nº 001/2023 (ATDEFN)

BOLETIM ORIENTATIVO

Adequação à Lei Geral de Proteção de Dados (LGPD)

1ª EDIÇÃO

NORONHA PERNAMBUCO
Secretaria de Meio Ambiente, Sustentabilidade e Fernando de Noronha
GOVERNO DE PERNAMBUCO ESTADO DE MUDANÇA

O QUE EU PRECISO SABER SOBRE A LGPD?

A LGPD institui um regime geral de proteção de dados no ordenamento brasileiro e disciplina as condições e os termos de compartilhamento de **dados pessoais** entre entidades que fazem uso de bancos de dados com informações dessa natureza, sejam eles físicos ou digitais, através da Lei Federal nº 13.709/2018.

ⓘ DADO PESSOAL:

Informação relacionada à pessoa natural identificada ou identificável.

Além das informações básicas relativas ao nome, número de inscrição no Registro Geral (RG) ou no Cadastro Nacional de Pessoas Físicas (CPF) e endereço residencial, são também **considerados dados pessoais** outras informações que estejam relacionadas com uma pessoa natural, tais como seus hábitos de consumo, sua aparência e aspectos de sua personalidade. Dentre as diversas categorias de dados pessoais, podemos destacar os seguintes:

1. Estado civil, identidade, dados de identificação, imagens;

2. Vida pessoal (estilo de vida, situação familiar etc.);

3. Informações econômico-financeiras (receita, situação financeira, situação tributária etc.);

4. Dados de conexão (endereço IP, logs etc.);

5. Dados de localização (movimentos, dados de GPS, GSM etc.);

6. Dados relacionados à Segurança Social (PIS, PASEP etc.);

7. Dados revelando origem racial ou étnica;

8. Dados revelando opiniões políticas;

9. Dados revelando crenças religiosas ou filosóficas;

10. Dados revelando associação sindical;

11. Dados genéticos;

12. Dados biométricos com o objetivo de identificar exclusivamente uma pessoa singular;

13. Dados relativos à saúde;

14. Dados relativos à vida sexual ou orientação sexual de uma pessoa singular;

15. Dados relativos a condenações e infrações cíveis, administrativas e penais.

ⓘ DADO PESSOAL SENSÍVEL:

Dado pessoal sobre origem racial ou

étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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.
Os dados pessoais sensíveis são aqueles aos quais a LGPD conferiu uma proteção ainda maior, por estarem diretamente relacionados aos aspectos mais íntimos da personalidade de um indivíduo.

ⓘ DADO PESSOAL ANONIMATO:

Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

TRATAMENTO DOS DADOS

ⓘ TRATAMENTO

Toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

O Guia de Boas Práticas – Lei Geral de Proteção de Dados Pessoais (LGPD) (UNIÃO, 2020) detalha as operações de tratamento da seguinte forma:

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

- **Armazenamento:** Ação ou resultado de manter ou conservar em repositório um dado;

- **Arquivamento:** Ato ou efeito de manter registrado um dado em qualquer das fases do ciclo da informação, compreendendo os arquivos corrente, intermediário e permanente, ainda que tal informação já tenha perdido a validade ou esgotado a sua vigência;

- **Avaliação:** Analisar o dado com o objetivo de produzir informação;

- **Classificação:** Maneira de ordenar os dados conforme algum critério estabelecido;

- **Coleta:** Recolhimento de dados com finalidade específica;

- **Comunicação:** Transmitir informações pertinentes a políticas de ação sobre os dados;

- **Controle:** Ação ou poder de regular, determinar ou monitorar as ações

sobre o dado;

- Difusão: Ato ou efeito de divulgação, propagação, multiplicação dos dados;

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

- Eliminação: Ato ou efeito de excluir ou destruir dado do repositório;

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

- Modificação: Ato ou efeito de alteração do dado;

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

- Produção: Criação de bens e de serviços a partir do tratamento de dados;

- Recepção: Ato de receber os dados ao final da transmissão;

- Reprodução: Cópia de dado preexistente obtido por meio de qualquer processo;

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

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

- Utilização: Ato ou efeito do aproveitamento dos dados.

Vale lembrar que a Lei destaca a aplicação de seus efeitos tanto nos meios digitais quanto nos meios físicos. Apesar da existência majoritária de dados pessoais encontrarem-se, atualmente, em meios digitais, dada a transformação digital em curso, os dados pessoais coletados e estruturados em formato físico também devem estar sujeitos aos mesmos mandamentos da Lei.

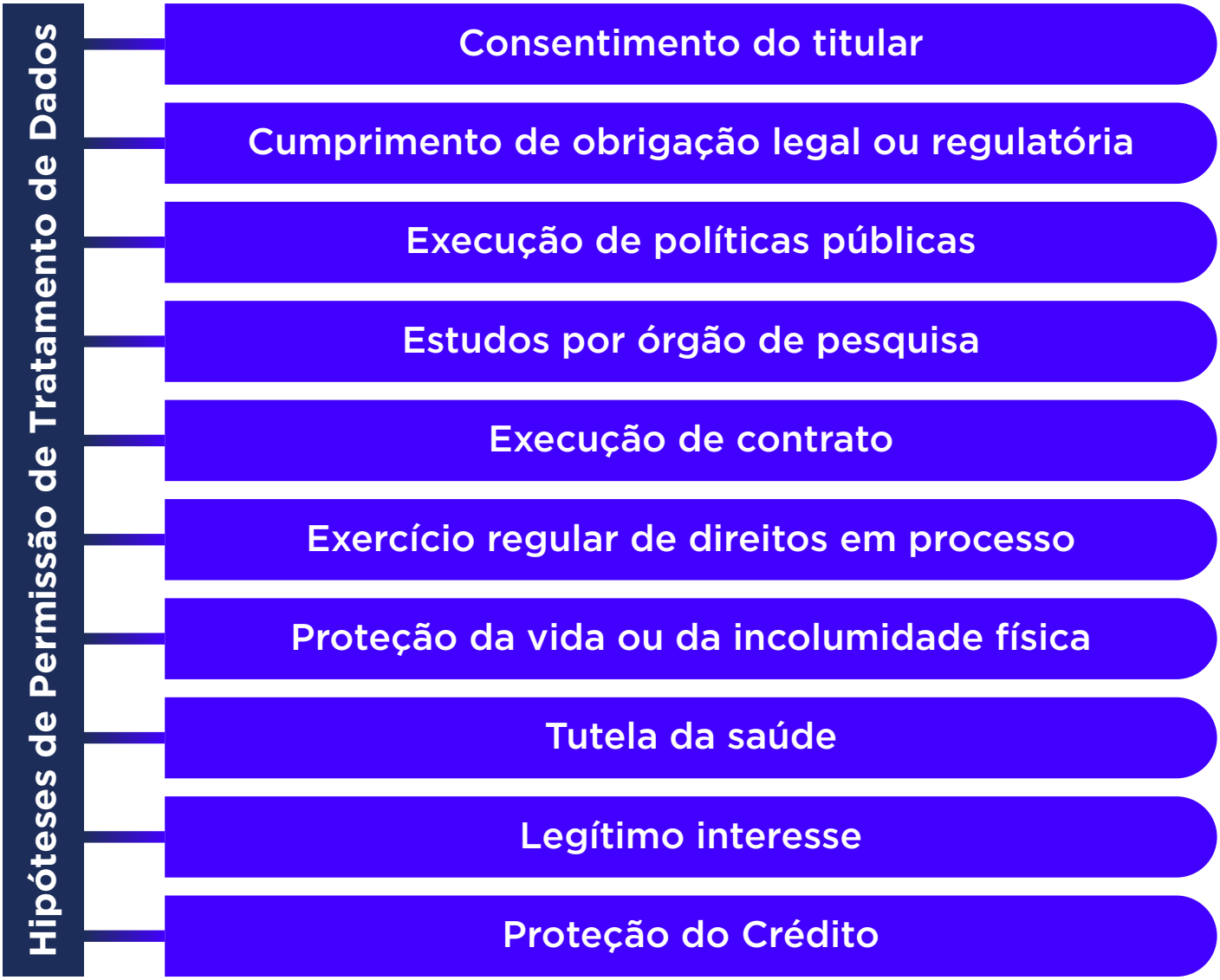
CICLO DE VIDA DO DADO

01 COLETA	Obtenção, recepção ou produção de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, sistema de informação, etc.).
02 RETENÇÃO	Arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, banco de dados, arquivo de aço, etc.).
03 PROCESSAMENTO	Qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.
04 COMPARTILHAMENTO	Qualquer operação que envolva transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais.
05 ELIMINAÇÃO	Qualquer operação que visa apagar ou eliminar dados pessoais. Esta fase também contempla descarte dos ativos organizacionais nos casos necessários ao negócio da instituição.

a) Coleta de Dados:

Os propósitos dos tratamentos de dados pessoais devem estar direcionados para o atendimento da **finalidade pública**, na persecução do **interesse público**, com o objetivo de **executar as competências legais ou cumprir as atribuições legais do serviço público**.

Pode-se dizer que a observação da finalidade é o princípio mais relevante do tratamento de dados pessoais. A coleta de dados pessoais sem finalidade específica, a coleta em excesso, o armazenamento por tempo indefinido, a ausência de política de descarte de dados, essas e outras práticas não são mais aceitas com a chegada da LGPD. O **tratamento de dados pessoais precisa ter propósitos legítimos, específicos e explícitos e informados ao titular**, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. No processo de transparência da proteção de dados pessoais não basta apontar a finalidade do tratamento, é preciso **associá-lo a uma das hipóteses de permissão de tratamento previstas na LGPD**, conforme observa-se a seguir:



Isto posto, não sendo uma das situações de exclusão citadas anteriormente, o tratamento de dados pessoais deverá estar enquadrado em, pelo menos, uma das hipóteses legais.

a.1) Consentimento:

Deve-se conter uma manifestação livre, informada e inequívoca do titular dos dados.

- **Livre:** O titular pode escolher entre aceitar ou recusar a utilização de seu dado, sem intervenções ou situações que viciem o seu consentimento.
- **Informada:** O titular do dado tem de ter ao seu dispor as informações necessárias e suficientes para avaliar corretamente a situação e a forma como seus dados serão tratados.
- **Inequívoca:** A manifestação de vontade deve ser não ambígua, evidente e ocorrer de forma clara.

Modelo Termo de Consentimento - ATDEFN

a.2) Cumprimento de obrigação legal ou regulatória:

Em circunstâncias em que, para cumprir uma lei ou regulamento específico, o controlador precisa realizar o tratamento dos dados pessoais.

Exemplo: Relacionados aos dados dos funcionários (Esocial, direitos trabalhistas entre outros).

a.3) Execução de políticas públicas previstas em leis e regulamentos:

Cumpre destacar que para que os dados sejam tratados pelo Poder Público, ou por quem lhe fizer às vezes, é preciso que exista um instrumento legal que minimamente institua a política pública e que crie suas diretrizes.

Exemplo: Política Habitacional do Distrito (PHD).

a.4) Estudos por órgão de pesquisa, desde que mantido o anonimato:

A LGPD também prevê o tratamento de dados pessoais para a realização de estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais. Conforme a Lei, em seu inciso XVII do art. 5º, órgão de pesquisa é "órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico".

a.5) Execução de contrato do qual é parte o titular dos dados:

Nesse caso, o tratamento de dados se dará a pedido do próprio titular dos dados para garantir a execução de um contrato ou de seus procedimentos preliminares.
Essa hipótese se assemelha um pouco com o tratamento de dados via consentimento.

a.6) Exercício regular de direitos em processo judicial, administrativo ou arbitral:

O inciso VI do art. 7º dá o permissivo legal para que o controlador trate dados pessoais quando tiver por finalidade subsidiar o exercício regular de direitos em processo judicial, administrativo ou arbitral, seja existente ou a ser movido no futuro. Os direitos podem ser tanto do controlador quanto de terceiros ou do próprio titular (MAIA et al, 2020).

a.7) Proteção da vida ou da incolumidade física do titular ou de terceiro:

Para enquadramento nessa hipótese, deve-se avaliar (UNIÃO, 2020):

a) O tratamento de dados pessoais se faz necessário para proteger a vida ou a incolumidade física do titular ou de terceiros?

b) O titular está impossibilitado de oferecer o consentimento para o tratamento do dado pessoal?

Exemplo: Situação de acidentes em que o titular sofre um acidente e é levado inconsciente ao hospital. Neste caso, para poder atendê-lo da maneira adequada, os médicos deverão acessar seu histórico de saúde e ter acesso a dados pessoais e dados sensíveis, no entanto, respeitando os demais princípios da LGPD e, levando-se em consideração restrição de acesso, ou seja, apenas deve ter acesso aos dados aquele que efetivamente necessitar (MAIA et al., 2020).

a.8) Tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias:

Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no nº 3; (...) 3. Os dados pessoais referidos no nº 1 podem ser tratados para os fins referidos no nº 2, alínea h), se os dados forem tratados por ou sob a 2.1.8 – Tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias 54 responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes.

a.9) Legítimo interesse do controlador ou de terceiros:

O legítimo interesse é a hipótese legal que visa possibilitar tratamentos de dados importantes, vinculados ao escopo de atividades praticadas pelo controlador, e que encontrem justificativas legítimas.
Por ser um tema de difícil aplicação prática é possível utilizar o modelo proposto pela autoridade de proteção de dados do Reino Unido, Information Commissioner's Office (ICO). A ICO propõe a realização de três questionários (Legitimate Interests Assessment (LIA) para avaliar a aplicabilidade do legítimo interesse como hipótese de tratamento de dados pessoais: **identificação da finalidade, teste de necessidade e teste de proporcionalidade**.

a.10) Proteção do crédito, nos termos do Código de Defesa do Consumidor:

A base legal de proteção de crédito tem por finalidade garantir que instituições financeiras busquem ampliar e facilitar a concessão de crédito, melhorar as análises de riscos e impulsionar o mercado.

Exemplo: Cadastro de inadimplentes

CRIANÇA E ADOLESCENTE. QUAL A DIFERENÇA PARA O TRATAMENTO?

A LGPD destacou uma seção (Seção III) específica para o tratamento de dados de crianças e adolescentes. A Lei, em seu art. 14, já estabelece que tal tratamento deverá ser realizado em seu melhor interesse, e em convergência com a legislação pertinente, em especial, com o Estatuto da Criança e Adolescente (ECA), Lei nº 8.069, de 13 de julho de 1990.
A Lei exige também que o consentimento seja específico e em destaque, dado por pelo menos um dos pais ou pelo responsável legal, conforme disposto no § 1º do art.14.

De acordo com a UNIÃO (2020), é também dever do controlador envidar todos os esforços razoáveis para verificar se o consentimento foi dado realmente pelo responsável da criança ou adolescente, consideradas as tecnologias disponíveis. Nesses casos, as hipóteses que dispensam o referido consentimento ocorrem quando:

a) A coleta for necessária para contatar os pais, ou o responsável legal, ou, ainda, para a própria proteção da criança ou adolescente. Nesses casos, os dados deverão ser utilizados uma única vez, vedados o armazenamento e o seu repasse a terceiros;

b) O tratamento de dados for imprescindível para o exercício de direitos da criança ou adolescente ou para lavratura de registros públicos.

COMO TRATAR OS DADOS PESSOAIS QUE RECEBO?

ⓘ SISTEMA ELETRÔNICO INTEGRADO:

O Sistema Eletrônico de Informações (SEI), desenvolvido pelo Tribunal Regional Federal da 4ª Região (TRF4), é um sistema de gestão de processos e documentos arquivísticos eletrônicos, com interface amigável e práticas inovadoras de trabalho. Uma das suas principais características é a libertação do papel como suporte físico para documentos institucionais e o compartilhamento do conhecimento com atualização e comunicação de novos eventos em tempo real.

Devido às características inovadoras e do sucesso da prática de cessão da ferramenta sem ônus para outras instituições, o SEI transcende a classificação de sistema eletrônico da Justiça Federal da 4ª Região para galgar a posição de **projeto estratégico para toda a administração pública**, amparando-se em premissas altamente relevantes e atuais, tais como: inovação, economia do dinheiro público, transparência administrativa, compartilhamento do conhecimento produzido e sustentabilidade.

Em 2017, o Estado de Pernambuco, através do Decreto Estadual nº 45.157/2017 dispôs sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública estadual direta, autárquica e fundacional. Em tal Decreto, ficou estabelecido, no art. 4º que "... os órgãos e as entidades da administração pública utilizarão o Sistema Eletrônico de Informações – SEI – como sistema oficial do Estado para a gestão e o trâmite de processos administrativos eletrônicos."

Em janeiro de 2020 foi publicada a Portaria SAD nº 123/2020, tendo como diretriz a orientação aos órgãos e entidades da Administração Pública do Poder Executivo Estadual quanto à uniformização dos procedimentos referente à utilização do Sistema Eletrônico de Informações - SEI PERNAMBUCO. A citada Portaria estabelece no seu art. 43 os níveis de acesso existentes no SEI, conforme trecho a seguir:

> ***Art. 43*** *Ao iniciar um processo, ou iniciar um documento no SEI PERNAMBUCO, o usuário deve classificá-lo quanto ao nível de acesso, que pode ser:*
>
> ***I - Público:*** *Quando o acesso ao conteúdo de todos os documentos em um determinado processo pode ser visualizado por qualquer usuário cadastrado no SEI;*
>
> ***II - Restrito:*** *Quando o acesso ao conteúdo dos documentos em um*

processo é restrito às unidades pelas quais o processo possa tramitar, e as usuários vinculados a essa unidade;

III - Sigiloso: *Quando o acesso aos documentos e ao processo é exclusivo aos usuários credenciados aos quais fora atribuída permissão específica para atuar no processo.*

Art. 44 *Os documentos e processos devem ser classificados no SEI PERNAMBUCO como públicos, à exceção daqueles que contenham informações sigilosas, pessoais, ou apenas utilizadas como subsídio para a tomada de decisões ou para a edição de ato normativo.*

Art. 45 *Ao classificar um documento como restrito o usuário deverá justificar o motivo da restrição, que pode ser:*
...

II - *Documentos que contenham* ***informações pessoais****: que trazem informações sobre pessoas identificadas ou identificáveis e que são restritas a servidores legalmente autorizados e à própria pessoa, conforme especificado a seguir:*

a) *Dados relativos a documentos de identificação pessoal: RG, CPF, Título de Eleitor, Documento de Reserva, dentre outros;*

b) *Informação sobre o estado de saúde do servidor;*

c) *Informações financeiras ou patrimoniais de determinada pessoa;*

d) *Informações sobre alimentados, dependentes ou pensões;*

e) *Endereço pessoal ou comercial de determinada pessoa;*

f) *Número de telefone ou endereço eletrônico de determinada pessoa;*

g) *Origem racial ou étnica, orientação sexual, convicções religiosas, filosóficas ou morais; opiniões políticas, filiação sindical, partidária ou a organização de caráter religioso, filosófico ou político.*
...

Art. 46 *Ao classificar um documento como sigiloso deverá ser justificado o motivo da restrição, que pode ser:*

I - *Documentos submetidos temporariamente à restrição de acesso em razão de sua imprescindibilidade para a* ***segurança da sociedade ou do Estado****;*

II - *Documentos que contenham informações protegidas por outras hipóteses legais de* ***sigilo fiscal, bancário, industrial****.*
(grifo nosso).

Na Autarquia Territorial do Distrito Estadual de Fernando de Noronha, o SEI passou a ser utilizado a partir de 2020, tendo atualmente vários processos com dados pessoais tramitando no sistema.

Diante das orientações contidas nesse Boletim, é necessário avaliar quais documentos de fato são imprescindíveis para o trâmite regular do processo e avaliar a classificação que esses deverão receber no SEI. A título exemplificativo, segue Quadro contendo processos desta Autarquia e a classificação no SEI que essa deve seguir:

Quadro 01. Classificação dos processos da ATDEFN no SEI

Processo	Classificação	Embasamento Legal
Formulários de solicitações de serviços que contenham dados pessoais (isenção de TPA, concessão de TPU, solicitação de passagem e hospedagem, solicitação de TFD, etc)	Restrito	Informação Pessoal (Art. 31 da Lei nº 12.527/2011) Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018)
Documentos pessoais (RG, CPF, Comprovante de Endereço, etc)	Restrito	Informação Pessoal (Art. 31 da Lei nº 12.527/2011) Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018)
Termos de Contrato	Público	Art 8º, inciso IV, da Lei 12.527/2011
Documentos de Empenho /Liquidação/Pagamento	Público	Art 7º, inciso VI, da Lei 12.527/2011
Ficha de Atendimento/ Internação/Receituário/ Prontuário e Laudos clínicos	Restrito	Informação Pessoal (Art. 31 da Lei nº 12.527/2011) Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018)
Relatórios Psicológicos/ Psiquiátricos	Restrito	Informação Pessoal (Art. 31 da Lei nº 12.527/2011) Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018)
Controle das frequências, férias, licença prêmio e maternidade dos servidores	Público (os atestados, quando acostados, no entanto, deverão ser restritos)	Entendimento CGU nº 06/2018
Concessão de benefícios assistenciais	Restrito	Informação Pessoal (Art. 31 da Lei nº 12.527/2011) Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018)
Contratação de Prestadores de serviços (Contratações eventuais)	Público	art 7º, inciso VI, da Lei 12.527/2011
Processo Licitatório	Restrito durante a fase interna. Público durante a fase externa	art 7º, inciso VI, § 3º, da Lei 12.527/2011

Fonte: Elaborado pela equipe da UCI/ATDEFN

Reforça-se que documentos pessoais deverão ser tramitados sempre na classificação RESTRITA, podendo ser utilizado como hipóteses legais de restrição no SEI/PE, qualquer uma das duas opções seguintes:
- Informação Pessoal (Art. 31 da Lei nº 12.527/2011)
- Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709/2018).

Importante destacar que, conforme definido no Guia Orientativo de Proteção de Dados Pessoais/SAD, alguns dados pessoais, por hipótese legal, tornam-se públicos, como é o caso dos dados respaldados pela Lei de Acesso à Informação, assim como dados publicados no Diário Oficial do Estado para fins nomeação, exoneração e alguns tipos de afastamento. Desse modo, são de acesso público os seguintes dados:

- Endereço do local de trabalho (exceto divulgação de escalas que colocam em risco a segurança do agente público);

- Horário do expediente (exceto divulgação de escalas que colocam em risco a segurança do agente público);

- Informações de contato institucional (telefone, e-mail etc.);

- Valores totais de remuneração.
No entanto, apesar de não haver restrição de acesso sobre os vencimentos de servidores públicos, devem ser classificados como **restritos** os documentos que contenham informações que compõem a folha de pagamento que estejam relacionadas à intimidade do servidor, como por exemplo, pensão alimentícia, empréstimo consignado, dentre outros.

Por fim, alguns alertas se fazem importantes:

- *Se o processo ou documento tramitado para a Unidade do usuário não for do seu interesse ou não for necessário para a execução de suas atividades, ele não deve ser acessado;*

- *Se o dado pessoal não for uma informação relevante e essencial, não deve constar ou ser inserido no documento ou processo;*

- *Se houver necessidade de que um documento que contenha informação pessoal restrita seja publicado, é preciso que os dados pessoais de acesso restrito sejam descaracterizados, tarjados ou pseudoanomizados (quando parte do dado é suprimido, exemplo: CPF: ***.000.000-**);*

- *É responsabilidade dos servidores e colaboradores também a guarda e sigilo de suas **credenciais de acesso ao SEI** e, das chefias, a gestão dos servidores que possuem acesso à unidade SEI que gerenciam como medida de proteção de dados pessoais e de segurança da informação.*

ⓘ CONTRATOS, CONVÊNIOS E AFINS:

A Lei 8.666/93 conceituou "Contrato" em seu art. 2º, Parágrafo único, como todo e qualquer ajuste entre órgãos ou

entidades da Administração Pública e particulares, em que haja um **acordo de vontades** para a formação de vínculo e a estipulação de obrigações recíprocas, seja qual for a denominação utilizada.

A Lei nº 12.527/201 (Lei de Acesso à Informação), estabelece no seu art. 8º, § 1º, inciso IV, que:

> ***Art. 8º*** *É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a* ***divulgação em local*** *de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.*
>
> ***§ 1º*** *Na divulgação das informações a que se refere o caput, deverão constar, no mínimo:*
>
> ***IV -*** *Informações concernentes a procedimentos licitatórios, inclusive os respectivos editais e resultados, bem como a todos os* ***contratos celebrados****;*

Nesse sentido, o Acórdão TCU nº 1855/2018 (Plenário) determinou aos órgãos e entidades da administração pública federal que publicassem o "**inteiro teor dos contratos administrativos**, seus anexos e aditivos nas páginas de transparência dos órgãos, com o intuito de aprimorar a transparência ativa e em atendimento aos fins do art. 8º, §1º, IV, da Lei 12.527/2011".

Sobre a temática a AGU se posicionou, através do Parecer 00001/2021/CONJUR-CGU/CGU/AGU, no sentido de que os dados pessoais inseridos nos **preâmbulos dos contratos**, convênios e afins, celebrados pela Administração Pública, devem **limitar-se aos nomes das partes e seus respectivos CPF/CNPJ e endereços**, por se tratarem dos elementos minimamente necessários à identificação e localização dos agentes para fins de controle social e de exigência de cumprimento das obrigações contratuais assumidas.

Por outro lado, quando se tratar de **representante legal** de pessoa jurídica da contratada, o **número de CPF deve ser divulgado de forma descaracterizada**, de modo a evitar, ao mesmo tempo, os homônimos e o uso desautorizado de tal dado por terceiros.

No âmbito do Estado de Pernambuco, seguindo as diretrizes federais, a Procuradoria Geral da União (PGE) emitiu orientação sobre a temática, no **Boletim nº 012/2020**, por oportuno transcrito a seguir:

> ***1 - Orientações quanto à inserção dos dados pessoais das partes e seus representantes no preâmbulo dos instrumentos contratuais e congêneres e respectivos extratos, para fins de atendimento à Lei Geral de Proteção de Dados Pessoais – LGPD.***
>
> *Esta Procuradoria, em sede de consulta formulada pela Secretaria da*

Controladoria Geral do Estado, visando à necessidade de compatibilização entre as disposições da Lei de Acesso à Informação – LAI (Lei nº 12.527/2011) e da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), em consonância com as orientações contidas no Acórdão TCU nº 1855/2018, ***firmou entendimento*** *no sentido de* ***que os dados pessoais inseridos nos preâmbulos dos contratos, convênios e afins****, celebrados pela Administração Pública Estadual,* ***devem limitar-se*** *aos* ***nomes das partes e seus respectivos CPF/CNPJ e endereços****, por se tratarem dos elementos minimamente necessários à identificação e localização dos agentes para fins de controle social e de exigência de cumprimento das obrigações contratuais assumidas.*

Quanto aos representantes legais*, concluiu-se* ***ser suficiente a indicação de seus nomes nos instrumentos****. Tal entendimento intentou compatibilizar o dever de a Administração disponibilizar, na íntegra, os instrumentos contratuais em sítios oficiais, à vista do disposto no art. 8º, § 1º, IV, da LAI, com as regras de proteção de dados mais rígidas introduzidas pela LGPD, que apenas autoriza o tratamento de dados pessoais nas estritas hipóteses previstas em seu art. 7º e limitando-o ao mínimo necessário ao atingimento da finalidade pública perseguida (art. 23 da LGPD).*

Nessa toada, reputou-se que o tratamento de dados dos representantes legais das partes contratantes/convenentes, limitado ao nome, encontra amparo no art. 7º, II, da Lei Federal 13.709/2018, na medida em que a Lei 8.666/93, em seu art. 61, prevê a necessidade de inclusão desses dados nos instrumentos contratuais.

Já a coleta e divulgação do nome, CPF e endereço da parte contratada, quando pessoa física, enquadra-se na base legal no art, 7º, V, da LGPD, já que tais dados se mostram necessários para a execução do contrato em que figura como parte seu titular. Sobreleva destacar que a proteção conferida ao tratamento de dados pessoais pela LGPD incide desde a coleta de tais dados até sua divulgação e descarte, não se dirigindo, porém, ao tratamento de dados relativos às pessoas jurídicas haja vista o disposto no art. 5º, I, V e X, da Lei em comento.

Quanto à publicação dos extratos *dos contratos, convênios e instrumentos congêneres, concluiu-se* ***ser suficiente a consignação dos nomes das partes e dos respectivos CNPJ/CPF, sendo desnecessário divulgar dados dos representantes legais****.*
(Precedentes: Parecer PGE nº 492/2020 (SAJ 2020.02.4099), Acórdão TCU nº 1855/2018).
(grifos nossos).

Por todo o exposto, resta claro que no preâmbulo dos termos de contratos, para a contratada, no caso de Pessoa Física, deverá constar dados de nome, CPF e endereço, já para os contratos com Pessoa Jurídica, é suficiente o uso do nome do representante legal, com o uso de CPF descaracterizado.

O citado Parecer da AGU, estabelece ainda, como sendo suficiente para identificação do representante da pessoa jurídica de direito público o uso da matrícula, por ser esse dado suficiente para identificação do

servidor responsável pelo ato, conforme pode se observar no enxerto a seguir:

> *"**9.** Com relação ao representante legal da pessoa jurídica de direito público (contratante), é possível a **substituição do número do CPF pelo número de matrícula** – que no âmbito federal é o número SIAPE – tanto na lavratura de contratos, termos aditivos e instrumentos congêneres, quanto em acordos de cooperação técnica, portarias de designação ou mesmo em relatórios e documentos relacionados às atividades finalísticas desta CGU, visto que se mostra suficiente para conseguir identificar o servidor responsável pelo ato (afastando-se os homônimos) e evitar o uso indevido do número de CPF por terceiros."*
> *(grifo nosso).*

Sendo assim, considera-se boa prática o uso da matrícula do representante legal da contratante, em substituição ao CPF.

Exemplo: Modelo Minuta PGE/PE

A PGE estabeleceu ainda diretriz, no Boletim nº 002/2021 referente ao compartilhamento de dados com terceiros contratados, por oportuno transcrito a seguir:

3. Cláusulas padrão em contratos administrativos que envolvem compartilhamento de dados pessoais com terceiros contratados.

A permissão para a realização de tratamento de dados pessoais constantes das bases de dados detidas pelo Poder Público com respaldo em contrato de prestação de serviços ancora-se no permissivo legal previsto no art. 26, §1º, IV, da Lei Federal nº 13.709/2018 (LGPD).
*Nesse contexto, o **ente ou entidade pública contratante figura como o "Controlador" do tratamento dos dados pessoais, a quem compete decidir sobre as formas e limites dos tratamentos a serem feitos, assim como instruir e fiscalizar as atividades de tratamento realizadas pelo Operador** (art. 5º, VI, da LGPD).*
*De outra ponta, **a empresa contratada assume o papel de "Operador", incumbida da tarefa de executar o tratamento de dados pessoais em nome do controlador e conforme suas instruções** (art. 39, da LGPD).*

*Embora as obrigações do controlador e do operador sejam solidárias em relação ao titular de dados pessoais (art. 42, §1º, I, LGPD), independentemente de previsão contratual, **necessário que sejam delimitados os papéis e garantias de cada parte nesse processo de tratamento, de modo a proteger o Controlador (Poder Público) quando o tratamento for realizado por terceiros;** mitigar a ocorrência de falhas e danos aos titulares; demonstrar diligência no papel fiscalizatório do Controlador e garantir eventuais ações regressivas, principalmente nas hipóteses em que haja claro descumprimento, por parte do Operador, de instruções constantes do contrato.*
Desta feita, recomenda-se que sejam incluídas cláusulas no bojo do próprio contrato de prestação de serviços ou que seja celebrado documento à parte, que será anexo necessário e indissociável do contrato principal.

Esse tipo de acordo escrito é denominado no GDPR (Regulamento Geral de Proteção de Dados da União Europeia) de Data Processing Agreement ou Addendum (DPA).

Imbuída do papel de assessoramento jurídico do Poder Executivo Estadual e em cumprimento à missão institucional prevista pelo art. 11 do Decreto Estadual nº 49.265/2020, ***a Procuradoria-Geral do Estado propõe a inclusão e previsão das seguintes cláusulas obrigacionais a serem contempladas nos instrumentos negociais celebrados pelo Estado e que envolvam o tratamento de dados pessoais pelo particular contratado****, com o registro de que constituem previsões genéricas que precisam ser complementadas e ou adaptadas ao caso concreto, a depender do formato e das particularidades de cada contratação. Registra-se que o compartilhamento de dados pessoais por força de relação convenial é igualmente permitido pela Lei Geral de Proteção de Dados (art. 26, §1º, IV), sendo recomendável que, nessas hipóteses, também sejam pactuadas cláusulas que delimitem o papel (controlador x operador), os limites e as responsabilidades de cada parte convenente, o que deverá ser feito com base nas cláusulas padrão sugeridas abaixo, ajustadas a cada situação.*

Acrescenta-se a ressalva de que a padronização de cláusulas contratuais técnicas para fins de compartilhamento e tratamento de dados pessoais ***não constitui*** *incumbência da Procuradoria e deve ser aprovada pelo Comitê Técnico de Governança Digital, nos termos do art. 8º, VI, do Decreto Estadual nº 49.265/2020.*

Eis as sugestões de obrigações relativas ao OPERADOR (CONTRATADO):

a) *Realizar o tratamento dos dados pessoais em estrita conformidade às instruções repassadas pelo Controlador/Contratante;*

b) *Adotar medidas técnicas e administrativas de segurança 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, segundo a Lei Geral de Proteção de Dados e os padrões técnicos mínimos exigidos pelo Controlador/Contratante;*
(...)

No que tange às obrigações da Administração Pública CONTRATANTE, na qualidade de CONTROLADORA dos dados pessoais, sugerem-se as seguintes previsões:

a) *Fornecer, observadas as diretrizes de sua Política Local de Proteção de Dados Pessoais e Política de Privacidade, as instruções e condições necessárias ao tratamento dos dados pelo Operador/Contratado;*

b) *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;*
(...)

Por fim, calha informar que, em trabalho conjunto com a Secretaria da Controladoria Geral do Estado, foi elaborado um modelo-padrão de termo de uso de sistemas e aplicativos para ser utilizado e adaptado pelos

órgãos e entidades da Administração do Estado de Pernambuco, que se encontra disponível na página eletrônica da SCGE dedicada à LGPD https://www.scge.pe.gov.br/lgpd/ juntamente dos demais materiais de apoio para a implementação da política de proteção de dados pessoais em cada unidade administrativa do Estado. (Precedente: Encaminhamento nº 373/2020 – SAJ 2020.02.4377).

Nesse sentido, faz-se necessária a inclusão de Obrigações explícitas tanto para o Contratante quanto para o Contratado, no caso de haver a disponibilização de dados pessoais entre esses, avaliando as sugestões da PGE e ajustando, quando necessário.

ⓘ ARQUIVOS FÍSICOS:

A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados), em seu art. 1º, estabelece:

Art. 1º *Esta Lei dispõe sobre o* ***tratamento de dados pessoais, inclusive nos meios digitais****, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.*

Do artigo resta claro que estão abrangidos pela citada legislação tanto os arquivos físicos, quanto os arquivos digitais, sendo necessário observar, no momento do tratamento dos dados recebidos de forma física, as diretrizes presentes na LGPD.
Sobre a Gestão Documental, o Estado de Pernambuco, dispôs sobre a Política Estadual a ser adotada, através da Lei nº 15.529/2015, estabelecendo que:

Art. 1º *É dever do Poder Público a* ***gestão documental e a proteção especial a documentos de arquivos****, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e de informação.*

Art. 2º *Arquivos públicos, para efeitos desta Lei, são o conjunto de documentos produzidos e recebidos, no exercício de suas atividades, por órgãos públicos estaduais em decorrência de suas funções administrativa, legislativa e judiciária.*

Art. 5º *É assegurado a todos o acesso aos documentos públicos, salvo aqueles considerados sigilosos, nos termos da legislação vigente.*

Considerando o acesso permitido a documentos públicos e a possibilidade desses conterem dados pessoais protegidos pela LGPD, é importante estar atento ao que pode ser disponibilizado.

Sendo assim, primeiramente, alguns cuidados devem ser observados no momento do arquivamento, quais sejam:
- Adoção de local físico adequado: determinar o lugar no qual pode residir de forma definitiva ou temporária uma informação de identificação pessoal de forma segura. Por exemplo, uma sala, um arquivo, um armário, etc.

- Restrição de Acesso Interno:
Determinar o nível de acesso dos servidores aos documentos (ex. delimitar acesso através de chave, credencial, etc);

- Restrição de Acesso Externo:
Determinar o nível de acesso de terceiros a documentos que contenham dados pessoais (ex. Prontuário médico - paciente e representante legal, Solicitação de TPU - solicitante e representante legal, etc);

- Definição de Tempo de guarda:
Estabelecer o tempo de guarda necessária para arquivamento da documentação.

Importante destacar ainda que a Lei nº 14.804/2012 em seu artigo 17 estabelece que:

> ***Art. 17º*** *O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.*
>
> ***§ 1º*** *As informações pessoais de que trata este artigo, relativas à intimidade, vida privada, honra e imagem:*
> *...*
>
> ***II -*** *Poderão ter autorizada sua* ***divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.***

Ou seja, desde que haja previsão legal ou consentimento expresso pelo proprietário do dado pessoal, terceiros poderão ter acesso a esses.

Destaca-se, por fim, que o Decreto Estadual nº 45.157/2017, que dispôs sobre o uso do meio eletrônico para a realização do processo administrativo, estabeleceu em seu art. 5º a obrigatoriedade da execução dos atos processuais em meio eletrônico e o processamento da digitalização desses, em seu art. 12, transcritos a seguir:

> ***Art. 5º*** *Nos processos administrativos eletrônicos,* ***os atos processuais deverão ser realizados em meio eletrônico****, exceto nas situações em que este procedimento for inviável ou em caso de indisponibilidade do meio eletrônico cujo prolongamento cause dano relevante à celeridade do processo.*
>
> *Parágrafo único. No caso das exceções previstas no caput, os atos processuais poderão ser praticados segundo as regras aplicáveis aos processos em papel, desde que posteriormente o documento-base correspondente seja digitalizado, conforme procedimento previsto no art. 12º*
> *...*
> ***Art. 12º*** *A digitalização de documentos recebidos ou produzidos no âmbito dos órgãos e das entidades da administração pública de que trata o art. 1º deverá ser acompanhada da conferência da integridade do documento digitalizado.*
>
> ***§ 1º*** *A conferência prevista no caput deverá registrar se foi apresentado*

documento original, cópia autenticada em cartório, cópia autenticada administrativamente ou cópia simples.

***§ 2º** Os documentos resultantes da digitalização de originais serão considerados cópia autenticada administrativamente, e os resultantes da digitalização de cópia autenticada em cartório, de cópia autenticada administrativamente ou de cópia simples terão valor de cópia simples.*

***§ 3º** A Administração deverá:*

***I** - Proceder à digitalização do documento apresentado e devolvê-lo imediatamente ao interessado;*

***II** - Determinar que a protocolização de documento original seja acompanhada de cópia simples, hipótese em que o protocolo atestará a conferência da cópia com o original, devolverá o documento original imediatamente ao interessado e descartará a cópia simples após a sua digitalização; ou*

***III** - Receber o documento em papel para posterior digitalização, considerando que:*

***a)** Os documentos em papel recebidos que sejam originais ou cópias autenticadas em cartório devem ser devolvidos ao interessado, preferencialmente, ou ser mantidos sob guarda do órgão ou da entidade, nos termos da sua tabela de temporalidade e destinação; e*

***b)** Os documentos em papel recebidos que sejam cópias autenticadas administrativamente ou cópias simples podem ser descartados após realizada a sua digitalização, nos termos do caput e do § 1º.*

***§ 4º** Na hipótese de ser impossível ou inviável a digitalização do documento recebido, este ficará sob guarda da administração e será admitido o trâmite do processo de forma híbrida, conforme definido em ato de cada órgão ou entidade.*

ⓘ SISTEMAS PRÓPRIOS:

O art. 49 da LGPD estabelece que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma ***a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD*** e nas demais normas regulamentares.

Considerando que atualmente a ATDEFN possui diversos sistemas próprios através dos quais são coletados uma série de dados pessoais, tais como o Sistema SIN (pagamento e isenção de TPA), Sistema de Arrecadação, Sistema do Controle Migratório, etc. necessária se faz estar atento para a implementação de alguns pontos de controle, conforme listado a seguir:

1) Controle de consentimento é fundamental:

A obtenção da ciência do usuário sobre o conteúdo da política de privacidade e termo de consentimento de uso é fundamental.

2) Segurança dos dados:

A Autoridade Nacional de Proteção de Dados (ANPD) possui um Guia

Orientativo com chek list dos requisitos básicos que a instituição tem que ter, utilizado aqui como boa prática a ser observada. Nesse documento é abordada todas as medidas técnicas para impedir o acesso indevido aos dados pessoais, além de garantir que não sejam alterados, compartilhados ou tratados de forma inadequada.

3) Empoderamento do titular de dados:

O usuário tem diversos direitos e deve ter, de forma facilitada o exercício destes, o que inclui a:

- Confirmação se está havendo tratamento de dados;

- Opção de solicitar acesso aos dados registrados pela instituição.

4) Pontos de atenção ao capturar os dados:

Reforçando o que já foi dito anteriormente, de maneira geral, a LGPD determina que devemos solicitar apenas os dados indispensáveis para atingir a finalidade da prestação do serviço pela empresa. Ou seja, na coleta dos dados deixar de fora informações excessivas/desnecessárias como data de nascimento e sexo, se de fato não serão utilizadas.

5) Alterações técnicas no sistema:

O compartilhamento interno de informações também é um ponto que mudou com a LGPD. Em razão dos princípios da finalidade, necessidade e adequação, podem acessar os dados apenas as áreas internas que tenham relação com os serviços prestados. A cópia de dados e a exportação também deve ser apenas por pessoas chave, com alto nível de segurança, ficando armazenados os logs de acesso. Por isso, devemos fazer alterações nos perfis de administradores, como:

- Identificação das pessoas que têm acesso ao sistema: incluir identificação da pessoa logada;

- Prevenir logins compartilhados: Exigir a autenticação de dois fatores ao fazer login pela primeira vez no browser (para isso, pode-se usar o aplicativo Google Authenticator ou token via e-mail/sms);

- Diferenciar níveis de acesso: em tese se a pessoa não tem uma razão para ter acesso aos dados pessoais, não deveriam aparecer;

- Restrições: a função de cópia de dados e de exportação dos dados deve ser exclusiva de superadministradores.

QUAIS PUNIÇÕES O SERVIDOR PODE RECEBER POR DIVULGAR DADOS PESSOAIS DE FORMA IRREGULAR?

É importante destacar que as penalidades elencadas na LGPD são aplicadas diretamente aos agentes de tratamento, que no caso da Administração Pública, referem-se aos órgãos ou às entidades, e não diretamente ao agente público autor da infração. Entretanto, a Lei ressalta a possibilidade das sanções administrativas aplicáveis aos agentes públicos - quer seja pela Lei de Improbidade Administrativa, quer seja disciplinarmente pelos respectivos estatutos de cada ente.

Ademais, a Lei de Proteção de Dados Pessoais não substitui a aplicação das sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), e em legislação específica. A LGPD prevê que o agente que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a repará-lo, podendo, inclusive, a reparação ser exercida coletivamente em juízo, observado o disposto na legislação pertinente, conforme destaca o art. 42. Sendo assim, o órgão ou entidade da Administração Pública pode ser, em juízo, obrigada a reparar dano patrimonial, moral, individual ou coletivo, independentemente de sanção administrativa pecuniária. Nesse caso, cumpre ressaltar o direito de regresso previsto no art. 37, § 6º da Constituição Federal, que estabelece que as pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.
Em especial, a Lei de Acesso à Informação define como conduta ilícita divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação pessoal. Nesses casos, conforme art. 34 da LAI, os órgãos e entidades públicas respondem diretamente pelos danos causados, cabendo a apuração de responsabilidade funcional nos casos de dolo ou culpa, assegurado o respectivo direito de regresso.

BIBLIOGRAFIA

Manual de Proteção de Dados Pessoais em Pernambuco. SCGE PE.
Disponível em:
https://www.scge.pe.gov.br/wp-content/uploads/2021/11/ManualLGPDv3-2.pdf

PGE – PROCURADORIA GERAL DO ESTADO DE PERNAMBUCO. Parecer PGE nº 12/2020 e 02/2021.
Disponível em:
https://www.pge.pe.gov.br/ProcConsultivaBoletins.aspx

UNIÃO, **Guia de Boas Práticas: Lei Geral de Proteção de Dados (LGPD)**, 2020. [Online].
Disponível em:
GuiaLGPD.pdf (*www.gov.br*).

Guia Orientativo de Proteção de Dados Pessoais, SAD PE, 2023.

NORONHA
PERNAMBUCO

Secretaria
de Meio Ambiente,
Sustentabilidade e
Fernando de Noronha

GOVERNO DE
PERNAMBUCO
ESTADO DE MUDANÇA