Relatório 2 do Projeto Conjunto
"Implementação e Regulamentação Efetiva sob a Nova Lei Geral de Proteção de Dados".

Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de Proteção de Dados (LGPD)

Centre for Information Policy Leadership (CIPL) e

Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público (CEDIS-IDP)

1 Setembro 2020

Este é o segundo documento do Projeto Conjunto especial "Implementação e Regulamentação Efetiva sob a Nova Lei Geral de Proteção de Dados (LGPD)", do CIPL e CEDIS/IDP. [i] *Esse projeto busca: facilitar o compartilhamento de informações sobre a LGPD; informar e avançar a implementação construtiva, prospectiva e consistente da LGPD; possibilitar o compartilhamento de experiências e melhores práticas da indústria; e promover estratégias regulatórias eficazes relativas à LGPD—mais informações e materiais produzidos como parte deste projeto podem ser encontradas em <https://www.informationpolicycentre.com/brazilian-data-protection-implementation-and-effective-regulation.html> e <www.idp.edu.br/cedis/>.*[ii]

Contents

Checklist: Etapas Prioritárias para a Adequação à LGPD

Prioridade 1. Entender o impacto da LGPD na organização e obter a adesão da alta administração

- ☐ Compreender o impacto das regras da LGPD na organização e o uso de dados pessoais como controlador e/ou operador.
- ☐ Explicar e demonstrar à alta administração a importância da adequação às regras de privacidade e os benefícios da prestação de contas.
- ☐ Solicitar apoio da alta administração, incluindo para orçamento e recursos.

Prioridade 2. Designar o encarregado pelo tratamento de dados pessoais, e identificar e envolver os principais stakeholders

- ☐ Designar o encarregado, documentar e comunicar internamente seu papel e suas responsabilidades.
- ☐ Identificar e envolver os principais stakeholders internos e líderes sêniores que patrocinarão o programa de governança de privacidade e proteção de dados pessoais e terão responsabilidade pela implementação do programa.
- ☐ Identificar e envolver os principais stakeholders externos.

Prioridade 3. Identificar as atividades de tratamento e os dados utilizados pela organização

- ☐ Definir a metodologia para mapear e registrar as atividades de tratamento de dados pessoais efetuadas pela organização (como controladora e/ou operadora) e revisar periodicamente o ciclo de vida dos dados.
- ☐ Mapear os dados pessoais e as respectivas atividades de tratamento o mais rápido possível.
- ☐ Considerar a anonimização e minimização de dados para reduzir os riscos e o ônus decorrente da obrigação de conformidade da organização.

Prioridade 4. Determinar o papel e as obrigações da organização ao atuar como controladora ou operadora

- ☐ Determinar o papel e as obrigações da organização como controladora ou operadora.
- ☐ Comunicar essas obrigações aos indivíduos e às equipes relevantes dentro da organização.
- ☐ Considerar atualizações necessárias aos contratos dos clientes para refletir o papel da organização.

Prioridade 5. Avaliar os riscos associados ao tratamento de dados pessoais

- ☐ Implementar processo de avaliação de riscos aos indivíduos relacionados ao tratamento de dados pessoais.
- ☐ Priorizar as medidas de conformidade relacionadas ao tratamento de dados pessoais que implicam maiores riscos para os indivíduos e para a organização.

Prioridade 6. Elaborar e implementar um programa de governança de privacidade e proteção de dados pessoais que cubra as exigências da LGPD

- ☐ Elaborar um programa de governança de privacidade e proteção de dados pessoais e um plano de ação para implementá-lo com base nos riscos identificados.
- ☐ Identificar quais são as ações mais simples e implementá-las o mais rápido possível.
- ☐ Manter e revisar o programa de governança de privacidade e proteção de dados pessoais de forma contínua.

Prioridade 7. Definir as bases legais para as atividades de tratamento de dados da organização

- ☐ Identificar os indivíduos ou equipes que serão responsáveis por determinar as bases legais para o tratamento de dados pessoais—esses indivíduos deverão, como prioridade, definir em quais bases legais a organização se baseará.
- ☐ Considerar quais processos devem ser implementados e/ou adaptados para a manutenção contínua das bases legais.

Prioridade 8. Definir medidas técnicas e administrativas para garantir a segurança dos dados pessoais, assim como para elaborar relatórios internos e gerenciamento efetivos de incidentes de segurança

- ☐ Trabalhar com as equipes de segurança da informação e de arquitetura de sistemas/dados para determinar as mudanças necessárias para implementar as medidas apropriadas de segurança.
- ☐ Estabelecer um processo para a elaboração de relatórios internos, gerenciamento de incidentes de segurança, violações de dados pessoais e notificação da ANPD, se necessário.

Prioridade 9. Identificar os terceiros com os quais a organização compartilha dados pessoais e estabelecer um processo de gestão de terceiros

- ☐ Identificar os terceiros que realizam tratamento de dados pessoais em nome da organização e determinar se a organização trata dados pessoais em nome de terceiros.
- ☐ Avaliar e adotar mecanismos de gerenciamento de terceiros, incluindo processos de due diligence e a celebração de contratos relacionados ao tratamento de dados.

Prioridade 10. Identificar os fluxos internacionais de dados da organização (entrada e saída) e estabelecer os mecanismos apropriados para permitir tal transferência de dados

- ☐ Identificar se a organização transfere dados pessoais para outros países e, se o faz, para quais finalidades e em qual capacidade (como controlador ou como operador).
- ☐ Avaliar e implementar os mecanismos de transferência de dados mais apropriados.

Prioridade 11. Construir processos eficazes para transparência e gerenciamento dos direitos dos titulares de dados pessoais

- ☐ Preparar avisos de privacidade e outros recursos para fornecer informações facilmente acessíveis aos titulares de dados sobre o tratamento realizado pela organização.
- ☐ Mapear os possíveis casos de exercícios de direitos pelos titulares relacionados aos seus dados pessoais, avaliar o tempo que a organização precisaria para responder e para desenvolver os processos relevantes.
- ☐ Desenvolver processos para responder a tais solicitações.

Prioridade 12. Treinar funcionários sobre as regras da LGPD e criar um programa de conscientização

- ☐ Implementar treinamento contínuo para todos os funcionários, incluindo os terceirizados e os recém-chegados.
- ☐ Planejar atividades de treinamento e comunicação tanto no início do programa de governança de privacidade e proteção de dados pessoais quanto de forma contínua.

Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a Lei Geral de Proteção de Dados (LGPD)

I. INTRODUÇÃO

A nova Lei Geral de Proteção de Dados Pessoais (LGPD)[iii] traz novos conceitos e regras de proteção de dados para o Brasil, que não possuía norma de privacidade abrangente ou "compreensiva". Tais regras serão aplicadas tanto às organizações do setor público quanto do privado, independentemente de sua localização, desde que se enquadrem no escopo da lei.[iv]

Algumas organizações já fizeram progressos notáveis em direção à adequação com a LGPD. Entretanto, muitas organizações ainda estão nos estágios iniciais de implementação das suas exigências. Este documento pretende auxiliar essas organizações a definir e priorizar as medidas necessárias para implementar a LGPD de forma eficaz.

O programa de adequação e as medidas que as organizações construirão e implementarão dependerão de uma série de variáveis, incluindo o tamanho da organização, setor de atuação, alcance geográfico e tipo de negócio, bem como o volume, a natureza e o nível de risco de suas operações de tratamento de dados pessoais. Além disso, como mencionado, as organizações estão em diferentes estágios de implementação de leis de proteção de dados pessoais, tanto em relação às normas brasileiras como em nível global. As organizações baseadas no Brasil, particularmente as pequenas e médias empresas (PMEs), provavelmente terão que implementar um maior número de medidas de adequação em comparação às sociedades afiliadas de organizações maiores, baseadas no exterior, as quais serão capazes de alavancar seus programas globais de governança de dados para adequação à LGPD.

Finalmente, sob a LGPD, o novo regulador de proteção de dados, a Autoridade Nacional de Proteção e Dados (ANPD) será encarregada de inúmeras tarefas regulatórias que informarão, orientarão e terão impacto nas medidas específicas de adequação e implementação tomadas pelas organizações.[v] Entretanto, como uma nova autoridade, a ANPD precisará de tempo antes de poder fornecer orientações sobre todas as disposições da LGPD[vi]. Cada um dos fatores mencionados acima pode impactar a seleção e priorização das ações de implementação que sugerimos neste documento.

II. PRIORIDADES ORGANIZACIONAIS PARA A IMPLEMENTAÇÃO DA LGPD

Prioridade 1. Entender o impacto da LGPD na organização e obter a adesão da alta administração

Embora o impacto da LGPD seja diferente de uma organização para outra, todas devem compreender a importância de assumir a responsabilidade pela forma como tratam os dados pessoais. A responsabilização e prestação de contas (*accountability*) é um dos princípios centrais da LGPD [vii] (artigo 6º, inciso X e artigo 50) e é aplicável tanto aos controladores quanto aos operadores (ver a Prioridade 4). Esse princípio significa que as organizações (i) tomam medidas para traduzir os requisitos legais de privacidade e proteção de dados pessoais em ações e controles concretos, verificáveis, aplicáveis, e baseados em uma abordagem de riscos através da implementação de programas de governança da privacidade e proteção de dados pessoais, e (ii) são capazes de demonstrar a existência e a eficácia de tais ações e controles interna e externamente.

A prestação de contas começa com a garantia de que a liderança da organização compreende o valor da proteção de dados pessoais e as possíveis ramificações do descumprimento das normas sobre o tema. Este primeiro passo de adesão da liderança é necessário para assegurar o alinhamento estratégico e os recursos que serão necessários para a organização adequar-se ao novo modelo regulatório. Isso também permitirá que os administradores sêniores compreendam o perfil de risco de sua organização relacionado à privacidade e proteção de dados pessoais e, assim, possam tomar decisões informadas sobre o tratamento de dados

pessoais, levando em conta as principais atividades, prioridades de negócio, ambições e valores da organização (ver a Prioridade 5). Organizações do setor de saúde, por exemplo, podem ter um perfil de risco relacionado à privacidade e proteção de dados pessoais maior do que organizações de outros setores, principalmente no contexto da COVID-19, o que justificaria avaliações e implementação de controles mais detalhadas e maior necessidade de recursos.

Portanto, a liderança deve entender que investir em um programa de governança de privacidade e proteção de dados pessoais será benéfico para a organização, já que:

- Possibilitará o cumprimento das exigências legais e regulamentares, além de possibilitar que a organização implemente atividades confiáveis de tratamento de dados, inclusive devido à reduzida exposição ao risco de não-adequação à LGPD;
- Criará uma cultura corporativa consciente sobre privacidade e proteção de dados pessoais dentro da organização;
- Ajudará a organização a oferecer melhor proteção de dados pessoais aos seus clientes, o que impactará positivamente a aquisição e a fidelização de clientes;
- Conduzirá oportunidades de negócios assegurando a elegibilidade para parcerias comerciais que envolvam tratamento de dados pessoais;
- Aumentará a confiança das outras partes envolvidas em relações com a organização, como a mídia, investidores, reguladores, clientes e funcionários;
- Preservará vantagens competitivas e permitirá que a organização se diferencie das demais; e
- Evitará ações sancionatórias, ou, no caso de fiscalização, simplificará e reduzirá o impacto financeiro das sanções, dado que a organização estaria equipada para fornecer provas à ANPD de seus esforços de adequação.

Antes de defender a adequação e a prestação de contas perante a liderança empresarial, os indivíduos responsáveis pelo cumprimento da LGPD dentro da organização devem primeiro considerar as seguintes questões:

- Como a LGPD se aplica à organização e quais são suas exigências legais?
- Quais são as atividades de tratamento de dados pessoais realizadas pela organização? Até que ponto elas são essenciais para as suas principais atividades comerciais?
- Qual é o custo (considerando orçamento, tempo e pessoal, por exemplo) necessário para a organização se alinhar aos padrões estabelecidos pela LGPD?
- Quais exigências são novidade em comparação a outras leis brasileiras aplicáveis e regulamentações setoriais (Código de Defesa do Consumidor, Marco Civil da Internet, por exemplo)?
- Quais exigências são novidade em comparação a leis internacionais às quais a organização está sujeita em outras jurisdições (Regulamento Geral sobre a Proteção de Dados (RGPD ou GDPR), Lei de Privacidade do Consumidor da Califórnia (CCPA), Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (Canadá—PIPEDA), por exemplo? O que pode ser estendido às operações da organização no Brasil para fins de adequação à LGPD? Essas perguntas não se aplicam a organizações que operam exclusivamente dentro do território brasileiro e tratam dados pessoais apenas de indivíduos brasileiros.
- A organização já cumpre alguns dos requisitos da LGPD (inclusive através de obrigações contratuais)?
- A organização pode impulsionar processos internos e programas de governança da privacidade e proteção de dados pessoais já existentes para atender às novas exigências da LGPD, tais como

gerenciamento de riscos e de projetos, segurança da informação e estruturas de governança de dados?

- Quanto custaria (incluindo contratação de pessoal, investimento em tecnologia, atualização de sistemas de TI, etc.) colocar em prática um programa de governança de privacidade e proteção de dados pessoais a organização adequar-se à LGPD?
- Qual seria o impacto da não-observância da LGPD sobre a receita, reputação, marca e confiança dos clientes na organização? Qual seria uma possível sanção/multa da LGPD para a organização por não se adequar?
- Existem oportunidades palpáveis de negócios resultantes da implementação da LGPD (por exemplo, aumentar a confiança do usuário, ofertar um novo produto, superar a concorrência, tornar os processos internos e externos mais eficientes)?
- Quais são as expectativas de terceiros que se relacionam com a organização (por exemplo, consumidores, parceiros, clientes, acionistas) em termos de adequação com a LGPD?

Realizar uma avaliação do nível de adequação (*gap assessment*) nos estágios iniciais desse processo poderia ajudar as organizações a determinar quais são as atividades de implementação que precisam para atingir um patamar razoável de conformidade com a LGPD (ou para atingir metas empresariais relacionadas à privacidade e proteção de dados pessoais relativamente mais altas do que tal patamar) a partir do nível atual de maturidade da organização. Os resultados dessas avaliações devem constituir uma base sólida para organizações planejarem seus programas de governança da privacidade e proteção de dados pessoais e estimar seus custos.

A apresentação de fatos e números à liderança também pode auxiliar na obtenção de sua adesão. O *Data Privacy Benchmark Study 2020* da Cisco[viii], por exemplo, apresenta fatos e números sobre o retorno que o investimento em privacidade dá a organizações. Ele demonstra que existem fortes correlações entre a forma como organizações observam o princípio da *accountability* e a diminuição do número de vazamentos de dados pessoais e dos atrasos nas vendas, assim como o aumento de retornos financeiros. Ele também mostra que mais de 40% das organizações, globalmente, estão vendo retornos em dobro, pelo menos, do que gastam em privacidade e proteção de dados pessoais.

A apresentação de casos concretos de sanções e como essas impactam os negócios e a reputação das organizações também pode ajudar a defender um caso para adequação à LGPD. Os casos Netshoes[ix], Banco Inter [x] e Drogaria Araújo[xi], por exemplo, podem ser instrutivos.

Uma vez que as pessoas e equipes responsáveis pela implementação da LGPD tenham compreendido suas regras, seu impacto na organização e os passos necessários para alcançar a adequação, eles estarão equipados a apresentar tais fatos à sua liderança e solicitar os recursos necessários para implementar o programa de governança de privacidade e proteção de dados pessoais (ver a Prioridade 6).

Principais etapas a serem consideradas:

- Compreender o impacto das regras da LGPD na organização e o uso de dados pessoais como controlador e/ou operador.
- Explicar e demonstrar à alta administração a importância da adequação às regras de privacidade e os benefícios da prestação de contas.
- Solicitar apoio da alta administração, incluindo para orçamento e recursos.

Prioridade 2. Designar o encarregado pelo tratamento de dados pessoais, e identificar e envolver os principais stakeholders

Encarregado (data protection officers)

A LGPD exige que os controladores nomeiem uma pessoa encarregada pelas atividades de tratamento de dados pessoais da organização (artigo 41), o que, na prática, significa pelo seu programa de governança de privacidade e proteção de dados pessoais. Neste documento, nos referimos a esta função como o encarregado (conhecido, seja no GDPR como em diversas outras jurisdições, como *data protection officer—DPO*). O encarregado irá:

- Trabalhar como o principal ponto de contrato entre o controlador, os titulares dos dados pessoais e a ANPD (artigo 5, inciso VIII);
- Ser responsável por agir de acordo com as solicitações do titular dos dados e da ANPD (artigo 41, §2º); e
- Fornecer orientação à organização sobre proteção de dados e cumprimento com a LGPD (artigo 42, §2º).

O encarregado tem um papel fundamental no planejamento, implementação e supervisão do programa de governança da privacidade e proteção dos dados pessoais. Ele também atua como conselheiro estratégico sobre o uso responsável, eficaz e inovador dos dados pessoais pelo controlador.

A princípio, todos os controladores são obrigados a nomear um encarregado, de acordo com a LGPD. Os operadores também podem decidir por nomear um encarregado, dado que também são obrigados a implementar medidas de governança de dados (artigo 50)—o que, na prática, significa a adoção de um programa de governança da privacidade e proteção dos dados pessoais. A ANPD pode instituir regras complementares prevendo outras exigências relativas aos encarregados, incluindo situações em que a sua nomeação não será necessária com base na natureza, tamanho da organização e volume de dados pessoais tratados (artigo 41, §3º).

Para que os encarregados possam cumprir efetivamente com suas responsabilidades, as organizações devem fornecer a ele ou ela recursos adequados, que dependerão do tamanho e do nível de risco da organização relacionado à privacidade. Tais recursos podem incluir:

- Recursos humanos;
- Certificação e/ou qualificação para assegurar que o encarregado tenha, e mantenha, a experiência necessária em matéria de privacidade e proteção de dados;
- Tecnologia e ferramentas para adequação;
- Acesso a assessoria jurídica externa e assessores técnicos e de consultoria;
- Orçamento adequado e separado para as atividades, treinamento e equipe do encarregado; e
- Autonomia e independência para executar as tarefas do encarregado.

Além disso, **as organizações devem designar encarregados que tenham pelo menos alguma experiência em privacidade e proteção de dados, assim como conhecimento sobre o modelo de negócios e a estrutura de governança da organização.** Com base na experiência de mercado, existem certas habilidades que são essenciais para que os encarregados e sua equipe exerçam efetivamente suas funções. Tais habilidades incluem:

- Habilidades de liderança;
- Habilidades interpessoais e de comunicação;
- Habilidades de gerenciamento de projetos que sejam executados em diversos departamentos;

- Habilidades analíticas;
- Habilidades comerciais, incluindo a compreensão do modelo de negócios e da infra-estrutura organizacional;
- Habilidades tecnológicas; e
- Habilidades de engajamento externo.

As organizações, portanto, devem designar o encarregado, ou determinar se o seu DPO global ou Chief Privacy Officer já designado poderia também cobrir as responsabilidades do encarregado no âmbito da LGPD. **É importante que organizações também documentem o papel e as responsabilidades do encarregado e comuniquem essas informações a todos os seus funcionários**—através por exemplo de um *DPO Charter* ou política interna.

Embora organizações maiores possam indicar um encarregado com dedicação exclusiva, isto pode não ser possível para outras organizações, tais como PMEs e *startups*, devido a restrições de recursos. Entretanto, todas as organizações devem alocar a responsabilidade pelo programa de governança de privacidade e proteção de dados pessoais e auas atividades relacionadas a um indivíduo determinado e habilitado, mesmo que ele trabalhe concomitantemente em uma função diferente.

A LGPD não exige explicitamente que o papel do encarregado seja independente ou livre de qualquer conflito de interesses, mas a ANPD pode, eventualmente, emitir essa e outras regras relativas a esse papel. Entretanto, como boas prática, as organizações devem evitar atribuir um mandato que possa estar em conflito com outras responsabilidades do encarregado, em termos de alocação de tempo ou capacidade de priorização, e devem ser capazes de comprovar essa lógica.

Promotores, parceiros e equipe do programa de governança de privacidade e proteção de dados pessoais (embaixadores da privacidade)

A *accountability* depende do esforço de vários agentes, devendo ser executada horizontalmente em toda a organização. Portanto, além de designar um encarregado pelo tratamento de dados pessoais, **as organizações devem também identificar os principais indivíduos que atuariam como promotores, parceiros e os integrantes da equipe central do programa de governança de privacidade e proteção de dados pessoais**. Devem haver funções e responsabilidades claras atribuídas a cada um desses representantes, e eles devem ter claridade em relação a quem eles reportarão dentro da organização.

Muitas vezes, alguns desses representantes formam um **comitê diretor interfuncional de privacidade e proteção de dados**. Coletivamente, este grupo deve ter um conhecimento profundo das operações e negócios da organização para assegurar que seus processos, serviços e produtos relevantes relacionados ao tratamento de dados pessoais sejam cobertos pelo programa de governança de privacidade e proteção de dados pessoais.

As principais equipes da organização, que normalmente estão intimamente envolvidos com o programa de governança de privacidade e proteção de dados pessoais, incluem a equipe jurídica e os times responsáveis pela administração de risco, compliance e segurança da informação. O envolvimento de outras equipes também é fundamental para a compreensão das práticas e necessidades de negócio da organização, bem como para a implementação e atualização de processos, particularmente os relacionados ao tratamento de dados pessoais sensíveis. O nível de envolvimento dessas equipes dependerá da estrutura da organização e de suas operações. Tais equipes incluem engenharia, equipes de produtos, marketing, recursos humanos e outras.

O encarregado deve engajar e obter a adesão dessas equipes o mais rápido possível, uma vez que elas irão:

- Informar o planejamento do programa de governança de privacidade e proteção de dados pessoais;
- Informar sobre quaisquer adaptações necessárias dos programas, sistemas, políticas e processos

existentes (se forem necessárias mudanças nos sistemas, por exemplo, a equipe de segurança da informação aconselhará quanto tempo isso demandará e qual será o custo);

- Ajudar a garantir a responsabilidade de certos atores e/ou equipes pela implementação de ações e controles específicos do programa de governança de privacidade e proteção de dados pessoais; e
- Facilitar a implementação do programa de governança de privacidade e proteção de dados pessoais.

Há muitas maneiras pelas quais as organizações podem envolver tais equipes e agentes em seu programa de governança de privacidade e proteção de dados pessoais, para ajudar por exemplo a definir quais serão seus grupos de trabalho e etapas fundamentais. Exemplos são workshops, reuniões periódicas com a equipe central do programa para analisar o progresso de cada grupo de trabalho, e comitês de direção para gerentes e patrocinadores do programa.

Agentes externos

Por fim, **as organizações também devem identificar os principais agentes externos relevantes, monitorar suas atividades e se envolver regularmente com eles.** Esses *stakeholders* podem fornecer informações úteis sobre os desenvolvimentos regulatórios e legais relacionados à proteção de dados pessoais e à interpretação da LGPD, as quais podem ser relevantes para suas atividades de adequação à LGPD. Algumas organizações também pedem *feedback* para agentes externos sobre suas atividades de adequação e buscam obter informações sobre como outras organizações estão se adequando a leis de proteção de dados para fins de comparação (*benchmarking*). Exemplos de agentes externos incluem os diretores e funcionários da ANPD (quando a ANPD for estabelecida), especialistas locais em privacidade e outras organizações do mesmo setor de indústria.

Principais etapas a serem consideradas:

- Designar o encarregado, documentar e comunicar internamente seu papel e suas responsabilidades.
- Identificar e envolver os principais stakeholders internos e líderes sêniores que patrocinarão o programa de governança de privacidade e proteção de dados pessoais e terão responsabilidade pela implementação do programa.
- Identificar e envolver os principais stakeholders externos.

Prioridade 3. Identificar as atividades de tratamento e os dados utilizados pela organização

É necessário que organizações compreendam o ciclo de vida dos dados e as suas atividades de tratamento de dados para que possam cumprir com uma série de exigências da LGPD, inclusive para:

- Garantir a precisão e relevância dos dados pessoais (artigo 6, V);
- Avaliar os riscos para os indivíduos relacionados às atividades de processamento de dados da organização, e consequentemente projetar e calibrar o programa de governança de privacidade e proteção de dados pessoais (artigo 50);
- Identificar as bases legais relevantes para o tratamento de dados pessoais (artigo 7);
- Fornecer informações corretas aos indivíduos sobre suas operações de tratamento (artigo 9, II e V);
- Responder às solicitações dos titulares de dados pessoais (artigo 6, IV; artigo 18);
- Determinar quais garantias devem ser implementadas para permitir transferências internacionais de dados pessoais (artigo 33 e seguintes);

- Estabelecer registros das atividades de tratamento (artigo 37);
- Preparar relatórios de impacto à proteção de dados; e
- Fornecer informações à ANPD, se necessário (artigo 38).

Para isso, muitas organizações fazem uso de metodologias e ferramentas de mapeamento de dados. O nível de profundidade de tal mapeamento dependerá das necessidades da organização, bem como do tipo e volume de suas atividades de tratamento. O mapeamento de dados não é, entretanto, uma exigência expressa da LGPD. Na prática, a compreensão do ciclo de vida dos dados e das atividades de tratamento de dados significa que as organizações devem ter uma visão clara sobre:

- Quais dados pessoais são coletados e para quais finalidades;
- Em quais sistemas/aplicações as organizações coletam e tratam dados pessoais;
- Quem tem acesso aos dados pessoais, com quem os compartilha e por quê;
- Se as organizações compartilham dados pessoais internacionalmente; e
- Quando os dados pessoais devem ser deletados.

Esse entendimento e visão geral dos dados e suas operações de tratamento também **beneficia as organizações a partir de uma perspectiva comercial**, uma vez que:

- Promove o bom gerenciamento de dados, segurança e "higiene dos dados";
- Permite que organizações criem relações de confiança com seus funcionários, clientes e parceiros, melhorando as práticas responsáveis de tratamento de dados e mitigando os riscos comerciais; e
- Permite que as organizações identifiquem oportunidades para usos adicionais dos dados de forma inovadora através, por exemplo, da anonimização. Como os dados anonimizados estão fora do escopo da LGPD (artigo 12), a anonimização é um mecanismo que permite o uso de dados para uma gama mais ampla de propósitos.

Principais etapas a serem consideradas:

- Definir a metodologia para mapear e registrar as atividades de tratamento de dados pessoais efetuadas pela organização (como controladora e/ou operadora) e revisar periodicamente o ciclo de vida dos dados.
- Mapear os dados pessoais e as respectivas atividades de tratamento o mais rápido possível.
- Considerar a anonimização e minimização de dados para reduzir os riscos e o ônus decorrente da obrigação de conformidade da organização.

Prioridade 4. Determinar o papel e as obrigações da organização ao atuar como controladora ou operadora

É importante que as organizações definam claramente seu papel nos múltiplos cenários de tratamento de dados (através de acordos de tratamento de dados ou cláusulas específicas em contratos gerais, por exemplo). De acordo com a LGPD, as organizações podem ser controladoras e/ou operadoras de dados pessoais (artigo 5, VI e VII; artigo 39), bem como co-controladoras (artigo 1, §1º, I):

- As organizações atuam como **controladoras** quando determinam os objetivos e tomam decisões a respeito do uso e tratamento de dados pessoais (tais como em relação a seus funcionários, candidatos a emprego, clientes, contatos comerciais, website, apps e outros usuários online). Os controladores às vezes usam os operadores para realizar algum tratamento em seu nome. Como exemplo, um controlador pode utilizar um terceiro para fornecer serviços de folha de pagamento

para seus funcionários. Os controladores também podem usar operadores de dentro do seu mesmo grupo econômico. Um exemplo seria quando todas as entidades desse grupo econômico utilizam um *help desk* de TI administrado por uma entidade específica desse mesmo grupo.

- As organizações atuam como **operadoras** quando agem sob as instruções e processam dados em nome dos controladores. Um exemplo seria quando uma organização fornece *call center* ou serviços de suporte de TI para outras organizações (de grupos econômicos distintos).
- As organizações podem também atuar simultaneamente como **controladoras e operadoras**. Por exemplo, uma organização seria uma controladora se usasse seus próprios recursos para tratar os dados pessoais de seus próprios clientes, mas também seria uma operadora se fornecesse soluções de TI para outras organizações.
- Duas ou mais organizações podem ser **co-controladoras** quando determinam conjuntamente os objetivos do tratamento de dados pessoais (e também podem utilizar terceiros como operadores). Um exemplo seria um franqueador e um franqueado que determinam em conjunto os meios de tratamento dos dados pessoais dos clientes no contexto de acordos de distribuição.

As responsabilidades previstas na LGPD para os controladores e os operadores variam. Tanto os controladores quanto os operadores devem manter registros das atividades de tratamento (artigo 37) e garantir a segurança dos dados pessoais. Existem, entretanto, mais obrigações explícitas para os controladores do que para os operadores (ver o Anexo 2). Além disso, em muitos casos, os controladores podem precisar do apoio dos operadores para realizar as atividades essenciais, tais como as seguintes:

- Desenvolvimento dos relatórios de impacto à proteção de dados pessoais e das avaliações do legítimo interesse (artigo 10, §3º; artigo 38);
- Demonstrar que o consentimento é válido (artigo 8, §2º; artigo 14, §5º);
- Fornecer informações a indivíduos (artigo 8, §6º; artigo 9, §2º; artigo 10, §2º; artigo 18; e artigo 20, §1º);
- Possibilitar o exercício dos direitos do titular (artigo 18); e
- Notificar a ANPD sobre a ocorrência de incidentes de segurança em caso de danos relevantes aos titulares (artigo 48).

Portanto, **os controladores e os operadores devem manter uma relação de confiança**. A LGPD reconhece expressamente que tal cooperação é necessária, como por exemplo, para operacionalizar os pedidos dos titulares dos dados (artigo 18, §3º). Na realidade, a LGPD estabelece que, em alguns casos, tanto os controladores quanto os operadores podem ser conjuntamente responsáveis por danos causados a indivíduos resultantes de tratamento de dados (artigo 42), e também prevê exceções a tal responsabilidade conjunta (artigo 43).

Principais etapas a serem consideradas:

- Determinar o papel e as obrigações da organização como controladora ou operadora.
- Comunicar essas obrigações aos indivíduos e às equipes relevantes dentro da organização.
- Considerar atualizações necessárias aos contratos dos clientes para refletir o papel da organização.

Prioridade 5. Avaliar os riscos associados ao tratamento de dados pessoais

A LGPD é uma legislação baseada em uma abordagem de risco. **As organizações devem compreender e avaliar os riscos aos direitos e liberdades fundamentais dos indivíduos associados às suas atividades de tratamento de dados pessoais, projetos, produtos e serviços, e consequentemente implementar controles e ações mitigantes adequados**. O elemento de risco para os indivíduos—que também poderia se traduzir em riscos para a própria organização (responsabilidade e riscos reputacionais, por exemplo)—sustenta muitas das exigências da LGPD, inclusive:

- As organizações devem adotar medidas a fim de evitar quaisquer danos aos indivíduos a partir de atividades de tratamento de dados (artigo 6, VIII);
- A LGPD prevê que o tratamento de dados é "irregular" quando não protege os indivíduos de acordo com os riscos existentes (artigo 44);
- As organizações devem calibrar seus programas de governança da privacidade e proteção de dados pessoais com base nos riscos para os indivíduos (artigo 50);
- As organizações devem notificar a ANPD quando incidentes de segurança possam resultar em riscos e danos relevantes aos indivíduos (artigo 48);
- A ANPD pode exigir que que os controladores preparem relatórios de impacto à proteção de dados (artigo 38) e avaliações do legítimo interesse das organizações (artigo 10, §3º); e
- A ANPD também pode editar normas técnicas relacionadas à medidas de segurança e estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais com base em avaliações de riscos (artigo 46, §1º e artigo 55-J, VIII, respectivamente).

Há muitas maneiras pelas quais as organizações podem identificar, avaliar e gerenciar riscos relacionados à privacidade e à proteção de dados pessoais[xii]. Essas incluem a realização de relatórios de impacto e avaliações de proporcionalidade relacionada ao interesse legítimo, a integração desses relatórios de impacto ao quadro geral de genernciamento de riscos da organização, a administração dos riscos no âmbito do programa de governança de privacidade e proteção de dados pessoais e nos níveis dos produto e serviços da organização (através de revisões periódicas, por exemplo), e a avaliação dos riscos relacionados especificamente ao uso de fornecedores e terceiros. As PMEs podem desenvolver formas mais simples e ágeis de identificar, rastrear e controlar os riscos relacionados à privacidade e proteção de dados pessoais.

Existem diversas metodologias, modelos e soluções de *software* disponíveis que organizações podem utilizar para realizar avaliações de risco relacionadas à privacidade e proteção dos dados pessoais, incluindo modelos de relatórios de impacto. Veja, por exemplo, as soluções fornecidas pela Autoridade Francesa de Proteção de Dados (CNIL)[xiii], o UK Information Commissioner's Office (UK ICO)[xiv], o US NIST Privacy Framework[xv], bem como as ferramentas automatizadas oferecidas por terceiros prestadores de serviços como OneTrust[xvi] e TrustArc[xvii].

É importante que o encarregado (ver a Prioridade 2) esteja envolvido nas avaliações de risco relacionadas à privacidade e proteção de dados pessoais. Além disso, as organizações devem considerar a necessidade de treinar funcionários específicos para a elaboração de relatórios de impacto à proteção de dados e as avaliações de proporcionalidade relacionadaso ao interesse legítimo, pois esses podem exigir conhecimentos técnicos sobre privacidade e proteção de dados pessoais.

Principais etapas a serem consideradas:

- Implementar processo de avaliação de riscos aos indivíduos relacionados ao tratamento de dados pessoais.
- Priorizar as medidas de conformidade relacionadas ao tratamento de dados pessoais que implicam maiores riscos para os indivíduos e para a organização.

Prioridade 6. Elaborar e implementar um programa de governança de privacidade e proteção de dados pessoais que cubra as exigências da LGPD

A LGPD exige que as organizações implementem programas de governança da privacidade e proteção de dados pessoais, os quais devem ser calibrados a partir dos riscos relevantes identificados pela organização (artigo 50, §1º) (ver a Prioridade 5). A LGPD também detalha alguns dos elementos que esses programas devem cobrir, como políticas e procedimentos, avaliações de riscos, transparência, entre outros.

Implementar um programa de governança de privacidade e proteção de dados pessoais adequado é um processo iterativo e dinâmico que requer que as organizações se adaptem constantemente a fatores internos e externos; abordem as mudanças regulamentares, legais e tecnológicas; e mitiguem os novos riscos relacionados à privacidade e proteção de dados pessoais que elas identifiquem ao longo do programa. Tais programas podem cobrir apenas as exigências da LGPD, ou podem ter um escopo maior para cobrir as exigências de outras jurisdições. Elas podem também implementar tais programas em escala global, alavancando os esforços de adequação a leis de privacidade e proteção de dados pessoais que as organizações já tomaram em outras jurisdições.

Organizações de todos os tipos, tamanhos, culturas corporativas, setores (inclusive do setor público) podem desenvolver e implementar programas de governança da privacidade e proteção de dados pessoais adequados a seu contexto, riscos e objetivos específicos. Embora possa ser mais desafiador para as PMEs implementar um programa completo, elas também podem adotar medidas para organizar e estruturar seus esforços de governança de privacidade e proteção de dados, muitas vezes de forma mais ágil do que organizações maiores, dependendo dos tipos de dados pessoais que tratam. Além disso, a ANPD pode estabelecer regras mais flexíveis para as PMEs, dependendo dos riscos associados às suas atividades de tratamento (artigo 55-J, XVIII).

As organizações devem passar por uma série de etapas para estabelecer e implementar seus programas de governança da privacidade e proteção de dados pessoais, conforme sua estrutura interna, nível de maturidade dos programas já estabelecidos e riscos (ver a Prioridade 5). Embora algumas dessas etapas estejam descritas abaixo, elas são ilustrativas e não abrangentes:

- Identificar as lacunas da adequação da organização à LGPD (ver a Prioridade 1);
- Designar indivíduos para serem responsáveis pelo programa e para apoiar a sua implementação (ver a Prioridade 2);
- Definir o escopo do programa, grupos de trabalho, marcos fundamentais e dependências externas ou internas (como relacionadas ao setor de tecnologia da informação e segurança da informação), com consideração ao tempo necessário e disponível para implementação do programa, bem como ao orçamento, recursos e mudanças tecnológicas ou procedimentais necessários;
- Identificação de tarefas fáceis que podem ser implementadas imediatamente;
- Desenvolver um plano de ação incluindo ações específicas para atingir cada um dos marcos fundamentais do programa, quais indivíduos ou equipes serão responsáveis pela implementação de tais atividades, e as prioridades relacionadas ao programa (desenvolvimento ou atualização de

políticas, processos e procedimentos internos; modelos a serem desenvolvidos; programas de treinamento, atualização de contratos), e acompanhar a implementação de tal plano;

- Iniciar a fase de implementação, envolvendo os agentes interessados e determinando formas de trabalho (grupos de trabalho, comitês, frequência de reuniões, registro de ações, por exemplo);
- Definir como os indivíduos responsáveis pelo programa apresentarão relatórios à liderança da organização sobre o progresso e os riscos relacionados, além de desenvolver modelos e a metodologia para a elaboração de tais relatórios (por exemplo, os líderes do grupo de trabalho podem preencher *dashboards* a cada semana/mês descrevendo o *status* das ações planejadas, as razões para os possíveis atrasos, questões específicas a serem levantadas e qualquer necessidade de alteração do plano de ações); e
- Considerar como será feita a transição da implementação do programa para a sua contínua manutenção e monitoramento.

O CIPL desenvolveu uma metodologia para apoiar as organizações na estruturação e implementação de programas de governança da privacidade e proteção de dados pessoais com base nos elementos da *accountability*—o chamado CIPL Accountability Framework[xviii] (ver a figura abaixo). Como parte desse trabalho, CIPL identificou exemplos de organizações que aplicam essa metodologia a seus próprios programas de governança da privacidade e proteção de dados pessoais e listou exemplos reais e concretos em um dos seus relatórios[xix]. No Anexo 1 deste relatório, há o mapeamento das regras da LGPD ao CIPL Accountability Framework.

Principais etapas a serem consideradas:

- Elaborar um programa de governança de privacidade e proteção de dados pessoais e um plano de ação para implementá-lo com base nos riscos identificados.
- Identificar quais são as ações mais simples e implementá-las o mais rápido possível.
- Manter e revisar o programa de governança de privacidade e proteção de dados pessoais de forma contínua.

O CIPL Accountability Framework—Elementos universais de accountability

Prioridade 7. Definir as bases legais para as atividades de tratamento de dados da organização

A LGPD exige que as organizações só realizem o tratamento de dados pessoais se puderem enquadrar a situação em uma das bases legais definidas na lei (artigo 7):

- Consentimento;
- Obrigação legal ou regulatória;
- Execução de políticas públicas, suas funções públicas ou a busca do interesse público pela administração pública;
- Realização de estudos por organizações de pesquisa;
- Execução de um contrato ou atividades preliminares relacionadas ao contrato;
- O exercício regular de direitos em procedimentos legais, judiciais ou administrativos;
- A proteção de interesses vitais e da segurança física dos titulares dos dados ou de terceiros;
- A proteção da saúde pelos profissionais de saúde;
- O interesse legítimo dos responsáveis pelo tratamento ou de terceiros; e
- A proteção do crédito.

Além disso, a LGPD prevê que as organizações só podem tratar dados pessoais sensíveis se obtiverem o consentimento do titular de dados, de forma específica e destacada, para uma finalidade específica. Na ausência do consentimento do titular para o uso de seus dados sensíveis, as organizações podem se fundar em todas as outras bases legais listadas no artigo 7, exceto o cumprimento contratual, legítimo interesse e proteção ao crédito (artigo 11). Ademais, as organizações podem tratar dados pessoais sensíveis para evitar fraudes e garantir a segurança dos titulares de dados no contexto da identificação e autenticação de registros em sistemas eletrônicos (artigo 11, II, g).

A LGPD, como outras normas de proteção de dados como o RGPD na Europa, não estabelece hierarquia entre as diferentes bases legais (exceto, de certo modo, em relação ao tratamento de dados pessoais sensíveis, como visto acima). Isso significa que o consentimento não é elevado à opção preferencial acima da execução contratual, do interesse legítimo ou dos interesses vitais. Na realidade, há contextos e circunstâncias em que a obtenção do consentimento pode ser impraticável, impossível, ineficaz ou sem sentido, e pode levar ao chamado "esvaziamento do consentimento" ou "*consent fatigue*":

- Quando não há interação direta com os indivíduos;
- Quando o uso dos dados é comum, trivial e não impõe nenhum risco real à privacidade dos titulares;
- Quando o tratamento de dados é repetido e referente a grandes volumes de dados; e
- Quando a obtenção do consentimento seria contraproducente, como nas situações em que os dados são processados para evitar fraudes ou crimes, ou para garantir a segurança da informação e do sistema.

As organizações devem primeiro definir os indivíduos ou equipes responsáveis pela determinação das bases legais para o tratamento. Elas devem ter um entendimento completo das exigências da LGPD para cada base legal. A organização deve considerar atarefá-las também com a realização de avaliação relacionada ao interesse legítimo—teste de proporcionalidade necessário para determinar se o interesse legítimo é a base legais mais apropriada para determinados tratamentos de dados pessoais.

Os indivíduos ou equipes responsáveis devem definir a base legal mais adequada para o tratamento, a qual deve ser a mais apropriada para a atividade operacional específica e para o tipo de dado utilizado. Quando as organizações realizam múltiplas atividades de tratamento, elas devem avaliar a base legal adequada a cada caso específico. Por exemplo, as organizações podem basear o tratamento de dados de funcionários

para fins de folha de pagamento na execução de um contrato por um lado, e por outro podem basear a medida de temperatura corporal de seus funcionários com o objetivo de evitar a propagação da COVID-19 na proteção dos seus interesses vitais e segurança física.

Manter registros desses processos decisórios também é importante para fins de prestação de contas, pois as organizações precisam ser capazes de demonstrar a conformidade com as regras da LGPD. Na realidade, a LGPD também exige que as organizações mantenham registros das atividades de tratamento de dados, especialmente quando baseadas no interesse legítimo (artigo 37).

As organizações também devem considerar os processos a serem implementados e/ou adaptados em conexão com a definição das bases legais para o tratamento de dados pessoais:

- Os indivíduos ou equipes responsáveis pela definição das bases legais devem ser capazes de rever suas decisões caso haja novas atividades de tratamento ou caso as atividades existentes sejam atualizadas ou modificadas.
- Processos adicionais devem ser implementados em relação a bases legais específicas, como por exemplo:
    - Comprovar a conformidade do consentimento (artigo 8, §2º);
    - Permitir que os titulares cancelem seu consentimento a qualquer tempo (artigo 8, §5º);
    - Realizar avaliação de proporcionalidade relacionada ao legítimo interesse (artigo 10, §3º)
    - Assegurar que a organização só utilize dados pessoais estritamente necessários no caso de legítimo interesse (artigo 10, §1º); e
    - Adotar medidas adicionais de transparência relacionadas ao legítimo interesse (artigo 10, §2º).
- As organizações também devem combinar processos internos sempre que possível (por exemplo, processos relacionados à definição das bases legais, ao mapeamento de dados, aos registros de atividades de tratamento, os relatórios de impacto, a avaliação do legítimo interesse, etc.). Isso lhes permitirá tomar decisões informadas sobre se devem deixar de coletar dados, e apagar ou anonimizar os dados pessoais que não são mais necessários para os fins das atividades de tratamento, de acordo com o princípio da necessidade (artigo 6, III; artigo 12).

Principais etapas a serem consideradas:

- Identificar os indivíduos ou equipes que serão responsáveis por determinar as bases legais para o tratamento de dados pessoais—esses indivíduos deverão, como prioridade, definir em quais bases legais a organização se baseará.
- Considerar quais processos devem ser implementados e/ou adaptados para a manutenção contínua das bases legais.

Prioridade 8. Definir medidas técnicas e administrativas para garantir a segurança dos dados pessoais, assim como para elaborar relatórios internos e gerenciamento efetivos de incidentes de segurança

Medidas técnicas e administrativas de segurança de dados

A segurança dos dados é um dos princípios da LGPD (artigo 6, VII e artigo 46), o qual exige que as organizações utilizem medidas técnicas e administrativas aptas a proteger os dados pessoais contra acesso não autorizado, e contra tratamento, destruição, perda, modificação, comunicação ou compartilhamento acidental ou ilegal dos dados pessoais. No contexto desse princípio, as organizações devem:

- Adotar medidas de segurança de dados durante todo o ciclo de vida e de desenvolvimento do produto e serviço (artigo 46, §2º);
- Adotar medidas de segurança de dados em todos os sistemas de tratamento de dados (artigo 49);
- Garantir a segurança dos dados mesmo após o término das atividades de tratamento de dados pessoais (artigo 47); e
- Abordar a segurança de dados nos relatórios de impacto (artigo 38, parágrafo único).

As organizações devem implementar medidas técnicas e administrativas de segurança com considerações aos riscos aos indivíduos a à organização relacionados ao tratamento de dados pessoais (ver a Prioridade 5). Muitas organizações globais dedicam grupos de trabalho específicos à implementação de medidas de segurança de dados em seus programas de governança da privacidade e proteção de dados pessoais. As equipes responsáveis por esse programas têm que trabalhar em conjunto com o diretor responsável por segurança da informação, bem como com as equipes de segurança da informação e de arquitetura de sistemas/dados para determinar as mudanças necessárias no programa de acordo com os riscos, para definir o tempo de implementação do programa, e para atualizar as políticas e processos internos de acordo.

Incidentes de segurança e vazamentos de dados pessoais

Além da segurança dos dados, a LGPD também tem requisitos específicos relativos a incidentes de segurança, incluindo o vazamento de dados pessoais:

- Os programas de governança da privacidade e proteção de dados pessoais devem abordar planos de resposta e remediação para incidentes de segurança (artigo 50, §2º, I, g);
- Os controladores devem notificar a ANPD e os titulares dos dados sobre incidentes de segurança que possam resultar em riscos ou danos relevantes para os indivíduos (artigo 48); e
- A ANPD pode determinar que o controlador implemente medidas para que os efeitos do incidente de segurança sejam mitigados (artigo 48, §2º).

A falta de medidas de segurança de dados apropriadas aumenta o risco de incidentes de segurança e de vazamento de dados. **Os vazamentos de dados podem ter um impacto significativo na organização a partir de várias perspectivas**:

- Perspectiva regulatória: a ANPD pode emitir multas e o controlador pode ser considerado responsável;
- Perspectiva judicial: os indivíduos podem ajuizar ações judiciais contra os controladores e operadores, e também algumas instituições públicas podem ajuizar ações civis coletivas contra tais agentes de tratamento; e
- Perspectiva reputacional: os vazamentos de dados atraem cada vez mais atenção da mídia.

Até mesmo as organizações mais estáveis provavelmente sofrerão vazamentos de dados. Portanto, as organizações devem definir claramente uma metodologia para prevenir, identificar, avaliar, gerenciar/conter, mitigar e notificar indivíduos e a ANPD sobre tais violações. Elas também devem estabelecer processos *ad hoc* de gerenciamento de crises e testar os processos através de exercícios teóricos com a liderança e com outros agentes relevantes dentro da organização (os chamados "*table top exercises*").

Ao elaborar um processo de resposta e mitigação de danos para incidentes de segurança e violação de dados, as organizações devem considerar a implementação das etapas a seguir:

- Nomear uma equipe específica—com representantes de equipes como segurança da informação, área jurídica, comunicação e o encarregado—para gerenciar os incidentes e definir se essa equipe deve estar sempre disponível;

- Definir uma metodologia de avaliação de risco relacionado a danos oriundos de incidentes de segurança, adotar medidas de mitigação de danos apropriadas e identificar se o incidente se qualifica como um "incidente de segurança notificável" sob a LGPD, considerando a exigência da LGPD de notificar a ANPD "dentro de um prazo razoável" que pode ser especificado pela ANPD (artigo 48, §2º).
- Fornecer treinamento especializado a todos os funcionários para assegurar que sejam capazes de identificar quando um incidente de segurança ocorrer e saber onde e como ele deve ser relatado;
- Entrar em acordo com operadores e contratados sobre como estes devem relatar e fornecer informações aos controladores sobre incidentes de segurança da maneira oportuna;
- Desenvolver ferramentas, ou adotar ferramentas disponíveis no mercado, para apoiar a gestão de violações—como as oferecidas pela OneTrust[xx], TrustArc[xxi] e outros fornecedores[xxii]; e
- Garantir que o processo estabelecido inclua etapas para revisão da causa principal do incidente de segurança e a implementação de medidas para mitigar ataques contínuos ou prevenir incidentes similares no futuro (treinamento adicional, mudanças no sistema, treinamento específico, por exemplo).

Principais etapas a serem consideradas:

- Trabalhar com as equipes de segurança da informação e de arquitetura de sistemas/dados para determinar as mudanças necessárias para implementar as medidas apropriadas de segurança.
- Estabelecer um processo para a elaboração de relatórios internos, gerenciamento de incidentes de segurança, violações de dados pessoais e notificação da ANPD, se necessário.

Prioridade 9. Identificar os terceiros com os quais a organização compartilha dados pessoais e estabelecer um processo de gestão de terceiros

A LGPD estabelece obrigações específicas para as organizações quando se qualificam como controladoras e/ou operadoras (ver a Prioridade 4), inclusive a possibilidade das controladoras verificarem se as operadoras estão agindo de acordo com as suas instruções (artigo 39). Além disso, a LGPD estabelece os seguintes princípios:

- O princípio da prevenção, que estabelece que as organizações devem adotar medidas para evitar danos resultantes do tratamento de dados (artigo 6, VIII); e
- O princípio da responsabilização e prestação de contas, que estabelece que as organizações devem ser capazes de demonstrar que adotaram medidas eficientes para cumprir as regras de proteção de dados (artigo 6, X).

Os terceiros, muitas vezes, representam riscos do ponto de vista da proteção de dados. **As organizações devem compreender claramente as organizações com as quais compartilham dados pessoais e as quais realizam tratamento de dados pessoais em seu nome**, além de compreender suas funções como controladoras e/ou operadoras nesse contexto. Além disso, organizações devem **gerenciar o relacionamento com operadores e terceiros para assegurar que os dados pessoais estejam protegidos em todo o ecossistema ao qual são submetidos**. Como uma questão de boa-fé, os controladores devem escolher apenas operadores que adotem medidas apropriadas de proteção e segurança de dados e que estejam dispostos a cooperar em questões relacionadas à proteção de dados.

Existem várias formas pelas quais as organizações podem gerenciar seu relacionamento com operadores e terceiros a fim de lidar com os riscos relacionados à proteção de dados. As medidas adotadas variarão de acordo com o contexto das atividades de tratamento de dados dos operadores e dos terceiros, dos tipos de

dados utilizados e em qual medida eles se envolvem com esses terceiros. Exemplos de atividades de gerenciamento de terceiros incluem:

- Implementar políticas e procedimentos específicos para a gestão de terceiros;
- Avaliar e reavaliar os riscos de terceiros, através de diligências e medidas de segurança—o que, em particular, também pode ser útil para determinar quais mecanismos devem ser implementados para mitigar tais riscos (como atualização de cláusulas contratuais, implementação de novos contratos, auditoria de operadores de forma contínua);
- Negociação e gerenciamento de contratos (implementação de acordos de tratamento de dados, atualização de cláusulas de proteção e segurança de dados em contratos existentes, por exemplo);
- Realização de auditorias sobre o tratamento de dados pessoais realizado por terceiros, que devem ser atualizadas periodicamente; e
- Manter uma relação de parceria com os terceiros e responder às suas dúvidas e questionamentos sobre o tratamento e proteção de dados pessoais.

Principais etapas a serem consideradas:

- Identificar os terceiros que realizam tratamento de dados pessoais em nome da organização e determinar se a organização trata dados pessoais em nome de terceiros.
- Avaliar e adotar mecanismos de gerenciamento de terceiros, incluindo processos de due diligence e a celebração de contratos relacionados ao tratamento de dados.

Prioridade 10. Identificar os fluxos internacionais de dados da organização (entrada e saída) e estabelecer os mecanismos apropriados para permitir tal transferência de dados

A LGPD permite que organizações transfiram dados para para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na mesma (artigo 33, I). Na ausência de decisões sobre o nível de adequação de países e organismos internacionais por parte da ANPD, as organizações podem transferir dados internacionalmente se implementarem qualquer um dos seguintes mecanismos[xxiii]:

- Adoção de cláusulas contratuais específicas para determinada transferência internacional (artigo 33, II, a);
- Adoção de cláusulas contratuais padrão (artigo 33, II, c)[xxiv];
- Adoção de normas corporativas globais (artigo 33, II, c)[xxv];
- Adesão aos selos, certificações e códigos de conduta (artigo 33, II, d);
- Obtenção do consentimento específico do titular para uma transferência internacional (artigo 33, VIII); e
- Fundamentação em uma base legal específica—a necessidade de proteger a vida e a segurança física dos indivíduos, o cumprimento de uma obrigação legal, cumprimento de um contrato ou transferência no contexto de um processo judicial (artigo 33, IX).

A LGPD também permite transferências internacionais de dados pessoais quando:

- Necessário para a cooperação judicial entre organizações públicas (artigo 33, III);
- Necessário para a proteção da vida ou segurança física dos indivíduos (artigo 33, IV);
- A ANPD autorizar a transferência (artigo 33, V);

- A transferência resultar em compromisso assumido em acordo de cooperação internacional (artigo 33, VI); e
- Necessário para a execução de políticas e serviços públicos (artigo 33, VII).

Alguns mecanismos de transferência internacional dependem de determinações da ANPD, uma vez que cabe a essa autoridade estabelecer e especificar o conteúdo dos mecanismos de transferência internacional de dados pessoais, incluindo as cláusulas contratuais padrão, cláusulas contratuais específicas para determinadas transferências, normas e selos corporativos globais, certificações e códigos de conduta. Quando a ANPD estabelecer mais regras para tais mecanismos ou revisar os já estabelecidos por certas organizações, as empresas precisarão se adaptar de acordo.

Transferências internacionais de dados pessoais são essenciais para empresas que atuam além das fronteiras nacionais, e essas transferências são cada vez mais comuns na era da economia digital. **A fim de determinar o mecanismo mais apropriado para suas transferências de dados específicas, as organizações devem primeiro identificar quando ocorrem tais transferências e para quais finalidades**. Por exemplo, uma organização pode se basear em cláusulas contratuais específicas, enquanto outras organizações podem utilizar normas corporativas globais ao realizarem transferências sistemáticas de dados pessoais para outras empresas do mesmo grupo econômico que estejam localizadas em outros países. Esse exercício de definição dos mecanismos de transferência internacional de dados pode ser feito no contexto do mapeamento de dados (ver a Prioridade 3).

Na ausência de regulamentação por parte da ANPD, algumas organizações brasileiras estão considerando as práticas regulatórias de outros países para cumprimento com as regras da LGPD relacionadas à transferência internacional de dados, tais como as cláusulas contratuais padrão aprovadas pela Comissão Europeia[xxv] e as orientações da Diretoria Europeia de Proteção de Dados (EDPB)[xxvi]. Além disso, alguns mecanismos já foram criados no contexto da LGPD[xxvii] e **muitas organizações adotam sistemas de certificação internacionais como parte de seus programas de prestação de contas e responsabilização mais amplos**—como as certificações fornecidas pela International Organization for Standardization (ISO), pela APEC Cross-Border Privacy Rules (CBPR), e pelo National Institute of Standards and Technology (NIST). Na realidade, **essas certificações permitem que as organizações adotem uma abordagem consistente em relação à privacidade e proteção de dados pessoais em ambos os contextos nacional e internacional, e proporcionam um grau de segurança jurídica a essas organizações, especialmente na ausência de orientações adicionais da ANPD**.

Principais etapas a serem consideradas:

- Identificar se a organização transfere dados pessoais para outros países e, se o faz, para quais finalidades e em qual capacidade (como controlador ou como operador).
- Avaliar e implementar os mecanismos de transferência de dados mais apropriados.

<u>Prioridade 11. Construir processos eficazes para transparência e gerenciamento dos direitos dos titulares de dados pessoais</u>

A LGPD dá o direito aos titulares de dados de obter informações sobre aspectos específicos do tratamento de seus dados e sobre os seus direitos como titulares. Os titulares de dados devem ser capazes de acessar tais informações facilmente e essas devem ser apresentadas de forma clara, adequada e abrangente (artigo 9). Além disso, os indivíduos têm o direito de obter informações específicas a respeito de:

- Compartilhamento de dados entre organizações públicas e privadas (artigo 18, VII);
- A opção de não fornecer seu consentimento e as consequências dessa decisão (artigo 18, VIII); e
- Os critérios e procedimentos utilizados em processos de decisões automatizadas (artigo 20, §1º).

Os controladores devem implementar meios eficazes para assegurar que as informações providas aos titulares sejam atualizadas e que todas as versões de políticas de privacidade fornecidas aos indivíduos sejam devidamente armazenadas e possam ser consultadas, se necessário. É importante que as informações sejam fornecidas adequadamente, caso contrário, podem haver consequências, como a invalidação do consentimento (artigo 9, §1º). **Os controladores devem, portanto, considerar se também devem utilizar outros recursos além de políticas de privacidade para prover informações relevantes aos indivíduos**, tais como portais de privacidade, painéis de controle, vídeos, perguntas e respostas, animações, ícones, e centros de privacidade, os quais devem atualizados continuamente.

De acordo com a LGPD, os titulares de dados têm outros direitos além do direito à informação. Indivíduos devem poder exercer tais direitos gratuitamente (artigo 19, §§ 3º e 5º). Eles são os seguintes:

- Confirmação do tratamento de seus dados pessoais e acesso a tais dados, imediatamente e em formato simplificado ou de forma abrangente dentro de 15 dias após o pedido, fornecido por meio eletrônico ou físico, conforme escolhido pelo titular (artigo 19);
- Correção (artigo 18, III);
- Anonimização, bloqueio do uso ou eliminação dos dados pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD (artigo 18, IV);
- Portabilidade (ainda depende de regulamentação da ANPD - artigo 18, V);
- Eliminação de dados tratados com base no consentimento do titular, com algumas exceções previstas no artigo 16;
- Revogação do consentimento (artigo 18, IX);
- Oposição ao tratamento de dados pessoais que seja realizado a partir de uma base legal diferente do consentimento, desde que o interesse dos titulares dos dados prevaleça sobre o interesse do controlador (artigo 18, §2º); e
- Revisão das decisões baseadas exclusivamente em processamento automatizado de dados que afetam os interesses dos titulares (artigo 20).

A LGPD exige que os controles adotem medidas para atender os pedidos relacionados à proteção de dados pessoais "imediatamente". Se o controlador não estiver envolvido no tratamento em questão, ele deve comunicar esse fato ao titular de dados e, na medida do possível, especificar quem é o controlador ou operador correto (artigo 18, §4º). Esses requisitos indicam que **a LGPD permite que os titulares de dados tenham seus pedidos atendidos dentro de um prazo razoável**. Esse prazo varia de acordo com o escopo e a natureza do pedido, o tamanho da organização, quantos sistemas e bancos de dados são utilizados pela organização para o tratamento de dados pessoais e se eles são interoperáveis, e o direito específico que está sendo exercido (apagar dados em vários sistemas pode levar mais tempo do que informar os indivíduos sobre quais dados a organização possui, por exemplo). **Há uma exceção—a LGPD estabelece prazo de 15 dias para que as organizações respondam aos pedidos de acesso a dados pessoais, ainda que uma resposta simplificada seja fornecida de maneira imediata** (artigo 19).

Experiências em outros países mostraram que leis abrangentes de proteção de dados levam a um pico de solicitações relacionadas ao exercício dos direito dos titulares—veja, por exemplo, os números encontrados em relatórios anuais das autoridades europeias de proteção de dados.[xxviii] É, portanto, importante que os controladores estabeleçam processos eficazes para responder a tais solicitações. **Explorar os diferentes cenários em que os titulares exercerão seus direitos pode ser útil para os controladores terem ideia de quanto tempo demorariam para responder a pedidos e quais medidas devem tomar e, assim, definir suas prioridades**. Por exemplo, eles podem decidir adotar processos manuais (que podem ser mais onerosos, mas são operacionalmente mais rápidos), desenvolver soluções automatizadas (que podem ser dispendiosas e demorar mais tempo para serem implementadas) ou terceirizar ferramentas de gerenciamento de direitos

do titular, como as fornecidas pela OneTrust,[xxix] TrustArc[xxx] e outros.[xxxi]

Ao desenvolver processos para gerenciar solicitações relacionadas ao exercício de direitos pelos titulares de dados, os controladores devem levar em conta os seguintes elementos-chave:[xxxii]

- Os indivíduos e as equipes que estarão envolvidas no processo;
- Como verificar a identidade de um solicitante;
- Qual seria o canal e/ou a ferramenta mais apropriada para permitir que os titulares façam solicitações (por exemplo, formulários online ou endereços de e-mail específicos);
- Como identificar quando uma solicitação está vindo de canais incomuns (por exemplo, indivíduos ligando para o número da central de atendimento ao cliente);
- Como definir o escopo da solicitação;
- Se as organizações devem utilizar respostas-padrão ou determinar equipes responsáveis por responder as solicitações;
- Se a organização pretende anonimizar o dado pessoal após uma solicitação de exclusão;
- Se é necessária a cooperação dos operadores para responder a solicitações; e
- Se há algum desafio tecnológico ou de infraestrutura que precisa ser resolvido.

Além disso, as organizações devem envolver o encarregado neste processo e nas comunicações com os titulares de dados (artigo 41, parágrafo 2, I e III) e notificar imediatamente outros controladores e operadores envolvidos nas operações de tratamento quando tais solicitações forem feitas (artigo 18, parágrafo 6).

Principais etapas a serem consideradas:

- Preparar avisos de privacidade e outros recursos para fornecer informações facilmente acessíveis aos titulares de dados sobre o tratamento realizado pela organização.
- Mapear os possíveis casos de exercícios de direitos pelos titulares relacionados aos seus dados pessoais, avaliar o tempo que a organização precisaria para responder e para desenvolver os processos relevantes.
- Desenvolver processos para responder a tais solicitações.

Prioridade 12. Treinar funcionários sobre as regras da LGPD e criar um programa de conscientização

A LGPD não exige explícita que as organizações forneçam treinamento aos seus funcionários sobre questões relacionadas à proteção de dados pessoais. Entretanto, **o treinamento e a conscientização são componentes-chave para a incorporação da responsabilização pela privacidade e proteção de dados na cultura das organizações, e são também componentes-chave dos programas de governança da privacidade e proteção de dados pessoais**. Na realidade, a LGPD estabelece que as organizações devem ser capazes de demonstrar que estão empenhadas em adotar processos e políticas internas que garantam o cumprimento das suas regras, além do cumprimento das boas práticas estabelecidas em seus programas de governança da privacidade e da proteção de dados (Artigo 50, parágrafo 2, I, a).

Exemplos de atividades de treinamento e conscientização implementadas pelas organizações incluem:[xxxiii]

- Treinamento geral sobre privacidade e proteção de dados pessoais fornecido a todos os funcionários, que inclua informações sobre o programa de governança e sobre os fundamentos da proteção de dados pessoais—tais como os princípios da LGPD, obrigações básicas, direitos dos titulares, e como identificar e relatar incidentes de segurança;

- Treinamento direcionado a equipes específicas como a equipe jurídica de engenharia, desenvolvimento de produtos, analistas de dados, recursos humanos, marketing e segurança da informação;
- Plataformas de ensino à distância, vídeos e outros elementos interativos e inovadores;
- Eventos dedicados à proteção de dados para discutir tópicos e desenvolver soluções de privacidade; e
- Comunicações regulares, concisas, visuais e práticas e lembretes a todos os funcionários para abordar tópicos específicos, como perguntas e respostas, *privacy by design*, relatórios de impacto e vazamentos de dados.

As organizações devem planejar as atividades de treinamento e conscientização mais apropriadas nos estágios iniciais do estabelecimento de seu programa de governança da privacidade e proteção de dados pessoais, e devem atualizá-las de forma contínua. Elas devem definir o número, abrangência e tipo de treinamento e atividades de conscientização com base em seu número de funcionários, outros programas de treinamento e conscientização existentes, e na cultura e estrutura interna da organização. As organizações maiores devem implementar um plano mais estratégico, abrangente e estruturado de comunicação e conscientização de proteção de dados em toda a organização, que pode ser global, local ou ambos. Elas devem planejar formalmente, orçar e estabelecer campanhas e estratégias de comunicação que sejam adaptadas aos seus negócios e à sua cultura corporativa interna.

Principais etapas a serem consideradas:

- Implementar treinamento contínuo para todos os funcionários, incluindo os terceirizados e os recém-chegados.
- Planejar atividades de treinamento e comunicação tanto no início do programa de governança de privacidade e proteção de dados pessoais quanto de forma contínua.

III. CONCLUSÃO

A LGPD mudou o cenário regulatório brasileiro de proteção de dados e de conformidade, e estabeleceu várias novas exigências que organizações públicas e privadas precisarão implementar. Para muitas organizações, esta é a primeira vez que elas terão que lidar com uma lei abrangente de proteção de dados pessoais, e há muitos requisitos em aberto na LGPD que ainda precisam ser melhor especificados, particularmente pela ANPD. A proteção de dados pessoais tem sido um tópico em debate em muitas jurisdições ao redor do mundo por décadas e, na medida do possível, estas organizações devem olhar e tirar proveito da experiência internacional ao lidar com requisitos similares na LGPD.

Este relatório traz para a comunidade brasileira um conjunto de áreas que as organizações devem priorizar para o cumprimento da LGPD, com passos práticos baseados em *accountability* que organizações globais implementaram para cumprir com várias leis de proteção de dados ao redor do mundo. As organizações devem adaptar esses passos ao seu próprio contexto, levando em conta seu tamanho, tipos de atividades de tratamento e dados pessoais tratados, sua cultura corporativa interna e práticas do setor empresarial.

Se você quiser discutir qualquer um dos comentários deste documento ou solicitar informações adicionais, favor contatar Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; Giovanna Carloni, gcarloni@huntonAK.com, Laura Schertel Mendes, lsm@lauraschertel.com.br; ou Danilo Doneda, danilo@doneda.net.

Este documento foi traduzido do seu original em inglês por Isabela Maria Rosal, Giovanna Milanez, e Gabriel Soares da Fonseca. Acesse o original aqui: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-idp_white_paper_on_top_priorities_for_public_and_private_organizations_to_effectively_implement_the_lgpd__1_september_2020_.pdf>.

Anexo 1. Elementos de conformidade da LGPD mapeados ao Accountability Framework do CIPL

Liderança e Supervisão	• Encarregado pela proteção de dados pessoais • Programa de governança da privacidade e proteção de dados obrigatório sob a LGPD, o qual deve ser integrado à estrutura geral de governança da organização	
Avaliação de Riscos	• Relatório de Impacto conforme solicitado pela ANPD • Avaliação de risco de incidentes de segurança	• Abordagem baseada em risco para o desenvolvimento de códigos de conduta • Avaliação sistêmica do impacto e risco à privacidade como parte do programa de governança da LGPD
Políticas e Procedimentos	• Bases legais e processamento legítimo • Procedimentos de anonimização • Retenção e eliminação • Revisão das decisões automatizadas • Mecanismos de transferência de dados • Medidas técnicas e organizacionais internas para cumprir com a LGPD	• Medidas de segurança para os operadores • Outras medidas técnicas exigidas pela ANPD • *Privacy by design* • Contratos com fornecedores e operadores • Procedimentos de resposta ao exercício dos direitos dos titulares • Códigos de Conduta
Transparência	• Acesso às informações sobre o tratamento de dados • Medidas especiais de transparência quando o tratamento for baseado no interesse legítimo • Avisos especiais para crianças e idosos	• Objetivo do programa de governança de LGPD de criar confiança nos indivíduos através de mecanismos de transparência e participação • Publicação de códigos de conduta
Treinamento e Conscientização	• Capacidade de demonstrar o compromisso em adotar procedimentos e políticas internas resultantes do programa de governança de LGPD (treinamento subentendido)	
Monitoramento e Verificação	• Evidenciar o consentimento • Verificação do consentimento dos pais ou responsáveis legais • Avaliação de Impacto do interesse legítimo • Registros internos do tratamento de dados pessoais	• Monitoramento interno e externo do programa de governança da LGPD • Avaliação de efetividade do programa de governança da LGPD
Resposta e Aplicação da Lei	• Planos de resposta, reparação e notificação de incidentes de segurança • Auditoria para discriminação resultante de tomadas de decisão automatizadas • Responsabilidade do operador	• Demonstração da efetividade do programa de governança da LGPD • Sações por não conformidade • Consulta pública obrigatória para orientação e regulamentação pela ANPD • Audiências públicas organizadas pelo Conselho Nacional

Anexo 2. Obrigações da LGPD para controladores e operadores

Nota: as obrigações listadas na tabela abaixo referem-se a determinações da LGPD em que os termos "controlador" e "operador" são mencionadas expressa ou implicitamente e não incluem obrigações endereçadas somente às organizações do poder público (Capítulo IV). Como mencionado na Prioridade 4 deste relatório, ainda que muitas das obrigações não se apliquem diretamente aos operadores, eles precisarão se disponibilizar para oferecer suporte aos controladores no cumprimento de tais obrigações.

Obrigação	**Referência na LGPD**	**Aplicável aos controladores**	**Aplicável aos operadores**
Definição das bases legais para o tratamento de dados pessoais	Artigo 7	✓ (implícito)	X
Fornecimento de informações aos titulares de dados sobre as atividades de tratamento de dados	Artigo 8, parágrafo 6 Artigo 9 Artigo 14, parágrafo 2	✓	X
Garantia da transparência do tratamento de dados pessoais baseado no legítimo interesse	Artigo 10, parágrafo 2	✓	X
Apresentação dos relatórios de avaliação de proporcionalidade ligada ao interesse legítimo para a ANPD se requisitado	Artigo 10, parágrafo 3	✓	X
Verificação da identidade dos responsáveis legais que fornecem o consentimento em nome das crianças	Artigo 14, parágrafo 5	✓	X
Deletar os dados pessoais ao final da atividade de tratamento de dados	Artigo 16	✓ (implícito)	✓ (implícito)
Receber e responder os pedidos de direitos do titular dos dados e informar os outros controladores e operadores sobre as ações necessárias para cumprir tais pedidos	Artigo 18 Artigo 18, parágrafo 6	✓	X
Instauração de mecanismos e salvaguardas apropriados para transferência de dados	Artigo 33, II	✓	X
Manutenção de registros das atividades de tratamento de dados pessoais	Artigo 37	✓	✓
Elaboração de relatórios de impacto e apresentação dos mesmos para a ANPD se requisitado	Artigo 38	✓	X
Tratamento de dados pessoais de acordo com as instruções dos controladores	Artigo 39	X	✓
Nomeação do encarregado	Artigo 41	✓	X
Indenização pelos danos e prejuízos relacionados às atividades de tratamento de dados pessoais	Artigo 42	✓	✓
Adotação de medidas técnicas e organizacionais para garantir a segurança dos dados pessoais	Artigo 46 Artigo 47	✓	✓
Notificação da ANPD e dos titulares de dados acerca dos incidentes de segurança e adotação de medidas requisitadas pela ANPD	Artigo 48 Artigo 48, parágrafo 2	✓	X
Implementação de programas de conformidade com a LGPD	Artigo 50 Artigo 50, parágrafo 2	✓	✓

[i] Este documento foi redigido pelo *Centre for Information Policy Leadership* (CIPL) em colaboração com o *Centro de Direito, Internet e Sociedade* do *Instituto Brasiliense de Público* (Cedis/IDP). CIPL é um *think tank* sobre privacidade e segurança de dados, sediado em Washington, DC, Bruxelas e Londres. O CIPL trabalha com líderes do setor industrial, autoridades reguladores e gestores de políticas públicas para desenvolver soluções globais e melhores práticas de privacidade e uso responsável de dados a fim de permitir o desenvolvimento moderno da era da informação. O Cedis/IDP é uma instituição focada na promoção de pesquisas e debates sobre a implementação de novas leis e regulamentos que impactam a sociedade da informação, tais como os relativos à privacidade e proteção de dados, concorrência e inovação, e governança da internet. Cedis/IDP organiza eventos, workshops, grupos de pesquisa e parcerias com organizações brasileiras e globais.

[ii] Para saber mais sobre o Projeto "Implementação e Regulamentação efetiva sob a Lei Geral de Proteção de Dados (LGPD)", veja <https://www.informationpolicycentre.com/brazilian-data-protection-implementation-and-effective-regulation.html>.

[iii] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

[iv] Este documento é aplicável às organizações que se enquadram no âmbito da LGPD, de acordo com os artigos 3 e 4.

[v] Ver o documento da CIPL sobre "O Papel da Autoridade Nacional de Proteção de Dados (ANPD) sob a Nova Lei Geral de Proteção de Dados (LGPD)", disponível em: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/[en]_cipl-idp_paper_on_the_role_of_the_anpd_under_the_lgpd 04.16.2020 3_.pdf>.

[vi] Até a publicação desse documento, a ANPD não assumiu suas operações. Contudo, em 27 de agosto de 2020, o Presidente do Brasil publicou no Diário Oficial o Decreto nº 10.474/2020 que aprova a estrutura regulatória e determina as funções da ANPD. Esse Decreto será aplicável a partir da nomeação oficial do Presidente-Diretor da ANPD. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226>.

[vii] O CIPL tem trabalhado extensivamente no conceito de responsabilidade organizacional e publicou uma série de artigos delineando os elementos de responsabilidade e como as organizações podem operacionalizar a prestação de contas e a responsabilização "What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework," disponível em <https://www.informationpolicycentre.com/organizational-accountability.html>; "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society", disponível em <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf>; e "Incentivizing Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability", disponível em < https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf>. Outros documentos da CIPL sobre responsabilidade e prestação de contas também estão disponíveis no site da CIPL em <https://www.informationpolicycentre.com/cipl- white-papers.html>.

[viii] From Privacy to Profit: Achieving Positive Returns on Privacy Investments—Cisco Data Privacy Benchmark Study 2020. Publicado em janeiro de 2020. Disponível em <https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=2047256&utm_source=newsroom.cisco.com&utm_campaign=Release_2047256&utm_medium=RSS>.

[ix] Em 16 de janeiro de 2019, a Unidade Especial de Proteção de Dados e Inteligência Artificial do Ministério Público do Distrito Federal e Territórios fez um acordo com a Netshoes no contexto de uma investigação sobre a violação de dados de quase dois milhões de indivíduos, que ocorreu entre 2017 e 2018. Segundo o acordo, a empresa se comprometeu a (1) implementar medidas adicionais a seu programa de proteção de dados, incluindo o cumprimento da LGPD; (2) notificar os indivíduos sobre as violações e aumentar a conscientização dos riscos de segurança de dados; (3) aumentar a conscientização de boas práticas de privacidade e proteção de dados de outras organizações, através da participação em discussões e eventos relevantes, por exemplo; e (4) pagar uma multa de R$500.000,00 por danos morais/não materiais coletivos. O Acordo faz referência a uma série de disposições legais relativas à proteção de dados pessoais dentro da Constituição Federal, do Marco Civil da Internet, do Código de Defesa do Consumidor, bem como da LGPD, observando que a LGPD

ainda não era aplicável. Se a Netshoes não cumprir com o acordo, o Ministério Público iniciará ação civil pública no valor de R$10 milhões. Disponível em: <https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados>.

[x] Em 18 de dezembro de 2018, o MPDFT resolveu uma ação civil pública que havia sido iniciada por sua Unidade Especial de Proteção de Dados e Inteligência Artificial contra o Banco Inter pela violação de dados pessoais de quase 19.000 indivíduos. Segundo o Acordo, o banco teve que pagar R$1,5 milhão, em que parte será destinada a instituições públicas que trabalham no combate de crimes cibernéticos. O Ministério Público tinha acusado o banco de violar o CDC, que estabelece que os prestadores de serviço são responsáveis pelos danos causados aos consumidores resultantes de serviços defeituosos, inclusive quando os serviços não oferecem o nível de segurança esperado pelos consumidores (artigo 14 do CDC). Disponível em <https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de- imprensa/noticias/noticias-2018/10524-2018-12-19-10-27-31>.

[xi] Em 5 de dezembro de 2018, o Procon-MG emitiu multa de R$7 milhões a uma farmácia (Drogaria Araújo) por exigir que os consumidores fornecessem seu número de identificação a fim de obter descontos nos itens que estão sendo comprados. A autoridade alegou violações ao Código de Defesa do Consumidor com relação ao fornecimento de informações claras aos consumidores, inclusive sobre os riscos à segurança dos dados, bem como a disposição que exige que as empresas comuniquem aos consumidores, por escrito, quando serão registrados em seus sistemas. A autoridade também questionou as capacidades da farmácia para garantir a segurança de tais dados pessoais e mencionou possíveis violações de dados. Disponível em <https://www.mpmg.mp.br/comunicacao/noticias/drogaria-araujo-devera-pagar-multa-de-r-7-milhoes-por-capturar-cpf-dos-consumidores.htm>.

[xii] Ver nota de rodapé n. vi.

[xiii] Relatório de impacto à privacidade, disponível em <https://www.cnil.fr/en/privacy-impact-assessment-pia>.

[xiv] Relatórios de impacto à proteção de dados, disponível em <https://ico.org.uk/for-organisations/guide-to-data- protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>.

[xv] Estrutura de privacidade da NIST, disponível em <https://www.nist.gov/privacy-framework>.

[xvi] Relatório de impacto à proteção de dados e avaliação de proporcionalidade do legítimo interesse da OneTrust , disponível em<https://www.onetrust.com/products/assessment- automation/>.

[xvii] Relatório de impacto à proteção de dados e avaliação de proporcionalidade do legítimo interesse da TrustArc, disponível em <https://trustarc.com/gdpr-dpia-pia-solutions/>.

[xviii] Ver nota de rodapé n. vi.

[xix] Ver nota de rodapé n. vi.

[xx] Ferramenta de Gerenciamento de Incidentes e Infrações da OneTrust, disponível em <https://www.onetrust.com/incident-and- breach/>.

[xxi] Ferramenta de Gerenciamento de Incidentes e Infrações da TrustArc, disponível em <https://trustarc.com/blog/incident- response-breach/>.

[xxii] A IAPP mantém uma lista de fornecedores de tecnologia que oferecem soluções de privacidade, incluindo a gestão de respostas a incididentes e direitos do titular de dados em <https://iapp.org/resources/article/privacy-tech-vendor-report/>. Outras ferramentas utilizadas por organizações no Brasil incluem: Privally <https://privally.global/>; Pontus Vision <https://www.pontusvision.com/>; Securiti.AI <https://securiti.ai/>; MD2Net <http://www.md2net.com.br/solucoes/lgpd-suite.php>; Axon Data Governance <https://www.informatica.com/br/products/data-quality/axon-data-governance.html>.

[xxiii] Algumas outras opções possibilidades de transferência de dados internacionais estabelecidas pela LGPD são especificamente relevantes para as organizações públicas - quando as transferências são necessárias para a cooperação internacional entre órgãos de inteligência, investigação e aplicação da lei e para a execução de políticas públicas.

[xxiv] Observe que a LGPD utiliza o termo "normas corporativas globais" em referência a instrumento mencionado em outras leis de proteção de dados, como o RGPD, que menciona "regras corporativas obrigatórias".

[xxv] As cláusulas contratuais padrão da Comissão Europeia, disponíveis em <https://ec.europa.eu/info/law/law-

topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en>.

[xxvi] Uma série de documentos da EDPB sobre recomendações de boas práticas pode ser encontradas <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en>.

[xxvii] Veja, por exemplo,as certificações Abemd-Bureau Veritas <https://abemd.org.br/LGPD/Programa_Abemd_LTSA_BV_LGPD.pdf>, Abradi-Bureau Veritas <https://abradi.com.br/projetos/abradi-lanca-certificacao-para-lgpd-e-cartilha-de-protecao-de-dados-pessoais/>.

[xxviii] Por exemplo, a Comissão Irlandesa de Proteção de Dados apontou em seu Relatório Anual de 2019 que recebeu 7.214 reclamações desde que o RGPD entrou em vigor e que 6.069 violações de segurança de dados foram notificadas, representando um aumento de 71% sobre o número total de infrações de segurança de dados (3.542) registros em 2018. Relatório Anual, 1 de janeiro-31 de dezembro de 2019. Disponível em <https://www.dataprotection.ie/en/data- protection-commission-publishes-2019-annual-report>.

[xxix] Ferramenta de Gestão de Direitos do Consumidor e do Titular de Dados da OneTrust, disponível em <https://www.onetrust.com/products/data-subject-access-requests-portal/>.

[xxx] Ferramenta de Gerenciamento de Direitos Individuais da TrustArc, disponível em <https://trustarc.com/individual-rights-manager/>.

[xxxi] Ver nota de rodapé n. xvi.

[xxxii] Ver o documento da CIPL sobre os direitos dos titulares sob o RGPd em um mundo global e movido por dados, disponível em <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_data_subject_rights_under_the_gdpr_in_a_global_data_driven_and_connected_world 8_july_2020_.pdf>.

[xxxiii] Veja mais exemplos em CIPL Accountability Mapping Report— ver nota de rodapé n. vi.