



EBOOK

GUIA DE BOAS PRÁTICAS
EM CARTÓRIOS



www.itware.com.br

ÍNDICE

- INTRODUÇÃO
- BOAS PRÁTICAS NO CARTÓRIO
- CATEGORIZAÇÃO DOS DADOS PELAS SERVENTIAS (CARTÓRIOS)
- FLUXO DE DADOS
- PADRÕES MÍNIMOS DE INFRAESTRUTURA E SEGURANÇA DA INFORMAÇÃO
- MINIMIZAÇÃO DO USO DE DADOS PESSOAIS
- ARMAZENAMENTO DE DADOS PESSOAIS
- TRANSPARÊNCIA COM RELAÇÃO ÀS ATIVIDADES DE TRATAMENTO DE DADOS PESSOAIS
- TRANSFERÊNCIA DE DADOS PESSOAIS PARA OUTROS ENTES PÚBLICOS
- TRANSFERÊNCIA PARA ENTES PRIVADOS COM FINS COMERCIAIS
- AJUSTE DE CONTRATOS QUE TRATAM DADOS PESSOAIS COM TERCEIROS
- ADOÇÃO DE POLÍTICAS E CONSOLIDAÇÃO DE PROCEDIMENTOS INTERNOS
- TREINAMENTOS E ENGAJAMENTOS
- REFERÊNCIAS BIBLIOGRÁFICAS



Introdução

A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709, de 14 de agosto de 2018) foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. Essa Lei versa sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

No âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por dois **“agentes de tratamento”**, o Controlador e o Operador:

1

Controlador

O Controlador é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, tais como as finalidades e os meios do tratamento (art. 5º, VI). No âmbito da Administração Pública, o Controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade imbuída de adotar as decisões acerca do tratamento de tais dados.





2 Operador

O Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII), aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada pelo Controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congêneres.

Além dos “**agentes de tratamento**”, outra figura essencial para o adequado cumprimento da LGPD é o “**Encarregado**”, definido pelo art. 5º, VIII, como a 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).

Outro conceito fundamental é o de “**tratamento de dados**”, que abrange qualquer atividade que utilize um dado pessoal na execução da sua operação, conforme conceitos trazidos abaixo, senão vejamos:

TRATAMENTO DE DADOS



ACESSO

Ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;



ARMAZENAMENTO

Ação ou resultado de manter ou conservar em repositório um dado;



ARQUIVAMENTO

Ato ou efeito de manter registrado um dado em qualquer das fases do ciclo da informação, compreendendo os arquivos correntes, intermediários e permanentes, ainda que tal informação já tenha perdido a validade ou esgotado a sua vigência;



AVALIAÇÃO

Analisar o dado com o objetivo de produzir informação;



CLASSIFICAÇÃO

Maneira de ordenar os dados conforme algum critério estabelecido;



COLETA

Recolhimento de dados com finalidade específica;



DISTRIBUIÇÃO

Ato ou efeito de dispor de dados de acordo com algum critério estabelecido;



ELIMINAÇÃO

Ato ou efeito de excluir ou destruir dado do repositório;



EXTRAÇÃO

Ato de copiar ou retirar dados do repositório em que se encontrava;



MODIFICAÇÃO

Ato ou efeito de alteração do dado;



PROCESSAMENTO

Ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;



PRODUÇÃO

Criação de bens e de serviços a partir do tratamento de dados;



RECEPÇÃO

Ato de receber os dados ao final da transmissão;



REPRODUÇÃO

Cópia de dado preexistente obtido por meio de qualquer processo;



TRANSFERÊNCIA

Mudança de dados de uma área de armazenamento para outra, ou para terceiro;



TRANSMISSÃO

Movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc.;



UTILIZAÇÃO

Ato ou efeito do aproveitamento dos dados.



BOAS PRÁTICAS NO CARTÓRIO

A partir deste ponto, serão abordados os aspectos mais importantes para a melhor adequação de referidas atividades à esta nova lei. Temos que ter em mente que a adequação é contínua, devendo estar sempre em contato com atualizações de sistemas, políticas e governanças, bem como às determinações da ANPD, que terá um papel fundamental na normatização da lei.





CATEGORIZAÇÃO DOS DADOS PELAS SERVENTIAS (CARTÓRIOS)

A primeira etapa a ser planejada é a categorização dos dados pessoais que trafegam pelo estabelecimento. É importante verificar se os dados são classificados como sensíveis:

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Dado pessoal sensível: dado pessoal 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, quando vinculado a uma pessoa natural.

Feita essa classificação temos que nos atentar ao fluxo desses dados.

FLUXO DE DADOS

A segunda etapa de adequação à LGPD é conhecer e mapear o fluxo de todos os dados de pessoas físicas que passam pelas serventias.

1

Por onde os dados pessoais entraram?

2

Qual a atividade?

3

Como foi realizada a coleta dos dados?

4

Quais dados foram coletados?

5

Qual a finalidade destes dados?

6

Existe a transferência dessas informações para terceiros?



7

Qual o tempo de armazenamento da informação?

8

De que forma ela é feita?

9

Estes dados são expurgados em algum momento?

Com essas perguntas, é possível traçar o fluxo do dado e, assim, manter o seu rastro para eventual apuração, caso ocorra algum incidente, ou para prestação de informações quando houver uma solicitação do titular ou da ANPD.



PADRÕES MÍNIMOS DE INFRAESTRUTURA E SEGURANÇA DA INFORMAÇÃO

Apesar de não tratar especificamente sobre proteção de dados pessoais, o Provimento nº 74/2018 CNJ aponta caminhos que auxiliam um aspecto importante de privacidade: a segurança da informação.

É importante que os sistemas utilizados em cada serventia identifiquem o usuário e os acessos que são feitos, a fim de manter um possível rastro para eventuais auditorias. É importante que sejam adotados sistemas que contenham logs de registro.



Assim, é importante que o acesso ao computador e aos programas seja feito por meio de senha pessoal, sem compartilhamento, em prol da rastreabilidade de todo o processo. Não basta ferramentas de segurança indicadas no Provimento nº 74/2018 CNJ, é necessária a análise de riscos à privacidade e a conscientização de todos.

MINIMIZAÇÃO DO USO DE DADOS PESSOAIS

Este princípio determina que a atividade de tratamento de dados pessoais deve se limitar ao mínimo de informações para a realização de determinada finalidade, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Logo, tem-se que os agentes de tratamento de dados pessoais, como é o caso dos Tabeliães, registradores, escreventes e atendentes, devem sempre prezar pela minimização do uso de dados pessoais. É claro que determinados formulários, procedimentos e sistemas estão amparados em leis, provimentos e/ou regulamentos que já determinam a forma de condução da atividade de tratamento de dados.

Porém, na atividade registratória, certamente haverá questões que poderemos aplicar a minimização do uso de dados pessoais e o princípio da necessidade. Por exemplo, nos casos de expedição de certidões, é estritamente necessário observar as restrições quanto à emissão de certidão em inteiro teor, limitando o seu acesso, nos estritos limites da lei, como é o caso de alteração de prenome e de sexo (gênero).

Outro exemplo seria não coletar informações sobre a religião ou filiação política do funcionário da serventia no momento de sua contratação.

ARMAZENAMENTO DE DADOS PESSOAIS

A LGPD classifica o armazenamento de dados pessoais como uma das várias formas de tratamento. Nesse sentido, a respectiva serventia só poderá armazenar dados pessoais se para isso houver uma finalidade específica.

Conforme as determinações do Provimento nº 58/89 CNJ sobre a possibilidade de inutilização de documentos após a sua digitalização, as serventias nas quais sejam mantidas as duas versões deverão redobrar a atenção para justificar a finalidade de documentos físicos, uma vez já digitalizados.

O Tabelião, em serventia de sua titularidade, deverá criar políticas de armazenamento e descarte de dados, inclusive redobrar a atenção se tais serviços são realizados por empresas terceirizadas, a fim de incluir cláusulas de segurança para proteger o acervo, caso ocorra algum incidente de proteção de dados.



TRANSPARÊNCIA COM RELAÇÃO ÀS ATIVIDADES DE TRATAMENTO DE DADOS PESSOAIS

A LGPD determina que o titular de dados pessoais tenha direito ao acesso facilitado sobre informações relacionadas ao tratamento de seus dados. Tais informações deverão ser disponibilizadas de forma clara, adequada e ostensiva, em atendimento ao princípio do livre acesso (art. 6º, IV) e abordar, por exemplo, os seguintes aspectos:

1

Finalidade específica do tratamento;

2

Forma e duração do tratamento, observados os segredos comerciais e industriais;

3

Identificação do Controlador;

7

Direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD.

4

Informações de contato do Controlador;

5

Informações acerca do uso compartilhado de dados pelo Controlador e a finalidade;

6

Responsabilidades dos agentes que realizarão o tratamento;



Portanto, dada a condição imposta pela LGPD, é recomendável que um aviso contendo as informações acima listadas seja implementado, variando o formato a depender das instalações, meios disponíveis e da realidade particular de cada Cartório, como forma de conferir uma maior transparência e sensação de segurança ao titular de dados pessoais.

Caso a serventia tenha contratado o Encarregado como Serviço da ITware, será disponibilizada uma Central de Serviços online para atendimento dos titulares e demais interessados.



TRANSFERÊNCIA DE DADOS PESSOAIS PARA OUTROS ENTES PÚBLICOS

Por força de Lei, os cartórios não somente devem realizar o tratamento de dados pessoais internamente, mas também prestar informações a outros entes públicos sobre as atividades ali realizadas. Vale dizer que, em razão do Cartório realizar a transferência de diversos dados pessoais, deverá prestar contas desta atividade.

Este procedimento exige certa atenção com a vigência da LGPD. O Cartório além de ter que informar ao titular dos dados pessoais como essa transferência é feita, para quem ela é feita e o porquê; deverá ainda se atentar a procedimentos e fluxos para que se mantenha em conformidade com a referida Lei.

TRANSFERÊNCIA PARA ENTES PRIVADOS COM FINS COMERCIAIS

A fim de catalisar a persecução do interesse público e auxiliar em algumas atribuições legais do serviço público, os cartórios devem fornecer acesso aos dados por meio eletrônico para a administração pública.

Os dados devem ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Tais fins perseguidos pelos entes e órgãos públicos deverão respeitar os Princípios de proteção de dados pessoais. No que diz respeito à transferência de dados pessoais constantes em bases cujo acesso seja permitido a entes privados, este está vedado, sobretudo quando para fins comerciais.





AJUSTE DE CONTRATOS QUE TRATAM DADOS PESSOAIS COM TERCEIROS

Sob um ponto de vista legal e prático, aspectos de proteção de dados pessoais devem constar nos corpos de contratos, a fim de trazer mais efetividade e segurança na prestação de serviços com contratos vigentes ou a serem contratados.

Assim, é de suma importância que sejam negociados alguns aditivos contratuais e/ou a inclusão de dispositivos que versem sobre a proteção de dados pessoais, abordando, por exemplo, as obrigações das partes, garantias com relação à adoção de medidas de segurança e ao cumprimento da legislação aplicável e, especialmente, do dever de informação em caso de incidentes de segurança envolvendo dados pessoais.

ADOÇÃO DE POLÍTICAS E CONSOLIDAÇÃO DE PROCEDIMENTOS INTERNOS

Com o devido engajamento da equipe de colaboradores, torna-se possível o aumento da satisfação e fidelização dos usuários dos serviços, redução de custos e melhoria da rentabilidade da serventia decorrente da otimização de processos internos, bem como por meio de uma melhor imagem institucional do segmento cartorário.

Aqui é importante tomar medidas como a criação de políticas ou até mesmo folders que fiquem em locais de fácil acesso para todos os funcionários, a fim de informar métodos e procedimentos de acordo com a LGPD. Por exemplo: avisos de atenção para a não utilização do celular ou de pen drives nos computadores dos cartórios.

Ainda, é importante manter o engajamento da equipe sobre o uso de dispositivos móveis pessoais. Apontar o risco do uso de aparelhos pessoais; WhatsApp; e-mail pessoal; pen drives; pois são ferramentas extremamente sensíveis no que tange ao tratamento de dados pessoais e podem ser alvos de invasores, vírus, spams, etc.



TREINAMENTOS E ENGAJAMENTOS

Para fortalecer e consolidar uma cultura de proteção de dados pessoais, é importante que os agentes de tratamento de dados pessoais, como é o caso dos cartórios, promovam regras de boas práticas e de governança que estabeleçam parâmetros com relação à proteção de dados pessoais, ajustadas à realidade vivenciada e à exposição de riscos relativas às atividades de tratamento.

Deste modo é importante oferecer periodicamente treinamento para esclarecer a importância de reter somente os dados pessoais estritamente necessários para o exercício da função, agir com zelo no armazenamento e descarte de dados e documentos, bem como estabelecer meios de controle de acesso dos colaboradores sobre as informações contidas em banco de dados e arquivos em formatos físicos e digitais.





Esses treinamentos também devem informar a obrigatoriedade legal, forma e prazo e qual canal será disponibilizado para responder solicitações dos titulares dos dados pessoais quanto aos tratamentos realizados na serventia.

Por fim, ressaltamos que os dispositivos e eventuais modelos desta cartilha possuem caráter instrutório e recomendativo e, em hipótese alguma, dispensam a análise e/ou verificação de situações específicas, caso a caso.



OBRIGADA



www.itware.com.br