PASSO A PASSO DE ADEQUAÇÃO À LGPD

PARA GRANDES EMPRESAS E EMPRESAS DE PEQUENO PORTE /STARTUPS

campos thomaz
& meirelles advogados

ÍNDICE:

1

A LGPD se aplica a minha organização?

A Lei Geral de Proteção de Dados ("LGPD") é uma lei que regulamenta o **tratamento** de **dados pessoais** realizados por organizações privadas e públicas, incluindo empresas de grande porte, pequeno porte e startups. A LGPD tem como objetivo proteger os direitos fundamentais à privacidade, a proteção dos dados pessoais e o livre desenvolvimento da personalidade de pessoas físicas.

O primeiro passo para entender se a LGPD se aplica a uma organização, é identificar se tal organização coleta ou utiliza de alguma forma **dados pessoais**. A LGPD define **dado pessoal** como qualquer "informação relacionada a pessoa natural identificada ou identificável". Pessoas naturais são pessoas físicas, como clientes pessoas físicas, indivíduos que são contatos/empregados de pessoas jurídicas, colaboradores, diretores, ou quaisquer terceiros que organização colete dados pessoais. Assim, quaisquer informações relacionadas a tais pessoas físicas, coletadas ou de qualquer forma tratadas pela organização, devem ser utilizadas de acordo com os requisitos da LGPD, por se tratar de um **dado pessoal**. Dados Pessoais tipicamente coletados incluem, mas não se limitam, ao nome, e-mail, telefone, CPF, RG, endereço residencial, informações comportamentais e de preferência pessoal. Em termos práticos, a grande maioria das organizações de caráter privado estão sujeitas as regras da LGPD, por tratarem dados pessoais de seus colaboradores, clientes e terceiros.

A LGPD impõe ainda requisitos mais restritivos para o tratamento de dados pessoais considerados como dados pessoais sensíveis. São informações origem racial ou étnica, informações relacionadas a convicção religiosa, opiniões políticas, informações referentes à filiação sindical ou organizações de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual de titulares ou dado genético ou biométrico. No dia a dia, essas informações estão refletidas, por exemplo, em exames e atestados médicos de colaboradores e na coleta de biometria para ponto eletrônico.

Ainda de acordo com a LGPD, qualquer atividade de **tratamento** deve ser adequada a LGPD. O tratamento é a nomenclatura geral utilizada para identificar qualquer operação realizada com os dados pessoais. Tais operações incluem, mas não se limitam a coleta, classificação, transferência, processamento, armazenamento e eliminação de dados pessoais. Em termos práticos, qualquer operação realizada com os dados pessoais é uma operação de **tratamento** sujeita as regras da LGPD.

Há algumas atividades de negócio que tipicamente trazem risco de violação à LGPD, por envolverem operações de tratamento dos dados pessoais. De forma não exaustiva, elencamos algumas dessas atividades:

- Tratamento de dados pessoais de candidatos em processos seletivos;
- Atividades de admissão, pagamento, avaliação e demissão de colaboradores;
- Tratamento de leads no contexto de atividades de marketing;
- Tratamento de dados pessoais de pessoas físicas no contexto de fornecimento de um produto ou serviço;
- Captação de informações de contato de colaboradores / contatos em um cliente pessoa jurídica, para fins de prospecção e atividades de marketing em negócios Business to Business (B2B); e
- Compartilhamento de dados de clientes e colaboradores com terceiros.

Caso a sua organização realize algumas das atividades acima, a adequação à LGPD deve ser realizada.

2 Porque devo adequar a minha organização à LGPD? O que pode acontecer se eu não me adequar?

Se chegou até aqui, provavelmente a sua organização realiza o tratamento de dados pessoais. Além dos problemas jurídicos identificados abaixo, há outras razões que extrapolam a esfera jurídica e que justificam o esforço de obter a adequação à LGPD. Assim, de forma não exaustiva, os benefícios e os riscos de não cumprir com os requisitos da LGPD incluem:

- Evitar riscos reputacionais, como a imagem e marca da empresa, decorrentes de um vazamento ou incidente
- Utilizar Vantagem competitiva frente aos concorrentes não adequados à lei
- Permitir a contratação com terceiros que exigem a conformidade com a LGPD como requisito para celebrar contratos
- Reduzir as chances de sofrer investigações administrativas pela ANPD e outras autoridade, e pagar multas administrativas
- Perda de confiança de clientes e parceiros de negócio
- Possibilidade de participar de licitações
- Reduzir as chances de ações judiciais e pagamento de indenizações
- Evitar a desvalorização de ações e ativos da organização
- Reduzir as chances de ser proibido de tratar dados pessoais ou realizar atividades de negócio envolvendo dados pessoais

3

Passo a passo para obter a adequação inicial à LGPD

Criamos abaixo um passo a passo para auxiliar as organizações a obter a adequação inicial à LGPD. O passo a passo definido abaixo é um modelo geral que deve ser adaptado as necessidades, tamanho e riscos específicos de cada organização.

PASSO 1

Mapeamento dos Dados Pessoais e Fluxo de Informações

Criamos abaixo um passo a passo para auxiliar as organizações a obter a adequação inicial à LGPD. O passo a passo definido abaixo é um modelo geral que deve ser adaptado as necessidades, tamanho e riscos específicos de cada organização.

- ☐ Identificar quais dados pessoais são tratados por cada uma das áreas de negócio da organização, incluindo para qual finalidade tais dados pessoais são utilizados em cada situação específica;
- ☐ Identificar os fluxos de dados internos e externos da organização;
- ☐ Identificar práticas específicas de coleta e tratamento de dados de colaboradores, clientes e terceiros;
- ☐ Identificar se há uma estrutura de governança em privacidade e proteção de dados na organização, incluindo quais medidas já foram adotadas para obter a conformidade com a LGPD e demais leis setoriais envolvendo privacidade e proteção de dados; e
- ☐ Documentar internamente as informações obtidas e fluxos de dados identificados nas etapas imediatamente anteriores acima; essa documentação é etapa obrigatória para adequação à LGPD.

A partir das informações acima, já é possível identificar preliminarmente qual o nível de maturidade do negócio em relação aos requisitos e ao cumprimento da LGPD.

PASSO 2

Plano de ação e Diagnóstico

A partir do resultado obtido na fase de mapeamento dos dados pessoais e dos fluxos de informações, deve ser elaborado um roteiro de trabalho que contará com um diagnóstico de requisitos da LGPD atendidos ou não pela organização. A partir do desenvolvimento do plano de ação e diagnóstico é possível identificar quais alterações documentais e procedimentais deverão ser implementadas.

Após a identificação, é importante organizar as atividades de adequação e priorizar a implementação de medidas que eliminem os principais riscos de violação da LGPD primeiro, para depois eliminar os riscos residuais.

PASSO 3

Implementação

Na implementação são criados ou revisados os documentos e procedimentos internos para adequação efetiva à LGPD, identificados a partir da fase anterior (passo 2). De forma não exaustiva, as atividades de implementação podem incluir o seguinte:

- [ ] Criação de programa de governança em privacidade e proteção de dados, com atribuição de responsabilidades de cada área de negócio envolvida;
- [ ] Nomeação do encarregado de proteção de dados (conhecido como Data Protection Officer ou DPO), se aplicável;
- [ ] Elaboração de canal para consulta interna e avaliação de novos processos de negócio, produtos e serviços, pelo DPO, sob a perspectiva da LGPD;
- [ ] Criação ou adaptação de canais de comunicação para atendimento aos direitos dos titulares de dados pessoais;
- [ ] Revisão ou elaboração de políticas corporativas, incluindo:
  - [ ] avisos de privacidade
  - [ ] políticas de uso aceitável dos dados pessoais
  - [ ] retenção e descarte de documentos
  - [ ] segurança da informação
  - [ ] uso aceitável de equipamentos corporativos
  - [ ] bring your own device
  - [ ] monitoramento de colaboradores
  - [ ] recrutamento e seleção, incluindo quando a realização de background check;
  - [ ] investigações internas
  - [ ] coleta, tratamento e compartilhamento de dados pessoais sensíveis de colaboradores, com aqueles relacionados a planos de saúde, atestados médicos, exames admissionais ou demissionais, ou acompanhamento de saúde de colaboradores;
  - [ ] coleta, tratamento e compartilhamento de dados pessoais de leads nas áreas de marketing;
  - [ ] práticas aceitáveis nas áreas de recursos humanos, marketing, comercial, e outras áreas de negócio;
- [ ] Elaboração de termos de consentimento para o tratamento de dados pessoais, quando aplicável;
- [ ] Elaboração de política de compartilhamento de dados com terceiros;

- Revisão de contratos de compartilhamento de dados pessoais com terceiros, como fornecedores;
- Implementação de mecanismo que permita a transferência internacional de dados;
- Revisão ou elaboração de plano de resposta a incidentes;
- Revisão ou elaboração de plano de comunicação com as autoridades competentes, incluindo a ANPD;
- Elaboração de relatórios de impacto à proteção dos dados pessoais; e
- Elaboração estrutura para treinamento e conscientização de colaboradores e terceiros.

PASSO 4

Treinamento e Manutenção

A cultura de privacidade e proteção de dados deve permear as atividades de negócio. Assim, as orientações quanto ao uso aceitável dos dados pessoais pelos colaboradores devem ser refletidas nos documentos internos da organização, mas também serem continuamente comunicadas por meio de treinamentos e ações de conscientização.

Depois de finalizar a etapa de adequação inicial da organização, novos produtos, serviços e processos de negócio devem ser continuamente avaliados pela perspectiva da LGPD. A manutenção da adequação à LGPD implica em um trabalho contínuo da organização em avaliar a legalidade de suas práticas de negócio, produtos e serviços.

4 Sou uma empresa de pequeno porte, devo que me adequar integralmente à LGPD ou há alguma flexibilização?

Por meio da Resolução CD/ANPD nº 2/2022 (“Resolução nº 2”), a ANPD flexibilizou alguns dos requisitos da LGPD para agentes de tratamento de pequeno porte. Nos termos da Resolução nº 2, são considerados agentes de tratamento de pequeno porte:

microempresas (ME)	Empresas de pequeno porte (EPP)	Startups
Faturamento até R$ 360 mil/ano	Faturamento até R$ 4.8 milhões/ano	Faturamento até R$ 16 milhões/ano*
Pessoas jurídicas sem fins lucrativos	Pessoas físicas que atuam como controladores (Ex.: Autônomos)	Entes despersonalizados (Ex.: Condomínios residenciais)

*Ou faturamento de R$ 1.33 milhões/mês, multiplicado pelo número de meses de atividade no ano anterior, quando inferior a 12 (doze) meses.

Conforme indicado adiante nessa cartilha, os agentes de tratamento de dados poderão se beneficiar da flexibilização de alguns dos requisitos previstos da LGPD.

Tal benefício, no entanto, não está disponível caso o agente de tratamento realize atividades de alto risco para os titulares dos dados pessoais. Nos termos da Resolução nº 2, são atividades de alto risco aquelas que combinam, no mínimo, um critério geral e um critério específico previsto abaixo:

Tratamento de Alto Risco para os Titulares de Dados =

Se identificado um critério geral + um critério específico na atividade de tratamento de dados

Critérios Gerais

- Tratamento de dados pessoais em larga escala

  (Avaliar: Volume de titulares, volume de dados e duração, frequência e extensão geográfica do tratamento para identificar se há larga escala no tratamento de dados);

- Tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares

  (Exemplos: utilização de dados pessoais sensíveis de saúde, orientação política ou religiosa, a utilização de dados biométricos, ou informações que revelem a capacidade financeira de um titular)

Critérios Específicos

- Uso de tecnologias emergentes ou inovadoras
- Vigilância ou controle de zonas acessíveis ao público
- Tratamento de dados pessoais sensíveis ou de titulares vulneráveis, incluindo crianças e adolescentes
- Decisões automatizadas que possam afetar os interesses dos titulares

Apresentamos abaixo um comparativo dos requisitos que foram flexibilizados pela ANPD no contexto da Resolução nº 2:

	SEM a Flexibilização prevista na Resolução nº 2 Agentes que não se enquadram como pequeno porte	**COM a Flexibilização prevista na Resolução nº 2** Agentes de pequeno porte
Registro de Operações de Tratamento (ROPA)	Deve elaborar e manter registro das operações de tratamento de dados pessoais, em formato completo	Deve elaborar e manter registro das operações de tratamento de dados pessoais em formato simplificado
Forma e Prazo de Comunicação de Incidentes de Segurança (Vazamento de dados, e incidentes de segurança que possam causar dano ou risco relevante ao titular de dados)	Deve comunicar incidentes de segurança nos termos da LGPD Prazo para notificação: Prazo razoável, a ser definido pela ANPD (a recomendação da ANPD, ainda não vinculante, é de comunicação dos incidentes em até 2 dias úteis, contados da data do conhecimento do incidente)	Deve comunicar incidentes de segurança, de forma flexibilizada e através de procedimento simplificado Prazo para notificação: Em dobro (O prazo em dobro não é aplicável em caso de incidentes que possam comprometer a integridade física ou moral dos titulares ou a segurança nacional)

	SEM a Flexibilização prevista na Resolução nº 2 Agentes que não se enquadram como pequeno porte	COM a Flexibilização prevista na Resolução nº 2 Agentes de pequeno porte
Nomeação de Encarregado de Proteção de Dados	Obrigatória	Não obrigatória
Segurança da Informação e Medidas Técnicas e Organizacionais	Deve adotar medidas técnicas e organizacionais de segurança para proteger os dados pessoais de qualquer forma de tratamento inadequado ou ilícito	Poderá adotar medidas técnicas e organizacionais essenciais, com requisitos mínimos de segurança da informação. (Para este item é indicado observar os requisitos mínimos de segurança da informação dispostos em guia orientativo elaborado pela ANPD em 2021)
	Devem implementar política de segurança da informação	Poderá implementar uma política de segurança da informação simplificada, que contemple apenas os requisitos essenciais e necessários
Direitos dos Titulares de Dados Pessoais	Deve responder às solicitações de titulares de dados no prazo de 15 dias	Poderá responder às solicitações dos titulares de dados no prazo de 30 dias

Apesar da flexibilização apresentada acima, os agentes de tratamento de pequeno porte precisam se adequar e implementar as medidas para conformidade com os demais requisitos previstos na LGPD, tal como ilustrado no item 3 dessa cartilha.

5 Após a adequação inicial, ainda preciso me preocupar com a LGPD?

Em muitos casos, as atividades de negócio mudam constantemente. Os fornecedores e funcionários mudam, os processos de negócio se alteram (alterando, portanto, como os dados pessoais são tratados), e novos produtos ou serviços podem ser desenvolvidos pela organização.

Neste sentido, o registro das operações de tratamento de dados pessoais e dos fluxos de informações deve ser continuamente documentado e atualizado. Novos processos de negócio, serviços e produtos desenvolvidos pela organização devem ser continuamente avaliados sob a perspectiva da LGPD, de modo que a conformidade com a legislação seja mantida. Também é comum que a ANPD atualize periodicamente recomendações sobre como obter o cumprimento da LGPD.

Assim, a manutenção do programa de governança em privacidade e proteção de dados é necessária ao longo de toda a existência da organização. Sem sermos exaustivos, as atividades de manutenção podem incluir:

- Avaliação de risco de novos processos de negócio, produtos e serviços oferecidos, com a implementação de medidas de mitigação de risco, sempre que possível;
- Elaboração de relatórios de impacto à proteção dos dados pessoais;
- Treinamento e conscientização contínuos dos colaboradores;
- Atualização do registro de processamento dos dados pessoais;
- Revisão periódica de documentos, como avisos de privacidade e políticas corporativas;
- Monitoramento de novas recomendações publicadas pela ANPD;
- Monitoramento e resposta a incidentes de segurança;
- Gestão de terceiros, a partir da inclusão de cláusulas de proteção de dados em contratos que envolvam o compartilhamento de dados pessoais.

Conclusão

Conforme demonstrado, a adequação à LGPD passo importante não só para manter a organização em conformidade com a legislação aplicável, mas também evitar que riscos de imagem, à marca ou aos relacionamentos comerciais com terceiros possam ser materializados, prejudicando o negócio como um todo. Apesar do projeto de adequação inicial ser complexo e robusto, contar com especialistas para auxiliar no desenvolvimento e criação de uma governança em privacidade e proteção de dados é uma das formas mais assertivas de passar por essa etapa.

Nossos reconhecimentos

Análise Advocacia (2021)

Chambers & Partners Brazil (2021 e 2022)

Leaders League (2021 e 2022)

Transactional Track Record (2021 e 2022)

The Legal 500 (2022)

Conheça nossos Sócios

Alan Campos Thomaz

Sócio

Tecnologia e Negócios Digitais, Privacidade e Proteção de Dados, Fintechs e Propriedade Intelectual

at@camposthomaz.com

+55 11 9 8375.2627 +1 (650) 6436652

Sérgio Meirelles

Sócio

Societário, M&A, Venture Capital e Wealth

sergio@camposthomaz.com

+55 11 9 7551.9865

Filipe Starzynski

Sócio

Contencioso & Law Enforcement, Consultivo Cível, Imobiliário, Trabalhista e Família

filipe@camposthomaz.com

+55 11 9 7151.9639

Juliana Sene Ikeda

Sócia

Propriedade Intelectual, Tecnologia, Contratos e Life Sciences

juliana@camposthomaz.com

+55 11 9 8644.1613

Nos acompanhe em nossas redes

campos thomaz & meirelles advogados

Assine nossa newsletter