



CONHECENDO A LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

Lei 13.709 de 14/8/2018



SUMÁRIO

O que é a Lei Geral de Proteção de Dados?	3
Quando a lei entrou em vigor?	4
Quais medidas estão sendo tomadas pela Cagece?	5
Quais são os impactos da LGPD na Cagece?	6
Há penalidades, caso a companhia não cumpra a lei?.....	7

Norma de Segurança da Informação Privacidade de Dados

1. Objetivo	8
2. Aplicação	8
3. Glossário	8
4. Papéis e Responsabilidades	12
5. Tratamento de Dados Pessoais	19
6. Da Segurança e Sigilo dos Dados	22
7. Direito dos Titulares	23
8. Compartilhamento e Transferência de Dados Pessoais	25
9. Violações	26
10. Disposições Gerais	26



O QUE É A LEI GERAL DE PROTEÇÃO DE DADOS?

A nova Lei Geral de Proteção de Dados (LGPD), Lei Federal 13.709/2018, tem por objetivo garantir mais segurança e transparência às informações pessoais coletadas por empresas públicas e privadas, com o intuito de assegurar direitos para os cidadãos e consumidores sobre como vai ocorrer o tratamento de seus dados pessoais.

Com a nova legislação, torna-se necessário um cuidado ainda mais rigoroso, por parte de todos que fazem a Cagece, com a identificação e a proteção dos dados de clientes e da empresa.



QUANDO A LEI ENTROU EM VIGOR?

A nova lei entrou em vigor no dia 18 de setembro e traz uma série de obrigações que deverão ser cumpridas pela Cagece e pelos seus colaboradores. Ou seja, todas as áreas devem estar atentas no trato com os dados de clientes e da empresa.



QUAIS MEDIDAS ESTÃO SENDO TOMADAS PELA CAGECE?

Diversas ações já foram implementadas, como a adequação do portal da companhia, criação de nova funcionalidade do Cagece App e Gesse para obtenção de consentimento dos usuários: disponibilização da política de privacidade de dados, que descreve as práticas da companhia em relação aos dados coletados por meio do site da empresa.

Além disso, foi criado um comitê específico formado por representantes de áreas diversas, como comercial, tecnologia da informação, comunicação, pessoal, jurídica, ouvidoria, entre outras para discutir, estudar e definir a melhor forma de proteger esses dados. Também encontra-se em fase de análise de propostas a contratação de consultoria para adequação da Cagece à Lei Federal 13.709/2018.



QUAIS SÃO OS IMPACTOS DA LGPD NA CAGECE?

A lei compreende todos os processos da companhia, inclusive será realizado o mapeamento do fluxo e proteção dos dados e adequação de contratos de trabalho e dos contratos com clientes e fornecedores.

No caso dos dados dos clientes da Cagece para o cadastro, por exemplo, deverão ser coletados somente os que são fundamentais à atividade fim da companhia, como faturamento, cobrança, envio de mala direta, e outros. Cada colaborador deve ficar atento às orientações da companhia com relação ao tratamento dos dados de terceiros.



HÁ PENALIDADES, CASO A COMPANHIA NÃO CUMPRA A LEI?

Empresas de economia mista, como é o caso da Cagece, que descumprirem as regras estão passíveis de sanções, com multas de até R\$ 50 milhões. As penalidades pelo descumprimento passarão a ser aplicadas a partir de agosto de 2021.

1. OBJETIVO

1.1 Essa norma interna tem como objetivo estabelecer um padrão e controles de segurança e privacidade para o tratamento e coleta de dados pessoais nos processos, ambientes físicos e lógicos da Cagece, seja o tratamento informatizado ou não.

2. APLICAÇÃO

2.1 Essa norma entra em vigor a partir da data de sua publicação e é aplicável a todos os colaboradores que possam realizar tratamento de quaisquer dados pessoais, informatizados ou não, não se limitando ao uso dos recursos de tecnologia da informação e comunicação.

2.2 Quanto aos colaboradores, a aplicabilidade será plena e imediata, independentemente do cargo ocupado, da unidade em que esteja alocado ou das funções que desempenhe.

2.3 Quanto aos fornecedores, parceiros e demais entidades que possam coletar, armazenar ou tratar dados pessoais de clientes ou colaboradores da companhia deverão estar de acordo com os requisitos de privacidade e proteção de dados dessa norma.

3. GLOSSÁRIO

Para os fins desta norma, considera-se:

I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de carácter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV – banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrónico ou físico;

V – titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII – operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII – encarregado dos dados: 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);

IX – agentes de tratamento: o controlador e o operador;

X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI – 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;

XII – consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII – bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV – eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV – transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI – uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por

órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII – relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVIII – órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019)

XIX – autoridade nacional: órgão da administração pública responsável por elaborar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

4. PAPEIS E RESPONSABILIDADES

4.1 Comitê de Privacidade e Proteção de Dados – CPPD

- Assegurar a implementação de medidas técnicas e administrativas para conformidade com a LGPD;
- Garantir o atendimento de demandas e questionamentos relacionados aos Direitos do Titular dos Dados;
- Analisar e emitir parecer sobre possíveis sanções ou questionamentos de órgãos reguladores e fiscalizadores;
- Avaliar riscos e emitir pareceres relacionados a reportes de incidentes, demandas de tratamento e compartilhamento de dados;
- Monitorar o cumprimento dos princípios da Lei, política e norma de privacidade de dados;
- Monitorar e controlar a execução dos projetos, ações e auditorias relacionados a LGPD;
- Promover a capacitação, comunicação e conscientização dos colaboradores;
- Assegurar a efetiva execução do papel do DPO (Data Protection Officer);
- Propor melhorias e recomendações de segurança e privacidade de dados;

- Controlar a conformidade com a Lei Geral de Proteção de dados – LGPD e com as políticas dos responsáveis pelo tratamento, incluindo a atribuição de responsabilidades, a sensibilização e a formação do pessoal envolvido no tratamento;
- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Avaliar, perante a LGPD, as solicitações de compartilhamento de dados pessoais advindas de órgãos externos.

4.2 Encarregado dos dados DPO(Data Protection Officer)

- A companhia deverá indicar um encarregado de dados também conhecido como DPO (Data Protection Officer), que terá como uma de suas funções a mediação entre a empresa, os titulares dos dados pessoais (funcionários, fornecedores e clientes) e órgãos reguladores/fiscalizadores (por meio da ANPD);
- A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico da companhia.

4.2.1 Responsabilidades do DPO(Data Protection Officer)

- Informar e aconselhar os responsáveis pela coleta e/ou tratamento de dados e os demais profissionais sobre suas obrigações nos termos da Lei Geral de Proteção de dados – LGPD;

- Prestar aconselhamento, se tal for solicitado, no que se refere à avaliação do impacto da proteção de dados, e acompanhar o seu desempenho;
- Receber comunicações da autoridade nacional e adotar providências.

4.3 Gerência de Tecnologia da Informação e Comunicação – GETIC

- Tomar medidas técnicas e administrativas que envolvam ações relacionadas à Segurança Digital e Cibernética que contemplem o ambiente organizacional, pessoas, processos e tecnologia;
- Realizar o tratamento e proteção dos dados pessoais de acordo com as solicitações formalizadas e aprovadas pelas devidas alçadas;
- Analisar e emitir parecer técnico referente às solicitações de acordos de cooperação compartilhamento e transferência de dados pessoais.

4.4 Gerência de Consultoria Jurídica – GCONS

- Analisar a conformidade jurídica dos processos e contratos com a Lei Geral de Proteção de Dados;
- Prestar consultoria jurídica visando a conformidade com a Lei Geral de Proteção de Dados;

– Analisar e emitir parecer jurídico referente às solicitações de acordos de cooperação, compartilhamento e transferência de dados pessoais.

4.5 Gerência de Serviços Contratados – GESEC

– Analisar a conformidade na coleta e tratamento dos dados pessoais dos colaboradores terceirizados da companhia;

– Analisar e viabilizar o cumprimento da Lei Geral de Proteção de Dados – LGPD no compartilhamento dos dados pessoais referentes aos contratos terceirizados com mão de obra;

– Realizar a comunicação referente a coleta e tratamento dos dados pessoais com os fornecedores de contratos terceirizados com mão de obra;

– Reportar incidentes gerados por colaboradores terceirizados para os fornecedores dos contratos terceirizados com mão de obra.

4.6 Gerência de Pessoas – GEPES

– Analisar a conformidade na coleta e tratamento dos dados pessoais dos colaboradores empregados, estagiários, comissionados, ex-empregados, jovens aprendizes e dependentes dos colaboradores;

– Analisar e viabilizar o cumprimento da Lei Geral de Proteção de Dados – LGPD no compartilhamento dos dados pessoais referentes aos colaboradores empregados, estagiários,

comissionados, ex-empregados, jovens aprendizes e dependentes dos colaboradores;

- Realizar a comunicação referente a coleta e tratamento dos dados pessoais referentes aos colaboradores estagiários e jovens aprendizes, com empresas contratadas;
- Reportar incidentes gerados por colaboradores estagiários e jovens aprendizes, para as empresas contratadas;
- Coordenar junto às empresas contratadas o tratamento dos dados pessoais dos colaboradores estagiários e jovens aprendizes.

4.7 Gerência de Comunicação – GERCO

- Realizar a comunicação corporativa para conscientização e sensibilização dos colaboradores referente a proteção e privacidade de dados pessoais;
- Analisar e adotar medidas de proteção e privacidade na utilização de dados pessoais nas comunicações e campanhas de marketing.

4.8 Gerência de Governança, Riscos e Conformidade – GRC

- Realizar auditorias internas para conformidade com essa norma e a Lei Geral de Proteção de Dados;
- Analisar e homologar a conformidade dos processos que tratam dados pessoais.

4.9 Gerência de Serviços Administrativos – GESAM

- Adotar medidas de proteção e privacidade na coleta, tratamento e armazenamento de dados pessoais físicos como documentos nos ambientes da companhia;
- Adotar medidas de proteção e privacidade na coleta, tratamento e armazenamento de dados pessoais no monitoramento e vigilância eletrônica nos ambientes da companhia;
- Adotar medidas de proteção e privacidade na coleta, tratamento e armazenamento de dados pessoais referentes aos acessos às dependências da empresa.

4.10 Gerência de Faturamento e Arrecadação – GEFAR

- Adotar medidas de proteção e privacidade na elaboração dos contratos com os clientes da companhia;
- Adotar medidas de proteção e privacidade na coleta, tratamento e armazenamento de dados pessoais dos clientes da companhia.

4.11 Ouvidoria – OUVID

- Receber solicitações de informações e reclamações dos titulares dos dados;
- Encaminhar as demandas relativas as solicitações de informações e reclamações dos titulares dos dados para as devidas áreas responsáveis;

- Prestar esclarecimentos aos titulares dos dados.

4.12 Gestores

Conscientizar suas equipes sobre a importância dessa norma e da sua conformidade.

4.13 Área proprietária de dados

- Analisar a viabilidade das solicitações de acordos de cooperação, compartilhamento e transferência de dados pessoais, referentes a sua área;
- Submeter as solicitações de compartilhamento e/ou transferência de dados pessoais para análises técnicas e jurídicas;
- Analisar e celebrar acordos de cooperação, compartilhamento e transferência de dados pessoais;
- Realizar análises de riscos e avaliações de impacto a proteção de dados visando a conformidade com essa norma e a Lei Geral de Proteção de Dados no tratamento de dados pessoais na companhia;
- Demandas de tratamento automático de dados, robotização, ou processamento em larga escala devem obrigatoriamente ser submetidas para análise técnica de privacidade e proteção de dados.

4.14 Colaboradores da companhia

- A leitura, ciência e cumprimento dessa norma;
- Adotar medidas de segurança e privacidade de dados pessoais sob sua responsabilidade, compreendendo e não se limitando a sistemas, softwares, mesa de trabalho, equipamentos de informática, telefones, documentos, relatórios, imagens, fotos, vídeos, rede de dados e divulgação de informações.

5. TRATAMENTO DE DADOS PESSOAIS

5.1 Todo processo que envolver coleta e tratamento de dados pessoais somente poderá ser realizado depois de analisado e homologado pelo encarregado dos dados DPO (Data Protection Officer);

5.2 Todo sistema ou produto deve ser construído e mantido pensando na máxima proteção da privacidade dos seus usuários (Privacy by Design, Privacy by Default);

5.3 Todo processo deve ser construído obtendo o mínimo possível de dados pessoais necessários para o processo, devendo ser observado sempre seus propósitos e o legítimo interesse para sua utilização;

5.4 Os processos da companhia devem estar mapeados a utilização dos dados pessoais e seus fluxos;

5.5 A utilização de dados pessoais para a realização de estudos

ou pesquisas científicas ou acadêmicas deve ser feita com a anonimização dos dados pessoais;

5.6 A coleta e tratamento de dados pessoais de crianças e de adolescentes só deverá ser realizada após validação da legitimidade do interesse e validação do encarregado de dados DPO (Data Protection Officer);

5.7 O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por, pelo menos, um dos pais ou pelo responsável legal;

5.8 Todos os contratos que envolvam dados pessoais devem ser adequados e conformes com a Lei Geral de Proteção de dados;

5.9 Todo processo e/ou sistema só poderá tratar dados pessoais se estiver respaldado em uma das bases legais da LGPD;

5.10 Toda utilização de dados pessoais para fins de comunicação e/ou marketing deverá estar em de acordo com as bases legais da LGPD;

5.11 Todo dado pessoal tratado pelos processos e/ou sistemas deve ser pertinente e limitado em relação aos fins para os quais será utilizado;

5.12 Devem ser realizadas análises de impacto a proteção de dados nos processos que envolvam dados pessoais sensíveis;

- 5.13** Devem ser realizadas, quando pertinente, análises de impacto a proteção de dados nos processos que envolvam dados pessoais;
- 5.14** Os dados pessoais devem ter seu período de utilizações mapeadas e ser eliminados após o fim do seu ciclo de vida;
- 5.15** Todos os dados pessoais devem estar devidamente categorizados;
- 5.16** Os dados categorizados como dados sensíveis devem ter seu acesso restrito ao menor número de colaboradores possíveis;
- 5.17** Devem ser configurados e enviados relatórios gerenciais periódicos sobre as ações relativas a proteção de dados, para as partes interessadas;
- 5.18** Tratamento automático de dados, robotização, ou processamento em larga escala deve obrigatoriamente ser realizado uma análise de impacto de privacidade e proteção dos dados;
- 5.19** Todas as decisões em última instância devem ser tomadas e validadas pelo Comitê de Privacidade e Proteção de Dados – CPPD.

6. DA SEGURANÇA E SIGILO DOS DADOS

6.1 É proibido deixar qualquer documento físico que tenha dados pessoais expostos nas mesas e ambiente de trabalho;

6.2 É proibida a exposição de qualquer dado pessoal na tela dos computadores ou demais dispositivos quando o colaborador não estiver presente, ao sair da estação de trabalho deve sempre bloquear a tela do dispositivo;

6.3 É terminantemente proibido o compartilhamento ou fornecimento de qualquer dado pessoal de clientes ou colaboradores, para outra pessoa, seja física ou jurídica, sem a devida autorização das alçadas necessárias;

6.4 Os dados pessoais de pessoas físicas devem ser armazenados e protegidos com controles de segurança efetivos;

6.5 O acesso aos dados pessoais devem ser acessados somente por pessoas autorizadas, devendo existir controles que possam garantir a rastreabilidade e auditoria dos acessos;

6.6 O uso e acesso as imagens das câmeras de monitoramento e vigilância, devem ser utilizadas exclusivamente para a garantia da segurança, e tratadas por pessoas devidamente autorizadas;

6.7 Todos os incidentes envolvendo dados pessoais devem seguir o processo de incidentes de segurança da informação;

6.8 Deverá existir registro e armazenamento dos consentimentos (escrito ou eletrônico) de todas as permissões solicitadas;

6.9 Todo incidente de vazamento de dados, que possa acarretar em algum tipo de prejuízo ao titular dos dados deverá ser comunicado;

6.10 A Cagece deverá tomar todas as medidas de proteção cabíveis para prevenir o vazamento de dados pessoais durante o compartilhamento dos dados;

6.11 Todo transporte de dados pessoais por meio digital deverá ser criptografado;

6.12 É proibido a divulgação, coleta ou compartilhamento não autorizado de dados pessoais, estruturados ou não estruturados, compreendendo e não se limitando a sistemas, softwares, telefones, documentos, relatórios, imagens, fotos, vídeos, ou qualquer outro dado coletado ou mantido nas dependências da empresa.

7. DIREITO DOS TITULARES

7.1 Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Norma;

7.2 Deverá existir canal facilitado para consulta dos dados pelo titular;

7.3 O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I – confirmação da existência de tratamento;

II – acesso aos dados;

III – correção de dados incompletos, inexatos ou desatualizados;

IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados - LGPD;

V – 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;

VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei Geral de Proteção de Dados LGPD;

VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

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

IX – revogação do consentimento, nos termos do § 5º do art. 8º da Lei Geral de Proteção de Dados LGPD.

7.4 O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na Lei Geral de Proteção de Dados LGPD;

7.5 Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento;

7.6 Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a Cagece.

8. COMPARTILHAMENTO E TRANSFERÊNCIA DE DADOS PESSOAIS

8.1 Todo compartilhamento de dados pessoais deverá estar respaldado por uma das bases legais da LGPD;

8.2 Nos casos de compartilhamento ou transferência de dados pessoais, o processador ou terceiro deverá:

- Solicitar formalmente via ofício, informando a finalidade sobre os dados solicitados;
- Enviar informações complementares a respeito da segurança dos dados;

- Realizar uma avaliação de impacto sobre a proteção de dados (AIPD);
- Informar o nome e contatos do responsável pelo tratamento de dados;
- Assinar os acordos de confidencialidade.

8.3 Nos casos de compartilhamento ou transferência de dados pessoais, a Cagece deverá:

- Elaborar minuta de acordo de confidencialidade;
- Realizar análise e parecer técnico, jurídico e administrativo;
- Assinar os acordos de confidencialidade.

9. VIOLAÇÕES

9.1 Quaisquer violações às regras e orientações contidas nessa norma deverão ser apuradas de acordo com a previsão do item 7 da Política de Segurança da Informação.

10. DISPOSIÇÕES FINAIS

10.1 A leitura e ciência dessa norma, bem como da PSI, é um requisito obrigatório do processo de contratação de colaboradores relativo à formalização das solicitações de concessão e liberação de Recursos de TIC;

10.2 Não será admissível que qualquer colaborador declare o desconhecimento dessa norma, como forma de arguir defesa

contra qualquer eventual alegação de violação à mesma;

10.3 Havendo dúvidas quanto à forma de execução de quaisquer das atividades descritas acima o colaborador deverá contatar a Área de Segurança da Informação.

10.4 Qualquer usuário que realize um ato contrário aos termos dessa norma, ainda que por mera omissão ou tentativa, conforme previsto no item 7 da PSI, estará sujeito à aplicação de penalidades;

10.5 Cabe ao colaborador reportar formalmente à Getic SER, nos termos do Procedimento de Infração de Segurança, qualquer ação ou evento, citado ou não nessa norma, e que acarrete em riscos que tenham impacto financeiro, operacional, legal, na imagem ou nos negócios da Cagece.



Siga no Instagram
/oficialcagece



CurtanoFacebook
/cageceoficial



Siga no Twitter
@cageceoficial



Siga no LinkedIn
Cagece

