CAPCO

LGPD: CONTAGEM REGRESSIVA

COMO ESTAR EM CONFORMIDADE COM
A LEI GERAL BRASILEIRA DE PROTEÇÃO DE DADOS

CONTEXTO GERAL DETALHADO – O QUE É A LGPD?

LGPD é o acrônimo de Lei Geral de Proteção de Dados e refere-se especificamente à lei número 13.709 do ano de 2018, que dispõe sobre o tratamento de dados pessoais, por pessoa física ou jurídica e objetiva principalmente proteger os direitos fundamentais de liberdade e de privacidade individual.

Qual a origem da LGPD?

As definições gerais da LGPD tiveram início com a lei 12.065/14, mais conhecida como "Marco Civil da Internet", mas após a Europa colocar em vigor a GDPR (General Data Protection Regulations), o órgão brasileiro responsável iniciou a revisão por meio da introdução de conceitos e regulações mais atuais, surgindo então, em 14 de agosto de 2018, a "primeira versão" da atual LGPD.

A quem se aplica?

A Lei aplica-se a qualquer operação de tratamento realizada por pessoa física ou jurídica, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

- A operação de tratamento seja realizada no território nacional;
- A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
- Os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Agora, atenção! A Lei não se aplica, principalmente, se o tratamento dos dados tiver caráter puramente particular e não econômico ou se for para fins jornalísticos, de segurança pública, defesa nacional ou investigações criminais.

Quando entra em vigor?

Até a última revisão deste artigo (Junho de 2020), a LGPD terá vigor em Janeiro de 2021, com sanções podendo ser aplicadas a partir de Agosto de 2021. No entanto, há discussões no Congresso Brasileiro sobre a postergação destas datas, devido à pandemia do COVID-19, entendendo que parte das empresas não estariam preparadas para atender as exigências da lei.

O que mudará nas organizações?

Muita coisa. A principal é o "sentido" da fiscalização. A partir da vigência, as empresas não devem esperar uma fiscalização ou auditoria para se adequarem, mas devem indicar espontaneamente à ANPD sua conformidade, principalmente no que se refere ao relacionamento com ao dono do dado pessoal (pessoa física) e os contratos com os processadores.

Outros pontos que mudaram são os conceitos sobre os papéis envolvidos durante todo o ciclo de vida do processamento do dado pessoal. São conceitos que todas as organizações devem conhecer e identificar dentro de suas estruturas, de modo que seja possível identificar os responsáveis e envolvidos para que possíveis ações possam ser direcionadas eficientemente.

Quais as consequências do não cumprimento? Qual o valor da multa?

Em caso de vazamento de dados, a organização pode sofrer sanções financeiras, que não são baixas, chegando a 2% do faturamento anual da empresa - limitado à R$ 50.000.000,00

(cinquenta milhões de reais). Esse valor é por incidente ocorrido. Outras consequências também estão previstas, tais como multa diária até a adequação organizacional e técnica, bloqueio dos dados pessoais (relacionados ao incidente) e advertências com indicação de prazo para adoção de medidas corretivas.

Atenção para o seguinte ponto: a responsabilidade em caso de qualquer infração é do CONTROLADOR e não do PROCESSADOR ou do ENCARREGADO DE DADOS, apesar de estarem envolvidos no plano de recuperação. Leia mais sobre estes papéis no capítulo 2 deste artigo.

Outra consequência está ligada à imagem da organização. Uma empresa que tem os dados de seus clientes vazados, pode, por exemplo, sofrer a retirada de investimentos de acionistas ou perder a confiança de seus clientes, que podem solicitar a portabilidade (vide item 1.6.6 deste artigo) de seus dados para o concorrente.

A ANPD avaliará caso a caso eventual infração, validando, por exemplo, se a organização adotou ações preventivas, tais como a adoção de política de boas práticas e governança ou medidas corretivas. Isso refletirá na sanção a ser aplicada.

Quais as vantagens para a população geral?

A partir do momento da vigência da LGPD, todo cidadão brasileiro terá uma série de direitos que, essencialmente, referem-se à transparência sobre o processamento de seus dados pessoais. Teremos:

- **Direito de ser informado:** os titulares dos dados deverão ser informados de forma clara e transparente sobre a coleta e processamento de seus dados, bem como a finalidade pretendida.
- **Direito de acesso:** os titulares deverão ter livre acesso a seus dados.
- **Direito de retificação:** os titulares terão direito à correção de dados que estiverem incorretos.
- **Direito de apagar:** o titular terá direito de ser esquecido, ou seja, de apagar seus dados da base do controlador. Contudo, aqui é importante atenção, pois havendo interesse legítimo, o controlador poderá manter certos dados, como por exemplo, dados sobre dívidas.
- **Direito de limitar o processamento:** o titular também terá direito de solicitar a interrupção do processamento de seus dados.
- **Direito de portabilidade dos dados:** refere-se à exportação dos dados para envio ao titular ou a outro controlador.
- **Direito de oposição:** refere-se ao direito de se opor ao processamento de seus dados.
- **Direito em relação a decisões automatizadas:** o titular tem o direito de não ficar sujeito exclusivamente a decisões baseadas em processamento automatizado, incluindo definição de perfis.

O que devo ser feito em caso de vazamento de dados pessoais?

Caso haja vazamento de dados pessoais, o controlador deverá comunicar o ocorrido à autoridade nacional e ao titular dos dados. Aqui cabem algumas observações importantes.

CONTEXTO GERAL DETALHADO – O QUE É A LGPD? (CONTINUED)

O artigo 48 da lei descreve que essa comunicação deve ser feita “em prazo razoável”. Portanto aqui, sugere-se seguir os padrões da GDPR, segundo os quais a comunicação deve ocorrer em até 72 horas a partir da ciência do fato.

A comunicação deverá mencionar, minimamente, a descrição da natureza dos dados pessoais afetados, as informações sobre os titulares envolvidos, as medidas técnicas e de segurança utilizadas para a proteção dos dados (observados os segredos comercial e industrial), os riscos relacionados ao incidente e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Sugere-se ainda que uma governança para tais vazamentos e comunicação sejam implementadas para garantir padronização e rastreabilidade junto à ANPD.

DEFINIÇÕES GERAIS

As definições abaixo deverão ser conhecidas por todas as organizações às quais a lei se aplica, pois as comunicações da ANPD utilizarão esses termos em comunicados ou auditorias.

ANPD - Autoridade Nacional de Proteção de Dados

Incluída pela lei 13.853 de 2019, a ANPD é um órgão da administração pública federal, integrante da Presidência da República, e ajudará a regular e fiscalizar o cumprimento da LGPD, incluindo editar as normas de proteção de dados, monitorar o cumprimento da lei, implementar ferramentas que melhorem a comunicação entre empresas, autoridades e titulares, fazer estudos sobre proteção de dados no exterior e aplicar sanções.

Controlador

A LGPD define o controlador como “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”.

Em outras palavras, o controlador é parte responsável por garantir que os dados pessoais sejam processados de acordo com os regulamentos da LGPD e geralmente será a entidade de contato direto com o público.

É sobre o controlador que GDPR e LGPD impõem maior peso jurídico; ou seja, o controlador é a parte responsável em caso de violações e deve garantir que os dados pessoais sejam processados de acordo com os regulamentos.

DEFINIÇÕES GERAIS (CONTINUED)

Suas tarefas principais são:

- Determinar a finalidade das atividades de processamento.
- Designar um DPO (se requerido pela lei).
- Cumprir os direitos dos titulares.
- Implementar medidas técnicas e organizacionais para garantir a proteção de dados e demonstrar que o processamento é realizado de acordo com os regulamentos.
- Implementar políticas e governança apropriadas.
- Realizar análises de impacto de proteção de dados (AIPDs).
- Assegurar que o processador terceirizado cumpra as regras do GDPR e da LGPD.
- Notificar violações de dados pessoais à autoridade supervisora e titular, quando requerido.

Processador

A LGPD define o processador como "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador". Em outras palavras, processadores são entidades contratadas pelo controlador para executar alguma função relacionada aos dados pessoais.

Suas tarefas principais são:

- Somente executar atividades de processamento sob controle de um controlador.
- Garantir que as pessoas autorizadas a processar os dados pessoais se comprometeram com a confidencialidade ou estão sob uma obrigação estatutária de confidencialidade.
- Tomar todas as medidas de segurança do processamento.
- Se um processador infringir a LGPD e for ele quem determina as finalidades e os meios de processamento, ele será considerado um controlador no que diz respeito a esse processamento. Significa que, em caso de violação, a responsabilidade maior recairá sobre o processador.
- Determinar aspectos técnicos do processamento, tais como os sistemas usados para processamento, a forma como os dados são armazenados, as medidas de segurança, os mecanismos de transferência etc.

Importante: O processador não deve subcontratar outro processador sem autorização prévia específica, por escrito, do controlador.

Encarregado pela proteção de dados (DPO)

Esse é um dos papeis incluídos tanto pela GDPR quanto pela LGPD.

Também globalmente conhecido como Data Protection Officer, ele(a) é, segundo a definição da LGPD, "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)".

Seguem abaixo algumas considerações sobre essa posição:

- Ele(a) deve reportar-se ao mais alto nível de gestão do controlador, idealmente, fazendo parte de uma área de risco/conformidade ou governança.

DEFINIÇÕES GERAIS (CONTINUED)

- Dentro do ciclo de vida do dado pessoal, ele(a) pode existir tanto para o controlador (Empresa A), quanto para o processador (Empresa B). Vide o item 2.5 deste artigo para maior clareza.

- O DPO não precisa ser um funcionário interno ou dedicado a esse papel.

- Um único DPO (se facilmente acessível) é permitido para "um grupo de empresas" e para "um grupo de autoridades ou organismos públicos". (Artigo 37 (2) do GDPR).

Suas tarefas primárias são:

- Informar e aconselhar o controlador ou o processador e os funcionários sobre suas obrigações referentes ao GDPR e à LGPR.

- Monitorar a conformidade com GDPR/LGPD, incluindo supervisionar documentação, processos e registros.

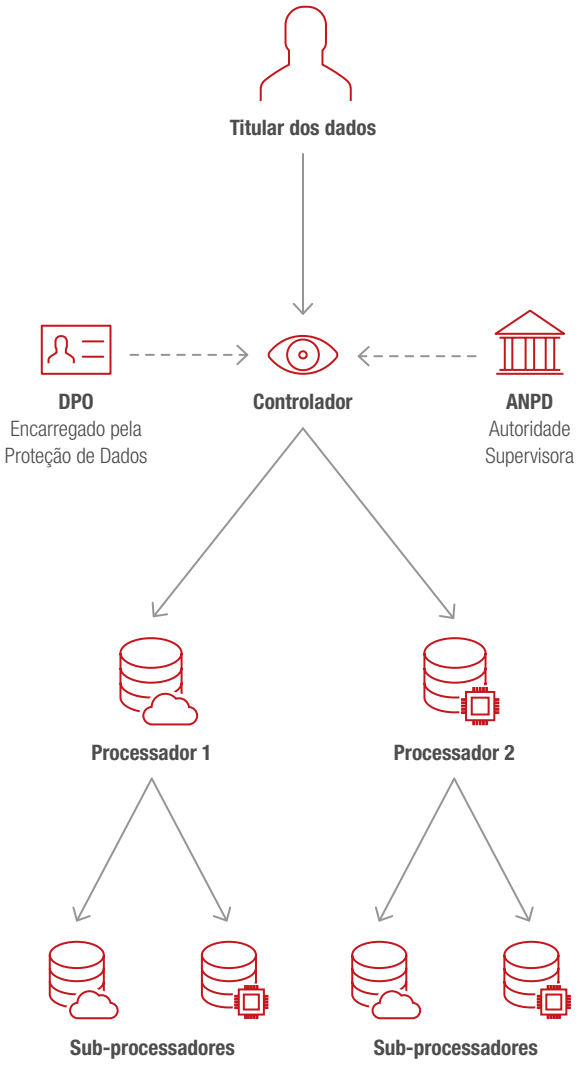
- Dar conselhos, quando solicitado, no que diz respeito à avaliação do impacto da proteção de dados (AIPD).

- Cooperar com a autoridade supervisora.

- Atuar como ponto de contato para a autoridade supervisora.

Relacionamentos entre Controlador, Processador, DPO e ANPD

O modo mais fácil de exemplificar o relacionamento entre esses papéis está apresentado na figura abaixo, mas não se limita apenas a esse formato, pois um processador também pode ser um controlador e vice-versa, dependendo da complexidade dos processamentos.



Relacionamento entre papéis na LGPD

Note que o DPO, ou Encarregado pela Proteção de Dados, pode ser uma figura externa à organização; ou seja, ele pode ser o encarregado em uma ou mais organizações. Apenas lembrando que, segundo a LGPD, conforme descrito neste artigo, deve ser uma pessoa física e não uma pessoa jurídica.

DEFINIÇÕES GERAIS (CONTINUED)

Dado Pessoal e Dado Pessoal Sensível

Segundo definição formal da lei, dado pessoal é a informação relacionada à pessoa natural identificada ou identificável.

O conceito de dados pessoais não se limita a informações que, se usadas indevidamente, possam ser consideradas prejudiciais à vida privada e familiar do indivíduo. O meio em que a informação está contida não é relevante: o conceito de dados pessoais inclui informações disponíveis sob qualquer forma – texto, figuras, gráficos, fotografia, vídeo, meio acústico ou qualquer outro meio possível que leve à identificação do sujeito de modo direto ou indireto.

Dado pessoal sensível é aquele sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

Para se processar dados sensíveis, as organizações precisam possuir justificativas muito bem embasadas e podem requerer autorização formal da ANPD. O DPO deverá orientar cada caso.

AIPD - Avaliação de Impacto à Proteção de Dados

Também conhecida como DPIA (Data Privacy Impact Assessment), a Avaliação de Impacto à Proteção de Dados serve para identificar riscos específicos aos dados pessoais como resultado das atividades de processamento. Ela é mais focada que a avaliação de riscos exigida pela ISO/IEC 27001.

É um processo exigido pela LGPD e deve ser realizado sempre pelo processador, com apoio do controlador e DPO, e executado quando houver necessidade de entender melhor o processamento, avaliando a necessidade e a proporcionalidade do tratamento.

Considerações:

- A AIPD identifica e minimiza os riscos de privacidade relacionados a um tratamento
- A AIPD deve ser realizada antes da implementação de novos processos, projetos ou políticas; ou
- A AIPD deve ser aplicada para revisar sistemas existentes

De acordo com o Artigo 38 da LGPD, o RIPDP (Relatório de Impacto à Proteção de Dados Pessoais) deverá conter, no mínimo:

- Descrição dos tipos de dados coletados
- Metodologia utilizada para a coleta e para a garantia da segurança das informações
- Análise do controlador com relação a:
    - Medidas
    - Salvaguardas
    - Mecanismos de mitigação de risco adotados.

O QUE MINHA EMPRESA PRECISA PARA ESTAR PREPARADA?

Caso você tenha lido o artigo até aqui, deve ter notado que a LGPD é muito mais ampla e complexa requerendo mais do que simplesmente adequar contratos ou adotar medidas técnicas de segurança, como firewalls, criptografia de dados etc.

Assegure-se que a partir daqui você realize uma avaliação global de sua organização sob a ótica jurídica e técnica. Abaixo estão listadas algumas ações que você pode adotar, separadas conforme os principais conceitos apresentados.

Políticas internas

- Revisar e adequar as políticas (internas e em relação a terceiros), contratos, procedimentos e demais atividades que envolvam tratamento de dados pessoais (tanto de clientes quanto de empregados) aos princípios estabelecidos na LGPD;

- Manter registros, preferencialmente por escrito, que demonstrem a adoção de medidas para adequação das operações de tratamento aos princípios estabelecidos na LGPD, independentemente do tamanho da base de dados existente.

Juridicamente

- • Revisar e adequar os contratos de terceiros (processadores), exigindo a comprovação das medidas técnicas adotadas por eles para atendimento da LGPD e garantindo a adequada clareza sobre qual processamento deve ser realizado;

- Avaliar cuidadosamente qual base legal para tratamento de dados pode ser utilizada em seu caso;

- Quando o tratamento de dados pessoais se basear no consentimento, o controlador deve manter documentação que comprove sua obtenção;

- Quando o tratamento de dados pessoais se basear no interesse legítimo, o controlador deve adotar medidas para garantir a transparência do tratamento (poderá sempre ser revisto pela ANPD), bem como manter registro do processamento.

Direito do titular

- Adequar a estrutura operacional e técnica de sua organização para viabilizar e cumprir todos os direitos que a lei garante ao titular dos dados;

- Desenvolver mecanismos para permitir que os titulares dos dados exerçam seus direitos (item 1.6 deste artigo), de forma facilitada e gratuita;

- Verificar se o conteúdo informativo proporcionado ao titular dos dados está com uma linguagem clara e adequada;

O QUE MINHA EMPRESA PRECISA PARA ESTAR PREPARADA? (CONTINUED)

- No caso de tratamento de dados pessoais de crianças, as informações devem ser fornecidas de maneira simples, clara e acessível, considerando as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do público-alvo.

Obrigações

- Adotar medidas técnicas que garantam que os dados sejam tratados de forma segura;
- Desenvolver processos internos e criar políticas que permitam realizar a criação e manutenção de registros das operações de tratamento de dados;
- Conservar os dados visando atender a finalidade para a qual foram coletados e para cumprir obrigações legais e regulatórias;
- Nomear o encarregado (DPO) pelo tratamento dos dados pessoais.

Transferência internacional de dados

- Ter cautela no envio de dados a organizações no exterior e assegurar que elas cumpram os requisitos estabelecidos na LGPD;
- Adotar procedimentos e elaborar documentos, incluindo contratos e regras corporativas vinculantes, que documentem a adequação do tratamento dos dados segundo a LGPD;
- Informar a autoridade nacional caso haja alteração nas garantias que tenham sido entendidas como suficientes para a realização de transferência internacional de dados.

Segurança e Notificações

- Desenvolver sistemas de identificação e combate de incidentes de segurança, bem como treinar uma equipe de TI para garantir a execução destes procedimentos;
- Criar políticas e governança, garantindo também que prestadores de serviços técnicos e de assessoria jurídica sigam o mesmo procedimento;
- Revisar os acordos de seguros para garantir cobertura em caso de incidentes de segurança.

Sanções

- Executar uma análise de conformidade dos procedimentos de tratamento dos dados com a LGPD, para identificar o cumprimento completo da norma. Em caso de descumprimento, buscar sempre cooperar e minimizar o dano prontamente;
- Ter à sua disposição uma equipe interna (e externa, se for possível) que possa atender prontamente às solicitações da autoridade nacional de proteção de dados, visando a diminuir o risco de aplicação de sanções em seus maiores níveis.

AUTHOR

Rodrigo Constantino, Principal Consultant
Data Protection Officer - Exin Certified
Rodrigo.Constantino@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO