é qualquer evento que não faz parte da operação padrão de um serviço. Pode causar uma interrupção do serviço ou uma redução da sua qualidade.
- **Violação de dados pessoais:** é uma espécie de incidente de segurança que pode levar à destruição, perda, alteração, divulgação não autorizada ou acesso indevido a dados pessoais.

Os gestores das unidades e das gerências da organização têm papel de suma importância na comunicação de incidentes que possivelmente violem os direitos dos titulares (art. 48), haja visto o grande volume de dados sob sua responsabilidade.

Tais responsáveis também têm função colaborativa com as investigações que venham a ser realizadas em decorrência do incidente.

Caso seja identificado um alto risco concreto de dano aos titulares, as violações de dados deverão ser comunicadas tanto à ANPD quanto aos titulares pelo controlador ou Encarregado, no prazo de até 02 (dois) dias úteis, a fim de que estes tenham ciência para atuarem com prazo razoável contra o vazamento de dados.

O objetivo do processo de resposta a incidentes é minimizar os danos que poderiam ser causados pela violação de dados pessoais, reduzir o tempo de ação e os custos de recuperação.

Aqueles que identificam o incidente têm papel fundamental na comunicação e colaboração no tratamento de incidentes que possam gerar danos aos titulares de dados pessoais.

• PRESTAR INFORMAÇÕES SOLICITADAS AO ENCARREGADO

Os direitos dos titulares de dados podem ser exigidos a qualquer momento e oportunidade.

Por isso, quando necessário, o Encarregado da organização poderá solicitar informações às áreas responsáveis pelo tratamento dos dados pessoais para melhor atendimento às solicitações dos titulares.
Neste momento, é dever de todos os departamentos responder e prestar informações de forma rápida e suficiente quando necessário.

O COMPROMISSO DE TODOS COM A PROTEÇÃO DE DADOS PESSOAIS É ESSENCIAL!

TODOS que se relacionam em algum momento com a organização e realizam tratamento de dados pessoais em seu nome devem zelar pela **PRIVACIDADE** na execução das atividades, bem como a conscientização daqueles que possuam acesso a dados pessoais, a fim de se evitar a aplicação de sanções previstas na **LGPD**.