Hospital das Clínicas da Faculdade de Medicina de Marília - HCFAMEMA

Cartilha de Conscientização sobre a Lei Geral de Proteção de Dados – LGPD

Comitê de Acompanhamento à LGPD no HCFAMEMA

Abril/2023

Introdução

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".*

A LGPD é baseada em princípios fundamentais, como a transparência, a finalidade, a necessidade, a segurança e não discriminação. Ela se aplica a todas as empresas e organizações que coletam, armazenam, processam ou compartilham dados pessoais, independente do seu tamanho ou setor de atuação. A legislação surgiu com o propósito de tutelar a privacidade, prevenindo incidentes de segurança e promovendo a responsabilização.

Nesse sentido, a LGPD prevê sanções para as empresas e organizações que não cumprem suas regras. As sanções podem incluir multas, advertências, bloqueio de dados e até mesmo a suspensão parcial ou total das atividades da empresa.

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 pacientes.

Diante disso, essa cartilha foi elaborada 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.

Os Agentes da LGPD

Para melhor compreensão da LGPD, são apresentados abaixo os principais agentes relacionados à Lei:

Titular: Pessoal naturala quem se referem os dados pessoais que são objetos de tratamento (art. 5, V). A LGPD fornece proteção apenas às pessoas físicas, não incluindo dados de pessoas jurídicas. Ex:dados pessoais de cliente pessoa naturais; representantes de empresas; colaboradores terceirizados; colaboradores internos.

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

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. 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 (ANPD): 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).

Definições dos Papéis e Responsabilidade dos Agentes

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.

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.

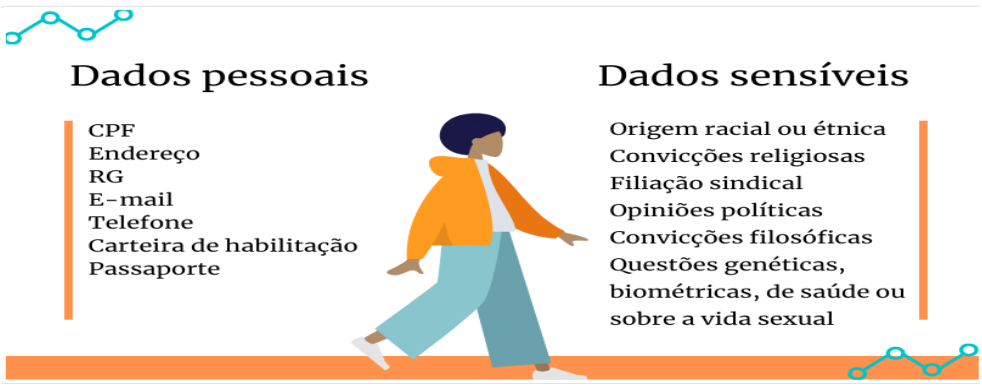
Para mitigar a ocorrência destes riscos, é importante que a organização e todos que possuem vínculo com o tratamento de dados pessoais auxiliem nas informações de incidentes e controle de acesso aos dados a fim de manter a cultura de privacidade.

Dado Pessoal x Dado Pessoal Sensível

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.

E, em seu 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.



Existem técnicas que são empregadas de forma a mascarar ou impedir a identificação do titular dos dados. Trata-se de tentativa de diminuição dos riscos de exposição dos dados pessoais ou sensíveis. Se tal técnica permitir a reidentificação do titular dos dados, será uma pseudonimização e a informação ainda estará dentro do escopo de aplicação da LGPD, mantendo-se na categoria de dado pessoal. Caso o dado seja alterado de forma a impedir, de fato, a possibilidade de reidentificação do titular, será um processo de anonimização e a informação perderá a natureza de dado pessoal. A seguir, trazemos mais detalhes a respeito destas duas técnicas:

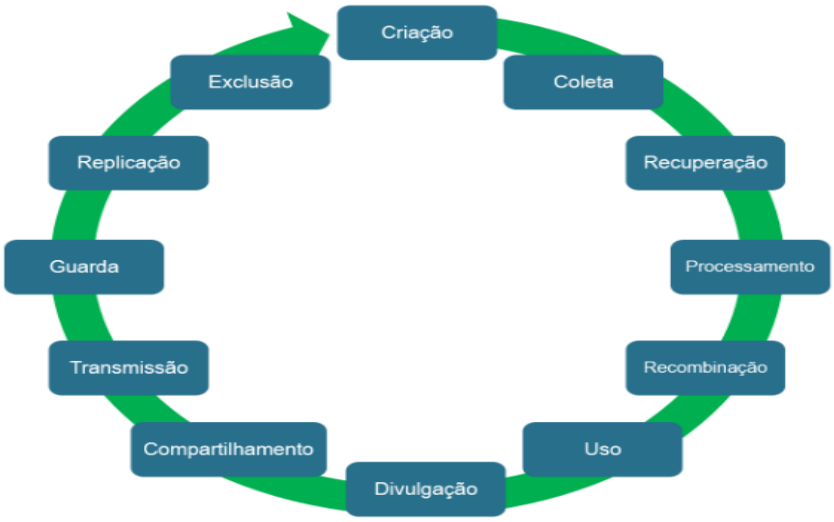
Pseudonimização: dados pseudonimizados ainda são considerados dados pessoais pela Lei. Trata-se de dados que passaram por um processo pelo qual a informação perde a possibilidade de associação, direta ou indireta, a um indivíduo, entretanto, a identificação do indivíduo continua possível pela utilização de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. Ou seja, os dados pseudonimizados permanecem dentro do escopo de aplicação da lei, porque há possibilidade do controlador reidentificar o titular por meio do recurso por ele utilizado para "mascarar" a identidade do indivíduo perante terceiros. Assim, dados pseudonimizados permanecem no conceito de dados pessoais.

Anonimização: os chamados dados anonimizados passam por técnica que exclui permanentemente seus caracteres identificáveis e impedem a identificação do titular definitivamente, de modo que não mais estarão no escopo de aplicação da LGPD. Portanto, dados anonimizados não são dados pessoais.

Definição de Tratamento de Dados

Diante do exposto, toda atividade que envolve e trabalha com dados de pessoas físicas ou jurídicas, passa pelo tratamento de dados.

Com efeito, 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 à 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 já caracteriza o tratamento.



Importância da Proteção de Dados

Por isso, 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.

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 da 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.

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.

1

Advertência, com indicação de prazo para adoção de medidas corretivas.

2

Multa simples, de até 2% 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 milhões por infração.

3

Publicização da infração após devidamente apurada e confirmada sua ocorrência.

4

Bloqueio dos dados pessoais a que se refere a infração até a sua regularização.

5

Eliminação dos dados pessoais a que se refere a infração.

6

Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; Proibição parcial ou total do exercício de atividades de tratamento de dados.

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 se torna 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 registro 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 às 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 vista 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, gerências e núcleos responder e prestar informações de forma rápida, adequada e suficiente quando necessário.

Obrigações de Medidas de Segurança

Por fim, a LGPD estabelece que os agentes 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 destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Deve-se, assim, garantir a segurança eletrônica, manutenção de softwares devidamente atualizados, redes seguras, confidencialidade, integridade, além de disponibilidade imediata das informações pessoais coletadas, caso solicitadas pelo cliente.

Em caso de incidentes de segurança, o controlador deverá comunicar à ANPD e o titular o fato, caso este possa acarretar risco ou dano relevante ao titular dos dados pessoais. Essa comunicação deverá ser realizada em prazo razoável e pelo Encarregado, seguindo o procedimento estabelecido na LGPD.

Compromisso de Todos é Essencial para a Proteção de Dados Pessoais.

O HCFAMEMA possui um Comitê de Acompanhamento da LGPD, que tem como objetivo aplicar e desenvolver ações em conformidade com a legislação e as diretrizes do governo do Estado de São Paulo.

A garantia da privacidade das informações é uma responsabilidade compartilhada por todos os colaboradores, especialmente os que lidam com a coleta e manipulação de dados pessoais.

É fundamental que aqueles que possuem acesso a essas informações estejam plenamente conscientes da importância da proteção desses dados, a fim de evitar possíveis sanções legais decorrentes da Lei Geral de Proteção de Dados.

Referências

Ministério da Saúde: Lei Geral de Proteção de Dados Pessoais (LGPD)
Disponível em: <https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd>
Acesso em: 24/03/2023

Autoridade Nacional de Proteção de Dados: No dia internacional da proteção de dados ANPD pública guia orientativo sobre tratamento de dados pessoais pelo poder público
Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/no-dia-internacional-da-protecao-de-dados-anpd-publica-guia-orientativo-sobre-tratamento-de-dados-pessoais-pelo-poder-publico>
Acesso em: 24/03/2023

Ministério da Economia: Lei Geral de Proteção de Dados pessoais de A a Z: semana de inovação detalha orientação para órgãos públicos e iniciativa privada
Disponível em:<https://www.gov.br/economia/pt-br/assuntos/noticias/2021/novembro/lei-geral-de-protecao-de-dados-pessoais-de-a-a-z-semana-de-inovacao-detalha-orientacoes-para-orgaos-publicos-e-iniciativa-privada>
Acesso em: 24/03/2023

Planalto:Lei nº 13.709, de 14 de agosto de 2018
Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>
Acesso em: 24/03/2023

Faculdade de Medicina da Universidade de São Paulo - FMUSP: Cartilha de Conscientização sobre a LGPD
Disponível em: <https://www.ffm.br/ffm/conteudo/cartilha_v1.pdf>
Acesso em: 24/03/2023

LGPD: desafios e oportunidades para organizações atuantes no Brasil e no Reino Unid. LUZ, Clarissa,2021.
Disponível em: < https://www.felsberg.com.br/wp-content/uploads/2021/05/relatorio-lgpd_uk-felsberg_29042021.pdf>
Acesso: 24/03/2023

HCFAMEMA

Rua Doutor Reinaldo Machado, 255
Fragata – Marília – SP – CEP: 17519-080

WhatsApp: (14) 99649-5783
Telefone: (14) 3434-2525

www.hc.famema.br
superintendencia@hcfamema.sp.gov.br

hcfamema