GESPERJ
GESTÃO DE PESSOAS DO ESTADO DO RJ

RH EM PRÁTICA

Lei Geral de Proteção de Dados Pessoais

Edição nº XL | Abril de 2026

1. O QUE É LGPD E QUAL É O OBJETIVO DA NORMA?

A Lei Geral de Proteção de Dados Pessoais (LGPD), estabelecida pela Lei Federal nº 13.709/2018, tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Com abrangência nacional, ou seja, incidindo sobre todos os entes federados, a norma dispõe sobre o tratamento de dados pessoais, armazenados em meios físicos ou digitais, realizado por pessoas físicas ou jurídicas, de direito público ou privado, abrangendo um amplo conjunto de operações efetuadas tanto de forma manual quanto automatizada.

A legislação estabelece diversas diretrizes, princípios e obrigações voltados à proteção de dados pessoais, definindo regras claras para a coleta, o armazenamento, o uso, o compartilhamento e a eliminação dessas informações. Outro ponto relevante é o direito do titular de saber quais dados estão armazenados. Por isso, de acordo com a LGPD, é fundamental que sejam criados processos internos que assegurem o cumprimento dessa determinação, promovendo a conformidade com a norma, bem como o fortalecimento da transparência e da confiança na relação entre a Administração Pública e seus servidores.

No âmbito do Poder Executivo do Estado do Rio de Janeiro, foi publicado o Decreto nº 48.891 de 10 de janeiro de 2024, que instituiu a Política de Governança em Privacidade e Proteção de Dados Pessoais do Estado do Rio de Janeiro, em conformidade com a LGPD.

2. QUAIS SÃO OS PRINCÍPIOS DA LGPD?

De acordo com a referida norma, as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

- **Adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- **Necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- **Livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- **Qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- **Transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- **Segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

- **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, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

3. O QUE SÃO DADOS PESSOAIS E SENSÍVEIS DE ACORDO COM A LGPD? O RH TEM ACESSO A ESSES DADOS?

De acordo com a norma, dados pessoais são todas as informações que identificam ou podem identificar uma pessoa natural (direta ou indiretamente), como por exemplo: nome, CPF, RG, data de nascimento, endereço, telefone, e-mail, dados bancários.

Já os dados pessoais sensíves, são aqueles relacionados a 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, quando vinculado a uma pessoa natural. No contexto do RH, temos como exemplos: atestados médicos, informações sobre deficiência (PCD), biometria para controle de ponto, filiação sindical, entre outros.

Nesse contexto, os servidores dos Órgãos Setoriais de Recursos Humanos possuem acesso aos dados pessoais dos servidores públicos por meio de sistemas corporativos estruturantes, principalmente através do SIGRH-RJ e SEI-RJ.

O SIGRH é utilizado para a gestão da vida funcional dos servidores, concentrando dados cadastrais, funcionais e financeiros, como nome completo, números de documentos, endereço, telefone, e-mail, histórico profissional, remuneração e benefícios, que são utilizados, entre outros fins, para gerenciamento e produção da folha de pagamento do Estado. Tendo em vista o grau de sensibilidade das informações, o sistema adota diferentes níveis de acesso para os usuários, com o propósito de assegurar a proteção dos dados.

Já o SEI-RJ é a plataforma oficial para a tramitação de processos administrativos eletrônicos, permitindo a produção, assinatura e circulação de documentos institucionais em meio digital, nos quais podem constar documentos contendo dados pessoais sensíveis, como laudos médicos, requerimentos de licença, processos disciplinares e demais registros funcionais. Por sua natureza, assim como no SIGRH, o sistema permite diferentes níveis de acesso, inclusive restrito e sigiloso, garantindo que apenas usuários autorizados tenham acesso a determinadas ações e informações.

Dessa forma, como ambos os sistemas concentram grande quantidade de informações sensíveis, os gestores de Recursos Humanos devem atuar de forma proativa para garantir que as ações das equipes estejam em conformidade com a LGPD, especialmente no que se

refere à segurança da informação, de forma a proteger os dados pessoais dos servidores e demais titulares envolvidos.

4. COMO OS PROFISSIONAIS DE RH DEVEM PROCEDER NO DIA A DIA?

A conformidade com a LGPD depende da atuação responsável de cada colaborador no tratamento de dados pessoais. De acordo com o art. 46 da LGPD, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

No dia a dia, a adoção de boas práticas de segurança da informação é essencial. A seguir, destacam-se algumas orientações amplamente reconhecidas por especialistas:

- **Senhas fortes:** Utilize senhas complexas, com letras maiúsculas e minúsculas, números e caracteres especiais, evitando informações óbvias e repetição entre sistemas.
- **Mesa limpa:** Evite deixar documentos, anotações ou qualquer informação sensível exposta sobre a mesa ou em locais de fácil visualização. Da mesma forma, imprima apenas quando realmente necessário e recolha imediatamente os documentos da impressora.
- **Bloqueio de tela:** Ao se ausentar do computador, mesmo que por pouco tempo, bloqueie a tela para impedir acessos indevidos.
- **Descarte seguro de documentos**: Realize a trituração ou descarte adequado de documentos físicos que contenham dados pessoais antes de eliminá-los.
- **Cuidado com e-mails e links de mídia social:** Não clique em *link* ou abra anexos de remetentes desconhecidos ou suspeitos, evitando golpes de *phishing*.
- **Uso de redes seguras:** Evite acessar sistemas institucionais em redes Wi-Fi públicas ou não confiáveis. Com a ampliação do trabalho remoto, é fundamental utilizar conexões protegidas, manter a rede doméstica com senha forte, além de evitar o compartilhamento do acesso com terceiros.
- **Controle de acesso:** Compartilhe informações apenas com pessoas autorizadas e conforme a necessidade para o desempenho das funções.
- **Atualização de sistemas:** Mantenha sistemas operacionais, antivírus e demais *softwares* sempre atualizados para reduzir vulnerabilidades.
- **Armazenamento seguro:** Utilize apenas sistemas institucionais oficiais para armazenar dados, evitando salvar informações em dispositivos pessoais.
- **Comunicação de incidentes**: Informe imediatamente à área responsável qualquer suspeita de vazamento, perda de dispositivos, acesso indevido ou falha de segurança.
- **Ambiente seguro:** Evite discutir informações sensíveis em locais públicos ou com pessoas não autorizadas.

- **Princípio do menor acesso:** Acesse apenas os dados estritamente necessários para o desempenho das suas atividades e evite consultas indevidas.

Nesse contexto, é importante promover reuniões periódicas, ações de capacitação e a divulgação contínua de boas práticas, de modo a manter a equipe atualizada e consciente de suas responsabilidades, de forma a evitar práticas inadequadas (como compartilhamento informal de dados, por exemplo), reconhecer riscos em potencial e agir corretamente em caso de incidentes.

5. QUAIS SÃO AS SANÇÕES ADMINISTRATIVAS APLICÁVEIS AOS AGENTES DE TRATAMENTO DE DADOS EM DECORRÊNCIA DE INFRAÇÕES À LGPD?

No âmbito geral, as sanções administrativas estão previstas no art. 52. Entre elas, estão:

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- 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 6 (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 6 (seis) meses, prorrogável por igual período;
- Proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados.

Destaca-se que a aplicação das sanções previstas na LGPD não afasta a incidência de penalidades estabelecidas em outras normas específicas aplicáveis aos servidores públicos, tais como: Decreto-Lei nº 220/1975 (Estatuto dos Funcionários Públicos Civis do Poder Executivo do Estado do Rio de Janeiro) e Decreto nº 2.479/1979 (Regulamento do Estatuto dos Funcionários Públicos Civis do Poder Executivo do Estado do Rio de Janeiro), Lei nº 8.429/1992 (Lei de Improbidade Administrativa), Lei nº 12.527/2011 (Lei de Acesso à Informação).

7. QUAIS LEGISLAÇÕES REGULAMENTAM OU SÃO PERTINENTES AO TEMA?

- Constituição da República Federativa do Brasil de 1988.
- Lei federal nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais - LGPD.
- Decreto nº 48.891 de 10 de janeiro de 2024 – Institui a Política de Governança em Privacidade e Proteção de Dados Pessoais do Estado do Rio de Janeiro.

O *RH em Prática* é uma série de guias para auxiliar os profissionais de Gestão de Pessoas nas atividades do dia a dia na Administração Pública do Estado do Rio de Janeiro. Cada produto aborda objetivamente um assunto específico. O *RH em Prática* foi idealizado pela Superintendência de Planejamento e Desenvolvimento de Pessoas - SUPDP, setor integrante da Subsecretaria de Gestão de Pessoas – SUBGEP, e é elaborado em conjunto com a área responsável pelo tema abordado. Caso haja dúvidas sobre o tema, o RH setorial deverá entrar em contato com a SUPDP.

https://www.rj.gov.br/gesperj/ @gesperj