# Entenda quais são os impactos e como adaptar a LGPD no setor de RH

Se a sua empresa tem deixado de lado a implementação de políticas e protocolos de segurança da informação de clientes e colaboradores é bom ter atenção, pois a Lei Geral de Proteção de Dados (LGPD) já está aí e este será o assunto deste artigo: LGPD no RH.

Caso esteja se perguntando qual é a relação entre Recursos Humanos e tratamento de dados pessoais, saiba que os dois assuntos têm tudo a ver um com o outro. Afinal, esse é um setor que trata diretamente das informações pessoais dos colaboradores e, certamente, a sua empresa não quer ter problemas com isso.

Então continue acompanhando porque aqui vamos tratar detalhadamente sobre o que é a LGPD, por que há a necessidade dessa lei, por que os dados precisam ser protegidos, como o RH pode contribuir para garantir esse tipo de segurança e muito mais. Boa leitura!

## O que é a Lei Geral de Proteção de Dados?

Você tem a impressão de que a LGPD é algo discutido há muitos anos e se surpreendeu com a informação de que ela passou a vigorar só agora? Saiba que isso não é apenas impressão, pois, de fato, apesar de ser debatida há muito tempo, só passou a valer recentemente — salvas as exceções que trataremos adiante.

A Lei 13.709, Lei Geral de Proteção de Dados é a norma que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, das pessoas que residem no Brasil, sendo naturais ou jurídicas, de direito público ou privado, e tem por objetivo proteger os direitos dessas pessoas, assim como a liberdade e a privacidade de suas informações.

Além disso, a lei aborda como as empresas devem coletar, armazenar e tratar dados sensíveis de clientes e do seu público em geral com o objetivo de preservar a sua segurança. Ela foi aprovada em agosto de 2018, mas só começou a valer no dia 18 de setembro de 2020, 24 meses após a sua aprovação.

Apenas as sanções da LGPD ficaram para depois: sua vigência começa a contar em 01 de agosto de 2021. Mas por que isso? Devido à pandemia causada pelo coronavírus (Covid-19), foi entendido que as empresas e o governo seriam incapazes de se adaptar, em tempo hábil, à nova realidade que já estava sendo agravada pela crise sanitária mundial.

Porém, saiba que a lei que tratamos aqui não foi a primeira iniciativa para preservação da segurança no colhimento, tratamento e armazenamento de dados pessoais. Inclusive, a LGPD veio para alterar alguns artigos do Marco Civil da Internet, de 2014, e estabelecer novas regras, com alcance além da internet.

Por isso, entenda que os dados pessoais a que se refere a lei podem ser obtidos por diversos meios: cadastros online, telefone, fichas eletrônicas, fichas impressas em papel e diversas outras formas de obtenção de dados dos cidadãos, especialmente os que utilizam inteligência artificial.

### O que a lei fala sobre penalidades no caso de descumprimento das normas?

Acima falamos que as sanções só começarão a valer em 2021, certo? As punições administrativas preveem:

- advertência, com indicação de prazo para adoção de medidas corretivas;
- multas simples, que podem chegar a R$ 50 milhões por infração;
- multa diária, observando o limite do faturamento da empresa;

- publicização da infração, após apurada e confirmada a ocorrência;
- bloqueio dos dados pessoais a que se refere a infração até a regularização;
- eliminação dos dados pessoais a que se refere a infração;
- suspensão parcial do funcionamento do banco de dados pelo prazo máximo de seis meses;
- suspensão do exercício da atividade de tratamento de dados pessoais;
- proibição parcial ou total do exercício das atividades relacionadas ao tratamento de dados.

Porém, mesmo com a vigência para 2021, empresas que não observarem a lei já poderão ter de responder por seus atos. Inclusive, já existem várias ações contra vazamentos de dados e informações dos clientes, como é o caso da Uber, que foi alvo de notificação do Ministério Público, em 2018, por vazar dados sensíveis de mais de 150 mil brasileiros.

A situação é tão séria que na Europa, o Google e o Facebook já receberam dívidas milionárias por não atuarem de acordo com o Regulamento Geral sobre Proteção de Dados (GDPR), válido na União Europeia. Porém, qualquer site que atenda a essa região também pode sofrer sanções, inclusive portais brasileiros.

## Quais são os principais objetivos da LGPD?

O primeiro entre os principais objetivos da LGPD é oferecer consentimento aos cidadãos para que seus dados sejam coletados, armazenados e utilizados, quando preciso. Agora, todos devem permitir que as empresas tenham acesso aos seus dados; sem isso, qualquer utilização de informações pessoais será proibida.

Por isso, desde o seu comportamento nas redes sociais até o preenchimento de um cadastro em uma loja virtual, por exemplo, tudo deverá ser consentido explicitamente pelo usuário. A partir da lei, as companhias também são obrigadas a informar aos cidadãos de que forma esses dados estão sendo coletados e para qual finalidade.

Um exemplo é quando você entra em um site pela primeira vez e logo se depara com a informação — geralmente, localizada no rodapé da página — de que seus dados poderão ser coletados e armazenados. Veja o modelo adotado por um grande portal de notícias de Minas Gerais:

*"Nós usamos cookies e outras tecnologias semelhantes para melhorar a sua experiência em nossos serviços, personalizar publicidade e recomendar conteúdo de seu interesse. Ao utilizar nossos serviços, você concorda com tal monitoramento. Informamos ainda que atualizamos nossa Política de Privacidade ".*

Por isso, a partir do dia em que a LGPD entrou em vigor, todos os portais, sites, blogs e qualquer meio eletrônico — entre outros recursos fora do ambiente digital — que possam coletar informações devem informar ao usuário sobre essa prática e colocar à disposição da sociedade todas as políticas de coleta, armazenamento e uso desses dados.

Outro objetivo importante aqui é oferecer garantias aos usuários como medidas punitivas para os infratores, o direito de solicitar que suas informações sejam excluídas de certos bancos de dados, o direito de revogar um consentimento, de corrigir dados incompletos ou desatualizados, entre outras prerrogativas agora legais.

## Qual a importância da LGPD em relação aos dados pessoais?

Entender os principais pontos da LGPD é muito importante para as empresas, pois a proteção é ampla e abrange todos os cidadãos que têm seus dados pessoais com órgãos e entidades em geral, inclusive suas empregadoras.

Por isso, é essencial o entendimento de que ter suas informações resguardadas é um direito de todo

cidadão brasileiro e isso está previsto desde a Constituição Federal de 1988. Porém, como você deve imaginar, naquela época não havia acesso à internet como hoje e a virtualização, ao longo dos anos, foi determinante para a necessidade de uma lei específica.

Como atualmente praticamente tudo é feito pela internet, com a coleta de dados as informações pessoais dos usuários se tornam ainda mais vulneráveis e sensíveis a fraudes, a atos ilícitos, golpes, manipulação de dados, entre outros tipos de crimes que se tornam fáceis de serem cometidos quando não há segurança da informação.

# Como a LGPD impacta o setor de RH?

Chegamos, finalmente, à prática da Lei Geral de Proteção de Dados para que a empresa possa tornar o RH estratégico, acima de tudo. Antes, foi necessário explicar os motivos que levaram à aprovação de leis para resguardar os cidadãos para que o entendimento seja completo.

Com o uso da tecnologia para preservar e garantir a segurança das informações dos colaboradores, é possível que a organização atente em oferecer medidas de segurança em suas diversas atividades e áreas de atuação. Veja!

## Dados pessoais dos colaboradores

A sua empresa já investe em um RH Tech para estar atualizada quanto às atividades voltadas para os colaboradores? Isso quer dizer que, quanto mais automatizado for o processo e mais investimentos forem feitos em ferramentas tecnológicas e em políticas de segurança, mais seguros estarão os dados dos funcionários.

Assim, o setor deve revisar as políticas de coleta e utilização de dados e permitir o conhecimento dos colaboradores sobre o armazenamento de suas informações pessoais. Como você percebeu, o consentimento deve ser dado por parte dos profissionais e eles precisam saber que seus dados estão sob fontes seguras.

## Banco de currículos

A segurança da informação também passa pelo banco de currículos da empresa. Quantos nomes, CPFs e endereços a companhia tem armazenados em seus sistemas? Eles estão seguros? Quem são os funcionários que manipulam esses dados?

Há senhas para acessar essas informações? Já foram excluídos dados de profissionais? De que forma eles foram retirados do sistema? Todas essas perguntas devem ser analisadas por companhias que pretendem andar de acordo com a lei e evitar constrangimentos e processos judiciais.

## Dados fornecidos às seguradoras

Muitas empresas têm seguradoras de planos de saúde, de assistência médica e odontológica como parceiras na oferta de benefícios para seus colaboradores. Acontece que esses dados são repassados para terceiros e esses também devem contar com normas para garantir a segurança e a proteção de dados dos funcionários da sua organização.

## Exames admissionais

Os exames admissionais também são dados privados dos colaboradores, pois contêm informações sobre o seu estado de saúde. Por isso, ainda nesse momento, a empresa deve adotar um sistema de

segurança que ofereça proteção a esses dados e informar ao funcionário para quais finalidades esses registros devem ser mantidos internamente.

# Como adequar o RH à LGPD?

Após entender a importância da proteção e segurança dos dados em uma empresa, é preciso colocar as disposições da lei em prática! Será necessário implementar uma gestão de mudança para que todos possam entender a relevância deste assunto e que a cultura da organização esteja alinhada com o que a lei propõe. Sugerimos algumas medidas.

## Criação e armazenamento de termos de consentimento

Se a empresa ainda não conta com termos de consentimento de coleta, armazenamento e tratamento de dados pessoais, será necessário criá-los com a ajuda do setor jurídico. Esses devem estar disponíveis para que o titular — pessoa natural a quem se referem os dados pessoais — possa excluir ou editar as suas informações a qualquer momento.

Além dessa garantia ao quadro de pessoal, também será preciso criar autorizações para os candidatos no processo de recrutamento. É essencial que esteja claro para os profissionais para quais finalidades aquelas informações serão utilizadas e como será feito o tratamento e armazenamento delas na empresa.

## Criação de políticas de segurança da informação

A LGDP chama a atenção para a necessidade de implementar políticas de segurança da informação na empresa e elas devem passar por todos os setores. É importante contar com a ajuda de setores auxiliares do RH como os da área da tecnologia da informação e o departamento jurídico.

Além dessa iniciativa, a organização também deverá designar um encarregado para lidar com as práticas da Lei Geral de Proteção de Dados. De acordo com a lei, essa pessoa será 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).

## Coleta de dados necessários e eliminação de dados sem justificativa

No processo de recrutamento e seleção, peça aos candidatos apenas os dados que são realmente necessários para dar andamento às atividades para contratação. Além disso, é importante não manter as informações dos profissionais que não foram aprovados e descartá-las de forma segura e no prazo acordado.

## Segurança de compartilhamento dos dados

Outro ponto importante ainda na seletiva é estipular um prazo para que os currículos fiquem armazenados na empresa e informar aos candidatos sobre esse processo. O compartilhamento de currículos com outras empresas também requer anuência do profissional.

O RH utiliza dados pessoais dos profissionais em várias etapas de suas atividades: na seleção de candidatos, na rotina operacional, até o desligamento do funcionário, e isso faz com que o setor seja responsável por todas as informações dessas pessoas.

Por isso, a área deve ter total atenção na hora de elaborar suas políticas de segurança de dados para atuar de acordo com as normas legais. Tenha em mente que o principal ponto da LGPD no RH é ter

transparência com os titulares dos dados. Adotando medidas de proteção dessas informações e sendo transparente com todos, não existe erro!

Muitas pessoas têm dúvidas sobre a LGPD e todas essas informações acima são essenciais para o conhecimento das empresas e, em especial, dos profissionais de RH. O que acha, então, de compartilhar este conteúdo e ajudar outras pessoas a compreenderem melhor o assunto?