SistemaOCB

inovacoop

# LGPD no cooperativismo:

## COMO SE ADAPTAR

A Lei Geral de Proteção de Dados traz impactos significativos em diversas áreas e processos. Veja como cooperativas e Unidades do Sistema OCB podem se preparar.

## CONTEÚDOS


1. Introdução: o contexto da LGPD
2. Conceitos e princípios: tudo que você precisa saber sobre a LGPD
3. Como se adaptar à LGDP
4. Oportunidades e boas práticas
5. Considerações finais

# INTRODUÇÃO:
# o contexto da LGPD

O crescimento dos casos de vazamentos de dados e fraudes na internet nos últimos anos ligou o alerta de governos, empresas e da sociedade no mundo todo. Era preciso criar mecanismos para evitar a invasão de privacidade e reduzir os ataques cibernéticos, que somente em 2019 representaram uma perda financeira de R$ 80 bilhões às empresas brasileiras, segundo levantamento da União Internacional de Telecomunicações (UIT), agência especializada da Organização das Nações Unidas (ONU).

Sob este contexto, foi criada, em 2018, a lei nº 13.709, conhecida como Lei Geral de Proteção de Dados, a LGPD. Em resumo, ela regulamenta o tratamento de dados pessoais realizado por pessoas físicas ou jurídicas no Brasil, tanto por meios físicos quanto digitais. E foi inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR, na sigla em inglês), criado em 2016 e que trata da segurança de informação dos cidadãos na Europa.

No Brasil, a LGPD vem também para suprir uma lacuna na legislação. Até então não havia uma lei específica sobre o tema, e sim algumas disposições gerais no Código Civil, Código de Defesa do Consumidor, na Lei de Acesso à informação e no Marco Civil da Internet.

O principal objetivo da LGPD é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa física. Para isso, a lei estabelece determinações que regram o tratamento de dados pessoais, afetando todos os setores da economia, incluindo as cooperativas e suas organizações de representação.

Neste manual serão abordados os principais pontos da LGPD, adequando a apresentação das determinações legais à realidade das cooperativas brasileiras e das Unidades do Sistema OCB e indicando medidas necessárias para adaptação à nova lei. Vamos começar pela teoria.


# Conceitos e princípios: tudo que você precisa saber sobre a LGPD

Para começar, você precisa entender que a lei apresenta diversos **sujeitos envolvidos** na disciplina do tratamento e da proteção de dados pessoais, cuja conceituação é de extrema importância para a compreensão e aplicação da LGPD.

Conheça-os a seguir (e guarde bem cada item, pois eles serão citados várias vezes ao longo deste e-book):

**Titular:** pessoa natural (física) a quem se referem os dados pessoais que são objeto de tratamento (exemplo de titular: cooperados, clientes, fornecedores cadastrados como pessoa física, empregados, beneficiários, entre outros);

**Controlador (agente de tratamento):** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (exemplo: o controlador pode ser a própria cooperativa ou Unidade do Sistema OCB);

**Operador (agente de tratamento):** pessoa natural ou jurídica, de direito público ou privado, que realiza (executa) o tratamento de dados pessoais em nome do Controlador;

**Encarregado (ou DPO - Data Protection Officer, de acordo com a GDPR):** pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, os Titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

A LGPD estabelece também, em seu art. 6º, **princípios que devem ser aplicados** a todas as atividades de tratamento de dados, conduzindo a interpretação e a aplicação concreta das regras dispostas na lei.

**SÃO ELES:**

- **Finalidade:** o tratamento de dados pessoais deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao Titular;
- **Adequação:** o tratamento deve ser compatível com as finalidades informadas ao Titular;
- **Necessidade:** o tratamento deve ser limitado ao mínimo necessário para a realização das finalidades, abrangendo os dados pertinentes, proporcionais e não excessivos;
- **Livre acesso:** o Titular dos dados pessoais deve ter garantia de consulta gratuita e facilitada sobre os detalhes do tratamento de seus dados;
- **Qualidade dos dados:** o Titular deve ter garantia de exatidão, clareza, relevância e atualização dos dados pessoais, de acordo com a finalidade do tratamento;
- **Transparência:** o Titular deve ter garantia de obtenção de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento de seus dados pessoais, observados os segredos comercial e industrial;
- **Segurança:** adoção de medidas técnicas e administrativas aptas à proteção dos dados pessoais contra acessos não autorizados e outros incidentes;

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

- **Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

- **Responsabilização e prestação de contas:** demonstração da adoção de medidas eficazes para comprovar o cumprimento das normas de proteção de dados.

Em resumo, com a nova legislação, o titular dos dados passa a ter direito de consultar quais dados a empresa, cooperativa, Unidades do Sistema OCB, dentre outros, tem sobre ele, como são armazenados, para qual finalidade e até pedir a retirada dos dados cadastrados. Mas de quais dados estamos falando? É isso que veremos a seguir.

## Dados pessoais

A LGPD conceitua dado pessoal como: **informação relacionada a pessoa natural identificada ou identificável.**

Ou seja, é dado pessoal tudo que possa identificar ou tornar identificável uma pessoa natural, como por exemplo, nome, dados cadastrais, endereço, profissão, localização, nacionalidade, interesses, entre outros. Importante ter atenção também com o termo "identificável" do conceito legal, pois amplia muito o conceito de dados pessoais.

### a) Dados pessoais sensíveis

Dentre os dados pessoais tratados pela lei, algumas categorias específicas receberam atenção e tratamento diferenciados pelo legislador. Destaca-se, a princípio, os dados caracterizados como dados pessoais sensíveis.

São aqueles que tratam de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referentes à saúde ou à vida sexual, genéticos ou biométricos quando vinculados a uma pessoa natural.

Além das hipóteses restritas de tratamento dos dados pessoais sensíveis, a lei **proíbe** o compartilhamento entre Controladores desses dados referentes à saúde com objetivo de obter vantagem econômica, exceto no caso de prestação de serviços de saúde, assistência farmacêutica e assistência à saúde.

### b) Dados pessoais de crianças e adolescentes

Outra categoria com tratamento diferenciado pela legislação refere-se aos dados pessoais de crianças e adolescentes, que deve ser realizado em seu melhor interesse, obedecendo ao disposto na legislação aplicável.

Para assegurar a obediência dessa determinação, a LGPD traz a obrigatoriedade de consentimento específico de um dos pais ou responsável legal da criança/adolescente, cujos dados estão sendo coletados e tratados.

A LGPD estabelece uma exceção que autoriza a coleta de dados pessoais de crianças sem o referido consentimento quando for necessária para contatar os pais ou responsável legal, desde que utilizados os dados uma única vez e sem armazenamento e qualquer forma de compartilhamento não consentida.

# Bases legais para o tratamento de dados pessoais

A LGPD apresenta dez hipóteses autorizadoras para o tratamento dos dados pessoais, previstas em um rol taxativo, que é uma lista determinada estabelecida pelo legislador, sem margem para interpretações extensivas. As cooperativas e Unidades do Sistema OCB deverão comprovar ao menos uma dessas situações a seguir para realizar o tratamento de determinados dados pessoais.

1. mediante o fornecimento de consentimento pelo Titular;

2. para o cumprimento de obrigação legal ou regulatória pelo Controlador;

3. pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições da Lei;

4. para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

5. quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o Titular, a pedido do Titular dos dados;

6. para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996;

7 para a proteção da vida ou da incolumidade física do Titular ou de terceiro;

8 para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

9 quando necessário para atender aos interesses legítimos do Controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do Titular que exijam a proteção dos dados pessoais;

10 para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Das hipóteses previstas na lei, é necessário explicar o conceito de “legítimo interesse”, que poderá ser adotado pelos Controladores como base legal para tratamento de diversos dados pessoais.

No art. 10, a LGPD determina que o tratamento dos dados pessoais deve ocorrer exclusivamente para finalidades legítimas relacionadas à operação do Controlador, consideradas a partir de situações concretas, ou seja, impede o uso dessa base de dados em situações hipotéticas e não suficientemente delineadas.

A GDPR, legislação europeia de proteção de dados, prevê que “poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o Titular dos dados e o responsável pelo tratamento, em situações como aquela em que o Titular

dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidadosa, notadamente da questão de saber se o Titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do Titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus Titulares já não esperam".

## Bases legais para o tratamento de dados pessoais sensíveis

Já o tratamento de dados pessoais sensíveis tem previsão diferenciada na legislação e deve respeitar as seguintes hipóteses:

- Com consentimento pelo Titular, de forma específica e destacada;
- Sem fornecimento de consentimento pelo Titular:
  - quando for indispensável ao cumprimento de obrigação legal ou regulatória pelo Controlador;
  - tratamento compartilhado de dados necessários à execução pela Administração Pública de políticas públicas previstas em leis ou regulamentos;
  - realização de estudos por órgão de pesquisa, garantida, sempre que possível, a **anonimização*** dos dados pessoais sensíveis;
  - processo judicial, administrativo e arbitral, este último nos termos da Lei de Arbitragem;

- proteção da vida ou da incolumidade física do Titular ou de terceiros;
- tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
- garantia da prevenção à fraude e à segurança do Titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

***Anonimização:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

## Direitos do titular dos dados pessoais

O Titular dos dados tem direito a obter do Controlador, em relação aos dados tratados por ele, a qualquer momento e mediante requisição:

- confirmação da existência de tratamento;
- acesso aos dados;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei;
- portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

- eliminação dos dados pessoais tratados com o consentimento do Titular, exceto nas hipóteses previstas no art. 16 da Lei;

- informação das entidades públicas e privadas com as quais o Controlador realizou uso compartilhado de dados;

- informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

- revogação do consentimento;

- revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

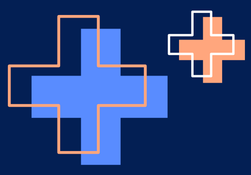
Ou seja, mediante requisição do Titular, o Controlador deve confirmar a existência do tratamento ou providenciará o acesso aos dados pessoais imediatamente (em formato simplificado) ou em até 15 dias, com declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial.

**Lembre-se**: os dados pessoais devem ser armazenados em formato que favoreça o exercício do direito de acesso pelo Titular, que poderá escolher entre obter as informações de forma impressa ou digital. Dessa forma, o Controlador deve adotar um canal de comunicação gratuito apto a gerir e atender aos direitos dos titulares.

## Situações excepcionais nas quais não se aplica a LGPD

A LGPD estabeleceu, em seu art. 4º, algumas hipóteses em que ela não se aplica ao tratamento de dados pessoais:

- quando realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
- quando realizado para fins exclusivamente jornalístico, artísticos ou acadêmicos, observados neste último caso as disposições dos arts. 7º e 11º da lei;
- quando realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, observados nestes casos as limitações imposta pelos parágrafos do art. 4º da lei;
- quando provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na lei.



# As atividades do Controlador, Operador e Encarregado

No começo do manual, nós explicamos a função de cada sujeito envolvido na LGPD. Agora, vamos entender as obrigações do Controlador e do Operador quando coletam e tratam dados pessoais. Entre outras responsabilidades, eles devem:

**a.** manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse;

**b.** quando solicitado pela Autoridade Nacional, elaborar relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados.

É de responsabilidade do Operador seguir todas as instruções fornecidas pelo Controlador, sob pena de responder solidariamente a eventuais danos causados aos Titulares.

E também cabe ao Controlador a indicação do Encarregado pelo tratamento de dados pessoais. Assim, é o Encarregado quem recebe as reclamações e comunicações dos Titulares, presta esclarecimentos, adota providências, recebe comunicações da autoridade nacional, orienta os funcionários e os contratados da cooperativa ou da Unidade do Sistema OCB a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, e executa as demais atribuições determinadas pelo Controlador ou estabelecidas em normas complementares.

Por isso, a cooperativa ou a Unidade do Sistema OCB deve indicar um profissional para ser o Encarregado de Proteção de Dados (*DPO*, na sigla em inglês), publicando a sua identidade e informações de contato, de forma clara e objetiva, preferencialmente no seu próprio site.

Com as modificações do conceito de Encarregado na LGPD, abriu-se a possibilidade dessa função ser desempenhada tanto por uma pessoa física quanto por uma pessoa jurídica, empregada ou não da cooperativa ou Unidade do Sistema OCB. Sendo assim, esse papel não precisa, necessariamente, ser exercido por um empregado, podendo, inclusive, ser terceirizado.

## Transferência internacional de dados pessoais

Se a sua cooperativa realiza operações em território internacional e, por consequência, o tratamento de dados pessoais fora do Brasil, ela precisa observar as regras previstas pela legislação, que permite a transferência internacional de dados nas seguintes hipóteses:

- para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD;
- quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência;
- quando a transferência for necessária para a proteção da vida ou da incolumidade física do Titular ou de terceiro;

- quando a autoridade nacional autorizar a transferência;
- quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
- quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público;
- quando o Titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação;
- quando o Controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do Titular e do regime de proteção de dados previstos na LGPD, na forma de:
  - Cláusulas contratuais específicas para determinada transferência
  - Cláusulas-padrão contratuais
  - Normas corporativas globais

Assim, a cooperativa ou Unidade do Sistema OCB deve ter cautela no envio de dados a organismos, companhias, outras cooperativas, empresas e entidades internacionais, respeitando sempre as hipóteses descritas pela lei e adotando procedimentos e cláusulas contratuais que documentem a adequação à LGPD.

# Regulação e fiscalização

Para garantir o bom funcionamento da lei era preciso criar um órgão responsável por regular, fiscalizar, sancionar e educar. Por isso, foi criada a **Autoridade Nacional de Proteção de Dados (ANPD)**, órgão da administração pública federal e por ora integrante da Presidência da República, submetendo-se a regime autárquico especial.

ENTRE AS FUNÇÕES DA ANPD ESTÁ, POR EXEMPLO:

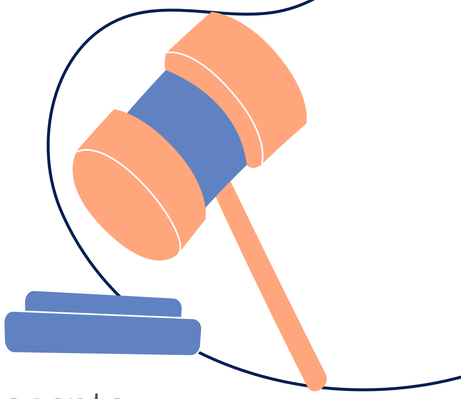
- zelar pela proteção dos dados pessoais, nos termos da legislação;
- zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos da LGPD;
- elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
- apreciar petições de Titular contra Controlador após comprovada pelo Titular a apresentação de reclamação ao Controlador não solucionada no prazo estabelecido em regulamentação;
- promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

- promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

- estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos Titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;

- promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

- dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial.



## Possíveis sanções

A LGPD prevê diversas sanções para o agente de tratamento de dados que cometer infrações às normas previstas na lei:

- advertência, com indicação de prazo para adoção de medidas corretivas;

- multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil, no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50 milhões de reais por infração;

- multa diária, observado o limite total a que se refere o inciso II;

- publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- eliminação dos dados pessoais a que se refere a infração;
- suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 06 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo Controlador;
- suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 06 (seis) meses, prorrogável por igual período;
- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Embora a lei tenha sido sancionada em 14/08/2018 e iniciado sua vigência em 18/09/2020, estas penalidades foram excepcionadas, entrando em vigor apenas 01/08/2021.

Essas penalidades serão aplicadas pela Autoridade Nacional após a instauração de procedimento administrativo, que garanta a oportunidade de defesa do agente infrator, observadas as peculiaridades do caso concreto, e considerados os seguintes parâmetros:

- a gravidade e a natureza das infrações e dos direitos pessoais afetados;
- a boa-fé do infrator;
- a vantagem auferida ou pretendida pelo infrator;
- a condição econômica do infrator;
- a reincidência;
- o grau do dano;
- a cooperação do infrator;
- a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados;
- a adoção de política de boas práticas e governança;
- a pronta adoção de medidas corretivas;
- e a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

# Como se adaptar à LGDP

Agora que você já conhece os principais conceitos da LGPD, vamos à parte prática, de adaptação.

As cooperativas e Unidades do Sistema OCB precisam implantar padrões de alta qualidade e medidas eficazes para proteger os dados pessoais que tratam e adequar suas operações às determinações legais. Para isso, é necessária a adoção de boas práticas de governança e segurança da informação, como veremos a seguir.

## Criar programa de governança

Em especial ao que se refere à proteção de dados pessoais, a LGPD determina que o Controlador poderá formular e implementar um programa de governança em privacidade.
E tal programa deve, no mínimo:

demonstrar o comprometimento da cooperativa ou Unidade do Sistema OCB em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

ser aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

ter o objetivo de estabelecer relação de confiança com o Titular, por meio de atuação transparente e que assegure mecanismos de participação do Titular;

estar integrado a sua estrutura geral de governança, estabelecendo e aplicando mecanismos de supervisão interna e externa;

contar com planos de resposta a incidentes e remediação;

ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Para tanto, as cooperativas e Unidades do Sistema OCB precisam estar com seus processos completamente adaptados à LGPD, devendo adotar um programa de conformidade específico para adequação de suas atividades aos ditames da lei, que poderá demandar a alteração de instrumentos internos, como por exemplo, estatuto social, regimento interno, etc. Para apoiá-lo nessa tarefa, sugerimos a seguir um fluxo de ações:

O primeiro passo é a realização de um **mapeamento completo**, indicando e diagnosticando todos os processos internos da cooperativa ou Unidade do Sistema OCB onde haja fluxo macro de dados pessoais, analisando a adequação das atividades realizadas e mensurando os graus de criticidade dos eventuais riscos existentes pela não conformidade dos tratamentos realizados com a LGPD.

Na prática, devem ser analisados, sob a ótica jurídica imposta pela LGPD, os processos operacionais, organizacionais e contratuais que envolvem os tratamentos de dados pessoais mediante o fornecimento de questionários e realização de entrevistas com áreas estratégicas, em conjunto com a análise de instrumentos jurídicos relevantes. Isso é necessário para se ter pleno conhecimento de como são utilizados os dados pessoais que circulam pela cooperativa ou Unidade do Sistema OCB e, com isso, planejar quais medidas devem ser tomadas visando um plano de ação.

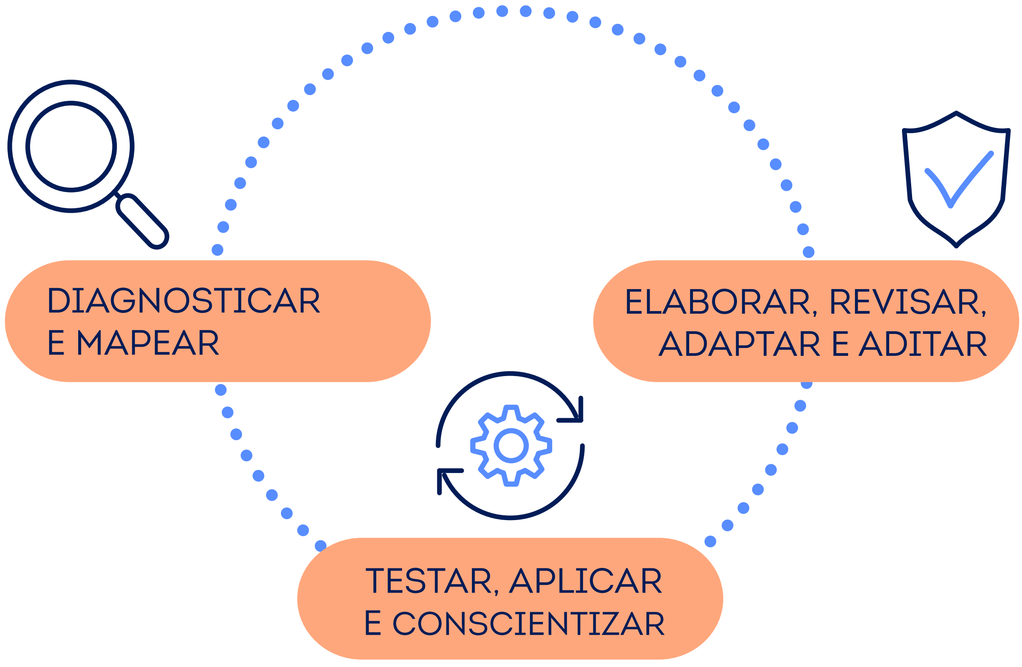
Assim, após identificados os pontos de atenção e traçadas as prioridades de ação, deve-se **elaborar, revisar, adaptar e aditar** políticas (eventualmente existentes), criar mecanismos adequados para atender aos direitos dos titulares, procedimentos e cláusulas contratuais aptas a adequar todos os processos internos da cooperativa ou Unidade do Sistema OCB com as determinações legais.

Deve-se também inserir uma rotina de treinamentos para **conscientização** da equipe quanto à importância da adoção das boas práticas recomendadas e das medidas delineadas no programa de governança.

A cooperativa ou Unidade do Sistema OCB deve, ainda, disponibilizar em seus meios de comunicação e atendimento (on-line e off-line) políticas que demonstrem a transparência no tratamento dos dados pessoais dos titulares e o atendimento das disposições trazidas pela lei.

## Análise do ciclo de vida dos dados

Todas as etapas do programa passam, necessariamente, pela análise do chamado “ciclo de vida dos dados”, que engloba três passos:

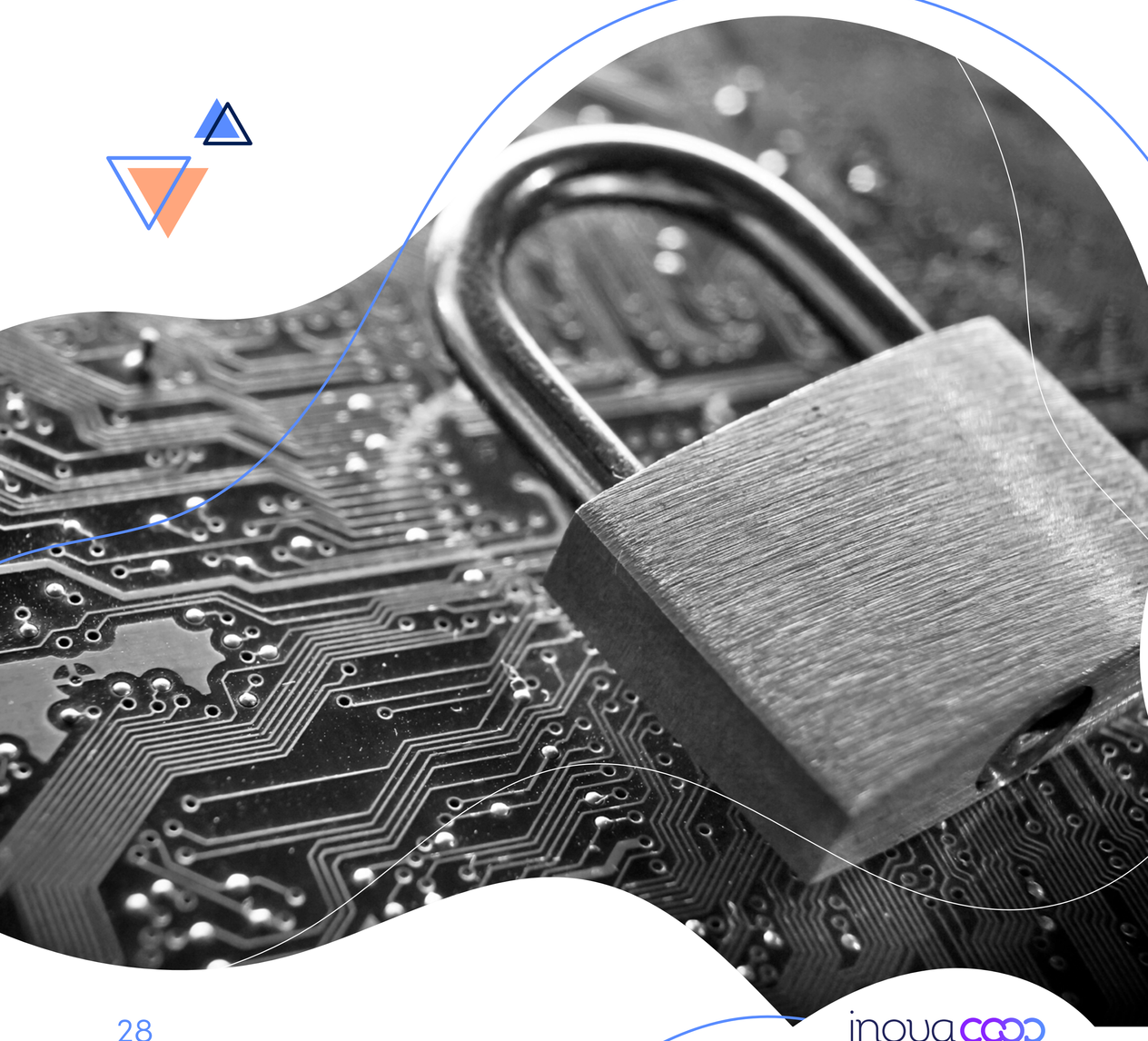


Portanto, o mapeamento e toda a condução do programa deve ser realizado mediante a obtenção de informações relevantes sobre:

1. o momento de coleta do dado pessoal pela cooperativa ou Unidade do Sistema OCB (por exemplo, o ato de realização do cadastro de novo cooperado; registro de visitas no dia de campo; assembleias; etc.);

2. o tratamento desses dados na atividade operacional da cooperativa ou Unidade do Sistema OCB, englobando as situações de compartilhamento de dados pessoais (por exemplo, o compartilhamento de dados pessoais de cooperados entre cooperativas ou com outras organizações);

3. a (in)existência de eliminação periódica dos dados pessoais a mando do Controlador (por exemplo, há eliminação de dados após certo tempo que a pessoa deixou de ser colaborador da cooperativa ou Unidade do Sistema OCB).



A implantação deste programa envolve diversas fases distintas e complementares, o que pode parecer muito complexo. Mas, em resumo, é possível estruturar uma metodologia da seguinte forma:


O andamento deste processo consome tempo e recursos e, por isso, é necessário que todas as etapas sejam conduzidas sob a ótica da materialidade e da relevância, priorizando processos importantes para os objetivos da cooperativa ou Unidade do Sistema OCB de acordo com o contexto existente.

Entenda, portanto, que o desenvolvimento de uma cultura de privacidade e proteção de dados é uma atividade contínua e que demanda aprimoramento constante. Uma vez que essa ideia esteja devidamente disseminada e internalizada nas cooperativas, haverá, além de um diferencial competitivo, a constatação de que a cooperativa se importa com a proteção dos dados pessoais que controla.

# Oportunidades e boas práticas

Sempre que surge uma mudança, seja na legislação ou não, também surgem oportunidades. No tópico anterior, trouxemos uma sugestão de programa de governança alinhado às exigências da LGPD. Para complementá-lo, vamos abordar aqui outras possibilidades e oportunidades (cooperativa ou Unidade do Sistema OCB).


A LGPD traz a oportunidade de revisar processos, áreas e até a forma de desenvolver projetos, o que demanda uma mudança contínua de cultura e, consequentemente, aumenta a segurança da organização como um todo.
No Sicredi, por exemplo, segundo Julio Cardozo, diretor executivo de riscos (e também *DPO*) da cooperativa, já existem áreas e processos dedicados à melhoria do tratamento dos dados e atendimento à legislação.
"O processo de mudança ocorre por meio de treinamentos online, workshops, ações de endomarketing, melhorias nos controles de segurança e na formação de facilitadores nas áreas, os chamados de Agentes de Riscos", conta.

Diversas áreas da cooperativa ou Unidade do Sistema OCB serão afetadas, em especial as de tecnologia e segurança da informação. Por exemplo, a LGPD prevê a criação do cargo de *DPO* (sigla em inglês para *Data Protection Officer*), um profissional que deve ficar inteiramente responsável pela segurança dos dados (de funcionários, indivíduos de fora da organização ou ambos). A lei não especifica a formação, mas precisa ser alguém com conhecimentos de legislação e também tecnologia da informação (TI). Esse profissional será responsável por prestar contas à ANPD, com o envio de relatórios sobre os impactos da proteção dos dados.

## Boas práticas para contratação do DPO

Ainda não temos na legislação ou normativos especificações de formação para indicação do DPO. Porém, para o setor público, a Instrução Normativa SGD/ME nº 117, de 2020, indica os requisitos mínimos para exercer o cargo de DPO e podem ser utilizados como referência de boa prática:

- Deverá possuir conhecimentos multidisciplinares essenciais à sua atribuição, preferencialmente, os relativos aos temas de: privacidade e proteção de dados pessoais, análise jurídica, gestão de riscos, governança de dados e acesso à informação no setor público.
- Não deverá se encontrar lotado nas unidades de Tecnologia da Informação ou ser gestor responsável de sistemas de informação do órgão ou da entidade.

Além da figura do *DPO*, existe uma tendência natural que o departamento de TI seja peça-chave do processo de adequação à LGPD e, com isso, exista uma demanda por mais investimentos na área. Os profissionais de TI já cuidam dos dados armazenados na nuvem ou em servidores das empresas, além de monitorarem riscos de ataques virtuais.

Com a LGPD, todos os dados terão de ser criptografados para que, em caso de vazamento, não possam ser lidos por terceiros. Também será preciso investir em soluções de VPN e firewall, além de outras opções de conexão e armazenamento seguros. E não podemos esquecer da atualização e conhecimento do profissional sobre boas práticas de segurança e de processamento de dados. Ou seja, investimentos em cursos e certificações.

## Segurança da informação para novos projetos

Segundo o Guia de Boas Práticas da LGPD, produzido pelo Governo Federal, outra área que ganha destaque é a da segurança da informação, que passa a ser essencial para a concepção e execução de produtos e serviços. Isso apresenta um conceito fundamental para a proteção da privacidade dos dados pessoais denominado **Privacidade desde a Concepção** (do inglês *Privacy by Design*).

O conceito de **Privacidade desde a Concepção (PdC)** significa que a privacidade e a proteção de dados devem ser consideradas durante todo o ciclo de vida de projetos, sistemas, serviços, produtos ou processos - o que tem relação direta com as iniciativas de inovação, tão atuais no momento. Tal privacidade pode ser alcançada por meio da aplicação de 7 princípios fundamentais, destacados a seguir.

## 1 Proativo, e não reativo; preventivo, e não corretivo

A abordagem de PdC é caracterizada por medidas proativas e não reativas. Ou seja, essa abordagem antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. Assim, sua cooperativa ou Unidade do Sistema OCB não precisa esperar que riscos de privacidade se materializem nem ofereçam soluções para as infrações de privacidade após a ocorrência, mas sim impedir que eles ocorram. Ou seja, a Privacidade desde a Concepção vem antes do fato, não depois.

Se aplicada a tecnologias da informação, práticas organizacionais, projeto físico ou em rede de ecossistemas de informação, a PdC começa com um reconhecimento explícito do valor e dos benefícios de adoção de práticas de privacidade fortes, de forma precoce e consistente. Por exemplo, prevenindo a ocorrência de violações de dados, internas ou externas.

## 2 Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio

A privacidade por padrão procura oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática de negócios. É uma forma de evitar que qualquer ação seja necessária por parte do titular dos dados pessoais para proteger a sua privacidade, pois ela já estará embutida no sistema, por padrão.

## 3 Privacidade incorporada ao projeto (design)

A privacidade deve estar incorporada ao projeto e arquitetura dos sistemas de TI e práticas de negócios. Isso significa que não deve ser considerada como complemento após o sistema, projeto ou serviço já estar em implementação ou em execução. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. Ou seja: a privacidade é parte integrante do sistema, sem diminuir a funcionalidade.

Ela deve ser incorporada às tecnologias, operações e arquiteturas de informação de maneira holística, integrativa e criativa. Para isso, deve-se adotar uma abordagem sistemática apoiada em padrões e frameworks reconhecidos, os quais devem dever ser revistos e passíveis de auditorias externas.

## 4 Funcionalidade total

A PdC não envolve simplesmente a formalização de declarações e compromissos de privacidade. Refere-se a satisfazer todos os objetivos do projeto, não apenas os objetivos de privacidade. A PdC é habilitadora duplamente em natureza, permitindo funcionalidade total com resultados reais e práticos.

Ao incorporar privacidade em uma determinada tecnologia, processo ou sistema, isso é realizado de uma forma que não comprometa a plena funcionalidade e permita que todas as exigências do projeto sejam atendidas.

A questão da privacidade é frequentemente vista como de nenhuma ou baixa relevância e que compete com a objetividade do projeto, com as capacidades técnicas de um produto ou serviço e com outros interesses das partes envolvidas. A PdC visa justamente contrapor essa visão, pois visa satisfazer todos os objetivos da instituição, e não somente os de privacidade.

## 5 Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados

Por ser incorporado ao sistema antes de o primeiro elemento de informação ser coletado, a PdC estende-se por todo o ciclo de tratamento dos dados envolvidos no projeto, sistema ou serviço. Medidas fortes de segurança são essenciais para a privacidade, do início ao fim.

A privacidade deve ser protegida continuamente em todo o domínio e ao longo do ciclo de vida do tratamento dos dados em questão. Não deve haver lacunas na proteção ou na prestação de contas. O princípio “Segurança” tem relevância especial porque, em sua essência, sem segurança forte, não pode haver privacidade.

Os padrões de segurança aplicados devem garantir a confidencialidade, integridade e disponibilidade dos dados pessoais durante todo o seu ciclo de tratamento, incluindo, entre outros, métodos de destruição segura, criptografia apropriada, e métodos fortes de controle de acesso e registro.

## 6 Visibilidade e transparência

A PdC busca garantir a todos os interessados que, independentemente da prática ou tecnologia comercial envolvida, está de fato operando de acordo com as premissas e objetivos declarados, os quais devem ser objeto de verificação independente. Esse cenário pode ser sintetizado pelo seguinte lema: **confie, mas verifique!**

Visibilidade e transparência são essenciais para estabelecer responsabilidade e confiança. A avaliação independente deste princípio fundamental deve concentrar-se sobre os seguintes aspectos: responsabilização, abertura para a prestação de contas e conformidade.

## 7 Respeito pela privacidade do usuário

Por fim, a cooperativa ou Unidade do Sistema OCB precisa entender que a privacidade desde a concepção exige respeito aos direitos dos titulares dos dados pessoais. Isso é alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular dos dados.

Os melhores resultados da privacidade desde a concepção, geralmente, são aqueles projetados de acordo com os interesses e necessidades dos titulares dos dados pessoais, que têm o maior interesse em gerenciar seus próprios dados.

Empoderar os titulares de dados a desempenhar um papel ativo no gerenciamento de seus próprios dados pessoais pode ser o meio mais eficaz de verificação contra abusos de e uso indevido.

# A adaptação das cooperativas

Segundo pesquisa da Serasa Experian, cerca de 86% das grandes corporações do país afirmam estar preparadas para garantir os direitos e deveres exigidos pela LGPD. E as cooperativas fazem parte dessa estatística. Muitas delas criaram site específicos sobre o tema, com explicações, política de uso de dados e espaço para apontamentos por parte dos seus associados e clientes. Como exemplo, selecionamos alguns dentre vários exemplos que existem no setor: Central Nacional Unimed, Sicredi, Sicoob, Ailos, Unicred.

A adaptação vem ocorrendo desde que a lei entrou em vigor, em especial para as cooperativas financeiras, que atuam em um setor marcado por fraudes e ataques cibernéticos. “No nosso segmento essa sempre foi uma preocupação, pela enorme quantidade de dados de clientes e associados, mas a legislação vai aumentar ainda mais os cuidados e, com isso, evitar os riscos de abusos e violação ao direito à privacidade”, afirma Maria Luisa Lasarim, diretora operacional do Sicoob Central SC/RS, em matéria da EasyCoop.

O gerente de TI, David Blasdavênio Machado, reforça que o Sicoob SC/RS vem cumprindo todas as regras da LGPD e que esta sempre foi uma preocupação da instituição. Por isso, tem realizado constantes treinamentos com os cerca de 6 mil funcionários e dirigentes.

Em webinar promovido pelo Grupo de Segurança e Privacidade de Dados da Assespro-RS, o gerente de riscos não-financeiros e controles internos do Sicredi, Jeferson Thomas, destacou que quatro pilares que foram escolhidos como processos-chave na organização da LGPD no Sicredi: treinamento e conscientização; ambiente de cibersegurança e infraestrutura; avaliação de cada operação de tratamento de dados; e o pilar jurídico.

Ele avaliou também o papel do Encarregado de Dados na estruturação de toda regulamentação permeada pela legislação. “Um *DPO* sozinho não vai realizar todas as ações que precisa fazer para responder à LGPD. É preciso ter uma série de processos bem estruturados”, disse.

# Considerações finais

Você já deve ter ouvido em algum momento que os dados são os bens mais valiosos atualmente. E quem tem informação tem poder, não é mesmo? Quanto mais informações sobre nós as organizações tiverem, mais terão condições de oferecer produtos e serviços com base em nosso comportamento on-line. Então, de fato, o tema é relevante e merece bastante atenção, e não apenas para cumprir a lei. Inclusive, falamos neste post do InovaCoop sobre a importância dos dados.

Tratar a LGPD de forma estratégica pode ser essencial para o negócio - inclusive para a criação de novos projetos já adaptados à lei, como vimos neste manual - e para melhorar a experiência dos cooperados e clientes.

Se você deseja se aprofundar no tema, assista ao webinar **Proteção de Dados na Prática, do Sistema OCB**, que contou com as participações de Patrícia Peck, advogada especialista em Direito Digital, Propriedade Intelectual, Proteção de Dados e Cibersegurança; e Cristhian Groff, advogado especialista em Direito Cível empresarial e Direito Digital. E veja também um "giro" pela lei, com as principais transformações que ela traz ao país.

inova.coop.br

SistemaOCB

sistemaocb

somoscooperativismo.coop.br

Contéudo desenvolvido em parceria com

MARTINELLI
ADVOGADOS

coonecta
COOPERATIVISMO E INOVAÇÃO

coonecta.me