



ADVOCACIA-GERAL DA UNIÃO
CONSULTORIA-GERAL DA UNIÃO
CONSULTORIA JURÍDICA JUNTO À CONTROLADORIA GERAL DA UNIÃO
COORDENAÇÃO-GERAL DE CONTROLE, OUVIDORIA E INTEGRIDADE PRIVADA
PARECER n. 00304/2023/CONJUR-CGU/CGU/AGU

NUP: 00190.105207/2023-84

INTERESSADOS: CONTROLADORIA-GERAL DA UNIÃO-CGU

ASSUNTOS: CONTROLE E LEI GERAL DE PROTEÇÃO DE DADOS

EMENTA: 1. Direito Constitucional e Administrativo. 2. Consulta da Secretaria Federal de Controle Interno da Controladoria-Geral da União acerca da utilização do sistema ALICE - Analisador de Licitações, Contratos e Editais e os impactos em relação à Lei Geral de Proteção de Dados (LGPD). 3. Tratamento de dados pessoais pelo Poder Público. 4. Possibilidade, na forma do artigo 7º, incisos II e III, da LGPD. 5. Previsão de cautelas na LGPD a serem seguidas pela Administração Pública.

Senhor Coordenador-Geral de Matéria de Controle, Ouvidoria e Integridade Privada,

1. RELATÓRIO

1. Trata-se de consulta da Secretaria Federal de Controle Interno da Controladoria-Geral da União (SFC/CGU) acerca das repercussões do sistema ALICE - Analisador de Licitações, Contratos e Editais e os impactos em relação à Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709, de 14 de agosto de 2018.

2. Segundo a SFC/CGU, considerando-se o avanço e aperfeiçoamento do sistema ALICE, "o Acordo de Cooperação Técnica CGU/SEGES-ME nº 135/2021 ([2037507](#)) previu a disponibilização dos alertas da ALICE para os Gestores Públicos, no âmbito do Portal de Compras do Governo Federal (Comprasnet 4.0)."

3. Segundo os autos, as funções do sistema ALICE serão, dentre outras, "identificar e realizar correções necessárias nos artefatos elaborados ao longo do processo de compras, desde a fase de planejamento das contratações, a partir das inconsistências apontadas pela ALICE, aumentando a eficiência do processo e mitigando riscos à administração pública." (SEI 2800687).

4. Ainda, conforme a SFC/CGU, "Atualmente a ALICE realiza as análises seguindo trilhas (de auditoria) que podem resultar em alertas. Esses alertas advêm de uma série de cruzamentos de dados realizados em diferentes bases de dados disponíveis na CGU, apresentando informações, a depender da análise realizada, como: CPF e SIAPE^[1] de sócios de empresa, servidores e empregados públicos; CNPJ, e-mail, telefone e endereço de licitantes e empresas contratadas, entre outras."

5. A consulta foi instruída (SEI 2816700) com documento em que consta a forma de apresentação dos alertas a serem realizados aos gestores públicos pelo Sistema ALICE.

6. A NOTA TÉCNICA Nº 2190/2023/CGGE/SE (SEI 2873454), que encaminhou o processo a esta Consultoria Jurídica, atestou a relevância dos cruzamentos de dados realizados pelo ALICE, mas alertou acerca da necessidade do cuidado em relação ao cumprimento das determinações da LGPD.

7. É o relatório.

2. FUNDAMENTAÇÃO

2.1.DA POSSIBILIDADE DE DEFLAGRAÇÃO DOS ALERTAS DO SISTEMA ALICE, DESDE QUE ATENDIDAS AS CAUTELAS CONSTANTES NA LEI GERAL DE PROTEÇÃO DE DADOS ACERCA DOS DADOS PESSOAIS DAS PESSOAS ENVOLVIDAS.

2.1.1. INTRODUÇÃO.

8. O documento juntado aos autos pela SFC/CGU demonstra de forma didática o tipo de informação que poderá constar nos alertas do Sistema ALICE. Como exemplo, podemos elencar algumas hipóteses que constam no documento (SEI 2818652), aqui colacionadas por amostragem. Vejamos:

Código e nome da trilha	Informações sensíveis envolvidas
2020 - Licitantes com sócios no BPC	- CPF/CNPJ/NOME do Vencedor/Sócios
Formato do texto do alerta dessa trilha	
Um ou mais itens deste pregão foram vencidos por um licitante que possui sócio registrado no banco de Benefícios de Prestação Continuada, e recebe benefícios assistenciais.	
<p>Vencedor: CPF/CNPJ: {VENCEDOR_CNPJ:formatar_cpf_cnpj} Nome/Razão Social: {VENCEDOR_NOME} Atividade: {VENCEDOR_ATIVIDADE} Total do Vencedor: {MATERIALIDADE:formatar_moeda} Sócio do Vencedor: CPF/CNPJ: {S1_CPF_CNPJ:formatar_cpf_cnpj} Nome/Razão Social: {S1_NOME} Data de entrada na sociedade: {S1_DATA_ENTRADA_SOCIEDADE:formatar_data} Data de exclusão na sociedade: {S1_DATA_EXCLUSAO_SOCIEDADE:formatar_data}</p> <p>Data de início do benefício: {S1_BEN_DATA_INICIO:formatar_data} Tipo de benefício: {S1_TIPO_BEN}</p> <p>Comprasnet: Resultado Atas do pregão Declarações dos participantes</p>	
Código e nome da trilha	Informações sensíveis envolvidas
2021 - Licitantes com sócios no Bolsa Família	- CPF/CNPJ/NOME do Vencedor/Sócios

Código e nome da trilha	Informações sensíveis envolvidas
2027 - Sócio fornecedor diretor de estatal compradora	- CPF/CNPJ/NOME do Vencedor/Sócios - Empregado de Estatal
Formato do texto do alerta dessa trilha	
ComprasNet: Sócio de empresa vencedora é Diretor da estatal contratante, em desacordo com o art. 38, inciso I da Lei Federal nº 13.303/2016 - Lei das Estatais.	
<p>Obs: deve-se atentar para as datas de vigência dos contratos, datas de entrada e saída da sociedade e datas de início e fim do vínculo empregatício/mandato (no caso de dirigentes) com a estatal. Vencedor: CPF/CNPJ: {VENCEDOR_CNPJ:formatar_cpf_cnpj} - {VENCEDOR_NOME} - Atividade: {VENCEDOR_ATIVIDADE} Total do Vencedor: {MATERIALIDADE:formatar_moeda} Sócio do Vencedor: CPF/CNPJ: {CPF:formatar_cpf_cnpj} - {NOME} - data de entrada na sociedade: {DATA_ENTRADA_SOCIEDADE:formatar_data} e data de exclusão na sociedade: {DATA_EXCLUSAO_SOCIEDADE:formatar_data} Data Entrada na Estatal: {DATA_ENTRADA_ESTATAL:formatar_data} Data Saída da Estatal: {DATA_SAIDA_ESTATAL:formatar_data}</p>	
Código e nome da trilha	Informações sensíveis envolvidas
2028 - Sócio fornecedor emp de estatal compradora	- CPF/CNPJ/NOME do Vencedor/Sócios - Empregado de Estatal
Formato do texto do alerta dessa trilha	
ComprasNet: Sócio de empresa vencedora é empregado da estatal contratante, em desacordo com o art. 38, inciso I da Lei Federal nº 13.303/2016 - Lei das Estatais.	
<p>Obs: deve-se atentar para as datas de vigência dos contratos, datas de entrada e saída da sociedade e datas de início e fim do vínculo empregatício/mandato (no caso de dirigentes) com a estatal. Vencedor: CPF/CNPJ: {VENCEDOR_CNPJ:formatar_cpf_cnpj} - {VENCEDOR_NOME} - Atividade: {VENCEDOR_ATIVIDADE} Total do Vencedor: {MATERIALIDADE:formatar_moeda} Sócio do Vencedor: CPF/CNPJ: {CPF:formatar_cpf_cnpj} - {NOME} - data de entrada na sociedade: {DATA_ENTRADA_SOCIEDADE:formatar_data} e data de exclusão na sociedade: {DATA_EXCLUSAO_SOCIEDADE:formatar_data} Data Entrada na Estatal: {DATA_ENTRADA_ESTATAL:formatar_data} Data Saída da Estatal: {DATA_SAIDA_ESTATAL:formatar_data}</p>	
Código e nome da trilha	Informações sensíveis envolvidas
2029 - Soc fornecedor diretor de estatal comp indireto	- CPF/CNPJ/NOME do Vencedor/Sócios

Código e nome da trilha	Informações sensíveis envolvidas
2016 - Licitantes com Tel ou Email em comum	- CPF/CNPJ/NOME do Vencedor/Sócios - E-mail, telefone e endereço dos LICITANTES - ORGAO SANCIONADOR
Formato do texto do alerta dessa trilha	
Um ou mais itens deste pregão foram vencidos por um licitante que apresenta telefone, fax ou e-mail iguais ao de outro licitante que participou deste mesmo pregão.	
<p>Vencedor: CPF/CNPJ: {VENCEDOR_CNPJ:formatar_cpf_cnpj} Nome/Razão Social: {VENCEDOR_NOME} Atividade: {VENCEDOR_ATIVIDADE} Total do Vencedor: {MATERIALIDADE:formatar_moeda} Contatos: telefone 1: {{V_DT1}} {V_T1}, telefone 2: {{V_DT2}} {V_T2}, fax: {{V_DF}} {V_F} e e-mail: {V_MAIL} Endereço: {V_TIPO_LOG}; {V_DESC_LOG}, n° {V_NUM_LOG}, complemento: {V_COMP_LOG}, bairro: {V_BAIRRO}, município: {V_MUN} {V_UF} - CEP: {V_CEP}</p> <p>Licitante relacionado: CPF/CNPJ: {RELACIONADO_CNPJ:formatar_cpf_cnpj} Nome/Razão Social: {RELACIONADO_NOME} Atividade: {RELACIONADO_ATIVIDADE} Contatos: telefone 1: {{R_DT1}} {R_T1}, telefone 2: {{R_DT2}} {R_T2}, fax: {{R_DF}} {R_F} e e-mail: {R_MAIL} Endereço: {R_TIPO_LOG}; {R_DESC_LOG}, n° {R_NUM_LOG}, complemento: {R_COMP_LOG}, bairro: {R_BAIRRO}, município: {R_MUN} {R_UF} - CEP: {R_CEP}</p> <p>Comprasnet: Resultado Atas do pregão</p>	

9. Verifica-se, portanto, que os principais dados pessoais que constarão nos alertas efetuados pelo sistema ALICE são: CPF, matrícula funcional (SIAPE), nome de pessoas, vínculos profissionais e societários, vínculos contratuais com a Administração, e-mail, telefone e endereços de pessoas (licitantes).

10. Cabe, ainda, salientar que, segundo a SFC/CGU (SEI 2873454), referidos alertas serão direcionados a **servidores específicos** que sejam gestores públicos responsáveis pelos processos de licitação. Vejamos:

4.4. Dessa forma, no caso específico sob análise, o uso dos dados constantes do portal de compras para análise pelo ALICE está amparado no inciso segundo que trata do cumprimento de obrigação legal, uma vez que a CGU, especificamente a SFC estaria alertando o gestor quanto a possíveis situações de irregularidades no processo de contratação, de modo que os Gestores Públicos possam identificar e realizar correções necessárias nos artefatos elaborados ao longo do processo de compras, desde a fase de planejamento das contratações, a partir das inconsistências apontadas pela ALICE, aumentando a eficiência do processo e mitigando riscos à administração pública.

[...]

4.6. Novamente, na presente situação, observa-se que os alertas são enviados apenas aos gestores que têm necessidade de conhecer os dados pessoais e que estão envolvidos no processo de contratação, o que atende ao princípio da necessidade. Além disso, quanto ao princípio da finalidade, também verifica-se, tendo em vista o que já foi relatado no item anterior. Dessa forma, com vistas a atender ao princípio da segurança, sugere-se que seja enviado, juntamente com os alertas do ALICE, um texto destacando ao gestor que contém dados pessoais e que deverão ser adotadas medidas de segurança para proteger esses dados, evitando o compartilhamento com quem não tenha necessidade de conhecer ou até um eventual vazamento do dado. Ademais, importante salientar que o gestor também deverá ser informado quanto à possível responsabilização se descumprir os dispositivos tanto da LGPD quanto da Lei de Acesso à Informação. Caso possível, o ideal seria que o gestor somente pudesse visualizar as informações do alerta após ler o texto com as ressalvas dos cuidados no tratamento dos dados pessoais e registrar sua ciência.

11. Portanto, o intuito dos referidos alertas desempenhados pelo sistema ALICE é o fortalecimento da primeira linha de defesa do controle, em perfeita obediência ao artigo 169, da Lei nº 14.133, de 1º de abril de 2021:

Art. 169. As contratações públicas deverão submeter-se a práticas contínuas e permanentes de gestão de riscos e de controle preventivo, inclusive mediante adoção de recursos de tecnologia da informação, e, além de estar subordinadas ao controle social, sujeitar-se-ão às seguintes linhas de defesa:

I - primeira linha de defesa, integrada por servidores e empregados públicos, agentes de licitação e autoridades que atuam na estrutura de governança do órgão ou entidade;

II - segunda linha de defesa, integrada pelas unidades de assessoramento jurídico e de controle interno do próprio órgão ou entidade;

III - terceira linha de defesa, integrada pelo órgão central de controle interno da Administração e pelo tribunal de contas.

[...]

12. Nesse sentido, a Consultoria-Geral da União, da Advocacia-Geral da União, por meio do PARECER n. 00009/2022/DECOR/CGU/AGU estabeleceu a necessidade de adaptação dos processo licitatórios em curso à LGPD, da seguinte maneira:

III. Os dados pessoais tratados em razão de licitações e contratos administrativos devem subsumir-se à nova Política desde a entrada em vigor da LGPD, mesmo no caso das licitações em curso e os contratos já firmados, que poderão ser revistos, caso necessário, para adaptação aos parâmetros impostos pela norma.

13. Apresentado o contexto geral, passemos à aplicação da LGPD ao caso concreto.

2.1.2. APLICAÇÃO DA LGPD AO CASO CONCRETO. BASE LEGAL PARA O TRATAMENTO DE DADOS.

14. Passando-se à análise da LGPD sobre o caso, a primeira consideração a ser feita é sobre a aplicabilidade da lei aos casos de tratamento de dados realizado pelo sistema ALICE. Para isso, colaciona-se os artigos 3º e 4º da norma, que determinam o seu espectro de aplicação da LGPD. Vejamos:

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou [\(Redação dada pela Lei nº 13.853, de 2019\) Vigência](#)

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV docaput do art. 4º desta Lei.

Art. 4º Esta Lei 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:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

15. Importante, ainda, estabelecer o conceito de **dado pessoal**, que são os dados relacionados à pessoa natural identificada ou identificável. Além disso, o **titular** dos dados seria a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, conforme artigo 5º, incisos I e V, da norma.

16. Com efeito, no artigo 5º da norma, além do conceito de **dado pessoal e titular**, há conceitos importantes para a presente consulta, como os de **controlador** dos dados, **tratamento**, **uso compartilhado** de dados. Vejamos os conceitos estabelecidos pelo artigo 5º da LGPD:

Art. 5º Para os fins desta Lei, considera-se:

I - **dado pessoal**: informação relacionada a pessoa natural identificada ou identificável;

II - **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;

III - **dado anonimizado**: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - **banco de dados**: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - **titular**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - **controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - **operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - **encarregado**: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); [\(Redação dada pela Lei nº 13.853, de 2019\) Vigência](#)

IX - **agentes de tratamento**: o controlador e o operador;

X - **tratamento**: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - **anonimização**: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - **consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - **bloqueio**: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do

banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - **uso compartilhado de dados**: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVIII - órgão de pesquisa: 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; e [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#) (destacamos)

17. A LGPD também impõe princípios que são voltados ao tratamento de dados pessoais e que devem ser seguidos pelas autoridades que realizarão o referido tratamento. Referidos princípios são os seguintes:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[...]

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - 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 \(Lei de Acesso à Informação\)](#);

II - (VETADO);

III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou [\(Incluído pela Lei nº 13.853, de 2019\)](#)

V - 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. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

(grifamos)

18. Sobre os referidos princípios, a NOTA TÉCNICA Nº 2190/2023/CGGE/SE (SEI 2873454), da Secretaria Federal de Controle Interno (SFC/CGU), já citada no presente parecer, defendeu que o tratamento de dados pessoais do sistema ALICE obedece aos princípios da necessidade e finalidade.

19. Há precedentes desta Consultoria Jurídica sobre o tratamento de dados pelo Poder Público. Nesse sentido, o PARECER n. 00429/2022/CONJUR-CGU/CGU/AGU, ao comentar o artigo 25 da LGPD, estabelece não somente um direito da

Administração em compartilhar os dados, mas a necessidade de manutenção dos dados de forma interoperável para compartilhamento. Vejamos as disposições do opinativo desta Consultoria Jurídica:

29. De acordo com a norma contida no art. 25 da LGPD *é possível se extrair um dever geral de compartilhamento das informações entre as esferas públicas quando útil e necessário a tornar efetiva execução de políticas públicas, a prestação de serviços públicos, a descentralização da atividade pública e a disseminação e ao acesso das informações pelo público em geral.*

20. Por sua vez, o Decreto nº 10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e estabelece diretrizes para tratamento de dados pelo Poder Público. Vejamos:

Art. 3º O compartilhamento de dados pelos órgãos e entidades de que trata o art. 1º observará as seguintes diretrizes:

I - a informação do Estado será compartilhada da forma mais ampla possível, observadas as restrições legais, os requisitos de segurança da informação e comunicações e o disposto na [Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais](#);

II - o compartilhamento de dados sujeitos a sigilo implica a assunção, pelo receptor de dados, dos deveres de sigilo e auditabilidade impostos ao custodiante dos dados;

III - os mecanismos de compartilhamento, interoperabilidade e auditabilidade devem ser desenvolvidos de forma a atender às necessidades de negócio dos órgãos e entidades de que trata o art. 1º, para facilitar a execução de políticas públicas orientadas por dados;

IV - os órgãos e entidades de que trata o art. 1º colaborarão para a redução dos custos de acesso a dados no âmbito da administração pública, inclusive, mediante o reaproveitamento de recursos de infraestrutura por múltiplos órgãos e entidades;

V - nas hipóteses em que se configure tratamento de dados pessoais, serão observados o direito à preservação da intimidade e da privacidade da pessoa natural, a proteção dos dados e as normas e os procedimentos previstos na legislação; ([Redação dada pelo Decreto nº 11.266, de 2022](#))

VI - a coleta, o tratamento e o compartilhamento de dados por cada órgão serão realizados nos termos do disposto no [art. 23 da Lei nº 13.709, de 2018](#) - Lei Geral de Proteção de Dados Pessoais; ([Redação dada pelo Decreto nº 11.266, de 2022](#))

VII - a eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados pessoais, nos termos do disposto no [inciso I do caput do art. 6º da Lei nº 13.709, de 2018](#) - Lei Geral de Proteção de Dados Pessoais; ([Incluído pelo Decreto nº 11.266, de 2022](#))

VIII - a compatibilidade do tratamento de dados pessoais com as finalidades informadas, nos termos do disposto no [inciso II do caput do art. 6º da Lei nº 13.709, de 2018](#) - Lei Geral de Proteção de Dados Pessoais; e ([Incluído pelo Decreto nº 11.266, de 2022](#))

IX - a limitação do compartilhamento de dados pessoais ao mínimo necessário para o atendimento da finalidade informada, nos termos do disposto no [inciso III do caput do art. 6º da Lei nº 13.709, de 2018](#) - Lei Geral de Proteção de Dados Pessoais, e o cumprimento integral dos requisitos, das garantias e dos procedimentos estabelecidos na referida Lei, no que for compatível com o setor público. ([Incluído pelo Decreto nº 11.266, de 2022](#))

Art. 4º O compartilhamento de dados entre os órgãos e as entidades de que trata o art. 1º é categorizado em três níveis, de acordo com sua confidencialidade:

I - compartilhamento amplo, quando se tratar de dados públicos que não estão sujeitos a nenhuma restrição de acesso, cuja divulgação deve ser pública e garantida a qualquer interessado, na forma da legislação;

II - compartilhamento restrito, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a todos os órgãos e entidades de que trata o art. 1º para a execução de políticas públicas, cujo mecanismo de compartilhamento e regras sejam simplificados e estabelecidos pelo Comitê Central de Governança de Dados; e

III - compartilhamento específico, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a órgãos e entidades específicos, nas hipóteses e para os fins previstos em lei, cujo compartilhamento e regras sejam definidos pelo gestor de dados.

§ 1º A categorização do nível de compartilhamento será feita pelo gestor de dados, com base na legislação.

§ 2º A categorização do nível de compartilhamento será detalhada de forma a tornar clara a situação de cada item de informação.

§ 3º A categorização do nível de compartilhamento como restrito ou específico observará as regras de compartilhamento de que trata o art. 31 e será publicada pelo respectivo gestor de dados, em prazo a ser definido pelo Comitê Central de Governança de Dados, que considerará, para a tomada de decisão, o disposto no [Decreto Legislativo nº 6, de 20 de março de 2020](#). ([Redação dada pelo Decreto nº 10.403, de 2020](#))

§ 4º A categorização do nível de compartilhamento como restrito e específico especificará o conjunto de bases de dados por ele administrado com restrições de acesso e as respectivas motivações.

§ 5º A categorização do nível de compartilhamento, na hipótese de ainda não ter sido feita, será realizada pelo gestor de dados quando responder a solicitação de permissão de acesso ao dado.

§ 6º A categorização do nível de compartilhamento será revista a cada cinco anos, contados da data de publicação deste Decreto ou sempre que identificadas alterações nas diretrizes que ensejaram a sua categorização.

§ 7º Os órgãos e entidades de que trata o art. 1º priorizarão a categoria de compartilhamento de dados de maior abertura, em compatibilidade com as diretrizes de acesso a informação previstas na legislação. (grifamos)

21. Portanto, é necessário que os servidores públicos que terão acesso aos dados pessoais e, portanto, sigilosos, devam ser cientificados da referida condição e dos deveres de sigilo e auditabilidade impostos ao custodiante dos dados. Além disso, devem ter ciência da necessidade de preservação da intimidade e da privacidade da pessoa natural, a proteção dos dados e as normas e os procedimentos previstos na legislação.

22. Ademais, entendemos que a categorização do compartilhamento, segundo o artigo 4º do Decreto nº 10.046, de 2019, deve seguir o compartilhamento específico, regulado pelo artigo 4º, inciso III do referido decreto. Para isso, deve-se seguir as regras previstas no artigo 14 do mesmo decreto.

23. Além disso, entendemos que as cautelas apontadas pela SFC/CGU na NOTA TÉCNICA Nº 2190/2023/CGGE/SE (SEI 2873454) são oportunas e guardam pertinência com os princípios contidos no artigo 6º da LGPD. Por isso, ratificamos a necessidade de cientificação dos servidores públicos que terão acesso aos dados pessoais e o alerta quanto à necessidade de resguardo e proteção dos referidos dados. Além disso, recomenda-se que a cientificação do servidor público que receberá os alertas do sistema ALICE seja feita anteriormente ao acesso propriamente dito. Abordaremos essa necessidade de cautela mais adiante, ocasião em que definiremos os conceitos de controlador e operador.

24. Apresentam-se no artigo 7º da LGPD, também, os requisitos para o tratamento de dados pessoais. Vejamos:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, 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, observadas as disposições do Capítulo IV desta Lei;

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

V - 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;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da [Lei nº 9.307, de 23 de setembro de 1996 \(Lei de Arbitragem\)](#);

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

§ 1º (Revogado). [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

§ 2º (Revogado). [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

25. Nesse ponto, importante ressaltar que os requisitos para o tratamento não são cumulativos. Ou seja, caso se verifique a ocorrência de apenas um dos requisitos para o tratamento, ele será autorizado. Além disso, o tratamento de dados pessoais no caso dos incisos II a X do artigo 7º - de acordo com as hipóteses previstas no texto legal, que o autor chama de "bases legais" - são independentes de consentimento pelo titular^[2]. Vejamos o que diz a doutrina de Caio César Carvalho Lima^[3]:

Antes de passarmos para os comentários específicos acerca deste artigo, importante apenas relembrar o conceito de "tratamento de dados pessoais" disposto no artigo 5º, X desta Lei, o que engloba diversas operações com dados pessoais, aí se incluindo, a coleta, o acesso, distribuição, armazenamento, eliminação, a estes não se limitando.

Com isso, podemos observar as dez hipóteses (bases legais) que legitimam o tratamento dos dados pessoais, as quais são taxativas (isto é, não existe nenhuma outra hipótese, além das expressamente descritas neste artigo). Ademais, **deve-se destacar que basta o atendimento de uma das dez bases para o tratamento ser considerado legítimo (sendo possível cumular bases legais dentro de uma mesma atividade, considerando diferentes dados pessoais), cabendo realçar que todas as demais bases legais mencionadas nos incisos II a X são independentes do consentimento.** (grifamos)

26. Nesse mesmo sentido da desnecessidade de consentimento pelo titular em casos como o dos autos, temos o entendimento do PARECER n. 00001/2021/CONJUR-CGU/CGU/AGU, desta Consultoria Jurídica:

5. No inciso V do art. 7º da LGPD há hipótese específica de tratamento de dados pessoais quando necessário à execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados. O consentimento específico do titular é tácito, nesses casos, em decorrência da autonomia da vontade expressa no momento da realização do instrumento contratual, ou seja, não sendo necessária nova previsão expressa para o tratamento decorrente do ato (art. 7º, inciso V, da LGPD);

27. Por outro lado, no caso do sistema ALICE, a primeira hipótese legal que melhor se enquadra no tratamento de dados pessoais é a que consta no artigo 7º, inciso II, da lei, ou seja, aquela feita para o cumprimento de obrigação legal ou regulatória pelo controlador. A doutrina de Caio César Carvalho Lima^[4] analisa a hipótese. Vejamos:

Caso exista determinação legal (quer em lei federal, estadual ou municipal), ou nas demais normas (decretos, resoluções, entre outros), o controlador (vide conceito no artigo 5º, VI) poderá realizar o tratamento de dados pessoais com fundamento nessa base legal.

Obrigações contratualmente assumidas não se encontram acobertadas pelo presente inciso, não podendo relações privadas serem utilizadas como fundamento para tratamento de dados pessoais. Assim, é relevante que a assinatura de contratos seja precedida de prévia e efetiva validação acerca da possibilidade de cumprir todas as disposições lá constantes à luz da legislação, a fim de que não haja a assunção de obrigação impossível.

Ademais, eventuais determinações previstas na legislação internacional, bem como em melhores práticas comprovadamente seguidas por determinado nicho da indústria, também poderão ser entendidos como fundamento para o tratamento de dados, sob pena de serem criados entraves de consequências relevantes, especialmente a companhias multinacionais. É importante que, previamente ao tratamento dos dados com base em previsões legais internacionais, haja extenso levantamento dos riscos relacionados para os titulares e para o agente de tratamento, especialmente por meio da elaboração de análise cotejando tais riscos, armazenando as evidências da realização de tal estudo.

28. O Guia Orientativo da Agência Nacional de Proteção de Dados (ANPD)^[5] também esclarece a hipótese de tratamento de dados para o cumprimento de obrigação legal ou regulatória:

Cumprimento de obrigação legal ou regulatória Conforme o art. 7º, ii, da LGPD, o tratamento de dados pessoais pelo Poder Público poderá ser realizado “para o cumprimento de obrigação legal ou regulatória pelo controlador”. A mesma hipótese está prevista no art. 11, ii, a, que rege o tratamento de dados sensíveis.

De forma geral, a aplicação desses dispositivos será efetuada em dois contextos normativos distintos, que se diferenciam em razão da espécie de norma jurídica que estabelece a obrigação a ser cumprida. É o caso, em especial, das normas de conduta e das normas de organização [8].

Na primeira hipótese, a obrigação legal decorre de uma norma de conduta, isto é, uma regra que disciplina um comportamento, em geral estabelecendo um fato ou uma hipótese legal, com uma possível consequência jurídica em caso de descumprimento. Caso o responsável não cumpra a obrigação legal (como, por exemplo, a divulgação da agenda de compromissos públicos de autoridades, conforme art. 11 da Lei nº 12.813/2013), poderá ser objeto das penalidades administrativas previstas na legislação[9].

Nessas situações, o tratamento de dados pessoais é necessário para atender a uma regra específica, ou seja, uma determinação legal expressa ou uma obrigação de natureza regulatória estabelecida por um órgão regulador. Não há, por isso, um vínculo necessário e direto entre o tratamento de dados e o exercício de atribuições e competências legais do controlador.

Já na segunda hipótese, a obrigação legal decorre de normas de organização, assim entendidas as normas que estruturam órgãos e entidades e estabelecem suas competências e atribuições[10]. Nesse contexto normativo, o tratamento de dados pessoais é parte essencial do exercício de prerrogativas estatais típicas, uma vez que necessário para viabilizar a própria execução das atribuições, competências e finalidades públicas da entidade ou do órgão público.

Assim, diferentemente das normas de conduta, que estabelecem obrigações de forma direta e expressa, prevendo uma consequência específica em caso de descumprimento, as normas de organização estabelecem obrigações que estão associadas, de forma mais geral, ao próprio cumprimento e à execução de atribuições legais típicas da entidade ou do órgão público responsável pelo tratamento de dados pessoais.

Vale ressaltar que essa interpretação do conceito de obrigação legal, conforme previsto no art. 7º, ii, e no art. 11, ii, a, da Lgpd, é reforçada pelo disposto no art. 23 da mesma lei, segundo o qual o tratamento de dados pessoais no setor público deverá ser realizado “com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público”, observando-se o interesse público e o atendimento da finalidade pública do controlador.

29. Além do tratamento de dados para o cumprimento de obrigação legal ou regulatória, outra hipótese de tratamento é o realizado pela Administração Pública "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, observadas as disposições do Capítulo IV desta Lei".

30. Parece-nos que o tratamento de dados pessoais realizado pela Administração, por meio do ALICE, seria também, para uma das políticas públicas levadas a efeito pelo Estado brasileiro, qual seja, a prevenção e combate a fraudes e à corrupção^[6], o exercício do controle interno pelo Poder Executivo^[7], controle da legalidade da gestão orçamentárias, financeira e patrimonial do Poder Executivo^[8] e, ao fim e ao cabo, a melhor execução da despesa pública, com a entrega eficaz do produto do orçamento à população por meio de um processo licitatório livre de irregularidades.

2.1.3. ESPECIFICAÇÃO DO OBJETO E FINALIDADE DO TRATAMENTO DE DADOS.

31. É importante que reste claro no processo que definirá a utilização do sistema ALICE quais serão, nominalmente, os dados que deverão ser objeto de compartilhamento e tratamento. Além disso, como já falado, a finalidade do compartilhamento deve ser específica, com a indicação das finalidades para as quais o compartilhamento será executado. Nesse sentido é o Guia Orientativo de Tratamento de Dados Pessoais da ANPD. Vejamos:

Deve ficar claro, em suma, quais dados pessoais serão compartilhados, bem como por que e para que serão compartilhados. Por exemplo, o ato formal pode prever que “serão compartilhados com a Entidade Pública x os

dados pessoais que constam da base de dados do Órgão Público y, consistentes em nome, CPF e endereço residencial, para a finalidade específica de realização de cadastro e identificação de cidadãos aptos ao recebimento do benefício social de que trata a Lei nº XYZ”.

32. Nesse mesmo sentido, já se posicionou a Consultoria-Geral da União, por meio do PARECER n. 00009/2022/DECOR/CGU/AGU, nos seguintes termos:

IV. O tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá guardar compatibilidade com a finalidade específica informada ao titular para o fornecimento dos dados (art. 6º) e “deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público” (art. 23)

33. Dessa forma, sugere-se a confecção nos autos de nota técnica que **analise de forma completa, enumerando-se especificamente quais os dados pessoais serão compartilhados, qual a razão do compartilhamento e para quem serão compartilhados**. Pelo que se depreendeu da NOTA TÉCNICA Nº 2190/2023/CGGE/SE, houve o esclarecimento a esse respeito em reuniões específicas, mas as características de atuação do sistema e quais seriam especificamente os dados, não constaram, salvo melhor juízo, em nota técnica específica.

2.2. CAUTELAS PREVISTAS NA LGPD PARA O TRATAMENTO DE DADOS PELO PODER PÚBLICO.

2.2.1. DA NECESSÁRIA TRANSPARÊNCIA AO TRATAMENTO DE DADOS A SER REALIZADO PELO SISTEMA ALICE.

34. A LGPD destina um capítulo - Capítulo IV - específico para o tratamento de dados pessoais pelo Poder Público. Mais precisamente, no artigo 23, são apresentadas as condições para o compartilhamento de dados pelas pessoas jurídicas de direito público. Vejamos as disposições do referido artigo:

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do [art. 1º da Lei nº 12.527, de 18 de novembro de 2011 \(Lei de Acesso à Informação\)](#), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - 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, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II - (VETADO); e

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

IV - (VETADO). [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a [Lei nº 12.527, de 18 de novembro de 2011 \(Lei de Acesso à Informação\)](#).

§ 3º 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 \(Lei de Acesso à Informação\)](#).

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

35. O artigo 23 da LGPD, portanto, define os requisitos para o tratamento de dados pessoais pela Administração Pública, estabelecendo que sejam informadas ao público as hipóteses em que os órgãos e entidades públicas realizam o tratamento dos dados pessoais, fornecendo “informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos”.

36. Portanto, a LGPD estabelece a **transparência no tratamento de dados pessoais**, ao determinar que o Poder Público informe as hipóteses em que realiza o tratamento de dados e que referida informação seja dada preferencialmente em seu sítio eletrônico. Vejamos o ensinamento da doutrina de Fernando Antônio Tasso^[9]:

O inciso I consagra a necessária transparência no tratamento de dados pessoais pelo Poder Público, ecoando o princípio da transparência²⁵ que permeia, juntamente dos outros nove, todas as operações de tratamento de dados pessoais e dados sensíveis. No contexto de uma relação assimétrica de poder, como a que caracteriza a estabelecida entre o poder público e o indivíduo, a transparência visa a inspirar no titular de dados a credibilidade no ente público controlador dos dados e a necessária responsabilidade a que está submetido, numa clara relação com um princípio peculiar da lei protetiva nacional²⁶, o da responsabilização e prestação de contas²⁷.

Determina que, ao fazê-lo, o ente público enuncie as hipóteses de tratamento, em expressa correspondência ao respaldo de investidura legal (exercício de suas competências). A existência de hipótese de tratamento consiste em clara remissão ao princípio maior da legalidade administrativa previsto na Constituição Federal.

São requisitos legais que tais informações sejam disponibilizadas de forma clara, atualizada e de fácil acesso, preferencialmente nos sítios eletrônicos dos entes administrativos. Denota-se o comprometimento da lei com a chamada publicidade real ou material, em contraposição à mera publicidade ficta ou formal, de modo a dar concretude aos princípios constitucionais da moralidade e eficiência, positivados no artigo 37 da Constituição

Federal.

37. Portanto, em obediência ao artigo 23, inciso I, da LGPD a Controladoria-Geral da União, como gestora do ALICE, deve informar em seu site que o referido sistema realiza o tratamento de dados pessoais, com informações sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades. Vejamos, também nesse sentido, o teor do Guia Orientativo para Tratamento de Dados Pessoais pelo poder Público, da ANPD¹⁰:

Em complemento a essas disposições gerais, a LGPD prevê o dever de publicidade em relação aos tratamentos realizados pelo Poder Público. Nesse sentido, os órgãos e entidades devem fornecer “informações claras e atualizadas sobre a previsão legal, finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades”, nos termos do art. 23, I. Tais informações devem estar em meios de fácil acesso, preferencialmente em sítios eletrônicos. Nos termos do art. 23, § 1º, da LGPD, a ANPD poderá dispor sobre as formas de publicidade das operações de tratamento[14].

Demonstrando a importância da publicidade no setor público, o art. 25 da LGPD prevê também que os dados devem ser mantidos “em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas”, visando, entre outras finalidades, “à disseminação e ao acesso das informações pelo público em geral”, sem, contudo, que deixem de ser observados os princípios que asseguram a proteção dos dados pessoais e a privacidade dos seus titulares.

As informações exigidas pela LGPD devem ser disponibilizadas de forma clara, adequada e ostensiva, em linguagem simples e acessível, de modo a assegurar o efetivo conhecimento do titular a respeito das atividades de tratamento realizadas pelo controlador, bem como sobre os seus direitos e a forma de exercê-los. Nesse sentido, constitui uma boa prática a disponibilização dessas informações na página eletrônica do órgão ou entidade responsável, da qual podem constar seções específicas relacionadas à “Lei Geral de Proteção de Dados Pessoais” e documentos como política de privacidade ou equivalente.

Exemplo 10

Princípio da transparência no setor público Uma pessoa tem seus dados coletados pela recepção de um órgão público para fins de segurança patrimonial e dos servidores. Para atender a outros dispositivos legais e dar publicidade a atos do órgão, caso essa pessoa realize uma reunião com uma autoridade, seu nome poderá ser divulgado na agenda pública da autoridade, salvo eventual restrição legal.

Em geral, essa pessoa deverá ser informada das finalidades que justificam a coleta e o tratamento, incluindo a de que parte ou a totalidade deles poderá ser divulgada para atender normas específicas que tratem de divulgação de agenda pública. Entre outras possibilidades, essas informações podem constar da política de privacidade ou documento equivalente, disponibilizado na página do órgão público na internet.

38. O Supremo Tribunal Federal, no mesmo sentido e em importante precedente, também estabeleceu a mesma exigência de transparência para o tratamento de dados pessoais. Vejamos:

Ementa: DIREITO CONSTITUCIONAL. DIREITOS FUNDAMENTAIS À PRIVACIDADE E AO LIVRE DESENVOLVIMENTO DA PERSONALIDADE. TRATAMENTO DE DADOS PESSOAIS PELO ESTADO BRASILEIRO. COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. ADI E ADPF CONHECIDAS E, NO MÉRITO, JULGADAS PARCIALMENTE PROCEDENTES. INTERPRETAÇÃO CONFORME À CONSTITUIÇÃO. DECLARAÇÃO DE INCONSTITUCIONALIDADE COM EFEITOS FUTUROS. [...] 4. Interpretação conforme à Constituição para subtrair do campo semântico da norma eventuais aplicações ou interpretações que conflitem com o direito fundamental à proteção de dados pessoais. **O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público.** 5. **O compartilhamento de dados pessoais entre órgãos públicos pressupõe rigorosa observância do art. 23, inciso I, da Lei 13.709/2018, que determina seja dada a devida publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco de dados pessoais, “fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos”.** [...] (ADI 6649, Relator(a): GILMAR MENDES, Tribunal Pleno, julgado em 15/09/2022, PROCESSO ELETRÔNICO DJe-s/n DIVULG 16-06-2023 PUBLIC 19-06-2023)

39. Importante ressaltar, nesse ponto, que a Lei de Governo Digital também exigiu os mesmos cuidados, em relação à transparência do poder público no tratamento dos dados pessoais. Vejamos o que diz a Lei nº 14.129, de 29 de março de 2021:

Art. 25. As Plataformas de Governo Digital devem dispor de ferramentas de transparência e de controle do tratamento de dados pessoais que sejam claras e facilmente acessíveis e que permitam ao cidadão o exercício dos direitos previstos na [Lei nº 13.709, de 14 de agosto de 2018](#) (Lei Geral de Proteção de Dados Pessoais).

§ 1º As ferramentas previstas no caput deste artigo devem:

I - disponibilizar, entre outras, as fontes dos dados pessoais, a finalidade específica do seu tratamento pelo respectivo órgão ou ente e a indicação de outros órgãos ou entes com os quais é realizado o uso compartilhado de dados pessoais, incluído o histórico de acesso ou uso compartilhado, ressalvados os casos previstos no [inciso III do caput do art. 4º da Lei nº 13.709, de 14 de agosto de 2018](#) (Lei Geral de Proteção de Dados Pessoais);

II - permitir que o cidadão efetue requisições ao órgão ou à entidade controladora dos seus dados, especialmente aquelas previstas no [art. 18 da Lei nº 13.709, de 14 de agosto de 2018](#) (Lei Geral de Proteção de Dados Pessoais).

§ 2º A Autoridade Nacional de Proteção de Dados (ANPD) poderá editar normas complementares para regulamentar o disposto neste artigo.

40. A transparência para o tratamento de dados pessoais também foi determinada pelo artigo 31 da Lei de Acesso à Informação.

41. Consignada, portanto, a necessidade de transparência, pela CGU, acerca do tratamento dos dados pessoais pelo ALICE, passemos à próxima cautela a ser tomada pelo órgão de controle interno.

2.2.2. NECESSIDADE DE INDICAÇÃO DO ENCARREGADO, NA FORMA DO ARTIGO 23, INCISO III, DA LGPD. ENCARREGADO DE DADOS DA CONTROLADORIA-GERAL DA UNIÃO JÁ É CONHECIDO E DIVULGADO.

42. O art. 23, inciso III, da LGPD, exige, como um dos requisitos para o tratamento de dados pessoais pelo Poder Público, o apontamento da figura do encarregado de dados. Na Controladoria-Geral da União, o encarregado de dados é o senhor Secretário-Executivo Adjunto^[11].

43. No site da CGU, também constam, conforme exigência da LGPD, o nome, cargo, endereço e contato do encarregado. Além disso, também no site da CGU, constam suas atribuições, replicando-se o parágrafo 2º, do artigo 41, da LGPD. Vejamos:

O Encarregado de Dados Pessoais da CGU atua como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Além de outras atribuições que venham a ser estabelecidas pela ANPD em normas complementares, o encarregado desenvolve, em observância ao § 2º do art. 41 da LGPD, as seguintes atividades:

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

44. Apresentados os requisitos para o tratamento de dados pessoais, passemos à figura dos agentes de tratamento, controlador e operador.

2.2.3. DOS AGENTES DE TRATAMENTO. DAS FIGURAS DO CONTROLADOR E DO OPERADOR.

45. A LGPD estabelece as funções do operador e do controlador da seguinte maneira:

Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

46. Por outro lado, no caso do Sistema ALICE, primeiramente é necessário definir quem seria(m) o(s) controlador(es) e operador(es) para fins da LGPD.

47. Induvidosamente, parece-nos que, para os fins do sistema ALICE, o controlador dos dados será a CGU, órgão representativo da desconcentração da Administração da União, pessoa jurídica de direito público. Nesse sentido é o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado^[12]

20. Nesses casos, deve-se considerar dois aspectos centrais. De um lado, conforme o art. 5º, VI, da LGPD, o controlador é a União, pessoa jurídica de direito público que, em última análise, é a responsável pelas obrigações decorrentes da lei, de instrumentos contratuais ou de atos ilícitos praticados pelos seus órgãos e servidores.

21. De outro lado, a LGPD atribuiu aos órgãos públicos obrigações típicas de controlador, indicando que, no setor público, essas obrigações devem ser distribuídas entre as principais unidades administrativas despersonalizadas que integram a pessoa jurídica de direito público e realizam tratamento de dados pessoais.

22. Nesse sentido, a União, como controladora, é a responsável perante a LGPD, mas as atribuições de controlador, por força da desconcentração administrativa, são exercidas pelos órgãos públicos que desempenham funções em nome da pessoa jurídica da qual fazem parte, fenômeno que caracteriza a distribuição interna das competências. É o que se verifica nas hipóteses de uso compartilhado de dados pessoais (art. 26), de atendimento às exigências da ANPD (art. 2911) e de aplicação de sanções administrativas (art. 52, § 3º).

48. Em relação ao conceito de operador para fins de LGPD, necessário consultarmos o Guia Orientativo para

Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, que traz o conceito de "operador". Vejamos:

56. De acordo com a LGPD, pessoas físicas e jurídicas de direito público e privado podem atuar como operadoras. Na maior parte das vezes, o operador é uma pessoa jurídica, que é contratada pelo controlador para realizar o tratamento de dados, conforme as instruções deste último. Contudo, não há óbices para que uma pessoa natural contratada como prestadora de serviços para uma finalidade específica possa ser considerada operadora de dados.

57. Em caso de pessoa jurídica, importa destacar que a organização ou empresa é entendida como agente de tratamento, de forma que seus funcionários apenas a representam. Assim como explicado no tópico 2.2 e de forma análoga à definição de controlador, a definição legal de operador também não deve ser entendida como uma norma de distribuição interna de competências e responsabilidades.

58. Nesse cenário, empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta não devem ser considerados operadores, tendo em vista que o operador será sempre uma pessoa distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de seus órgãos.

49. Ainda de acordo com o referido Guia Orientativo^[13], não é possível que um servidor público seja considerado operador para os fins da LGPD. De acordo com o referido documento, somente uma pessoa física ou jurídica contratada pela Administração e que realize o tratamento de dados em determinada tarefa poderia ser considerado operador. Com efeito, segundo a ANPD, o operador será sempre uma pessoa distinta do controlador, ou seja, deve ser pessoa "que não atua como profissional subordinado a este ou como membro de seus órgãos.". Nesse sentido é o "Exemplo 10" constante no referido Guia Orientativo:

Exemplo 10 - Servidores públicos

Uma autarquia, entidade da administração pública indireta, com personalidade jurídica própria, deseja utilizar um novo software para aprimorar o gerenciamento dos funcionários da instituição. Para isso, a Secretaria de Gestão Corporativa da entidade delega à Diretoria de Gestão de Pessoas(DGP) a tarefa de determinar os meios pelos quais este software será implementado. Após algumas reuniões, a DGP decide pela contratação da empresa terceirizada SIERRA para desenvolver o software em parceria com a equipe interna da Diretoria de Tecnologia da Informação (DTI).

Embora a delegação de decisão quanto aos meios para a DGP possa sugerir que essa diretoria atue como operadora de dados, esta não é a análise correta: como a DGP é uma unidade administrativa da autarquia, a delegação interna não altera o papel do agente de tratamento., uma vez que, como exposto, o operador será sempre pessoa distinta do controlador. O mesmo raciocínio se aplica para a DTI. Desse modo, a autarquia será a controladora de dados e a empresa SIERRA será a operadora de dados. A Secretaria e as Diretorias, assim como os seus respectivos servidores, são apenas unidades organizacionais do ente controlador de dados, razão pela qual não se caracterizam como agentes de tratamento.

50. Dessa forma, entendemos que os servidores públicos que receberão os "alertas" do ALICE não serão operadores para os fins da LGPD, mesmo não tendo hierarquia com a Controladoria-Geral da União. Isto porque, ao fim e ao cabo, o controlador seria a própria União (o que inclui seus servidores) havendo a distribuição da figura de controlador entre os órgãos apenas para fins de desconcentração administrativa.

51. Portanto, os servidores que receberão os alertas serão agentes do controlador, no caso, a União, por meio da CGU. Por isso, deverão guardar as obrigações de controlador e receberem, antes de terem acesso ao sistema ALICE, advertências sobre essa qualidade de agentes do controlador. Nesse caso, mesmo eles não sendo servidores com relação de hierarquia com a CGU, deverão ser considerados como representantes do controlador (no caso, a CGU apresentando a União).

52. Por outro lado, em contato com a SFC/CGU, nos foi informado que para a operação do sistema ALICE não haveria nenhuma empresa contratada pela CGU ou outro terceiro. Portanto, para a operação do sistema ALICE, não haveria a figura do operador para fins da LGPD.

53. A doutrina de Rony Vainzof^{[14][15]} define o conceito de controlador para os fins da LGPD. Vejamos o conceito de controlador, bem como as obrigações constantes na LGPD que, no que couber, se aplicam a ele:

Serão tratados os dois conceitos conjuntamente visando facilitar o entendimento das obrigações e responsabilidades. É sobre o **controlador** que a LGPD impõe o seu maior peso jurídico, pois é ele o responsável pela tomada de decisões sobre o tratamento de dados pessoais. De igual forma, definir quem é o controlador em cada caso concreto é fundamental para que a LGPD seja devidamente cumprida na prática, afinal de contas, será ele que:

- Deve avaliar o enquadramento de ao menos uma das bases legais para a realização de cada tratamento de dados pessoais^[16];
- Deve acompanhar o ciclo de vida completo dos dados, descartando-os ou determinado o descarte quando do término do tratamento;
- Deve indicar o encarregado^[17];
- É competente pela elaboração do relatório de impacto à proteção de dados pessoais^[18];
- Cabe o ônus da prova sobre o consentimento do titular^[19];
- Deve cumprir os direitos dos titulares^[20];
- Deve manter registro das operações de tratamento de dados pessoais^[21];
- Deve demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas^[22];
- Deve transmitir as instruções para o tratamento de dados quando resolver envolver um operador^[23];

- Será responsabilizado civilmente, no caso de violação à LGPD^[24];
- Será sancionado administrativamente em razão de infrações cometidas às normas previstas na LGPD^[25];
- Deve comunicar a ANPD e ao titular sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares^[26];
- Deve formular e empregar regras de boas práticas e governança em proteção de dados pessoais, levando em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular^[27];
- Deve 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^[28];
- Deve prestar informações quando solicitadas pela ANPD^[29].

[...]

Assim, definir quem é o controlador e o operador em cada caso é imprescindível, mas pode ser tarefa complexa, pois, devido à evolução da tecnologia da informação e da comunicação e à tendência de entidades serem e proverem serviços multidisciplinares, por vezes, haverá situações em que uma mesma pessoa jurídica será controladora e operadora.

Porém, para o titular e para a ANPD não pode haver dúvidas. Por isso, o controlador deverá se identificar, com informações de contato, perante o titular dos dados, de forma facilitada, clara, adequada e ostensiva, além de prestar informações sobre o tratamento dos dados, como a finalidade específica do tratamento, forma e duração; e informações acerca do uso compartilhado de dados e a finalidade.

O conceito de controlador contempla absolutamente todas as decisões sobre as atividades que refletem o ciclo de vida dos dados pessoais. Desde o projeto, passando pela coleta ou recepção, todas as formas de processamento, até o descarte. As seguintes perguntas podem contribuir para a identificação do controlador: qual o motivo de determinado tratamento de dado estar ocorrendo? Quem teve essa ideia? Quem efetivamente deu início a qualquer uma das hipóteses previstas de tratamento?

Mesmo em casos nos quais o controlador não se identifica como tal e executa o tratamento de dados sem cumprir quaisquer dos fundamentos e princípios estabelecidos pela LGPD, identificá-lo é crucial para a execução do devido processo legal e eventuais sanções, como ocorreu no já mencionado caso Tudo sobre Todos.

O Art. 29 WP, em sua *Opinion* 1/2010, traz algumas considerações e divisões relevantes para identificação do controlador:

- Controlador decorrente de competência legal explícita, seja no caso de qualquer legislação nomear expressamente um controlador, seja no caso de prever determinadas tarefas que envolvam tratamento de dados sem o definir. Por exemplo, o dever de guarda de determinados dados pessoais decorrente de obrigação legal impõe que determinadas entidades sejam controladoras desses dados, mesmo que não nomeadas em lei;**
- Controlador decorrente de competência legal implícita: decorre normalmente de disposições legais comuns a diversas áreas, como Direito Civil e Direito do Trabalho, em que as funções usuais das entidades determinam quem é o controlador, como uma editora que trata os dados dos seus clientes ou uma empresa que trata os dados dos seus funcionários. São atividades do controlador naturalmente vinculadas ao seu papel funcional;
- Controlador oriundo de uma influência concreta: quando há a necessidade de ser analisada as circunstâncias do caso em concreto, como na avaliação das cláusulas contratuais entre as diferentes partes envolvidas, visando identificar qual a real atividade de cada uma delas no tratamento de dados, grau de controle e quem exerce o papel dominante na tomada de decisões. Os termos do contrato podem ajudar a identificar o controlador, mas não necessariamente será o fator determinante, pois podem não corresponder com a realidade.

54. Não obstante os gestores que receberão os alertas do sistema ALICE não serem considerados operadores, serão agentes do controlador, razão pela qual recomenda-se que **cada gestor que utilizará o Sistema ALICE manifeste ciência, por meio do próprio sistema ou por outro meio**, de que terá acesso a dados pessoais, pois atuarão como representantes do controlador.

55. Portanto, depreendemos da consulta que os gestores públicos do Portal de Compras do Governo Federal (Comprasnet), mesmo que recebam apenas um "alerta" do sistema ALICE, serão considerados como representantes da CGU (agentes do controlador) para os fins da LGPD, na medida em que receberão os dados e, com isso, efetuarão tratamento, na forma do artigo 5º, inciso X, da LGPD. Além disso, conforme Cláusula Oitava do ACORDO DE COOPERAÇÃO TÉCNICA CGU/SEGES-ME Nº 135/2021 (SEI 2037507) será possível a consulta ao sistema pelos gestores públicos, o que também coloca os gestores na condição de agentes do controlador.

56. Não se pode esquecer que a primeira obrigação do controlador consta no artigo 37 da LGPD. Trata-se da obrigação de manutenção de registro das operações de tratamento de dados pessoais realizadas. Dessa forma, recomenda-se que a Controladoria-Geral da União, na condição de controlador, por meio do sistema o ALICE, preserve o registro em arquivo de cada tratamento realizado (cada compartilhamento feito pelo sistema), no sistema ou em outro banco de dados acessível.

57. Por fim, ainda em relação aos agentes de tratamento, deve-se seguir a recomendação constante na LGPD e no PARECER n. 00009/2022/DECOR/CGU/AGU, da Consultoria-Geral da União, no seguinte sentido:

VI. Os atos da Administração Pública são regidos pelo princípio da publicidade (CRFB/88, art. 37, c/c §3º, art. 3º, da Lei n.º 8.666/93). Assim, *"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."* (art. 46), *"com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."*(art. 1º)

58. Enfrentada a questão dos agentes de tratamento, passemos à duração do tratamento de dados.

2.2.4. DEFINIÇÃO DA DURAÇÃO DO TRATAMENTO DE DADOS.

59. Em relação à duração do tratamento (do compartilhamento), importante estabelecer um prazo para a **eliminação** dos dados. Cabe, portanto, à gestão da CGU, de acordo com sua conveniência e oportunidade, que somente poderá ser percebida por meio do profundo conhecimento do sistema, que escapa deste parecerista, o melhor prazo e a melhor maneira para se definir a eliminação dos dados.

60. O fato é que o artigo 16 da LGPD define como regra a eliminação dos dados pessoais após o término do tratamento, estabelecendo exceções nas quais os dados podem ser conservados. Dentre os casos em que é autorizada a conservação está o cumprimento de obrigação legal ou regulatória pelo controlador, justamente a hipótese de tratamento de dados realizado pelo ALICE. Vejamos:

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais **serão eliminados** após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. (destacamos)

61. Assim, deve-se estabelecer um prazo para a eliminação dos dados pessoais tratados por meio do sistema ALICE. Tal prazo deve estar de acordo com as necessidades administrativas que deram origem ao tratamento. Portanto, se o tratamento deu-se em razão do exercício de uma competência ou obrigação legal, os dados serão preservados enquanto ainda forem essenciais para o exercício dessa competência e tal avaliação deve ser feita em cada caso concreto.

2.2.5. FORMALIZAÇÃO E REGISTRO DO TRATAMENTO.

62. O Guia Orientativo para Tratamento de Dados Pessoais pelo Poder Público da ANPD também sugere a formalização e o registro do referido tratamento. Vejamos:

Além disso, recomenda-se que o compartilhamento seja estabelecido em ato formal, a exemplo de contratos, convênios ou instrumentos congêneres firmados entre as partes. Outra possibilidade é a expedição de decisão administrativa pela autoridade competente, que autorize o acesso aos dados e estabeleça os requisitos definidos como condição para o compartilhamento.

Especialmente nos casos em que o órgão ou a entidade pública compartilha dados pessoais com frequência, sugere-se avaliar a conveniência de editar ato normativo interno, a exemplo de portarias e instruções normativas, com o objetivo de, além de proporcionar o devido formalismo, conferir maior padronização e celeridade a essas operações. O ato normativo pode, por exemplo, definir competências e estabelecer procedimentos, prazos e requisitos essenciais a serem observados nos processos de compartilhamento.

63. No caso do sistema ALICE, parece-nos que tal formalização foi realizada por meio do Acordo de Cooperação Técnica CGU/SEGES-ME nº 135/2021 (SEI [2037507](#)), no qual foram delimitados os deveres e responsabilidades dos partícipes. No entanto, verifica-se que no acordo de cooperação não há a indicação com detalhes de quais dados serão tratados, nem estão registradas as cautelas específicas para o compartilhamento.

64. Portanto, recomenda-se a elaboração de documento em que constem: a enumeração dos dados efetivamente tratados, com a hipótese legal do tratamento; como será realizado o tratamento e onde serão publicadas as informações sobre o tratamento.

2.2.6. DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS EM RELAÇÃO À UTILIZAÇÃO DO SISTEMA ALICE.

65. Recomenda-se, por cautela, ainda, a elaboração de Relatório de Impacto à Proteção de Dados Pessoais para a utilização do Sistema ALICE. O relatório é previsto no artigo 5º, inciso XVII, da LGPD que o define como sendo a "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco."

66. O Guia Orientativo para Tratamento de Dados Pessoais pelo Poder Público sugere a avaliação do gestor público, em cada caso concreto, acerca da necessidade de elaboração do relatório para o tratamento de dados pessoais pelo Poder Público. Vejamos:

A elaboração de relatório de impacto à proteção de dados pessoais pode auxiliar a motivação da decisão a ser proferida pela autoridade competente, além de fortalecer a sua conformidade com a legislação de proteção de

dados pessoais. A avaliação quanto à necessidade de elaboração do documento deve considerar as peculiaridades do caso concreto, em particular, a existência de riscos às liberdades civis e aos direitos fundamentais dos cidadãos, observado o disposto nos art. 5º, xvii e no art. 38 da LGPD.

67. Como se trata de um sistema que, presumo, realizará grande volume de compartilhamento de dados e durante um período duradouro, entendemos como necessária a elaboração do referido relatório.

3. CONCLUSÃO

68. Diante do exposto e do que dos autos consta, abstraídos os aspectos de conveniência e oportunidade da consulta, opinamos pela possibilidade de tratamento de dados pela Administração Pública em decorrência da utilização do Sistema ALICE e de sua base de dados, independentemente do consentimento dos titulares, na forma do artigo 7º, incisos II e III, da LGPD.

69. Contudo, a LGPD estabelece diversas cautelas a serem seguidas pelo Poder Público para o tratamento de dados pessoais. Além da obediência aos princípios contidos no artigo 6º da LGPD, as cautelas indicadas a seguir devem ser seguidas no manejo do sistema ALICE pela CGU:

a) limitação do compartilhamento ao mínimo necessário para a execução da obrigação legal ou política pública e que o referido compartilhamento seja, para fins do artigo 4º do Decreto nº 10.046, de 2019, o compartilhamento específico;

b) a identificação dos servidores públicos que receberão os alertas do sistema ALICE, por meio do próprio sistema ou por outro meio, de que terão acesso a dados pessoais. Referida identificação deve ser feita de maneira prévia ao acesso e de forma que conste a necessidade de resguardo, proteção e manutenção do sigilo dos dados pessoais. Além disso, devem ter ciência da necessidade de preservação da intimidade e da privacidade da pessoa natural e da proteção dos dados;

c) a identificação dos servidores públicos que receberão os alertas do sistema ALICE de que: *"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."* (art. 46), *"com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."*(art. 1º)

d) a confecção nos autos de nota técnica ou complementação da NOTA TÉCNICA Nº 2190/2023/CGGE/SE que analise de forma completa quais os dados pessoais serão compartilhados e qual a razão do compartilhamento. Pelo que se depreendeu da NOTA TÉCNICA Nº 2190/2023/CGGE/SE, houve o esclarecimento a esse respeito em reuniões específicas, mas as características de atuação do sistema e quais seriam especificamente os dados, não constaram de nota técnica específica;

e) na nota técnica sugerida no item anterior, recomenda-se que constem as informações sobre como será realizada a operação de tratamento e onde serão publicadas as informações sobre o tratamento no site da CGU;

f) publicação no site da CGU da informação de que o sistema ALICE realiza o tratamento de dados pessoais, com informações sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades;

g) recomenda-se que o ALICE preserve o registro em arquivo de cada tratamento realizado no sistema ou em outro banco de dados acessível, em nome do controlador;

h) estabelecimento de um prazo para a eliminação dos dados pelo Sistema ALICE. Cabe, portanto, à gestão da CGU, de acordo com sua conveniência e oportunidade, que somente poderá ser percebida por meio do profundo conhecimento do sistema, que escapa deste parecerista, o melhor prazo e a melhor maneira para se definir a eliminação dos dados. Recomenda-se, nesse ponto, a utilização de prazos prescricionais previsto na legislação anticorrupção e de correição;

i) recomenda-se, por fim, a elaboração de Relatório de Impacto à Proteção de Dados Pessoais, pois o ALICE será um sistema que realizará grande volume de compartilhamento de dados e durante um período duradouro.

À consideração superior.

Brasília, data da assinatura eletrônica.

[Documento assinado eletronicamente]
ANTONIO DAVID GUERRA ROLIM DE OLIVEIRA
ADVOGADO DA UNIÃO

Atenção, a consulta ao processo eletrônico está disponível em <https://supersapiens.agu.gov.br> mediante o fornecimento do Número Único de Protocolo (NUP) 00190105207202384 e da chave de acesso 9fa840ae

Notas

1. [^] Especificamente sobre o número *SIAPE*, esta Consultoria Jurídica junto à Controladoria-Geral da União já se manifestou, por meio do *PARECER n. 00001/2021/CONJUR-CGU/CGU/AGU*, no seguinte sentido: "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. O número SIAPE diz respeito à matrícula que identifica o servidor público no órgão em que desempenha suas atividades, e, embora se enquadre na definição de dado pessoal, à luz da LGPD, não possui repercussões para além da vida pública do servidor, não havendo razões para que esse dado tenha restrição de acesso."

2. [^] A desnecessidade de consentimento pelo titular no caso analisado também é corroborada pelo artigo 31, parágrafo 3º, inciso V, da Lei de Acesso à Informação, que dispensa o consentimento do titular para o acesso às informações pessoais quando forem necessárias à proteção do interesse público e geral preponderante.
3. [^] Maldonado, Viviane Nóbrega; Blum, Renato Opice. LGPD : Lei Geral de Proteção de Dados Pessoais comentada (p. 191). Edição do Kindle.
4. [^] Maldonado, Viviane Nóbrega; Blum, Renato Opice. LGPD : Lei Geral de Proteção de Dados Pessoais comentada (Portuguese Edition) (p. 195). Edição do Kindle.
5. [^] Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 22.8.2023.
6. [^] Artigo 49, inciso VI, da Lei nº 14.600, de 19 de junho de 2023.
7. [^] Artigo 70 da Constituição Federal.
8. [^] Artigo 74 da Constituição Federal.
9. [^] Maldonado, Viviane Nóbrega; Blum, Renato Opice. LGPD : Lei Geral de Proteção de Dados Pessoais comentada (Portuguese Edition) (pp. 269-270). Edição do Kindle.
10. [^] Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 22.8.2023
11. [^] Disponível em: <https://www.gov.br/cgu/pt-br/acesso-a-informacao/privacidade-e-protecao-de-dados/encarregado-de-dados-pessoais-na-cgu>. Acesso em: 30.8.2023.
12. [^] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 28.8.2023.
13. [^] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 30.8.2023.
14. [^] Maldonado, Viviane Nóbrega; Blum, Renato Opice. LGPD : Lei Geral de Proteção de Dados Pessoais comentada (Portuguese Edition) (p. 111-114). Edição do Kindle.
15. [^] As notas de rodapé inseridas pelo parecerista no texto colacionado foram elaboradas pelo autor.
16. [^] Art. 7º, da LGPD, para dados pessoais, e art. 11 para dados pessoais sensíveis.
17. [^] Art. 5º, inciso VIII, e art. 41, caput, da LGPD.
18. [^] Art. 5º, inciso XVII, da LGPD.
19. [^] Art. 8º, parágrafo 2º, da LGPD.
20. [^] Art. 18, caput, da LGPD.
21. [^] Art. 37, da LGPD.
22. [^] Art. 6º, inciso X, da LGPD.
23. [^] Art. 39, da LGPD.
24. [^] Art. 42, caput, da LGPD.
25. [^] Art. 52, caput, da LGPD.
26. [^] Art. 48, caput, da LGPD.
27. [^] Art. 50, caput, da LGPD.
28. [^] Art. 46, caput, da LGPD.
29. [^] Art. 55-J, inciso IV, da LGPD.



Documento assinado eletronicamente por ANTONIO DAVID GUERRA ROLIM DE OLIVEIRA, com certificado A1 institucional (*.agu.gov.br), de acordo com os normativos legais aplicáveis. A conferência da autenticidade do documento está disponível com o código 1254963436 e chave de acesso 9fa840ae no endereço eletrônico <https://sapiens.agu.gov.br>. Informações adicionais: Signatário (a): ANTONIO DAVID GUERRA ROLIM DE OLIVEIRA, com certificado A1 institucional (*.agu.gov.br). Data e Hora: 31-08-2023 19:57. Número de Série: 51385880098497591760186147324. Emissor: Autoridade Certificadora do SERPRO SSLv1.



ADVOCACIA-GERAL DA UNIÃO
CONSULTORIA-GERAL DA UNIÃO
CONSULTORIA JURÍDICA JUNTO À CONTROLADORIA GERAL DA UNIÃO
COORDENAÇÃO-GERAL DE ASSUNTOS ESTRATÉGICOS
DESPACHO n. 00323/2023/CONJUR-CGU/CGU/AGU

NUP: 00190.105207/2023-84

INTERESSADOS: CONTROLADORIA-GERAL DA UNIÃO-CGU

ASSUNTOS: COMPRA E VENDA

1. Trata-se de consulta da Secretaria Federal de Controle Interno da Controladoria-Geral da União (SFC/CGU) acerca das repercussões do sistema ALICE - Analisador de Licitações, Contratos e Editais e os impactos em relação à Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709, de 14 de agosto de 2018.

2. Aprovo, por seus fundamentos fáticos e jurídicos, o **PARECER n. 00304/2023/CONJUR-CGU/CGU/AGU**, de autoria do Advogado da União ANTONIO DAVID GUERRA ROLIM DE OLIVEIRA, que opina pela possibilidade de tratamento de dados pela Administração Pública em decorrência da utilização do Sistema ALICE e de sua base de dados, independentemente do consentimento dos titulares, na forma do artigo 7º, incisos II e III, da LGPD.

3. Destacam-se as observações feitas pelo parecerista, acerca da observância dos princípios contidos no artigo 6º da LGPD, recomendando-se a adoção das seguintes cautelas:

a) limitação do compartilhamento ao mínimo necessário para a execução da obrigação legal ou política pública e que o referido compartilhamento seja, para fins do artigo 4º do Decreto nº 10.046, de 2019, o compartilhamento específico;

b) a identificação dos servidores públicos que receberão os alertas do sistema ALICE, por meio do próprio sistema ou por outro meio, de que terão acesso a dados pessoais. Referida identificação deve ser feita de maneira prévia ao acesso e de forma que conste a necessidade de resguardo, proteção e manutenção do sigilo dos dados pessoais. Além disso, devem ter ciência da necessidade de preservação da intimidade e da privacidade da pessoa natural e da proteção dos dados;

c) a identificação dos servidores públicos que receberão os alertas do sistema ALICE de que: *"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."* (art. 46), *"com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."*(art. 1º)

d) a confecção nos autos de nota técnica ou complementação da NOTA TÉCNICA Nº 2190/2023/CGGE/SE que analise de forma completa quais os dados pessoais serão compartilhados e qual a razão do compartilhamento. Pelo que se depreendeu da NOTA TÉCNICA Nº 2190/2023/CGGE/SE, houve o esclarecimento a esse respeito em reuniões específicas, mas as características de atuação do sistema e quais seriam especificamente os dados, não constaram de nota técnica específica;

e) na nota técnica sugerida no item anterior, recomenda-se que constem as informações sobre como será realizada a operação de tratamento e onde serão publicadas as informações sobre o tratamento no site da CGU;

f) publicação no site da CGU da informação de que o sistema ALICE realiza o tratamento de dados pessoais, com informações sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades;

g) recomenda-se que o ALICE preserve o registro em arquivo de cada tratamento realizado no sistema ou em outro banco de dados acessível, em nome do controlador;

h) estabelecimento de um prazo para a eliminação dos dados pelo Sistema ALICE. Cabe, portanto, à gestão da CGU, de acordo com sua conveniência e oportunidade, que somente poderá ser percebida por meio do profundo conhecimento do sistema, que escapa deste parecerista, o melhor prazo e a melhor maneira para se definir a eliminação dos dados. Recomenda-se, nesse ponto, a utilização de prazos prescricionais previsto na legislação anticorrupção e de correição; e

i) recomenda-se, por fim, a elaboração de Relatório de Impacto à Proteção de Dados Pessoais, pois o ALICE será um sistema que realizará grande volume de compartilhamento de dados e durante um período duradouro.

4. **Sugere-se a inclusão do parecer e demais despachos de aprovação na base de conhecimento da CGU.**

À consideração superior. Após, se aprovado, encaminhe-se à SFC.

Brasília, 01 de setembro de 2023.

JÔNITAS MATOS DOS SANTOS DUARTE
Advogado da União
Coordenador-Geral de Assuntos Estratégicos

Atenção, a consulta ao processo eletrônico está disponível em <https://supersapiens.agu.gov.br> mediante o fornecimento do Número Único de Protocolo (NUP) 00190105207202384 e da chave de acesso 9fa840ae



Documento assinado eletronicamente por JONITAS MATOS DOS SANTOS DUARTE, com certificado A1 institucional (*.agu.gov.br), de acordo com os normativos legais aplicáveis. A conferência da autenticidade do documento está disponível com o código 1270177410 e chave de acesso 9fa840ae no endereço eletrônico <https://sapiens.agu.gov.br>. Informações adicionais: Signatário (a): JONITAS MATOS DOS SANTOS DUARTE, com certificado A1 institucional (*.agu.gov.br). Data e Hora: 01-09-2023 14:10. Número de Série: 51385880098497591760186147324. Emissor: Autoridade Certificadora do SERPRO SSLv1.



ADVOCACIA-GERAL DA UNIÃO
CONSULTORIA-GERAL DA UNIÃO
CONSULTORIA JURÍDICA JUNTO À CONTROLADORIA GERAL DA UNIÃO
GABINETE

DESPACHO DE APROVAÇÃO n. 00265/2023/CONJUR-CGU/CGU/AGU

NUP: 00190.105207/2023-84

INTERESSADOS: CONTROLADORIA-GERAL DA UNIÃO-CGU

ASSUNTOS: COMPRA E VENDA

1. Concordo com os fundamentos, e, portanto, APROVO, nos termos do Despacho nº. 00323/2023/CONJUR-CGU/CGU/AGU, o Parecer nº. 00304/2023/CONJUR-CGU/CGU/AGU.

2. Ao Apoio Administrativo desta CONJUR, para trâmite via SEI à SFC.

3. Sugere-se a inclusão do parecer e demais despachos de aprovação na base de conhecimento da CGU.

Brasília, 07 de setembro de 2023.

FERNANDO BARBOSA BASTOS COSTA
CONSULTOR JURÍDICO/CGU

Atenção, a consulta ao processo eletrônico está disponível em <https://supersapiens.agu.gov.br> mediante o fornecimento do Número Único de Protocolo (NUP) 00190105207202384 e da chave de acesso 9fa840ae



Documento assinado eletronicamente por FERNANDO BARBOSA BASTOS COSTA, com certificado A1 institucional (*.agu.gov.br), de acordo com os normativos legais aplicáveis. A conferência da autenticidade do documento está disponível com o código 1275135133 e chave de acesso 9fa840ae no endereço eletrônico <https://sapiens.agu.gov.br>. Informações adicionais: Signatário (a): FERNANDO BARBOSA BASTOS COSTA, com certificado A1 institucional (*.agu.gov.br). Data e Hora: 07-09-2023 21:36. Número de Série: 51385880098497591760186147324. Emissor: Autoridade Certificadora do SERPRO SSLv1.
