GOVERNO DO ESTADO DE MINAS GERAIS

SECRETARIA DE ESTADO DE JUSTIÇA E SEGURANÇA PÚBLICA

Lei Geral de Proteção de Dados

Memorando-Circular nº 2/2021/SEJUSP/LGPD

Belo Horizonte, 30 de novembro de 2021.

Aos Senhores Gestores e demais servidores da Secretaria de Estado de Justiça e Segurança Pública.

Assunto: Boas práticas para a conformidade à Lei Geral de Proteção de Dados Pessoais - LGPD

Prezados(as) Senhores(as),

A Lei Geral de Proteção de Dados Pessoais - LGPD regula o tratamento de dados pessoais de pessoas naturais/físicas, dentro e fora do país. Ela visa proteger direitos fundamentais, como a liberdade, a privacidade, o livre desenvolvimento e a personalidade. A Lei traz parâmetros para que o tratamento de dados pessoais ocorra sem infringir sua privacidade e proteção. Estabelece também regras de atuação para o Poder Público e o setor privado.

Ressalta-se que as diretrizes da política nacional de proteção de dados pessoais e privacidade são elaboradas pela Autoridade Nacional de Proteção de Dados - ANPD, a quem compete, também, a edição de regulamentos, procedimentos e guias orientativos sobre proteção de dados pessoais e privacidade.

O Grupo de Trabalho de Implementação da LGPD na Sejusp (34017548) foi instituído com a finalidade de promover a implementação das disposições da LGPD e do Decreto Estadual nº 48.237, de 22 de Julho de 2021 que dispõe sobre a aplicação da LGPD no âmbito Secretaria de Estado de Justiça e Segurança Pública (Sejusp/MG). Este Grupo também tem por objetivo elaborar um projeto, plano de ações e coordenar as atividades necessárias para que a Sejusp/MG esteja em conformidade com a referida Lei.

Diante do exposto, apresentam-se a seguir orientações destinadas a todos os servidores desta Secretaria de Justiça e Segurança Pública, bem como boas práticas a serem seguidas em prol da adequação à LGPD.

1) DOS CURSOS E MATERIAIS GRATUITOS PARA CAPACITAÇÃO DOS SERVIDORES

É recomendado que todos os servidores públicos realizem cursos de capacitação sobre a legislação brasileira sobre proteção de dados pessoais, na medida em que quase totalidade dos servidores realizam o tratamento de dados pessoais em suas atividades laborais, em maior ou menor grau. Dessa forma, orienta-se que as chefias incentivem suas equipes a realizarem os cursos e a fazerem a leitura e estudo dos materiais abaixo elencados.

Cursos gratuitos:

- Curso Introdução à Lei Brasileira de Proteção de Dados Pessoais, pela Escola Nacional de Administração Pública (Enap);
- Curso Fundamentos da Lei Geral de Proteção de Dados, pela Enap;
- Curso Proteção de Dados Pessoais no Setor Público, pela Enap.

Portal LGPD em Minas Gerais:

- Site organizado pelo Comitê Estadual de Proteção de Dados Pessoais (CEPD), contendo diversos documentos, explicações acerca da legislação, consultas jurídicas realizadas, bem como a funcionalidade de Fale Conosco, que pode ser utilizada para solicitar orientações específicas, caso necessário;

Materiais de estudo e cartilhas:

- Guia de Boas Práticas (38945197): elaborado pelo Comitê Central de Governança de Dados (Governo Federal);
- Manual de Interpretação da LGPD: (38945388): elaborado pela Advocacia

Geral do Estado - AGE/MG;

- Cartilha LGPD (38945653): elaborado pelo Comitê Estadual de Proteção de Dados Pessoais (CEPD), contém conceitos e explicações de maneira simplificada para primeiro contato com a LGPD;

2) DAS BOAS PRÁTICAS A SEREM UTILIZADAS NO SISTEMA SEI PARA EVITAR O VAZAMENTO E GARANTIR A SEGURANÇA DE DADOS

- Ao receber no SEI um processo que contenha dados pessoais e que não seja de competência da sua unidade, devolva-o ao remetente ou redirecione à unidade competente para adotar as providências necessárias, encerrando-o em seguida.

- Crie um processo SEI para cada expediente em que se necessite providências de outro setor/órgão; não crie "processos mestre" em que diversos expedientes, relativos a diferentes demandas, unidades, autoridades e pessoas se confundem.

- Não deixe processos abertos desnecessariamente na caixa de entrada da sua unidade. Caso já tenham sido tomadas as providências necessárias, conclua-o e utilize a função de Bloco Interno ou Acompanhamento Especial para acessá-lo futuramente, se necessário.

- Ao criar processos e inserir documentos, utilize a correta classificação quanto ao nível de acesso dos processos e dos documentos: processos e documentos que contenham dados pessoais necessariamente deverão ser classificados como "Restritos". Mas é importante anotar que além da LAI e LGPD existem outros dispositivos legais que impõem a classificação do processo/documento como restrito ou mesmo sigiloso. Por isso, é importante conhecer as rotinas e competências desenvolvidas no seu setor para classificar corretamente o nível de acesso aos processos e documentos da sua unidade. Alguns exemplos já estabelecidos no ordenamento jurídico:

❖ Acesso restrito: informação pessoal (art. 31, LAI); documento preparatório (§3º, art. 7º, LAI); informe de rendimentos (art. 16, Lei 19.490/2011).

❖ Acesso sigiloso: informação pessoal de caráter médico (art. 31, LAI); investigação de responsabilidade de servidor - PAD ou sindicância administrativa (§2º, art. 220, Lei 869/52); fiscalização em andamento (inc. VIII, art. 23, LAI); trabalho de auditoria não concluído (inc. V, art. 13, Res. CGE nº 15/2015).

A correta classificação dos processos e documentos quanto ao seu nível de acesso, em vista do que dispõe a LGPD e demais normas aplicáveis é imprescindível para se resguardar não só os dados pessoais ali contidos como, também, a legalidade e segurança jurídica dos procedimentos adotados pela administração.

- Envio de Processos SEI: conforme o teor dos dados pessoais que estiverem em processo SEI, o servidor deve procurar minimizar a exposição das informações contidas no processo, enviando o processo SEI apenas para as unidades necessárias para execução da atividade. Ao enviar um processo, certifique-se de enviá-lo à unidade/órgão correto, detentor(a) de competência normativa para tomar as providências necessárias, evitando-se o envio a múltiplas unidades sem a certeza quanto a qual delas deverá dar andamento ao expediente

Outras boas práticas:

- Evitar, na medida do possível, salvar arquivos com dados pessoais nos computadores de trabalho, computadores particulares, pen drive, entre outros dispositivos, para evitar a possibilidade de vazamento de dados. O mesmo procedimento se aplica para arquivos físicos que devem ser preservados para evitar seu extravio.

- Em caso de vazamento de dados, adotar medidas para mitigar a situação, como exclusão de arquivos inseridos indevidamente, solicitação de retirada dos dados inseridos indevidamente ao responsável por sistema , entre outras medidas aplicáveis ao caso concreto.

- Acesse o site de Boas práticas fornecidas pela SEF/MG.

Para conhecer mais sobre os trabalhos de adequação à LGPD que a Sejusp realiza, ou em caso de dúvidas, entre em contato com o GT/LGPD/SEJUSP pelo endereço de e-mail lgpd@seguranca.mg.gov.br.

Atenciosamente,

Adão Jairo Souza Porto

Superintendência de Tecnologia da Informação e Comunicação

Coordenador do Grupo de Trabalho de implementação da LGPD na Sejusp/MG

Documento assinado eletronicamente por **Adão Jairo Souza Porto**, **Superintendente de Tecnologia da Informação e Comunicação**, em 03/12/2021, às 09:04, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **38793186** e o código CRC **717A5CA5**.

Referência: Processo nº 1450.01.0145086/2021-88 SEI nº 38793186