

LEI GERAL DE PROTEÇÃO DE DADOS. DIFUSÃO DE DADOS DE SERVIDORES NO SISTEMA SGP-E. DIREITOS DOS TITULARES E DEVERES DO CONTROLADOR DE DADOS. DESCUMPRIMENTO, A *PRIORI*, DE DIRETRIZES DA LGPD POR PARTE DA SECRETARIA DE ESTADO DE ADMINISTRAÇÃO - SEA. RECOMENDAÇÃO DE QUE SEJA REQUERIDO À SEA ESCLARECIMENTOS A RESPEITO DA EXPOSIÇÃO DOS DADOS, DE ACORDO COM A LEI.

I – CONSULTA FORMULADA

O Sindicato dos Policiais Civis de Santa Catarina SINPOL-SC honra-nos com consulta jurídica acerca da legalidade da exposição de dados de servidores no sistema SGP-e, nos seguintes termos:

Boa Tarde,

Tenho um questionamento com relação ao SGP-e, em consulta realizada em diversos processos, ao lado do nome do interessado tem um icone azul, clicando voce terá acesso a todos os dados como, CPF, endereço residencial, telefone, e-mail.

Me informam através de chat do sistema SGP-e que esses dados migraram do sistema SIGRH, **questiono se isso é legal, todos nossos dados exposto num sistema amplamente utilizado por inumeras pessoas.**

E a Lei de Proteção de Dados? (Grifou-se)

A consulta será respondida com base na legislação vigente, bem como em diligências realizadas junto ao Centro de Informática e Automação do Estado de Santa Catarina e ao setor de Ciência de Dados da Secretaria de Estado de Administração – SEA.

II – FUNDAMENTOS

A Lei Geral de Proteção de Dados – LGPD (13.709/2018) entrou em vigor esse ano. Com o escopo de proteger direitos constitucionais de fundamental

importância, a LGPD regulamenta o tratamento de dados pessoais no território brasileiro, definindo questões como bases legais, atores envolvidos na proteção de dados e os princípios que a norteiam.

Referida lei terá um impacto colossal no universo jurídico pátrio, vez que, de acordo com o texto normativo, suas diretrizes deverão ser adotadas por qualquer pessoa, natural ou jurídica, de direito público ou privado, que pratiquem quaisquer modalidades de tratamento de dados pessoais (art. 1).

Desse modo, cabe ao Estado de Santa Catarina, na qualidade de pessoa jurídica de direito público e, mais ainda, de ente federativo (§ 1º do art. 1º), a observância da Lei n. 13.709/2018.

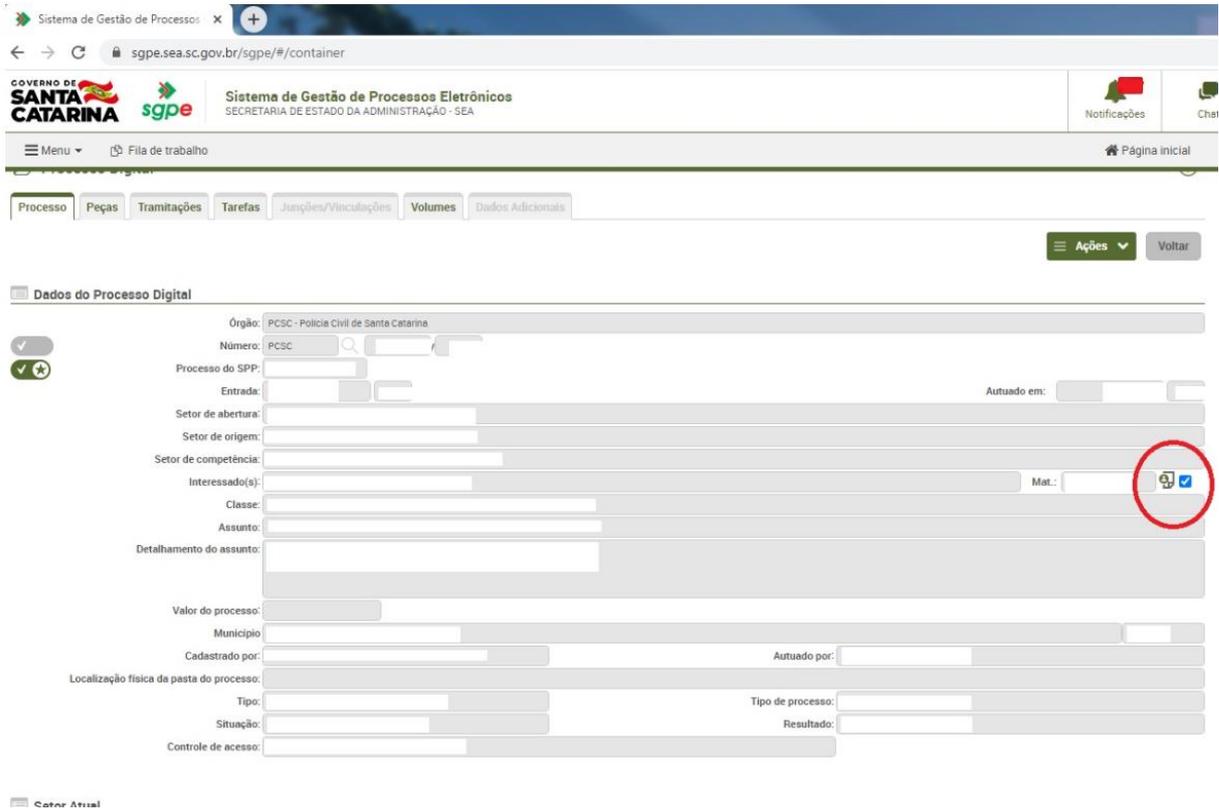
Imprescindível destacar que o fato de as sanções administrativas iniciarem somente em agosto de 2021 (art. 65, I-A, da LGPD) não constitui fator minorativo da necessidade de obediência à Lei, seja por parte do Estado, empresas, associações civis ou pessoas físicas que efetuarem tratamento de dados.

Isso porque, com a entrada em vigor da norma, os direitos e deveres nela elencados já produzem seus efeitos jurídicos que podem ser, inclusive, objeto de controle judicial.

Estabelecido que o Estado de Santa Catarina e seus órgãos submetem-se à LGPD quando procederem ao tratamento de dados, cumpre analisar a abrangência deste conceito, que abarca *“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”* (art. 5º, X, da LGPD).

Na hipótese em tela, os dados encontram-se expostos no sistema SGP-e ao

pesquisar qualquer processo administrativo, em cuja página de consulta aparece um ícone azul clicável:



Sistema de Gestão de Processos

sgpe.sea.sc.gov.br/sgpe/#/container

GOVERNO DE SANTA CATARINA sgpe Sistema de Gestão de Processos Eletrônicos SECRETARIA DE ESTADO DA ADMINISTRAÇÃO - SEA

Notificações Chat

Menu Fila de trabalho Página inicial

Processo Peças Tramitações Tarefas Junções/Vinculações Volumes Dados Adicionais

Ações Voltar

Dados do Processo Digital

Órgão: PCSC - Polícia Civil de Santa Catarina

Número: PCSC

Processo do SPP: [input]

Entrada: [input] Autuado em: [input]

Setor de abertura: [input]

Setor de origem: [input]

Setor de competência: [input]

Interessado(s): [input] Mat.: [input] 

Classe: [input]

Assunto: [input]

Detalhamento do assunto: [input]

Valor do processo: [input]

Município: [input]

Cadastrado por: [input] Autuado por: [input]

Localização física da pasta do processo: [input]

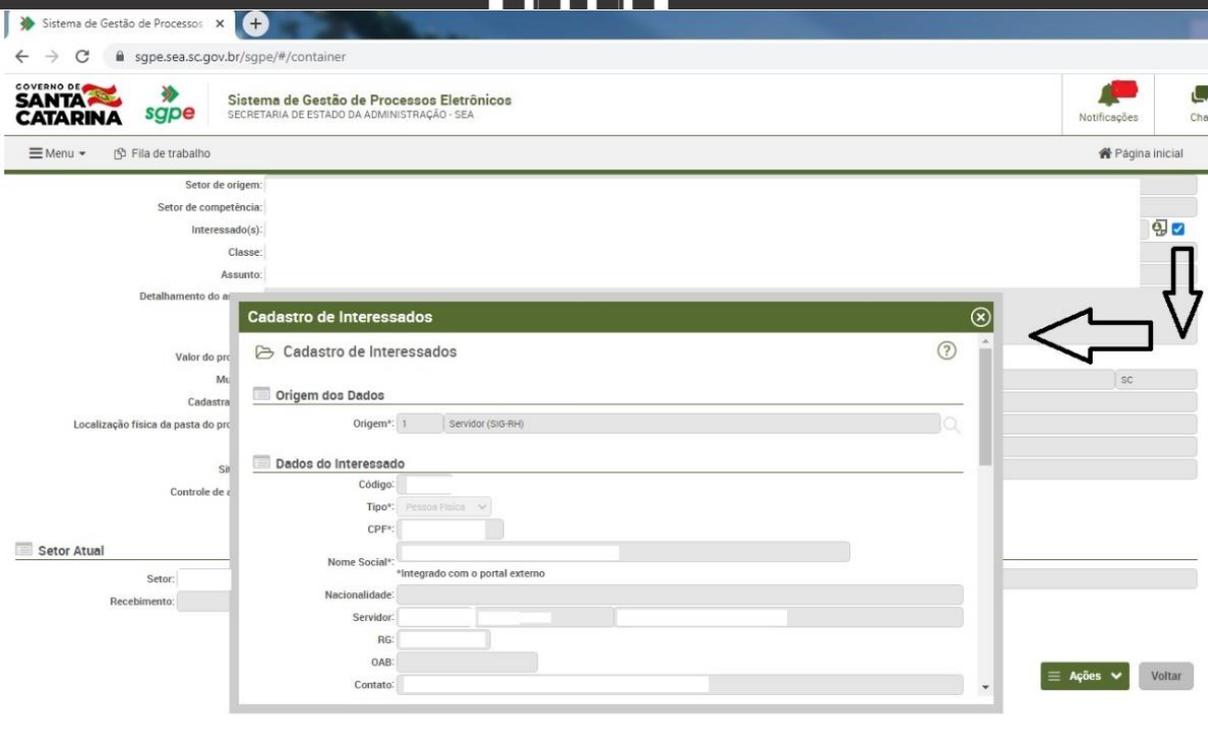
Tipo: [input] Tipo de processo: [input]

Situação: [input] Resultado: [input]

Controle de acesso: [input]

Sator Atual

Ao clicar no ícone, é apresentada uma janela de “Cadastro de Interessados”, nos quais constam diversos dos dados pessoais do servidor, tais quais CPF e RG, nome, telefone, e-mail e endereço completo, além de dados tidos como sensíveis pela lei, tal qual o nome social. Veja-se:



Sistema de Gestão de Processos: x +

sgpe.sea.sc.gov.br/sgpe/#/container

GOVERNO DE SANTA CATARINA sgpe Sistema de Gestão de Processos Eletrônicos SECRETARIA DE ESTADO DA ADMINISTRAÇÃO - SEA

Notificações Chat

Menu Fila de trabalho Página Inicial

Setor de origem: []
Setor de competência: []
Interessado(s): []
Classe: []
Assunto: []

Detalhamento do a []

Valor do pro []
Mu []
Cadastra []
Localização física da pasta do pro []
Sit []
Controle de e []

Setor Atual []

Setor: []
Recebimento: []

Cadastro de Interessados

Cadastro de Interessados

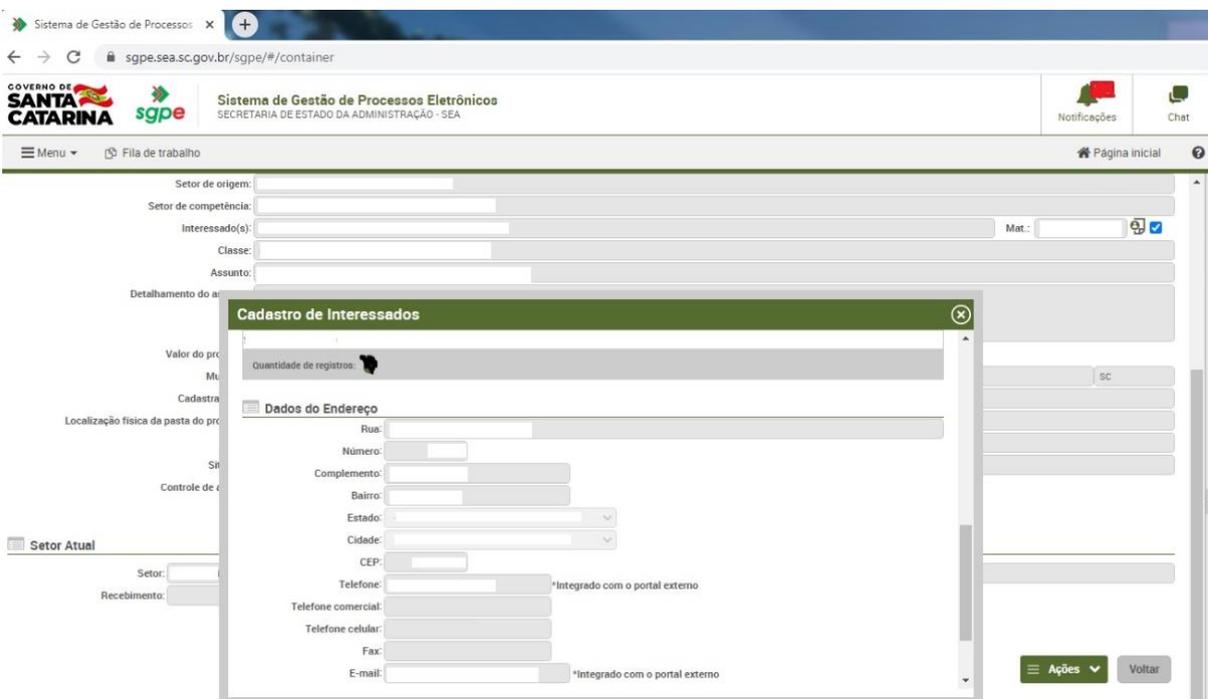
Origem dos Dados

Origem: 1 Servidor (SIG-RE)

Dados do Interessado

Código: []
Tipo: Pessoa Física
CPF: []
Nome Social: []
Nacionalidade: []
Servidor: []
RG: []
OAB: []
Contato: []

Ações Voltar



Sistema de Gestão de Processos: x +

sgpe.sea.sc.gov.br/sgpe/#/container

GOVERNO DE SANTA CATARINA sgpe Sistema de Gestão de Processos Eletrônicos SECRETARIA DE ESTADO DA ADMINISTRAÇÃO - SEA

Notificações Chat

Menu Fila de trabalho Página Inicial

Setor de origem: []
Setor de competência: []
Interessado(s): [] Mat.: []
Classe: []
Assunto: []

Detalhamento do a []

Valor do pro []
Mu []
Cadastra []
Localização física da pasta do pro []
Sit []
Controle de e []

Setor Atual []

Setor: []
Recebimento: []

Cadastro de Interessados

Quantidade de registros: []

Dados do Endereço

Rua: []
Número: []
Complemento: []
Bairro: []
Estado: []
Cidade: []
CEP: []
Telefone: []
Telefone comercial: []
Telefone celular: []
Fax: []
E-mail: []

Ações Voltar

Como se vê, basta um lançar de olhos sobre o sistema SGP-e para concluir que os dados ali expostos necessariamente passaram por processos de coleta, recepção, classificação, processamento e armazenamento, entre outros dos núcleos abrangidos no conceito de tratamento de dados.

In casu, a modalidade de tratamento que mais causa preocupação é a difusão (divulgação, propagação) indevida dos dados, que aparentam estar exteriorizados a todos os servidores com acesso ao sistema.

Nesse contexto, e levando em conta a ausência de causas de inaplicabilidade da Lei pela Administração¹, cabe analisar se a conduta da Administração subsume-se a algum dos cenários nos quais é permitido o tratamento de dados, os quais estão elencados no art. 7 da LGPD, *in verbis*:

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;

¹ Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

[...]

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;

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.

Diante da natureza do caso em tela, exclui-se de pronto os critérios estabelecidos nos incisos I, IV, V, VI, VII, VIII, IX e X, vez que **(i)** para a difusão dos dados inexistiu consentimento ou celebração de contrato por parte do titular; **(i)** não trata a SEA de órgão vinculado à pesquisa, tutela da saúde ou proteção do crédito; e **(iii)** a exposição dos dados pessoais a todos os servidores vinculados à SEA não está relacionada à proteção da vida ou ao regular exercício de direitos em processos judiciais ou administrativos.

Resta, assim, a possibilidade – ainda que remota – de que os dados estejam sendo tratados para cumprimento de obrigação legal, para a execução de políticas públicas previstas em lei ou contrato, ou para atender interesse legítimo do controlador ou de terceiro.

Quanto ao eventual cumprimento de obrigação legal, uma análise das principais legislações que autorizam hipóteses específicas de tratamento de dados² não revela qualquer disposição legal que implique na permissão ou determinação de que os dados pessoais de servidores sejam veiculados livremente, tais como o são na plataforma SGP-e.

A propósito, lembra-se que o STF já decidiu que, sob determinadas circunstâncias, o interesse público se sobressai ao interesse do particular, de modo a legitimar a mitigação do direito à intimidade, à honra e à vida privada. Foi o que aconteceu no julgamento do Tema de Repercussão Geral n. 483, que consolidou o

² Entre elas: Lei n° 9.507/1997 (*habeas data*), Lei n° 9.784/1999 (lei do processo administrativo federal), LC n. 491/2010 (lei do processo administrativo estadual), Lei n. 12.527/2011 (Lei de Acesso à Informação); Lei n. 12.965/2014 (marco civil da internet).

seguinte entendimento:

É legítima a publicação, inclusive em sítio eletrônico mantido pela Administração Pública, dos nomes dos seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias.

Ou seja, plataformas tais quais os portais de transparência, que publicizam o nome, a remuneração, a função e unidade à qual está vinculada o servidor não violariam os direitos de titulares de dados, porquanto atreladas à consecução do princípio da transparência na Administração Pública, princípio de elementar interesse da coletividade.

Nada obstante ter julgado constitucional a exposição de dados nesse tipo de portal, oportuno citar, do voto do Ministro Relator no ARE 652.777/SP - *leading case* do Tema de Repercussão Geral n. 483 -, o seguinte excerto:

E quanto à segurança física ou corporal dos servidores, seja pessoal, seja familiarmente, claro que ela resultará um tanto ou quanto fragilizada com a divulgação nominalizada dos dados em debate, mas é um tipo de risco pessoal e familiar **que se atenua com a proibição de se revelar o endereço residencial, o CPF e a CI de cada servidor**. No mais, é o preço que se paga pela opção por uma carreira pública no seio de um Estado republicano. (Grifou-se).

Como se vê, se por um lado o STF declarou que a exposição do nome e remuneração de servidores em plataformas governamentais atenderiam ao cumprimento de preceitos constitucionais, também indicou que a exposição de dados mais reservados, tais como endereço e documentos de identificação, seriam vetadas no direito brasileiro.

Outra possibilidade elencada pela LGPD é 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 (art. 7º, III e art. 26).

Aliás, a presente consulta jurídica questiona a respeito do

compartilhamento dos dados entre os sistemas SPG-e e SIGRH.

Nos casos de transferências entre órgãos diversos do Poder Público para os fins de consecução de políticas públicas dispostas em lei, o titular de dados deve ser informado sobre os tratamentos efetuados, explicitando-se claramente a finalidade da transferência.

Quando o compartilhamento se dá entre sistema de um mesmo órgão, como aparenta ser o caso do SGP-e do SIGRH, ambos vinculados à SEA, o tratamento dos dados deverá observar, em cada sistema, os princípios da finalidade e necessidade, previstos no art. 6º, da LGPD³.

Isso porque, apesar de serem perceptíveis a finalidade e necessidade do tratamento de dados relativos à identificação e à residência dos servidores por parte

³ 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.

do setor de recursos humanos do órgão (SIGRH), não é possível compreender os motivos destes mesmos dados estarem expostos no sistema SGP-e, plataforma à qual todos os servidores públicos estaduais têm acesso.

Além da determinação de que os propósitos do tratamento sejam legítimos e afeitos a finalidade específica, a lei confere ao titular de dados o direito à informação clara e facilitada, veja-se:

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; (Grifou-se).

A priori, não é possível identificar à qual finalidade está vinculado o tratamento de dados pessoais de servidores expostos no SGP-e, tampouco sua necessidade, não sobressaindo quais seriam as políticas públicas, os instrumentos contratuais, as previsões ou obrigações legais que determinem ou sequer permitam a exposição dos referidos dados.

Assim, demonstrados os direitos do titular e os deveres do Estado, recomenda-se que seja exercido o direito à informação citado acima, apresentando-se requerimento à SEA para que se manifeste a respeito do tratamento de dados no SGP-e, especificamente **(i)** como foram tratados, **(ii)** sua finalidade e necessidade, bem como **(iii)** as bases legais que fundamentam a importação e exposição de dados pessoais dos servidores na referida plataforma.

Com a apresentação das justificativas por parte da Administração, essas

serão analisadas e, a depender das circunstâncias, poderão implicar na tomada das medidas administrativas e/ou judiciais necessárias à devida salvaguarda dos direitos dos servidores titulares de dados.

III – CONCLUSÃO

Diante do exposto, conclui-se pela possibilidade imediata de solicitar-se à Secretaria de Estado de Administração esclarecimentos a respeito do tratamento das informações pessoais expostas no sistema SGP-e, visto que a difusão e ampla publicização dos dados na plataforma aparentam contrariar as diretrizes da LGPD.

Após, a resposta administrativa deverá ser analisada, verificando-se o cumprimento, ou não, dos pressupostos indicados na Lei Geral de Proteção de Dados, permitindo que sejam adotadas as medidas adequadas para resguardar os direitos dos servidores.

É o parecer.

Florianópolis, 10 de novembro de 2020.



NOEL ANTÔNIO BARATIERI
OAB/SC 16.462



RICARDO BURATTO
OAB/SC 40.963

GIANCARLO FACHINETTO OLIVEIRA
ESTAGIÁRIO