CARTÓRIOS DE PROTESTO SP

INSTITUTO DE PROTESTO – IEPTB

LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

SUMÁRIO

1 INTRODUÇÃO

ATIVIDADE EXTRAJUDICIAL DO PROTESTO E A PROTEÇÃO DE DADOS

O Tabelionato de Protesto, no exercício de suas atividades, concede publicidade ao inadimplemento de uma obrigação originada em títulos e outros documentos de dívida, trazendo ao credor a possibilidade de dar publicidade ao descumprimento de obrigações.

Mas, mesmo a atividade tendo como o objetivo dar publicidade à inadimplência de obrigações, não significa que seja possível a publicação indiscriminada, ou a difusão dos dados para levar a situação de inadimplência ao conhecimento do público em geral de qualquer forma, ou, ainda, o acesso de terceiros à banco de dados massivos indiscriminadamente.

O tabelião tem o dever ético e legal de guardar sigilo profissional sobre as informações a que tem acesso no seu exercício profissional, como também o dever específico de conservar funcionalmente os documentos físicos ou eletrônicos a ele confiados, observando os regramentos normativos e legais.

Com a edição da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD), o tabelião também deverá observar os regramentos nela contidos e efetuar as adequações para sua atividade.

Em relação aos fundamentos da proteção de dados não estamos falando de sigilo, como veremos a seguir, mas de uma série de procedimentos necessários ao controle do fluxo adequado dos dados pessoais em cada contexto.

A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) SE APLICA A TODOS OS DADOS PERTENCENTES A PESSOAS FÍSICAS, NÃO IMPORTANDO SE ELAS ESTÃO EM MEIO FÍSICO (PAPÉIS, LIVROS E DOCUMENTOS) OU ELETRÔNICOS (COMPUTADOR, OUTROS DISPOSITIVOS OU ACESSADOS POR SISTEMAS OU PELA INTERNET).

O QUE É PROTEÇÃO DE DADOS

Apesar de estarem intimamente ligados, o direito à privacidade e o direito à proteção de dados pessoais são distintos.

Quando falamos de direito à privacidade, estamos falando da inviolabilidade da intimidade, da vida privada, da honra e imagem, bem como da casa e do sigilo das telecomunicações. Trata-se de uma proibição da interferência estatal na vida privada, exceto excepcionalmente, desde que de acordo com a lei por importante razão e legítimo interesse público.

Com o advento da internet e do cada vez mais presente espaço digital, surgem novos riscos à vida privada relacionados à coleta e ao uso de dados e informações pessoais nesses ambientes, emergindo um novo conceito de privacidade: a privacidade informacional ou o direito à autodeterminação informacional.

Apesar de protegerem valores similares – a autonomia e a dignidade humana dos indivíduos,

bem como a garantia de uma esfera pessoal em que se possa livremente desenvolver a personalidade, o pensamento e as opiniões –, os dois direitos são diferentes em suas formulações e escopos.

Enquanto o direito à privacidade consiste em uma proibição geral de interferência estatal, o direito à proteção de dados pessoais é um direito novo e ativo que impõe o funcionamento de um sistema de conformidade para proteger o indivíduo sempre que seus dados pessoais sejam coletados e tratados.

Assim, a autodeterminação informativa seria ligada ao controle efetivo do titular dos dados em relação à exatidão das informações e real utilização dos seus dados pessoais, bem como a transparência em relação aos motivos e às finalidades do tratamento dos dados pessoais.

Portanto, o direito à proteção de dados pessoais de modo algum vem para impor o sigilo ou vedar o fluxo de dados pessoais, mas sim para determinar que seu processamento seja justo, com propósito específico, baseado no consentimento dos titulares ou em base legítima determinada por lei. Garante aos titulares o direito de acessá-los e retificá-los, bem como determina que a fiscalização seja feita por autoridade independente.

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) - LEI Nº 13.709/2018

A Lei Geral de Proteção de Dados brasileira é totalmente inspirada na legislação de Proteção de Dados da União Europeia, a GDPR.

Sua ideia central, que parte do conceito de autodeterminação informativa, é de que as pessoas possam conhecer e controlar a coleta e o processamento de seus dados, permitindo que a limitação desse processamento seja tanto por parte de particulares como pelo Estado, e trazendo práticas transparentes e seguras para quando esses dados são tratados, com o objetivo de garantir direitos e liberdades fundamentais. A lei estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, oferecendo segurança jurídica para o uso e tratamento deles.

A LGPD então proíbe o tratamento de dados? Não! A lei disciplina a forma como esses dados podem e devem ser tratados. Pela legislação, são definidos aspectos importantes, tais como:

- as hipóteses nas quais o tratamento de dados é legalmente autorizado (as chamadas "bases legais");
- os direitos dos titulares que precisam ser preservados e respeitados;
- como tratar dados da forma mais segura possível e o que fazer na hipótese de um incidente de segurança.

Essas e outras questões relevantes serão tratadas no decorrer desta cartilha.

O QUE PRECISAMOS SABER SOBRE A LGPD

A LGPD cria todo um novo regramento para o uso de dados pessoais no Brasil que:

• regula o tratamento de dados relacionados a pessoas físicas (dados de pessoas falecidas e de pessoas jurídicas estão excluídos dessa legislação);

• se aplica independentemente do meio e/ou forma de tratamento de dados, dentro ou fora da internet, utilizando ou não meios digitais;

• se aplica a qualquer operação de tratamento realizada no território nacional, ou mesmo fora do território nacional no caso: (i) dos dados serem coletados no Brasil ou estejam relacionados a indivíduos localizados no território brasileiro ou (ii) do tratamento dos dados ter como objetivo a oferta de produtos e/ou serviços ao público brasileiro;

• não se aplica ao tratamento de dados pessoais: (i) realizado por pessoa natural para fins exclusivamente particulares e não econômicos; (ii) realizado para fins exclusivamente jornalísticos, artísticos, acadêmicos; (iii) realizado para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou atividades de investigação e repressão de infrações penais; e (iv) provenientes e/ou destinados a outros países, que apenas transitem pelo território nacional, sem que aqui seja realizada qualquer operação de tratamento;

se aplica ao setor privado e ao setor público, aqui entendido como qualquer órgão ou entidade pública, inclusive empresas públicas e sociedades de economia mista.

A NATUREZA PÚBLICA DOS CARTÓRIOS

De acordo com o art. 236 da Constituição Federal, os serviços notariais e de registro são exercidos em caráter privado, mas por delegação do poder público. Isso significa que eles são, na verdade, uma função pública delegada a particulares, via concurso público, para fins de otimização da sua execução. Tendo em vista a natureza pública desses serviços, incidem sobre eles as diretrizes basilares da Administração Pública (legalidade, impessoalidade, moralidade, publicidade e eficiência, presentes no caput do artigo 37 da Constituição Federal), e têm sua atuação regulada por lei (nº 8.935/94), bem como devem perseguir o fim maior de toda a atividade estatal: o interesse coletivo.

É claro que as relações sociais e econômicas modernas permitem que o Estado delegue a particulares a execução de certos serviços públicos. No entanto, essa delegação não descaracteriza o serviço como público, vez que o Estado sempre se reserva o poder jurídico de regulamentar, alterar e controlar o serviço. (CARVALHO FILHO, 2015, p. 334).[1]

Exatamente em virtude da natureza pública desses serviços, a LGPD determinou, em seu art.23, §4º, que os serviços notariais e de registro terão o mesmo tratamento dispensado às pessoas jurídicas de direito público. A LGPD dispôs também que os órgãos notariais e de registro devem fornecer, para a Administração Pública, o acesso aos dados por meio eletrônico.

[1] Extraído do Manual de Direito Administrativo. São Paulo: Atlas, 2015, 28 ed.

A LGPD foi publicada em 14 de agosto de 2018 e sua vigência é considerada a partir de 16 de agosto de 2020. Apesar de ainda ser necessária regulamentação específica de alguns de seus aspectos e efeitos, os seus princípios, diretrizes e alguns dos direitos ali previstos já deverão ser observados a partir dessa data, sendo a adequação dos métodos e procedimentos extremamente recomendável.

Vale salientar que a LGPD não revoga ou impede a aplicação de normas setoriais que também regulamentam dados pessoais.
Para o caso específico dos cartórios de protesto situados em São Paulo (inclusive os que possuem outras naturezas cumuladas ao protesto), além das determinações da LGPD sob a ótica do setor público, devem ser avaliadas as disposições específicas das seguintes normas:

- Provimento da Corregedoria Geral de Justiça nº 23/2020 do Tribunal de Justiça de São Paulo, que dispõe sobre o tratamento e proteção de dados pessoais pelos responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro e acrescenta os itens 127 a 152.1 do Capítulo XIII do Tomo II das Normas de Serviço da Corregedoria Geral da Justiça.
- Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data); Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) e Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
- Lei nº 6.015, de 31 de dezembro de 1973 (dispõe sobre os registros públicos e dá outras providências); Lei nº 8.935, de 18 de novembro de 1994 (lei dos cartórios); Lei nº 9.492, de 10 de setembro de 1997 (define competência, regulamenta os serviços concernentes ao protesto de títulos e outros documentos de dívida e dá outras providências); Lei Estadual de São Paulo nº 11.331/02 (lei de emolumentos dos serviços notarias e de registro de São Paulo); Provimento nº 74/2018 do Conselho Nacional de Justiça (dispõe sobre padrões mínimos de tecnologia da informação para a segurança, integridade e disponibilidade de dados para a continuidade da atividade pelos serviços notariais e de registro do Brasil), além de outras aplicáveis;
- Sanções previstas na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)[2]; e na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa), em caso de descumprimento do disposto na LGPD, além das sanções previstas pela própria norma.

[2] WO Conselho Nacional de Justiça já emitiu entendimento no qual considerou aplicável a Lei de Acesso à Informação às atividades realizadas pelos cartórios (CNJ – Consulta nº 0003410-42.2013.2.00.0000 – Distrito Federal e dos Territórios – Rel. Cons. Emmanoel Campelo de Souza Pereira – DJ 26.11.2013).

2 CONCEITOS LEGAIS ESSENCIAIS PARA COMPREENSÃO DO CONTEÚDO DESTA CARTILHA

DADO PESSOAL:

toda informação relacionada à pessoa natural identificada ou identificável, ou seja, qualquer informação que identifique ou possa identificar uma pessoa, tais como nomes, números de documento, endereços, número de telefone, e-mail, identificadores únicos eletrônicos (como IP, cookies e beacons), entre outros.

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.

DADO ANONIMIZADO:

dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento[1].

TITULAR:

pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

TRATAMENTO DE DADOS:

é toda a operação realizada com o dado pessoal, tais como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, comunicação, transferência, difusão ou extração.

CONTROLADOR:

pessoa natural ou jurídica, de direito público ou privado, que tem competência para tomar decisões referentes ao trata-mento de dados pessoais.

[1] O dado anonimizado não será considerado dado pessoal para os fins da LGPD, salvo quando o processo de anonimização ao qual foi submetido for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. Com exceção se o uso desses dados forem destinados à formação de perfil comportamental (profiling). Nesse caso, mesmo que anonimizados serão considerados dados pessoais para fins da lei.

OPERADOR:

pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

AGENTES DE TRATAMENTO:

são o controlador e o operador, teremos um capítulo específico para abordar esses conceitos.

AUTORIDADE NACIONAL:

órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei. Caberá à autoridade estabelecer diretrizes para a promoção da proteção de dados pessoais no Brasil. Ela deverá zelar pela proteção dos dados pessoais, elaborar a Política Nacional de Proteção de Dados e da Privacidade, como definida pela lei, fiscalizar e aplicar sanções em caso de violação às leis pertinentes, atender petições de titulares de dados contra os responsáveis pelo seu tratamento, regulamentar as matérias sobre proteção de dados, entre outras atividades.

A LGPD prevê também a criação do Conselho Nacional de Proteção de Dados, órgão de caráter meramente consultivo, que pode propor diretrizes e estratégias, realizar estudos e disseminar conhecimento sobre proteção de dados no Brasil.

A Autoridade Nacional Brasileira foi instituída pelo decreto 10.474, de 26 de agosto de 2020, que passará a vigorar na data de publicação da nomeação do diretor-presidente da ANPD no Diário Oficial da União.

ENCARREGADO (DPO):

pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. O capítulo abaixo irá explicar melhor a figura do encarregado e suas atribuições.

Na prática, todas as atividades realizadas pelos cartórios que envolvam dados pessoais serão consideradas tratamento de dados. O simples armazenamento de dados, em meio físico ou digital, é considerado tratamento para fins da lei.

3 OS AGENTES DE TRATAMENTO

3.1 O ENCARREGADO DE PROTEÇÃO DE DADOS PESSOAIS (OU DPO)

O chamado DPO da legislação europeia de proteção de dados (GDPR) foi traduzido pela LGPD como o "encarregado".

Nos termos do art. 41 da Lei 13.709 (LGPD):

• A identidade e as informaçõ**õ**es de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

• As atividades do encarregado consistem em:
I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - receber comunicações da autoridade nacional e adotar providências;
III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Recomenda-se que o encarregado seja o responsável dentro da instituição pela supervisão do cumprimento das regras previstas na lei, de forma contínua.

A princípio, a LGPD prevê que toda e qualquer entidade que trate dados pessoais deve indicar um encarregado, mas prevê expressamente que a Autoridade Nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa.

Não é previsto em lei, mas é comumente aceito nos países em que existe a legislação a figura do "*DPO as a Service*", ou seja, um prestador de serviços que oferece ou o serviço de DPO em si ou a assessoria técnica e/ou jurídica para apoiar o preposto que exercerá a função de DPO na instituição.

No caso dos cartórios do Estado de São Paulo, a corregedoria definiu no Provimento 23/2020 que:

133. Cada unidade dos serviços extrajudiciais de notas e de registro deverá manter um encarregado que atuará como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

133.1 Os responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro poderão nomear encarregado integrante do seu quadro de prepostos ou prestador terceirizado de serviços técnicos.

133.2 Poderão ser nomeados como encarregados prestadores de serviços técnicos com remuneração integralmente

[1] Extraído do Provimento CGJ nº 23/2020, disponível em: https://www.cnbsp.org.br/__Documentos/Uploads/Parecer%20n%203772020-E%20-%20Provimento%20CGJ%20n%2023-2020.pdf. Acesso em: 7/10/2020.

paga, ou subsidiada, pelas entidades representativas de classe.

133.3 A nomeação do encarregado será promovida mediante contrato escrito, a ser arquivado em classificador próprio, de que participarão o controlador na qualidade de responsável pela nomeação e o encarregado.

133.4 A nomeação de encarregado não afasta o dever de atendimento pelo responsável pela delegação dos serviços extrajudiciais de notas e de registro, quando for solicitado pelo titular dos dados pessoais.

133.5 A atividade de orientação dos prepostos e prestadores de serviços terceirizados sobre as práticas a serem adotadas em relação à proteção de dados pessoais, desempenhada pelo encarregado, não afasta igual dever atribuído aos responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro1. (Provimento CG nº 23/2020, p. 6 e 7)

É importante que o **encarregado** responda diretamente ao tabelião, não devendo se reportar a outros níveis hierárquicos na estrutura, dada a responsabilidade pessoal do tabelião.

Embora não previsto na lei, as boas práticas pedem para que o **encarregado pela proteção de dados pessoais** possua conhecimento especializado das leis e práticas de proteção de dados, além de outras qualidades profissionais, para garantir que a serventia cumpra os requisitos da LGDP e das leis e regulamentos relevantes de proteção de dados que estiverem vigentes.

É sob sua gestão que a documentação para demonstrar conformidade com a LGDP, como políticas e procedimentos, deve ser mantida e atualizada, em especial o registro de operações de processamento dos dados pessoais (ROPA).

Deverá também contribuir para o desenvolvimento e manutenção de todas as politicas, procedimentos e processos de proteção de dados pessoais e buscar que o treinamento e a conscientização estejam disponíveis e entregues a todos os funcionários envolvidos nas operações de processamento relacionadas aos dados pessoais.

É importante que ele monitore regularmente a conformidade com as leis de proteção de dados pessoais, relatando eventuais observações, por escrito, ao tabelião.

É seu papel também acompanhar e aprovar eventual teste de balanceamento de legítimo interesse, bem como Relatório de Impacto à

Proteção de Dados Pessoais, qualquer que seja a base legal utilizada.

É fundamental que ele traga ao tabelião quaisquer assuntos que sejam potenciais fatores de risco para a proteção adequada dos dados pessoais que observar.

3.2 O CONTROLADOR E O OPERADOR

A LGPD definiu como:
CONTROLADOR:
pessoa natural ou jurídica, de direito público ou privado, que tem competência para tomar decisões referentes ao tratamento de dados pessoais.

OPERADOR:
pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.

Apesar de parecer um conceito simples, na prática essa definição às vezes é complexa e tem gerado interpretações que se afastam dos conceitos técnicos da LGPD e das legislações de proteção de dados em geral, causando consequências jurídicas e práticas.

COMO DEFINIR QUEM É O CONTROLADOR?
A definição legal diz que o controlador é aquele que toma a decisão em relação aos dados pessoais. Portanto, a maioria das responsabilidades relacionadas à conformidade com a lei são tarefas do controlador, já que ele é quem define as finalidades e os meios de processamento (mesmo que dentro de parâmetros estabelecidos por lei).

O controlador decide sobre quais os dados que serão coletados, quem irá coletar os dados, o porquê da coleta dos dados (finalidade) e de que modo irá fazê-lo (base legal).

O CONTROLADOR

É importante ressaltar que, como a atividade notarial e de registro é delegada a uma pessoa física, mediante concurso público de provas e títulos, o papel de controlador será exercido pelo tabelião. No que se refere às atividades relacionadas com sua atividade fim, na maioria, o tabelião exercerá o papel de controlador, tomando decisões referentes ao tratamento dos dados pessoais que maneja.

De acordo com o Provimento CG 23/2020, os responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro, na qualidade de titulares, interventores ou interinos, são controladores e responsáveis pelas decisões referentes ao tratamento dos dados pessoais".

E O OPERADOR?

O controlador de dados pode contratar um terceiro para realizar o processamento dos dados que estão sob sua responsabilidade. Aqueles que processam os dados em nome do controlador são os chamados de operadores.

O operador não controla os dados e não pode alterar a finalidade ou o uso daqueles dados que processa em nome do operador. O operador estará sempre limitado ao processamento dos dados de acordo com as instruções e propósito dados pelo controlador. Geralmente o processador de dados é um parceiro terceiro especializado, contratado para executar tarefas específicas definidas pelo controlador de dados.

Sempre será uma outra pessoa física ou jurídica, diferente do controlador, e que processará os dados pessoais em nome dele.

Os exemplos mais comuns são a contratação de nuvem para armazenamento dos dados ou um terceiro que processa folha de pagamentos.

AS PRINCIPAIS RESPONSABILIDADES DOS CONTROLADORES SÃO:

- Obter consentimento, quando necessário, assim como demonstrar, em caso de necessidade, como o consentimento foi obtido (art. 7°, §5°; art. 8°, §6°);
- Informar e prestar contas; garantir a portabilidade (art. 9°; art. 18; art. 20);
- Garantir a transparência no tratamento de dados baseado em legítimo interesse (art. 10, §2°);
- Manter registro das operações de tratamento de dados pessoais, especialmente quando baseado no legítimo interesse (art. 37);
- Elaborar relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, com observância dos segredos comercial e industrial (art. 10; §3°; art. 38);
- Indicar o encarregado pelo tratamento de dados (art. 41);
- Reparar danos patrimoniais, morais, individuais ou coletivos causados por violação à legislação de proteção de dados pessoais (art. 42);
- Comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48);
- Salvaguardar os direitos dos titulares mediante a adoção de providências, e.g., divulgação do fato em meios de comunicação; medidas para reverter ou mitigar os efeitos do incidente (art. 48, §2°);
- Observar as boas práticas e padrões de governança (art. 50).

Já os operadores devem fornecer garantias contratuais de que foram implementadas as medidas técnicas e organizacionais adequadas, de modo que o processamento cumpra os requisitos legais e de segurança da informação, para manter os dados pessoais protegidos, por exemplo, de acesso não autorizado, vazamento, destruição ou perda acidental.

Importante ressaltar que os operadores devem processar dados pessoais estritamente sob instruções do controlador.

Apesar dessas definições técnicas já serem consolidadas, algumas regulamentações infra-legais vêm trazendo conceitos bastante diferentes dos já estabelecidos. Isso também aconteceu com o Provimento 23/2020 da Corregedoria Geral da Justiça do TJ-SP, que traz uma imprecisão técnica relativa aos agentes de tratamento, no item 132 das Normas de Serviço, devido a conceitos inéditos como de "operador integrante" ou do "operador preposto".

Operador é uma categoria de agente de tratamento relativa a outro ente legal, jamais poden-

do ser classificado o funcionário ou preposto de uma entidade, no caso, da serventia.

Publicado recentemente pelo Comitê Europeu para a Proteção de Dados (EDPB), o "Guideline 07/2020"**,** que traz os conceitos de controladores e operadores na GDPR, é bastante esclarecedor sobre quem pode ser Controlador e o Operador.

Dentro de uma organização, pode-se designar uma pessoa específica para ser responsável pela execução das operações de processamento. Mesmo que uma pessoa física específica seja nomeada para garantir o cumprimento das regras de proteção de dados, ela não será o operador, mas sempre agirá em nome da organização que compõe o quadro, que será a responsável final em caso de violação das regras na sua qualidade de controlador.

Essa questão é de fundamental importância especialmente, pela **responsabilidade dos agentes de tratamento imputada pela lei, que prevê que os** diferentes agentes de tratamento - o controlador e o operador - podem ser solidariamente responsabilizados por incidentes de segurança da informação e/ou o uso indevido e não autorizado dos dados, ou pela não conformidade com a lei.

Pela legislação, a responsabilidade do operador pode ser limitada às suas obrigações contratuais e de segurança da informação, caso não viole as regras que lhe são impostas pela LGPD.

Para suportar tais responsabilidades, os funcionários (ou prepostos) do controlador não dispõem de meios necessários para impor as condições ideais de trabalho que garantam a implementação das medidas técnicas e organizacionais adequadas. Assim, **não podem recair sobre** eles, pessoalmente, as responsabilidades impostas pela lei o que é diferente no caso de um terceiro prestador de serviços. Isso também exigiria, por parte do controlador, a necessidade de contratação de seguro, por exemplo, para seus prepostos que assumissem quaisquer atividades laborais relacionadas ao tratamento dos dados pessoais.

Desta forma, urge a necessidade de rever o conceito de "operadores integrantes" previsto no item 132 do Provimento.

TRATAMENTO DE DADOS PESSOAIS

4

CONSTA NO PROVIMENTO CG 23/2020:

132. Para o tratamento dos dados pessoais os responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro, sob sua exclusiva responsabilidade, poderão nomear operadores integrantes e operadores não integrantes do seu quadro de prepostos, desde que na qualidade de prestadores terceirizados de serviços técnicos.

132.1 Os prepostos e os prestadores terceirizados de serviços técnicos deverão ser orientados sobre os deveres, requisitos e responsabilidades decorrentes da Lei n. 13.709, de 14 de agosto de 2018, e manifestar a sua ciência, por escrito, mediante cláusula contratual ou termo autônomo a ser arquivado em classificador próprio.

132.2 Os responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro orientarão todos os seus operadores sobre as formas de coleta, tratamento e compartilhamento de dados pessoais a que tiverem acesso, bem como sobre as respectivas responsabilidades, e arquivarão, em classificador próprio, as orientações transmitidas por escrito e a comprovação da ciência pelos destinatários.

132.3 Compete aos responsáveis pelas delegações dos serviços extrajudiciais de nota e de registro verificar o cumprimento, pelos operadores prepostos ou terceirizados, do tratamento de dados pessoais conforme as instruções que fornecer e as demais normas sobre a matéria.

132.4 A orientação aos operadores, e qualquer outra pessoa que intervenha em uma das fases de coleta, tratamento e compartilhamento abrangerá, ao menos:

I - as 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;

II - a informação de que a responsabilidade dos operadores prepostos, ou terceirizados, e de qualquer outra pessoa que intervenha em uma das fases abrangida pelo fluxo dos dados pessoais, subsiste mesmo após o término do tratamento.

132.5 Também serão arquivados, para efeito de formulação de relatórios de impacto, os comprovantes da participação em cursos, conferências, seminários ou qualquer modo de treinamento proporcionado pelo controlador aos operadores e encarregado, com indicação do conteúdo das orientações transmitidas por esse modo.

QUANDO É PERMITIDO TRATAR DADOS PESSOAIS?

Os dados pessoais somente poderão ser tratados com fundamento em alguma das hipóteses previstas na lei (é o que se denomina "base legal" de tratamento).

A lei previu as seguintes bases legais que autorizam o tratamento:

I . Com o devido consentimento do titular

Consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Caso haja alguma mudança nessa finalidade originalmente informada, o titular precisa ser devidamente informado.

Para ser válido, o consentimento do titular **não pode ser implícito nem genérico.** Além disso, o consentimento, diferentemente das demais bases legais que serão abordadas adiante, pode ser revogado a qualquer momento!

Atenção! Em se tratando de dados sensíveis, o consentimento precisa, ainda, ser dado de forma específica e destacada para finalidades determinadas.

II - Sem o consentimento do titular, nas seguintes hipóteses:
Para o cumprimento de **obrigação legal ou regulatória** pelo controlador;

Essa é uma das bases legais que mais se deve aplicar aos cartórios, uma vez que sua atuação é regulamentada por leis específicas, que atribuem aos notários e registradores diversas obrigações legais. Um exemplo do tratamento de dados com fundamento nessa base legal é o caso da obrigação de emitir certidões dos registros, efetuadas pelo cartório sempre que for solicitado por qualquer pessoa, sem necessidade desta informar o motivo ou interesse do seu pedido, conforme dispõem os artigos 16 e 17 da lei nº 6.015/73.

Isso também está expresso no Provimento CG 23/2020 do TJ/SP que prevê:

130. O tratamento de dados pessoais destinado à prática dos atos inerentes ao exercício dos respectivos ofícios será promovido de forma a atender à finalidade da prestação do serviço, na persecução do interesse público, e com os objetivos de executar as competências legais e desempenhar atribuições legais e normativas dos serviços público delegados.

130.1 Consideram-se inerentes ao exercício dos ofícios os atos praticados nos livros mantidos por força de previsão nas legislações específicas, incluídos os atos de inscrição, transcrição, registro, averbação, anotação, escrituração de livros de notas, reconhecimento de firmas, autenticação de documentos; as comunicações para unidades distintas, visando as anotações nos livros e atos nelas mantidos; os atos praticados para a escrituração de livros previstos em normas administrativas; as informações e certidões; os atos de comunicação e informação para órgãos públicos e para centrais de serviços eletrônicos compartilhados que decorrerem de previsão legal ou normativa.

No caso da Administração Pública, permitido também para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;[1]

Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.[2]

Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

Para a proteção da vida ou da incolumidade física do titular ou de terceiro;

Para a tutela da saúde em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

[1] Em se tratando de dados pessoais sensíveis, o tratamento só é permitido quando for necessário à execução de políticas públicas exclusivamente previstas em leis ou regulamentos (excluídas aqui as hipóteses de política pública respaldada em contrato, convênios ou instrumentos congêneres);
[2] Essa hipótese não se aplica aos dados sensíveis.

Quando necessário para atender **aos interesses legítimos** do controlador ou de terceiro, exceto quando se tratar de dados sensíveis que não se submetam a essa hipótese.[3]

Para a proteção do crédito, salvo quando se tratar de dados sensíveis, que não se submetem a essa hipótese de tratamento;

Como garantia da prevenção à fraude e da segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

4.1 O TRATAMENTO DE DADOS PESSOAIS PELOS CARTÓRIOS

O tratamento de dados pessoais realizado pelos cartórios - destinados à prática dos atos inerentes ao exercício dos respectivos ofícios - deve visar ao atendimento de sua finalidade da prestação do serviço público, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir com as atribuições legais inerentes aos serviços notariais e de registro e **não dependem, nesses casos, de autorização específica da pessoa natural que deles for titular.**

PARA ISSO É NECESSÁRIO:

Ser transparente: é importante que sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal (base legal), a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, em seus sites, aplicativos, assim como afixados na própria serventia;[4]

Ter uma **Política de Privacidade** que descreva os direitos dos titulares de dados pessoais, de modo claro e acessível, os tratamentos realizados e a sua finalidade;

Manter um sistema de controle do fluxo abrangendo a coleta, tratamento, armazenamento e compartilhamento de dados pessoais, até a restrição de acesso futuro (também chamado ROPA Record of Processing Activities - ou **Registro de Operações**);

Possuir um **Canal de Atendimento para o exercício dos Direitos dos Titulares,** adequado para informac ões, reclamações e sugestões ligadas ao tratamento de dados pessoais, com fornecimento de formulários para essa finalidade.

Indicar um **Encarregado pelo Tratamento de Dados Pessoais** (DPO) em cada serventia (ou compartilhar um encarregado com outras serventias), podendo ser contratado serviço de terceiros para este fim;

Elaborar um Relatório de Impacto à Proteção de Dados Pessoais sobre as atividades de tratamento de dados pessoais sensíveis, bem como para fins de avaliação para atividades que possam causar maior risco aos direitos e liberdades dos titulares;

Fornecer acesso aos dados por meio eletrônico para a Administração Pública, que exerce sobre os cartórios o poder de fiscalização;

Mapear a existência de atividades, atuais ou projetos futuros, em que haveria emprego de decisões **automatizadas** para a adequação da atividade nos termos da LGPD.

Sobre o uso compartilhado de dados pelos cartórios, inclusive em relação ao poder p**úblico, a LGPD determina que esse tipo de uso somente deve se dar para atender às finalidades específicas de execução de políticas públicas e à atribuição legal dos serviços notariais e de registro, respeitados os princípios de proteção de dados pessoais já mencionados**.

Atenção!
A regra para o poder público, que se aplica aos cartórios, é não poder transferir para entidades privadas dados pessoais constantes de bases de dados em relação às quais

[3] Será permitido o tratamento de dados com base no legítimo interesse, desde que tal tratamento não viole os direitos e liberdades fundamentais do titular dos dados e que medidas para garantir a transparência de tal tratamento sejam adotadas. O "legítimo interesse" permite o uso dos dados para finalidades além daquelas originalmente autorizadas pelos seus titulares ou para os quais eles foram originalmente coletados. Por meio de um teste de proporcionalidade, que leva em consideração os interesses dos agentes de tratamento e os direitos dos titulares, é possível novos usos - o que continua permitindo diversos modelos de negócios baseados no uso de dados pessoais.

[4] É importante salientar a diferença de uma Política de Privacidade (mais abrangente, que abarca a totalidade dos fluxos de dados de cada serventia) e do Aviso de Privacidade (que comunica de forma clara com o titular do dado pessoal).

tenha acesso. A comunicação ou o uso compartilhado desses dados com pessoas de direito privado deverão ser informados à Autoridade Nacional e dependerão de consentimento do titular.

Excepcionalmente, no entanto, esse consentimento do titular e a informação à Autoridade Nacional serão dispensados. São os casos de:

• hipóteses de dispensa de consentimento previstas na LGPD;
• nos casos de uso compartilhado de dados, em que será dada publicidade (sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal (base legal), a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sites;
• em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
• em que os dados forem acessíveis publicamente, observadas as disposições da lei;
• **quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres** (nesse caso, o teor desses contratos e convênios devem ser informados à Autoridade Nacional, a ser implementada);
• na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

A Autoridade Nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

O Provimento CG 23/2020 do TJ SP prevê que:

149. É vedado aos responsáveis pelas delegações de notas e de registro, aos seus prepostos e prestadores de serviço terceirizados, ou qualquer outra pessoa que deles tenha conhecimento em razão do serviço, transferir ou compartilhar com entidades privadas dados a que tenham acesso, salvo mediante autorização legal ou normativa.

149.1 As transferências, ou compartilhamentos, de dados pessoais para as Centrais de Serviços Eletrônicos Compartilhados, incluídos os relativos aos sistemas de registro eletrônico sob a sua responsabilidade, serão promovidas conforme os limites fixados na legislação e normas específicas.

150. Para o recebimento de informações que contenham dados pessoais, previstas nas Normas de Serviço da Corregedoria Geral da Justiça, as Centrais de Serviços Eletrônicos Compartilhados deverão declarar que cumprem, de forma integral, os requisitos, objetivos, fundamentos e princípios previstos nos arts. 1o, 2o e 6o da Lei n. 13.709, de 14 de agosto de 2018.

150.1 A declaração poderá ser encaminhada aos responsáveis pelas delegações de notas e de registro por meio escrito, eletrônico, ou outro que permita a confirmação do envio.

150.2 Iguais declarações deverão ser encaminhadas pelas Centrais de Serviços Eletrônicos Compartilhados para a Corregedoria Geral da Justiça.

ATÉ QUANDO É PERMITIDO TRATAR OS DADOS PESSOAIS?

O tratamento dos dados deverá ser encerrado quando:
• A finalidade para a qual o consentimento foi obtido for alcançada;
• Os dados pessoais coletados deixam de ser necessários à finalidade pretendida;
• Transcorrer o período de tratamento;
• O titular dos dados retirar o consentimento que fundamentou o tratamento;
• Houver uma determinação legal nesse sentido.

Uma vez encerrado o tratamento, os dados pessoais deverão ser corretamente eliminados. Em alguns casos, a LGPD autoriza a guarda desses dados de forma segura, como por exemplo, para atender **às seguintes finalidades:**
• Cumprimento de obrigação legal ou regulatória pelo controlador

Isso se aplica aos cartórios no cumprimento de suas atividades inerentes a sua função, que deverá sempre obedecer ao prazo de temporalidade estabelecido por lei.

O Provimento CG 23/2020 do TJSP prevê que:

148. A inutilização e eliminação de documentos em conformidade com a Tabela de Temporalidade de Documentos prevista no Provimento no 50/2015, da Corregedoria Geral da Justiça, será promovida de forma a impedir a identificação dos dados pessoais neles contidos.

148.1 A inutilização e eliminação de documentos não afasta os deveres previstos na Lei n. 13.709, de 14 de agosto de 2018, em relação aos dados pessoais que remanescerem em índices, classificadores, indicadores, banco de dados, arquivos de segurança ou qualquer outro modo de conservação adotado na unidade dos serviços extrajudiciais de notas e de registro.

A lei também permite a manutenção desses dados nos seguintes casos:
• Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
• Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na legislação;
• Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Anonimização é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais determinado dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

O QUE CONSIDERAR PARA TRATAR DADOS PESSOAIS?

Ao tratar dados pessoais, os agentes precisam considerar:
• os princípios norteadores estabelecidos na LGPD, que estabelecem as diretrizes e as limitações sobre como os dados poderão ser tratados, bem como ter como norte seus objetivos e fundamentos;
• os direitos que precisam ser garantidos aos respectivos titulares.

O Provimento CG 23/2020 do TJ-SP prevê que "no tratamento dos dados pessoais, os responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro deverão observar os objetivos, fundamentos e princípios previstos nos arts. 1o, 2o e 6o da Lei n. 13.709, de 14 de agosto de 2018".

O principal **objetivo da LGPD** é a proteção dos direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade, tendo assim como seu vetor a dignidade da pessoa humana (art. 1º da LGPD e art. 1º, inc. III da CF/88).

Seus **fundamentos** são alguns princípios já consagrados no nosso ordenamento jurídico: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Além disso, deve-se observar a boa-fé que pauta todas as relações jurídicas.

PRINCÍPIOS DA LGPD

- **FINALIDADE:**
  O tratamento dos dados deve ter propósitos legítimos, específicos, explícitos e informados ao titular;

- **ADEQUAÇÃO:**
  O tratamento dos dados deve ser compatível com as finalidades originalmente informadas ao titular;

- **NECESSIDADE:**
  Os dados tratados devem ser pertinentes, proporcionais e não excessivos. O tratamento desses dados deve ser limitado ao mínimo necessário para o cumprimento de suas finalidades;

- **LIVRE ACESSO E TRANSPARÊNCIA:**
  Devem ser garantidos aos respectivos titulares acesso livre e gratuito às informações sobre quais dados pessoais estão sendo tratados, bem como a forma e a duração desse tratamento;

- **QUALIDADE DE DADOS:**
  Os dados devem ser exatos, claros e adequados, de acordo com a finalidade;

- **SEGURANÇA E PREVENÇÃO:**
  Devem ser utilizadas medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e prevenir acidentes passíveis de gerar a destruição, perda, alteração, comunicação ou difusão desses dados pessoais;

- **RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS:**
  A adoção das normas de proteção de dados pessoais deve ser demonstrada e ter sua eficácia comprovada;

- **NÃO DISCRIMINAÇÃO:**
  Não será permitido o tratamento de dados para fins discriminatórios, ilícitos ou abusivos.

OS DIREITOS DOS TITULARES DOS DADOS

Conforme o artigo 18 da LGPD, o titular dos dados tem o direito de:

- Confirmar a existência de tratamento sobre esses dados (Informação);
- Acessar os dados;
- Correção de seus dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou em desconformidade com a lei;
- Portabilidade dos dados a outro fornecedor de serviço ou produto;
- Eliminação dos dados pessoais após o tratamento consentido, salvo nas hipóteses em que a lei permite a manutenção desses dados;
- Informação sobre entidades com as quais os dados foram compartilhados;
- Informação sobre a possibilidade de não fornecer consentimento e consequências;
- Revogação do consentimento.

A lei também traz o direito do titular de peticionar para a Autoridade Nacional contra o controlador dos dados. Quando o tratamento dos dados for baseado exclusivamente em decisões automatizadas, o titular dos dados tem o direito de solicitar a revisão de tal tratamento por pessoa natural.

Esse é o ponto central da LGPD: o estabelecimento de um novo direito aos titulares dos dados pessoais, que além de terem sido ampliados (já existiam nas relações consumeristas, ou em relação ao Estado), garanta seu exercício de forma acessível e eficaz, uma vez que a lei fala em "procedimento gratuito e facilitado".

Vale lembrar que nenhum desses direitos é absoluto e deve ser analisado no seu contexto fático, legal e regulatório.

A exclusão dos dados, por exemplo, deve ocorrer quando há a revogação do consentimento. Quando o tratamento dos dados é realizado com fundamento em outra hipótese (ou base legal) de dispensa de consentimento, o direito de opor-se ao tratamento só é possível quando o controlador descumpre a lei. Exceto no caso do tratamento ser baseado no legítimo interesse do controlador, hipótese em que o direito de oposição pode ser exercido (inclusive ser facilitado).

Ressalte-se que, mesmo no caso em que os agentes de tratamento não tenham como cumprir com a solicitação do titular dos dados como, por exemplo, na não eliminação dos dados para cumprimento de obrigação legal ou regulatória – como é o caso dos cartórios – é necessária a criação de um canal de atendimento aos direitos dos titulares e que as solicitações sejam respondidas, explicando "as razões de fato ou de direito" (§ 4º do artigo 18 da LGPD.) que levam à impossibilidade de atendimento.

REGULAMENTAÇÃO DO ACESSO

No caso dos cartórios, o Provimento CG 23/2020 do Tribunal de Justiça do Estado de São Paulo detalhou algumas questões sobre a forma que deve ser feito o atendimento dos direitos dos titulares: "141. Os titulares terão livre acesso aos dados pessoais, mediante consulta facilitada e gratuita que poderá abranger a exatidão, clareza, relevância, atualização, a forma e duração do tratamento e a integralidade dos dados pessoais".

O Provimento deixa clara a necessidade de atendimento aos direitos dos titulares, em especial **na confirmação do tratamento e no acesso. É importante ressaltar que as informações que devem constar na resposta à consulta** além de não terem o valor legal de uma certidão, **não devem, necessariamente, ter o conteúdo idêntico ou assemelhado, em determinados casos, da certidão.**

Os requisitos sugeridos como boa prática – uma vez que a lei diz que "poderá" e não que "deverá" são:

EXATIDÃO E INTEGRALIDADE – devem conter todos os dados pessoais que estão sob tutela do controlador, da exata maneira que constam dos bancos de dados (online e offline);

CLAREZA – os termos das respostas aos titulares devem ser de fácil compreensão;
RELEVÂNCIA – priorizar os dados de maior importância;

ATUALIZAÇÃO – a resposta ao titular deverá mostrar sempre os dados que estão sob responsabilidade do controlador no momento da consulta;

A FORMA E DURAÇÃO DO TRATAMENTO – deve estar claro como os dados estão sendo tratados (exemplo: simples guarda e armazenamento disponibilizados para consultas de terceiros) e o prazo que eles devem ser excluídos.

"142. O livre acesso é restrito ao titular dos dados pessoais e poderá ***ser promovido mediante*** informação verbal ou escrita, conforme for solicitado".

Nesse item, o Provimento reforça que o acesso deve ser feito somente por requerimento expresso do titular (ou representante legalmente constituído) ao agente de tratamento. **Não será permitido que o direito de acesso seja exercido por terceiros, associações, instituições ou empresas, independentemente da finalidade**.

O provimento também possibilita que o requerimento seja feito de forma verbal pelo titular do direito, devendo aos cartórios estabelecer na sua Política de Atendimento aos Direitos dos Titulares uma forma de registro e um procedimento próprio para essa forma de demanda. Vale ressaltar que a lei prevê que o responsável deverá comunicar de maneira imediata aos agentes de tratamento que tenha compartilhado os dados pessoais, caso haja alguma alteração (correção, eliminação, correção etc.), para que se repita o mesmo procedimento.

Outra questão importante é a forma e o prazo de acesso. A LGPD prevê:

ART. 19. A CONFIRMAÇÃO DE EXISTÊNCIA OU O ACESSO A DADOS PESSOAIS SERÃO PROVIDENCIADOS, MEDIANTE REQUISIÇÃO DO TITULAR:
I - EM FORMATO SIMPLIFICADO, IMEDIATAMENTE; OU

II - POR MEIO DE DECLARAÇÃO CLARA E COMPLETA, QUE INDIQUE A ORIGEM DOS DADOS, A INEXISTÊNCIA DE REGISTRO, OS CRITÉRIOS UTILIZADOS E A FINALIDADE DO TRATAMENTO, OBSERVADOS OS SEGREDOS COMERCIAL E INDUSTRIAL, FORNECIDA NO PRAZO DE ATÉ 15 (QUINZE) DIAS, CONTADO DA DATA DO REQUERIMENTO DO TITULAR.

Como no âmbito da LGPD os cartórios têm o mesmo tratamento dispensado ao poder público (art. 23, §4º) está previsto no § 3º do art. 24, que:

OS PRAZOS E PROCEDIMENTOS PARA EXERCÍCIO DOS DIREITOS DO TITULAR PERANTE O PODER PÚBLICO OBSERVARÃO O DISPOSTO EM LEGISLAÇÃO ESPECÍFICA, EM ESPECIAL AS DISPOSIÇÕES CONSTANTES DA LEI Nº 9.507, DE 12 DE NOVEMBRO DE 1997 (LEI DO HABEAS DATA) , DA LEI Nº 9.784, DE 29 DE JANEIRO DE 1999 (LEI GERAL DO PROCESSO ADMINISTRATIVO) , E DA LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011 (LEI DE ACESSO À INFORMAÇÃO).

Na administração p**úblic**a federal está se adotando o prazo previsto pela Lei de Acesso a Informação, que é "*prazo não superior a 20 (vinte) dias*", e que ainda "*poderá ser prorrogado por mais 10 (dez) dias, mediante justificativa expressa, da qual será cientificado o requerente*" nos termos do artigo 10 da Lei 12.527.

POR TEREM O MESMO TRATAMENTO DISPENSADO AO PODER PÚBLICO (ART. 23, §4º), OS PRAZOS E PROCEDIMENTOS PARA

EXERCÍCIO DOS DIREITOS DO TITULAR PERANTE OS CARTÓRIOS DEVEM OBSERVAR O DISPOSTO NAS REFERIDAS LEIS, ALÉM DO QUE FOR DETERMINADO PELA LEGISLAÇÃO ESPECÍFICA DOS SERVIÇOS NOTARIAIS E DE REGISTRO.

Quanto **à** forma, a LGPD prevê que as informações e os dados poderão ser fornecidos, a critério do titular, por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa.

No Provimento CG n.o 23/2020 ainda está previsto que:

142.1 NA INFORMAÇÃO, QUE PODERÁ SER PRESTADA POR MEIO ELETRÔNICO, SEGURO E IDÔNEO PARA ESSE FIM, OU POR DOCUMENTO IMPRESSO, DEVERÁ CONSTAR A ADVERTÊNCIA DE QUE FOI ENTREGUE AO TITULAR DOS DADOS PESSOAIS, NA FORMA DA LEI N. 13.709, DE 14 DE AGOSTO DE 2018, E QUE NÃO PRODUZ OS EFEITOS DE CERTIDÃO E, PORTANTO, NÃO É DOTADA DE FÉ PÚBLICA PARA PREVALÊNCIA DE DIREITO PERANTE TERCEIROS.(P. 11)

Cumpre destacar a diferença entre as informações prestadas por meio de canais de exercício dos direitos dos titulares e as certidões.

Neste sentido, o Provimento CG n.o 23/2020 esclarece que "143**. As certidões e informações sobre o conteúdo dos atos notariais e de registro, para efeito de publicidade e de vigência, serão fornecidas mediante remuneração por emolumentos, ressalvadas as hipóteses de gratuidade previstas em lei específica**".

Quanto ao direito de retificação, também deixa claro que "146. A **retificação de dado pessoal** constante em registro e em ato notarial **deverá observar o procedimento, extrajudicial ou judicial, previsto na legislação ou em norma específica**".

Em relação aos outros direitos dos titulares, a LGPD também fala do formato dos dados, que deve ser interoperável, nos casos em que a base para o tratamento é o consentimento do titular. O que não se aplica no caso dos cartórios, como expressamente previsto no Provimento CG 21/2020:

147. OS RESPONSÁVEIS PELAS DELEGAÇÕES DOS SERVIÇOS EXTRAJUDICIAIS DE NOTAS E DE REGISTRO NÃO SE EQUIPARAM A FORNECEDORES DE SERVIÇOS OU PRODUTOS PARA EFEITO DE PORTABILIDADE DE DADOS PESSOAIS, MEDIANTE SOLICITAÇÃO POR SEUS TITULARES, PREVISTA NO INCISO V DO ART. 18 DA LEI N. 13.709, DE 14 DE AGOSTO DE 2018. (P.13)

6 UM PROGRAMA MÍNIMO DE ADEQUAÇÃO

6.1 ROTEIRO PARA A CONFORMIDADE COM A LGPD (ROADMAP DO COMPLIANCE)

Existem muitos fatores que devem ser levados em conta para elaboração de um programa de adequação à LGPD e que dependem do tipo de organização, do tamanho, do modelo de negócios, da estrutura organizacional; da maturidade em relação à segurança de informação, por exemplo; do tempo e recursos disponíveis; da avaliação de risco; entre outros.

É importante ter claro que a adequação é um programa de melhoria contínua e permanente. É também criar uma cultura e, a cada novo produto ou serviço, a cada nova mudança na estrutura organizacional, atualizá-lo.

A LGPD é uma lei de caráter procedimental, ou seja, ela determina que uma série de procedimentos que devem ser feitos para que o tratamento de dados seja adequado. Existem diferentes propostas e metodologias para que isso seja feito, mas aqui iremos nos concentrar no programa mínimo que é exigido pelo Provimento 23/2020.

A primeira etapa deve ser de **conscientização e avaliação,** em que são levantados os processos de cada cartório e a equipe é conscientizada sobre o projeto. A conscientização é essencial para que se tenha a colaboração necessária na próxima fase, em que será necessário fazer o mapeamento dos processos e fluxos de dados.

É importante, nessa fase, já ocorrer a designação do encarregado de Proteção de Dados, para que ele possa acompanhar desde o princípio a implementação do programa.

Vale destacar que a nomeação do encarregado, interno ou prestador de serviços externo, é obrigatória pelo provimento:

"133. Cada unidade dos serviços extrajudiciais de notas e de registro deverá manter um encarregado que atuará como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)".

Mais detalhes sobre a figura do encarregado estão no capítulo próprio desta cartilha.

Embora o Provimento 23/2020 destaque somente alguns dos principais pontos do projeto para a conformidade da LGPD , conforme elencamos acima, o artigo 50 da LGPD prevê a formulação de "regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais".

A lei estabelece alguns parâmetros para a implementação de um Programa de Governança em Privacidade e Proteção de Dados Pessoais, que no mínimo devem:

• Demonstrar comprometimento do controlador em adotar processos e políticas inter-

nas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
• Ser aplicável em todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
• Ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
• Estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
• Ter o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
• Estar integrado a sua estrutura geral de governança e estabelecer e aplicar mecanismos de supervisão internos e externos;
• Conter planos de resposta a incidentes e remediação;
• Ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

A legislação determina que as regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela Autoridade Nacional (Art. 50, § 3o, LGPD).

Assim, tendo em vista um Programa de Governança em Privacidade e Proteção de Dados Pessoais nos termos propostos pela LGPD, assim como as exigências do Provimento 23/2020, o Programa de Adequação deverá no mínimo com as seguintes medidas:
• A nomeação de um Encarregado pelo Tratamento de Dados Pessoais, conforme destacado acima;
• Mapeamento do Fluxo dos Dados Pessoais;
• Elaboração e manutenção de um sistema de controle do fluxo de dados pessoais, ou Registro de Operações de Tratamento de Dados Pessoais abrangendo a coleta, tratamento, armazenamento e compartilhamento de dados pessoais, até a restrição de acesso futuro;
• Diagnóstico de *Gap Analysis*, que consiste em um relatório de análise de falhas nos processos, dos riscos e não conformidades;
• Relatório com medidas para mitigar riscos e preencher lacunas, bem como um Plano de Ação que deverá nortear a implementação das medidas.
• A partir do *Gap Analysys* deverá ser construída também, entre outras políticas, a Política de Segurança da Informação, que norteará a revisão técnica de todos os dispositivos e locais de armazenamento de dados para implantação de novos sistemas de segurança que será tratado em capítulo específico;

• A estruturação de politicas e procedimentos internos incluindo:

Política de Privacidade, que nos termos do Provimento 23/2020 "descreva os direitos dos titulares de dados pessoais, de modo claro e acessível, os tratamentos realizados e a sua finalidade". É importante uma Política de Privacidade Interna, corporativa, que englobe todos os setores do cartório incluindo Recursos Humanos, Tecnologia da Informação, Administrativo, Financeiro e a Política de Privacidade Externa, que é em relação ao público externo.

Política e Procedimento de Direitos dos Titulares de Dados

Política de Notificação de Incidente de Segurança da Informação, que será tratada em sessão específica;

Política de Retenção de Dados que deve refletir a Tabela de Temporalidade instituída pelo TJ/SP;

Política de Realização de Relatório de Impacto à Proteção de Dados (DPIA);

Política de Revisão Periódica do Programa de Governança em Privacidade e Proteção de Dados;

• A revisão de contratos e documentos com fornecedores, clientes e colaboradores para inclusão de cláusulas de Proteção de Dados Pessoais e outros documentos como Termo de Confidencialidade, Proteção de Dados e Privacidade;
• Criação de um canal de atendimento adequado para informações, reclamações e sugestões ligadas ao tratamento de dados pessoais, com fornecimento de formulários para essa finalidade
• Criação de indicadores de performance, monitoramento e auditoria do programa de privacidade/proteção de dados;

• Quando for necessário, a Elaboração Relatório de Impacto à Proteção de Dados Pessoais;
• Criação do plano de capacitação e treinamento para a equipe;
• Criação do Plano de Resposta a Incidentes
• Construir relacionamento com a Autoridade Nacional de Proteção de Dados e outras autoridades reguladoras, em especial o órgão corregedor.

6.2 - O PROGRAMA MÍNIMO DO PROVIMENTO CG Nº 23/2020

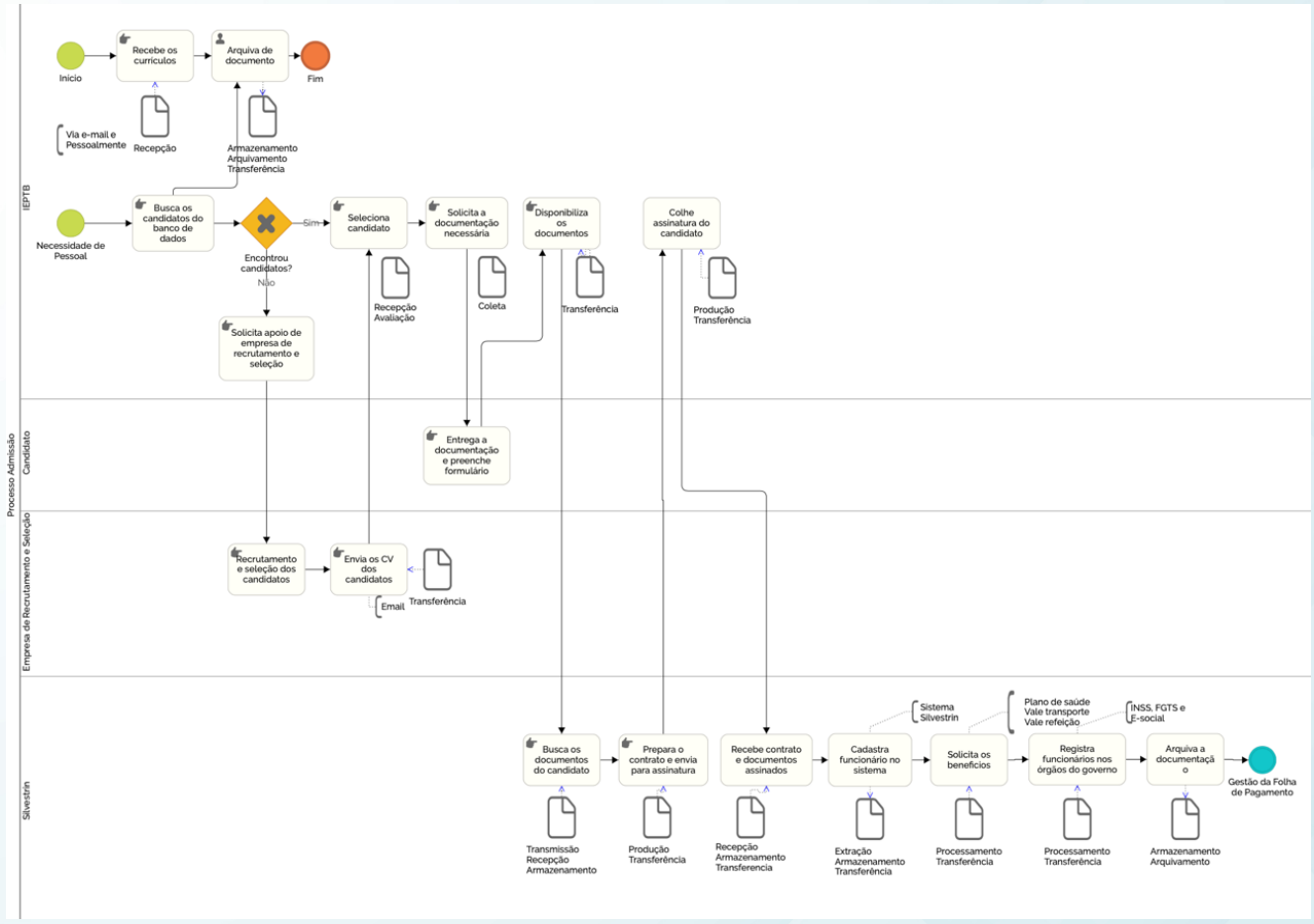
Após uma ideia geral do que é um roteiro para um Programa de Conformidade com a LGPD, vamos priorizar aqui os pontos estabelecidos pela regulamentação da Corregedoria, nos termos do Provimento 23/2020:

133.6 Os responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro manterão em suas unidades:

I – sistema de controle do fluxo abrangendo a coleta, tratamento, armazenamento e compartilhamento de dados pessoais, até a restrição de acesso futuro;
II – política de privacidade que descreva os direitos dos titulares de dados pessoais, de modo claro e acessível, os tratamentos realizados e a sua finalidade;
III – canal de atendimento adequado para informações, reclamações e sugestões ligadas ao tratamento de dados pessoais, com fornecimento de formulários para essa finalidade. (p. 7)

O item 1 refere-se à necessidade da elaboração de um mapeamento dos fluxos de dados pessoais, internos ou externos, de cada serventia. Trata-se do caminho dos dados pessoais nas respectivas atividades de processamento, para dentro e para fora da organização.

Segue um modelo do que é o chamado de **Fluxo de Dados Pessoais:**



Já o Sistema de Controle de Fluxo de Dados Pessoais ou o Registro de Operação de Tratamento de Dados pode ser elaborado por meio de planilhas ou sistema automatizado.

Esse registro deve ter uma linha para cada finalidade do tratamento de dados pessoais. Para cada finalidade deve ser atribuída uma base legal.
De acordo com o Provimento 23/2020:

"O controle de fluxo, abrangendo coleta, tratamento, armazenamento e compartilhamento de dados pessoais, conterá:

I – a identificação das formas de obtenção dos dados pessoais, do tratamento interno e do seu compartilhamento nas hipóteses em que houver determinação legal ou normativa;

II – os registros de tratamentos de dados pessoais contendo, entre outras, informações sobre:
1 – finalidade do tratamento;
2 – base legal ou normativa;
3 – descrição dos titulares;
4 – categoria dos dados que poderão ser pessoais, pessoais sensíveis ou anonimizados, com alerta específica para os dados sensíveis;
5 – categorias dos destinatários;
6 – prazo de conservação;
7- identificação dos sistemas de manutenção de bancos de dados e do seu conteúdo;
8 – medidas de segurança adotadas;
9 – obtenção e arquivamento das autorizações emitidas pelos titulares para o tratamento dos dados pessoais, nas hipóteses em que forem exigíveis;
10 – política de segurança da informação;
11 – planos de respostas a incidentes de segurança com dados pessoais.

A seguir, um exemplo de conteúdo do Registro de Operações de Tratamento de Dados Pessoais:

MODELO DE REGISTRO OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS

Área	Processo	Responsável	Agente de tratamento	Titular	Finalidade
RH	Seleção	Gerente de RH	Controlador	Candidatos a emprego,	Candidatos a emprego: Realizar processo seleção
Base legal	**Coleta**	**Dados coletados**	**Aplicativos envolvidos**	**Acesso**	**Armazenamento**
Consentimento	Os dados são coletados por um formulário preenchido pelo candidato que foi enviado pela empresa de recrutamento	Dado pessoal: Nome completo, data de nascimento, número de documento de identidade, endereço completo, nacionalidade, dados de formação e de empregos anteriores.	Sistema da empresa de recrutamento	Limitado ao Gerente de RH e ao funcionário de apoio XYZ	Rede interna E-mail Sistema empresa de recrutamento
Periodo de retenção	**Processamento**	**Atualiação dos dados**	**Transferência**	**Nac Int.**	**Finalidade**
Currículos serão armazenados por um ano.	Realizar processo de seleção Entrevista	Sim	Empresa de Recrutamento	NAC	Seleção de cadidato à vaga de emprego

MEDIDAS ADOTADAS

1 - Elaborado termo de privacidade para os processos do RH;
2 - Os termos contratuais com os fornecedores envolvidos foram revisados para que garantam o atendimento a LGPD;
3 - Destruição dos corrículos impressos anualmente;
4 - Restrição o acesso aos sistemas somente aos profissionais envolvidos no processo;
5 - Minimização os dados coletados;
6 - Centralização do banco de dados de Currículos no Sistema e eleiminando e-mails ou arquivos duplicados;
7 - Implantados processos e controles para garantir a segurança da informação.

O item 9, "obtenção e arquivamento das autorizações emitidas pelos titulares para o tratamento dos dados pessoais, nas hipóteses em que forem exigíveis", se refere **à** existência de um sistema de gestão de consentimento, ou seja, nos casos em que a base legal é o consentimento do titular, é necessário que a forma de obtenção seja documentada (impressa ou online) e arquivada.

Já os itens 10 (Política de Segurança da Informação) e 11 (planos de respostas a incidentes de segurança com dados pessoais), tratam de políticas gerais, que deverão ser criadas e serão tratadas em capítulos específicos.

Além disso, o Provimento pede uma "política de privacidade que descreva os direitos dos titulares de dados pessoais, de modo claro e

acessível, os tratamentos realizados e a sua finalidade"

A Política de Privacidade deve ser disponibilizada "de forma clara, adequada e ostensiva", de acordo com o art. 9º. da LGPD, e deve conter os seguintes elementos:

I - finalidade específica do tratamento;
II - forma e duração do tratamento, observados os segredos comercial e industrial;
III - identificação do controlador;
IV - informações de contato do controlador;
V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
VI - responsabilidades dos agentes que realizarão o tratamento; e
VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

Deverá, ainda, salientar que o tratamento de dados pessoais é condição para o fornecimento de produto ou de serviço ou para o exercício de direito, com destaque.

A POLÍTICA DE PRIVACIDADE, EM SEU CONTEÚDO MÍNIMO, DEVERÁ RESPONDER ÀS SEGUINTES PERGUNTAS:

QUEM TRATA OS DADOS PESSOAIS?
(Identificação do controlador e informaçõ**õ**es de contato do controlador e com quem os dados são compartilhados)

QUEM É RESPONSÁVEL PELO QUE?
(responsabilidades dos agentes que realizarão o tratamento)

QUAIS SÃO OS DADOS E PARA QUE?
(finalidade específica do tratamento e do compartilhamento)

COMO OS DADOS SÃO TRATADOS E ATÉ QUANDO?
(forma e duração do tratamento)

QUAIS OS DIREITOS DOS TITULARES DOS DADOS?
(direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD e como eles podem ser exercidos)

Importante lembrar que o art. 41 também prevê que é necessário constar a IDENTIDADE e as INFORMAÇÕES DE CONTATO do encarregado de Proteção de Dados.

Ainda é necessária a criação de um "canal de atendimento adequado para informações, reclamações e sugestões ligadas ao tratamento de dados pessoais, com fornecimento de formulários para essa finalidade".

Assim, é exigido que, tanto na página na internet, como nas próprias serventias, seja disponibilizado ao público um canal de atendimento, em que o titular possa fazer sua solicitação em um formulário próprio.

O Provimento 23/2020 também prevê que:

134. A política de privacidade e o canal de atendimento aos usuários dos serviços extrajudiciais deverão ser divulgados por meio de cartazes afixados nas unidades e avisos nos sítios eletrônicos mantidos pelas delegações de notas e de registro, de forma clara e que permita a fácil visualização e o acesso intuitivo.

134.1 A critério dos responsáveis pelas delegações, a política de privacidade e a identificação do canal de atendimento também poderão ser divulgados nos recibos entregues para as partes solicitantes dos atos notariais e de registro. (p. 7)

Apesar de o provimento prever que as políticas e a identificação do canal do atendimento podem ser divulgadas nos recibos, a critério dos responsáveis das delegações, trata-se de um programa novo a

ser implementado, que poderá precisar de ajustes ao longo desse período. Portanto, é aconselhável entregar um link do site ou QR Code para esse fim de divulgação, para que o usuário tenha acesso às políticas sempre atualizadas, sem ficar com um documento que poderá sofrer alterações.

FORMULÁRIO
DE SOLICITAÇÃO DE INFORMAÇÕES DE DADOS PESSOAIS

Prezado(a) Sr(a).

De acordo com a Lei No 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) e o Provimento CGJ nº 23/2020 (Dispõe sobre o tratamento e proteção de dados pessoais pelos responsáveis pelas delegações dos serviços extrajudiciais de notas e de registro), SOLICITO a V.S.a. exercer meu direito como TITULAR DOS DADOS para a seguinte situação:

( ) Confirmação de existência de tratamento;
( ) Acesso aos dados;
( ) Correção ou atualização dos dados;
( ) Anonimização, bloqueio ou eliminação de dados tratados em desconformidade com a lei;
( ) Informações das entidades públicas e privadas com as quais os dados foram compartilhados;
( ) Vedação de compartilhamento de dados;
( ) Exclusão de dados pessoais tratados com o consentimento;
( ) Revogação do consentimento;
( ) Oposição de tratamento de dados tratados com o Legítimo Interesse nos termos da Política de Privacidade;
( ) Outros _____

DADOS DO TITULAR SOLICITANTE

Nome completo:	
RG:	CPF:
E-mail:	Celular:

Dados necessário para localização perfeita do titular

Declaro sob as penas da lei, que são verdadeiras as informações prestadas neste formulário.

_____
Assinatura do titular

7 O PLANO DE RESPOSTA A INCIDENTES

Qualquer resposta a um incidente deve ser decisiva e executada rapidamente. Assim, o plano deve ser objetivo e claro, orientar todas as etapas necessárias, indicar responsáveis e recursos.

O PLANO DEVE CONTER:

AÇÃO IMEDIATA PARA INTERROMPER OU MINIMIZAR O INCIDENTE: sempre deve, primeiramente, mostrar como a equipe pode identificar um incidente e como deve agir de forma imediata. E, ao mesmo tempo, como acionar o comitê de crise;

NOMEAÇÃO DE UM COMITÊ DE CRISE: é necessária a nomeação prévia da equipe que atuará diante de um incidente e o papel de cada um. Deve fazer parte da equipe o encarregado de Proteção de Dados, além do setor de Tecnologia da Informação. Dependendo da extensão do incidente, envolver apoio jurídico e de comunicação. Caso não haja equipe ou prestadores de serviços já contratados, é importante ter uma seleção prévia de quais prestadores de serviços poderão ser contratos.

ESTRUTURAÇÃO PRÉVIA DA EQUIPE PARA AS RESPOSTAS NECESSÁRIAS: muitas vezes, a notícia de um incidente vem de uma ligação da imprensa pedindo uma declaração. Pode haver questionamentos de clientes ou até da própria corregedoria. É necessário dar respostas aos titulares dos dados, se for o caso. É importante a definição de quem irá elaborar a comunicação (o ideal é que, além da equipe técnica, o jurídico e a comunicação estejam envolvidos), assim como essas respostas serão validadas.

COMUNICAÇÃO ÀS AUTORIDADES COMPETENTES: De acordo com a LGPD, a ANPD deverá ser comunicada em caso de incidente relevante de dados pessoais. De acordo com a lei, a comunicação deve apresentar, no mínimo:

"I - a descrição da natureza dos dados pessoais afetados;
II - as informações sobre os titulares envolvidos;
III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
IV -os riscos relacionados ao incidente;
V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo".

E mesmo enquanto ela ainda não estiver em funcionamento, o Provimento CG 23/2020 criou também a **obrigação de comunicação ao juiz corregedor permanente e à corregedoria geral da Justiça, no prazo máximo de 24 horas, com esclarecimento da natureza do incidente e das medidas adotadas para a apuração das suas causas e a mitigação de novos riscos e dos impactos causados aos titulares dos dados.**

Se o incidente envolver a prática de algum crime, como nos casos de ransomware (sequestro da base de dados e a exigência de valor em contrapartida para liberação) deve-se apresentar pedido de instauração de inquérito policial, para que a apuração se dê no âmbito da Polícia Judiciária.

INVESTIGAÇÃO DO INCIDENTE: incluindo a identificação, coleta e preservação das provas e evidências. É importante buscar descobrir o que deu causa ao incidente, como por exemplo, a identificação do usuário responsável pelo vazamento de dados pessoais. É sempre bom lembrar que as sanções ou eventuais valorações de dano são minimizadas nos casos das organizações agirem com transparência e rapidez, comunicar as autoridades e aos titulares quando for o caso, além de buscarem a responsabilização daqueles que deram causa.

O plano deve prever, ainda, recursos físicos, como armazenamento redundante, sistemas de *standby* e serviços de *backup* e restauração dos recursos afetados para não comprometer, além dos dados pessoais, a integridade e a disponibilidade dos dados de modo geral, que estarão previstos na Política de Segurança da Informação

E por fim, a elaboração de relatório final do incidente e revisão dos procedimentos para evitar novos incidentes.

SEGURANÇA DE INFORMAÇÃO

São cada vez mais constantes os episódios de vazamentos de dados e ameaças cibernéticas. Nesse sentido, ganham relevância as estratégias de segurança de informação. São muitas as dimensões de um programa de adequação à LGPD e todas devem ser avaliadas conforme as características da organização. Entretanto, como mínimo, é importante destacar:

1. Investimento em ferramentas e arquitetura de sistemas de TI (o Provimento nº 74 apresenta os requisitos para cada cartório a partir de critérios previamente estabelecidos);
2. Compreensão da importância da segurança da informação para os programas de adequação a Lei Geral de Proteção de Dados (LGPD);
3. Auditoria de vulnerabilidade dos sistemas atuais;
4. Mapeamento dos processos e entendimento do escopo organizacional do cartório;
5. Conscientização e treinamento com noções de segurança da informação e proteção de dados;
6. Plano de incidentes de segurança de informação;
7. Mapeamento do ciclo de vida dos dados pessoais;
8. Plano de contingência e responsabilidades.

SEGURANÇA DA INFORMAÇÃO NO PROGRAMA DE CONFORMIDADE PARA A LEI GERAL DE PROTEÇÃO DE DADOS

É fundamental estar em conformidade com a LGPD. Sob a ótica da Segurança de Informação, o caminho correto é começar pela organização dos processos. Em síntese:

1º PASSO: CLASSIFICAR AS INFORMAÇÕES
Para a implementação de uma Política de Segurança da Informação eficaz, é necessário, preliminarmente, definir claramente o valor atribuído a cada informação.

Somente a partir da classificação das informações que circulam em um determinado tratamento de dados é possível compreender quais são as medidas necessárias para garantir a confidencialidade, integridade e disponibilidade desses dados.

A análise do valor de uma informação tem como fundamento principal o mapeamento de quais são as principais ameaças à proteção daquela informação e qual é a gravidade das consequências, em caso de eventual vazamento ou perda desses dados.

2º PASSO: ESTABELECER E IMPLEMENTAR AS POLÍTICAS DE SEGURANÇA
Uma vez estabelecida a ordem de classificação das informações, o próximo passo é implementar as ações necessárias para garantir a segurança dessas informações:

- Adoção de medidas de segurança apropriadas ao acesso de dados de acordo com a sua classificação, como a utilização de senhas, confirmação por duplo fator, adoção de tokens, entre outros;
- Análise interna do banco de dados, a fim de verificar os processos de tratamento e os riscos envolvidos;

- Adoção de medidas tecnológicas internas que garantam a segurança das informações, tais como a eliminação de dados desnecessários, anonimização e pseudoanonimização de dados, criptografia, etc.;
- Elaboração de uma Política de Segurança da Informação, com orientações objetivas de métodos e processos para o tratamento de dados e medidas de segurança apropriadas;
- Realização de treinamentos e divulgação de materiais de conscientização para funcionários e clientes.

ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

Os cartórios devem determinar o seu papel de controladores ou operadores, bem como fatores internos e externos que sejam pertinentes para o seu contexto. É possível que, em dado momento, ambos os papéis sejam exercidos. Nesse caso cada qual estará sujeito a um conjunto separado de controles.

É importante que os cartórios indiquem uma ou mais pessoas responsáveis pelo desenvolvimento, implementação, manutenção e monitoramento de um programa amplo de privacidade e governança para assegurar *compliance* com todas as leis e regulamentações aplicáveis relacionadas ao tratamento de dados pessoais. Essas informações organizacionais devem ser registradas em um fluxograma de trabalho.

SEGURANÇA EM RECURSOS HUMANOS

É importante que sejam realizadas atividades de conscientização sobre notificação de incidentes, para que todos estejam cientes das consequências legais, reputacionais e disciplinares da violação das regras de segurança e procedimentos relacionados ao tratamento de dados. Esses processos devem ser considerados nos momentos de:
Seleção;
Termos e condições de contratação;
Encerramento de contrato.

GESTÃO DE ATIVOS

PROPRIEDADE:
Todos os ativos tangíveis e intangíveis, em especial as informações criadas, acessadas, compartilhadas, manuseadas, armazenadas ou disponibilizadas ao usuário ou de quem tiver acesso no exercício de suas atividades devem ser de propriedade e/ou de direito de uso e/ou exploração patrimonial exclusivos dos cartórios, e somente ele pode determinar seu destino e finalidade.

USO CORPORATIVO DOS ATIVOS:
Todos os ativos, tangíveis e intangíveis, devem ser utilizados apenas para o cumprimento das atividades profissionais, limitados à alçada e função do usuário, dentro do padrão de conduta ética e moral estabelecida pela empresa, sempre atendendo à obrigação de sigilo profissional.

CLASSIFICAÇÃO DA INFORMAÇÃO

É importante que todas as informações sejam classificadas e rotuladas de forma a permitir fácil identificação e o tratamento adequado, no momento em que for obtida ou gerada, em um dos seguintes níveis:

INFORMAÇÃO PÚBLICA:
informação que pode ou deve ser tornada disponível para distribuição pública por meio dos canais institucionais. Sua divulgação não causa qualquer dano ao cartório ou aos seus usuários;

INFORMAÇÃO INTERNA:
informação que pode ser divulgada para todos os usuários, enquanto estiverem desempenhando atividades e desde que estejam comprometidos com a confidencialidade das informações. Sua divulgação não autorizada ou acesso indevido podem causar impactos operacionais;

INFORMAÇÃO CONFIDENCIAL:
informação que requer tratamento especial, contendo conteúdo estratégico, dados pessoais e privados que, se divulgada, poderia violar a privacidade de indivíduos ou causar impactos graves, sob o aspecto financeiro, legal, normativo, de reputação e de imagem.

Atenção: O usuário deve respeitar o nível de segurança requerido pela classificação indicada na informação que vier a tomar contato ou manusear e, em caso de dúvida, deverá tratá-la como de uso interno, não passível de divulgação.

TRATAMENTO DE MÍDIAS

GERENCIAMENTO DE MÍDIAS REMOVÍVEIS: é importante que o uso de mídia removível seja documentado quando do uso para armazenamento de dados pessoais. É indicado o uso de criptografia. Caso não seja possível, é indicado o uso de complementos para tratar os riscos aos dados pessoais.

DESCARTE DE MÍDIAS: é importante que sejam incluídos procedimentos de descarte seguro para que os dados pessoais armazenados não sejam mais acessíveis. Alternativas como a sanitização são adequadas.

TRANSFERÊNCIA FÍSICA DE MÍDIAS: é importante que sejam registradas as entradas e saídas, incluindo o tipo de mídia física, o receptor autorizado, bem como data, horário e o número.

Atenção: um procedimento de autorização antes de deixar as instalações físicas dos cartórios é indicado. É indicado o uso de criptografia.

CONTROLE DE ACESSO

É importante que sejam executados procedimentos para registro e cancelamento de usuários que administram ou operam sistemas e serviços que tratam dados pessoais.

- Não reemitir qualquer *login* expirado ou desativado;
- Conferência rotineira da segurança das senhas;
- Manutenção de registro preciso e atualizado dos perfis dos usuários.

O perfil compreende um conjunto de dados sobre aquele usuário, incluindo o ID de usuário necessário para implementar os controles técnicos identificados que fornecem acesso autorizado.

Essa medida é essencial para manutenção de uma trilha que proteja tanto os cartórios quanto os colaboradores.

Vale destacar que, para o acesso físico e lógico aos ambientes, devem ser fornecidos aos colaboradores e usuários uma identidade digital de uso individual e intransferível, podendo abranger crachá, *login*, senha, *token*, certificado digital e outros recursos que venham a ser implantados.

Além disso, o colaborador é responsável pelo uso e o sigilo de sua identidade digital, não sendo permitido fazer o seu uso não autorizado, compartilhar, divulgar ou transferir a terceiros.

REGISTROS E MONITORAMENTO

É importante que seja implementado um processo para analisar criticamente os registros de eventos (*logs*) usando processos contínuos de alerta e monitoramento automatizados, ou mesmo manuais. Isso deve ser feito de forma periódica. Além disso, em locais com múltiplos provedores de serviços envolvidos é importante que os papéis estejam claramente definidos e documentados.

Os processos de armazenamento devem conter:

- Quem
- Quando
- Quais dados pessoais foram acessados
- Quais mudanças foram feitas (adições, modificações ou exclusões)

PRIVACY BY DESIGN E PRIVACY BY DEFAULT

om o *privacy by design*, a privacidade é incorporada à própria arquitetura dos sistemas e processos desenvolvidos. Com o *privacy by default*, as configurações padrão são sempre para garantia da maior privacidade para o titular de dados. Nesse sentido, é importante que os sistemas e/ou componentes relativos ao tratamento de dados pessoais sejam projetados seguindo os princípios de *privacy by design* e *privacy by default*.

As políticas que contribuem para *privacy by design* e *privacy by default* devem considerar:
a) diretrizes sobre proteção de dados pessoais e implementação de princípios de privacidade no ciclo de vida de desenvolvimento do software;
b) requisitos de proteção e privacidade de dados pessoais na etapa de design do software;
c) por regra, minimização do tratamento de dados pessoais.

Atenção: é importante que os dados pessoais não sejam usados para testes. É indicado que sejam usados dados pessoais falsos. Em casos que o uso de dados pessoais para propósitos de teste não puder ser evitado, convém que sejam implementadas medidas técnicas e organizacionais para minimizar os riscos.

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 (LGPD, art. 46, §2o).

IDENTIFICANDO SEGURANÇA DA INFORMAÇÃO NOS ACORDOS COM FORNECEDORES

É importante que sejam especificados nos acordos e contratos com fornecedores se dados pessoais são tratados e as medidas mínimas técnicas e organizacionais que o fornecedor precisa atender para que sejam cumpridas suas obrigações de proteção de dados pessoais e de segurança da informação.

GESTÃO DE INCIDENTE DE SEGURANÇA

O QUE É?

- Para a Lei Geral de Proteção de Dados, podem ser considerados um incidente de segurança:
- Qualquer acesso não autorizado a dados que contenham informações pessoais que possam identificar o indivíduo;
- Vazamento de informações de um único registro ou base de dados contendo informações pessoais;
- Perda das informações pessoais.

O QUE FAZER CASO OCORRA UM INCIDENTE DE SEGURANÇA?

É recomendável que, toda instituição que trabalhe com tratamento de dados possua uma política clara sobre o que fazer na hipótese da ocorrência de um incidente de segurança.

A LGPD determina expressamente que os incidentes de segurança que importarem em "acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" deverão ser notificados à Autoridade Nacional e ao titular dos dados. A responsabilidade por essa notificação é do controlador e o ideal é que a seja feita, em prazo razoável, tanto para a Autoridade Nacional como para os respectivos titulares dos dados.

A depender da gravidade do incidente, a Autoridade Nacional pode determinar a adoção de outras providências, tais como: i) ampla divulgação do fato em meios de comunicação e ii) medidas para reverter ou mitigar os efeitos do incidente.

Como parte do processo de gestão de incidentes de segurança da informação, é importante que sejam estabelecidas responsabilidades e procedimentos para identificação e registro de violações de proteção de dados. Além disso, vale estabelecer responsabilidades e procedimentos relativos à notificação para as partes envolvidas nas violações de dados pessoais (incluindo o tempo de tais notificações) e à divulgação para as autoridades.

Os casos de incidentes de segurança que possam acarretar risco ou dano relevantes aos titulares de dados, deverão ser comunicados:

(i) autoridade nacional;
(ii) titular dos dados, em prazo razoável (a ser definido pela autoridade);
(iii) órgãos reguladores setoriais.

RESPOSTA AOS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

- O primeiro passo é identificar a natureza dos dados que foram objeto do incidente. As comunicações devem conter detalhes como:
- uma descrição do incidente;
- os riscos relacionados ao incidente;
- os titulares envolvidos;
- período de tempo;
- consequências do incidente;
- nome do relator;
- para quem o incidente foi reportado;
- o fato de que um incidente resultou em indisponibilidade, perda, divulgação ou alteração de dados pessoais;
- um ponto de contato para que mais informações podem ser obtidas;

- uma descrição da violação e a probabilidade das consequências;
- uma descrição da violação, incluindo o número de indivíduos envolvidos, bem como o número de registros relacionados;
- medidas tomadas ou planejadas para serem tomadas.

O QUE FAZER PARA EVITAR UM INCIDENTE DE SEGURANÇA?

Para evitar com eficiência e manter o controle de incidentes de segurança, recomenda-se a implementação de mecanismos internos de controle e auditoria.

Importante ressaltar que controlador e operador respondem solidariamente pelos danos decorrentes da violação da segurança a partir de falhas identificadas na adoção das medidas de segurança previamente estipuladas. Logo, a escolha dos terceiros que farão o tratamento de dados para o controlador deve ser criteriosa.

Partindo da premissa de que boa parte dos incidentes são causados por falha humana, o aconselhável é que esses mecanismos sejam compilados em uma política interna de segurança, que deve ser disponibilizada para todos os colaboradores que atuam direta e indiretamente com o tratamento de dados. Incentiva-se, ainda, a realização periódica de treinamentos e atualizações dessa política.

Uma boa política de segurança norteia-se pelas seguintes diretrizes:

- Implementação de um processo contínuo de revisão dos relatórios de impacto de proteção de dados;[1]
- Monitoramento contínuo do ambiente no qual os dados pessoais são tratados, visando identificar e alertar previamente um possível incidente;
- Disponibilização de um canal externo para comunicação de um possível incidente;
- Monitoramento dos canais internos e externos de divulgação de incidentes de segurança.

ANÁLISE CRÍTICA DA CONFORMIDADE TÉCNICA

É importante que sejam incluídos no processo organizacional testes específicos de vulnerabilidade ou invasão.

A SEGURANÇA DA INFORMAÇÃO NO SETOR DOS CARTÓRIOS

De acordo com o Provimento nº 74/2018 do Conselho Nacional de Justiça, os cartórios devem adotar políticas de segurança de informação com relação à:

- confidencialidade
- disponibilidade
- autenticidade
- integridade
- mecanismos preventivos de controle físico e lógico da informação

Os cartórios deverão, portanto, instituir uma política de segurança da informação, exercendo as seguintes atividades, minimamente:

- ter um plano de continuidade de negócios que preveja ocorrências nocivas ao regular funcionamento dos serviços;
- atender às normas de interoperabilidade, legibilidade e recuperação, a longo prazo, na prática dos atos e comunicações eletrônicas.
- sobre os livros e atos eletrônicos praticados pelos cartórios, a norma prevê que eles sejam arquivados de forma a garantir a segurança e a integridade do seu conteúdo, devendo ser adotadas as seguintes medidas:
- Os livros e atos eletrônicos que integram o acervo dos cartórios deverão ser arquivados mediante cópia de segurança (*backup* feito tanto em mídia eletrônica de segurança quanto em serviço de cópia de segurança na internet - *backup* em nuvem), feita em intervalos não superiores a 24 horas;
- A mídia eletrônica de segurança deverá ser armazenada em local diverso de onde o cartório está instalado, observada a segurança física e lógica necessárias;
- Ao longo dessas 24 horas, deverão ser geradas imagens ou cópias incrementais dos dados que permitam a recuperação dos atos praticados a partir das últimas cópias de segurança até, pelo menos, 30 minutos antes da ocorrência do evento que possa comprometer a base de dados e informações associadas;
- Garantir que os meios de armazenamento utilizados para todos os dados e componentes de informação relativos aos livros e atos eletrônicos tenham recursos de tolerância a falhas;
- O titular delegatário ou o interino/interventor, os escreventes, os prepostos e os colaboradores dos cartórios devem possuir formas de autenticação por certificação digital própria ou por biometria, além de usuário e senha associados aos perfis pessoais com permissões distintas, de acordo com a função, não sendo permitida a utilização de "usuários genéricos".

O sistema informatizado dos cartórios deverá ter as seguintes características:

- trilha de auditoria própria que permita a identificação do responsável pela confecção ou por eventual modificação dos atos, bem como da data e hora de efetivação;
- a plataforma de banco de dados deverá possuir recurso de trilha de auditoria ativada;
- as trilhas de auditoria do sistema e do banco de dados deverão ser preservadas em *backup*, visando a eventuais auditorias;

Os cartórios deverão observar os seguintes padrões mínimos, de acordo com a classe em que se encaixar:

CLASSE 1

Cartórios com arrecadação de até R$ 100 mil por semestre, equivalente a 30,1% dos cartórios

PRÉ-REQUISITOS

- Energia estável, rede elétrica devidamente aterrada e link de comunicação de dados mínimo de 2 megabits
- Endereço eletrônico (e-mail) da unidade para correspondência e acesso ao sistema Malote Digital
- Local técnico (CPD) isolado dos demais ambientes, preferencialmente por estrutura física de alvenaria ou, na sua impossibilidade, por divisórias. Em ambos os casos, com possibilidade de controle de acesso (porta com chave) restrito aos funcionários da área técnica
- Local técnico com refrigeração compatível com a quantidade de equipamentos e metragem
- Unidade de alimentação ininterrupta (no-break) compatível com os servidores instalados, com autonomia de pelo menos 30 minutos
- Dispositivo de armazenamento (storage), físico ou virtual
- Serviço de cópias de segurança na internet (backup em nuvem)
- Servidor com sistema de alta disponibilidade que permita a retomada do atendimento à população em até 15 minutos após eventual pane do servidor principal
- Impressoras e scanners (multifuncionais);
- Switch para a conexão de equipamentos internos
- Roteador para controlar conexões internas e externas
- Softwares licenciados para uso comercial (é permitido o uso de softwares de código aberto e os de livre distribuição)
- Software antivírus e antissequestro
- Firewall
- Proxy
- Banco de dados
- Mão de obra: pelo menos 2 funcionários do cartório treinados na operação do sistema e das cópias de segurança ou empresa contratada que preste o serviço de manutenção técnica com suporte de pelo menos 2 pessoas

CLASSE 2

Cartórios com arrecadação entre R$ 100 mil e R$ 500 mil por semestre, equivalente a 26,5% dos cartórios

PRÉ-REQUISITOS

- Energia estável, rede elétrica devidamente aterrada e link de comunicação de dados mínimo de 4 megabits
- Endereço eletrônico (e-mail) da unidade para correspondência e acesso ao sistema Malote Digital
- Local técnico (CPD) isolado dos demais ambientes, preferencialmente por estrutura física de alvenaria ou, na sua impossibilidade, por divisórias. Em ambos os casos, com possibilidade de controle de acesso (porta com chave) restrito aos funcionários da área técnica
- Local técnico com refrigeração compatível com a quantidade de equipamentos e metragem
- Unidade de alimentação ininterrupta (no-break) compatível com os servidores instalados, com autonomia de pelo menos 30 minutos
- Dispositivo de armazenamento (storage), físico ou virtual
- Serviço de cópias de segurança na internet (backup em nuvem)
- Servidor com sistema de alta disponibilidade que permita a retomada do atendimento à população em até 15 minutos após eventual pane do servidor principal
- Impressoras e scanners (multifuncionais)
- Switch para a conexão de equipamentos internos
- Roteador para controlar conexões internas e externas
- Softwares licenciados para uso comercial (é permitido o uso de softwares de código aberto e os de livre distribuição)
- Software antivírus e antissequestro
- Firewall
- Proxy
- Banco de dados
- Mão de obra: pelo menos 2 funcionários do cartório treinados na operação do sistema e das cópias de segurança ou empresa contratada que preste o serviço de manutenção técnica com suporte de pelo menos 2 pessoas

CLASSE 3

Cartórios com arrecadação acima de R$ 500 mil por semestre, equivalente a 21,5% dos cartórios

PRÉ-REQUISITOS

- Energia estável, rede elétrica devidamente aterrada e link de comunicação de dados mínimo de 10 megabits
- Endereço eletrônico (e-mail) da unidade para correspondência e acesso ao sistema Malote Digital
- Local técnico (CPD) isolado dos demais ambientes, preferencialmente por estrutura física de alvenaria ou, na sua impossibilidade, por divisórias. Em ambos os casos, com possibilidade de controle de acesso (porta com chave) restrito aos funcionários da área técnica
- Local técnico com refrigeração compatível com a quantidade de equipamentos e metragem
- Unidade de alimentação ininterrupta (no-break) compatível com os servidores instalados, com autonomia de pelo menos 30 minutos
- Dispositivo de armazenamento (storage), físico ou virtual
- Serviço de cópias de segurança na internet (backup em nuvem)
- Servidor com sistema de alta disponibilidade que permita a retomada do atendimento à população em até 15 minutos após eventual pane do servidor principal
- Impressoras e scanners (multifuncionais)
- Switch para a conexão de equipamentos internos
- Roteador para controlar conexões internas e externas
- Softwares licenciados para uso comercial (é permitido o uso de softwares de código aberto e os de livre distribuição)
- Software antivírus e antissequestro
- Firewall
- Proxy
- Banco de dados
- Mão de obra: pelo menos 3 funcionários do cartório treinados na operação do sistema e das cópias de segurança ou empresa contratada que preste o serviço de manutenção técnica com suporte de pelo menos 3 pessoas

[1] Relatório de impacto à proteção de dados pessoais é a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

[2] O Cogetise é formado pelas seguintes entidades: Corregedoria Nacional de Justiça, na condição de presidente; Corregedorias de Justiça dos Estados e do Distrito Federal; Associação dos Notários e Registradores do Brasil (Anoreg/BR); Colégio Notarial do Brasil – Conselho Federal (CNB/CF); a Associação Nacional dos Registradores de Pessoas Naturais do Brasil (Arpen/BR); o Instituto de Registro Imobiliário do Brasil (Irib/BR); o Instituto de Estudos de Protesto de Títulos do Brasil (IEPTB/BR); e o Instituto de Registro de Títulos e Documentos e de Pessoas Jurídicas do Brasil (IRTDPJ/BR).

O Comitê de Gestão da Tecnologia da Informação dos Serviços Extrajudiciais (Cogetise) é o responsável pela atualização anual desses pré-requisitos mínimos, além de ser responsável por divulgar, estimular, apoiar e detalhar a implementação das diretrizes do Provimento nº 74/2018 e pela fixação de prazos para adequação dos cartórios às obrigações ali previstas.[2]

Os cartórios deverão adotar rotina que possibilite a transmissão de todo o acervo eletrônico pertencente à serventia, inclusive banco de dados, *softwares* e atualizações que permitam o pleno uso, além de senhas e dados necessários ao acesso a tais programas, garantindo a continuidade da prestação do serviço de forma adequada e eficiente, sem interrupção, em caso de eventual sucessão.

É importante ressaltar que o descumprimento dessas medidas de segurança da informação, previstas no Provimento nº 74/2018, ensejará a instauração de procedimento administrativo disciplinar, sem prejuízo de responsabilização cível e criminal e das sanções previstas na LGPD.

IMPORTANTE

COMO POSSO UTILIZAR AS INFORMAÇÕES E OS RECURSOS TECNOLÓGICOS DISPONÍVEIS NO AMBIENTE DE TRABALHO?

Somente para execução das atividades profissionais e de acordo com suas atividades.

COMO DEVO PROTEGER AS INFORMAÇÕES DO AMBIENTE DE TRABALHO?

- Bloqueie a sua estação de trabalho sempre que se ausentar, a fim de evitar acessos não autorizados e o vazamento de informações;
- Mantenha seu local de trabalho organizado, e não corra o risco de deixar informações expostas em salas de reuniões, áreas comuns, lixeiras, mesas e impressoras;
- Classifique todas as informações que você criar quanto ao seu nível de sigilo e de criticidade. Na dúvida, trate a informação como interna e verifique com seu gestor qual a classificação adequada antes de compartilhá-la com terceiros;

- Salve todas as informações relacionadas às suas atividades de trabalho na rede do cartório para que fiquem seguras e disponíveis para quem precisar delas.
- Não abra e-mails suspeitos ou desconhecidos, jamais clique em links suspeitos. Chame sempre o responsável de TI em caso de dúvidas para que ele analise os e-mails.
- Computadores de trabalho não são para uso pessoal e pesquisas particulares. Evite visitas a sites fora do contexto do seu trabalho.

POSSO SALVAR AS INFORMAÇÕES DO TRABALHO NO MEU DISPOSITIVO PARTICULAR, COMO *PENDRIVE, TABLET, NOTEBOOK, SMARTPHONE*?

Somente com autorização prévia e com o uso de mecanismos de segurança apropriados, como bloqueio por senha e *softwares* de proteção (ex. antivírus e *firewall*) e de apagamento remoto.

DE QUE FORMA POSSO ME PROTEGER CONTRA A ENGENHARIA SOCIAL?

Seja discreto e cuidadoso ao tratar com terceiros, verifique sempre a identidade do interlocutor ou destinatário antes de compartilhar a informação. As práticas de engenharia social utilizam as fragilidades humanas, como ingenuidade e distração, para obter acesso às informações confidenciais. Sigilo profissional é sério e deve ser respeitado.

QUAL É A LINGUAGEM MAIS ADEQUADA AO AMBIENTE DE TRABALHO?

Ao enviar mensagens ou conversar com seus colegas ou clientes, evite o uso de termos de dupla interpretação, apelidos e diminutivos ou que possam denotar excesso de intimidade, assédio, discriminação, perseguição, ofensa ou abuso de poder. A redação deve ser formal, clara e objetiva.

POSSO UTILIZAR QUALQUER *SOFTWARE* OU EQUIPAMENTO PARA REALIZAR O MEU TRABALHO?

Não. Utilize somente *hardwares* (ex. computadores, *notebooks*, *tablets* e *smartphones*), mesmo que particulares, e *softwares* autorizados.

POSSO COLOCAR AS INFORMAÇÕES DO CARTÓRIO EM SERVIÇOS E CANAIS PÚBLICOS DA INTERNET?

Evite compartilhar as informações em serviços públicos da Internet, como Facebook, Twitter, Google Drive, SkyDrive, Dropbox e iCloud. Esses ambientes não garantem a proteção e a confidencialidade que as nossas informações requerem.

A MINHA IDENTIDADE DIGITAL PRECISA DE CUIDADOS ESPECÍFICOS?

A identidade digital diz quem você é nos ambientes digitais. Cuide do seu usuário e senha, não compartilhe seu acesso às informações, equipamentos e ambientes. Sua conta de acesso e seu crachá são individuais e intransferíveis.

Crie senhas seguras e de difícil adivinhação. Além disso, troque-as regularmente ou em caso de qualquer suspeita de incidente.

QUAL A MELHOR POSTURA NAS MÍDIAS SOCIAIS?

Separe sua vida pessoal da profissional. Tenha muito cuidado com interações nas mídias sociais, saiba preservar a sua privacidade, o sigilo das informações e

- Aja com discrição e não discuta questões internas por meio das mídias sociais.
- Utilize nossos ambientes e canais internos para isso;
- Esteja atento ao que você está publicando. Em caso de dúvida quanto à procedência, veracidade ou segurança de um conteúdo que encontrou nas mídias sociais, não o dissemine;
- Não faça nas mídias sociais o que você não faria pessoalmente. Não as utilize para desrespeitar, humilhar ou ridicularizar pessoas;
- Cuidado ao filmar ou fotografar! Não compartilhe fotos do ambiente interno de trabalho ou de seus colaboradores nas mídias sociais. Sempre peça permissão e respeite os direitos de terceiros.

10 RESPONSABILIDADES E SANÇÕES

Um tratamento de dados é considerado irregular quando realizado em desconformidade com as determinações legais ou quando não é fornecida ao titular a segurança esperada. Nessa análise, deve-se levar em conta:

- O modo como o tratamento é realizado;
- Se os direitos do titular foram garantidos;
- Quais foram os riscos informados e assumidos pelo titular;
- Tecnologia disponível à época do tratamento de dados.

Além da responsabilidade de indenizar o titular dos dados, a LGPD prevê sanções administrativas na hipótese de seu descumprimento. São elas:

- advertência, com indicação de prazo para adoção de medidas corretivas;
- multa de até 2% do faturamento da empresa ou do grupo, limitada, no total, a R$ 50 milhões por infração (não aplicável aos cartórios pois se equiparam à administração pública);
- publicização da infração, após devidamente apurada e confirmada a sua ocorrência;
- bloqueio dos dados pessoais correspondentes à infração até a sua regularização;
- eliminação dos dados pessoais correspondentes à infração.

Os cartórios, equiparados à administração pública, não estão sujeitos às penas pecuniárias previstas em lei. No entanto, estão sujeitos a outras sanções, em especial as impostas pela Corregedoria do Tribunal de Justiça do Estado de São Paulo.

As sanções serão precedidas de um procedimento administrativo que garanta a ampla defesa do infrator e podem ser aplicadas cumulativamente, por dia e infração, dependendo das particularidades de cada caso e considerando alguns parâmetros: (i) a gravidade e extensão da violação; (ii) o grau do dano; (iii) boa-fé e cooperação do infrator; (iv) agilidade na adoção das medidas corretivas; (v) reincidência, dentre outros.

A adoção comprovada de uma política interna de boas práticas e governança é um dos fatores que contribuem para a redução significativa de uma potencial sanção em função de uma indesejada infração.

No caso dos cartórios, aplicam-se ainda, a depender do caso, as sanções da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação); e da Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa).

A LGPD NOS RECURSOS HUMANOS DOS CARTÓRIOS

A legislação trabalhista brasileira, como a Consolidação das Leis do Trabalho (CLT) e portarias emitidas pelo Ministério do Trabalho e Emprego, estabelecem obrigações em relação à coleta de dados pessoais de empregados para cumprimento do contrato de trabalho e de determinadas exigências legais, como os dados necessários para registro de funcionários, relatórios atualizados de saúde e segurança e outras informações que são necessariamente enviadas para órgãos governamentais, como

as constantes da folha de pagamento além outras obrigações trabalhistas, previdenciárias e tributarias (e-Social). Além disso, o empregador costuma manter os contatos pessoais, como endereço e telefone, e pode também coletar dados para outros benefícios que não são obrigatórios pela legislação do trabalho, assim como acesso ao local de trabalho ou determinados sistemas.

É importante que esses processos sejam devidamente mapeados e que as serventias revisem todos os processos de RH, da contratação ao desligamento, buscando melhorias em relação à privacidade dos empregados.

A ÁREA DE RECURSOS HUMANOS SEMPRE DEVERÁ:

- Certificar-se de que a coleta se restringirá aos dados estritamente necessários;
- Atentar sempre para base legal que justifique o tratamento dos dados pessoais de seus empregados;
- Ser transparente e fazer com que os empregados tenham ciência das operações de tratamento de dados que são realizadas e que os dados coletados estão atualizados e corretos;
- Atender aos direitos dos titulares de dados, no caso empregados ou prepostos, dentre outras obrigações trazidas pela lei.

Como de modo geral não há consentimento livre na relação de trabalho, uma vez que se constitui em uma relação de hierarquia e esses dados pessoais, muitas vezes, são necessários para a formalização do emprego ou para a relação de trabalho, o controlador deverá também buscar outras bases legais para que se assentem esses fluxos de dados. Assim, no Registro Operações de Tratamento de Dados Pessoais geralmente a execução de contrato e obrigação legal deverão ser as bases legais em que se assentarão o tratamento desses dados.

É no RH em que deverão se concentrar os dados sensíveis dos funcionários ou prepostos, como os referentes à saúde ou dados biométricos. Esses dados requerem cuidado maior para seu processamento.

- A LGPD se aplica a dados como e-mail, login ou telefone corporativo, pois ela se aplica a todo e qualquer dado que identifique ou torne identificável uma pessoa física.
- Em relação à coleta de dados de antecedentes criminais de empregados ou candidatos a emprego: importante lembrar que esta prática tem restrições da Justiça do Trabalho. Conforme entendimento do Tribunal Superior do Trabalho, a exigência de certidão de antecedentes criminais é legítima para, por exemplo, (i) motoristas rodoviários de carga, (ii) empregados que laboram no setor da agroindústria no manejo de ferramentas de trabalho perfuro cortantes, (iii) bancários e afins, (iv) trabalhadores que atuam com substâncias tóxicas e entorpecentes e armas, e (v) trabalhadores que atuam com informações sigilosas.
- A empresa poderá monitorar atividades dos empregados, mas deverá deixar claro como se dá esse monitoramento (por exemplo, se há câmera de monitoramento, deverá ter um aviso claro antes do ingresso do local monitorado, além das políticas e avisos internos de privacidade e segurança da informação da empresa) e deverá priorizar sempre as formas menos invasivas.
- A empresa não poderá manter, por tempo indeterminado, um banco de currículos com dados de candidatos não selecionados. Caso a empresa deseje manter o currículo para outras oportunidades, deverá informar o candidato sobre essa possibilidade, indicando o tempo determinado de guarda dos dados. O candidato poderá, nesse caso, pedir a exclusão dos dados.

Guia de referência elaborado pelas advogadas Estela Aranha e Samara Castro. Apoio de pesquisa e elaboração: Carolina Bassin e CM Advogados

CARTÓRIOS DE PROTESTO SP

INSTITUTO DE PROTESTO – IEPTB

www.protestosp.com.br

CM ADVOGADOS | Celso Cordeiro Marco Aurélio de Carvalho

EA | ESTELA ARANHA ADVOGADA

Samara® Castro ADVOCACIA