Orientações sobre a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados Pessoais

O acesso à informação é um direito fundamental. A publicidade deve ser observada como preceito e o sigilo como exceção. As informações de interesse público devem ser disponibilizadas e publicizadas independentemente de solicitação, favorecendo o controle social da administração pública. No entanto, existem algumas informações submetidas a um regime jurídico diferenciado, que são consideradas sigilosas ou pessoais.

Informação Sigilosa

A informação sigilosa é aquela submetida temporariamente à restrição de acesso público devido à sua imprescindibilidade para a segurança da sociedade e do Estado.

São assim consideradas as informações cuja divulgação ou acesso irrestrito possam:

- Pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional
- Prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais
- Pôr em risco a vida, a segurança ou a saúde da população
- Oferecer elevado risco à estabilidade financeira, econômica ou monetária do País
- Prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas
- Prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional
- Pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares
- Comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de informações

Tais informações podem ser classificadas como ultrassecretas, secretas ou reservadas, com prazos máximos de restrição de acesso de 25 anos, 15 anos e 5 anos, respectivamente. Após o prazo de classificação ou verificado o termo final, a informação se torna automaticamente de acesso público.

As informações que possam colocar em risco a segurança do Governador, do Vice-Governador do Estado e de seus respectivos cônjuges e filhos serão classificadas como reservadas até o término do mandato em exercício ou do último mandato, em caso de reeleição.

Para a classificação da informação em um dos graus de sigilo, devem ser observados o interesse da informação, a gravidade do risco (ou dano) e o prazo máximo, adotando-se o critério menos restritivo possível.

A classificação de sigilo é de competência das seguintes autoridades:

a) No grau de ultrassecreto: do Governador do Estado, do Vice-Governador do Estado, dos Secretários de Estado, do Controlador-Geral do Estado e do Procurador-Geral do Estado.

b) No grau de secreto: das autoridades acima mencionadas e das autoridades máximas das entidades da Administração Indireta.

c) No grau de reservado: das autoridades acima mencionadas e das que ocupem cargo ou função de coordenador ou de hierarquia equivalente ou superior.

A competência para a classificação de sigilo nos graus ultrassecreto e secreto pode ser delegada a agente público ocupante de cargo ou função de coordenador, ou de hierarquia equivalente ou superior, sendo vedada a subdelegação.

O acesso à informação classificada como sigilosa, seja em qual categoria for, cria para quem a obteve a obrigação de resguardar o sigilo. As credenciais de segurança referentes aos graus de sigilo serão também classificadas nos graus ultrassecreto, secreto e reservado, e serão concedidas aos agentes públicos quando imprescindível ao desempenho de suas funções, mediante termo de compromisso de preservação de sigilo. A emissão da credencial de segurança compete à autoridade máxima da Pasta, podendo tal atribuição ser objeto de delegação.

A Secretaria de Meio Ambiente, Infraestrutura e Logística possui uma Comissão de Avaliação de Documentos e Acesso – CADA (Resolução SEMIL nº 82, de 08 de outubro de 2023), cujas atribuições são: (i) assessorar a autoridade competente quanto à classificação de informação em grau de sigilo; (ii) elaborar e encaminhar à autoridade máxima da Pasta o rol anual de informações classificadas e o rol anual das informações desclassificadas para publicação; (iii) propor o destino final das informações desclassificadas, indicando aquelas para guarda permanente.

As áreas técnicas devem encaminhar à autoridade responsável pela classificação que se pretende a informação a ser analisada e as justificativas para a restrição de acesso.

Informação Pessoal

A informação pessoal é aquela relacionada à pessoa natural identificada ou identificável. As informações pessoais, relativas à intimidade, vida privada, honra e imagem, terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 anos a contar da data de sua produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem (titular).

Essas informações podem ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. Aquele que tiver acesso à informação pessoal será responsabilizado por

seu uso indevido. As informações pessoais relativas à intimidade, vida privada, honra e imagem, solicitadas pelo titular ou seu representante legal ou procurador, somente poderão ser fornecidas mediante certificação de identidade.

O consentimento para a divulgação da informação ou acesso por terceiros **não** será exigido quando ela for necessária para:

a) a prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico

b) a realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem

c) ao cumprimento de ordem judicial

d) a defesa dos direitos humanos

e) a proteção do interesse público e geral preponderante

Atenção:

a) a restrição de acesso à informação pessoal protegida não pode ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância

b) não poderá ser negado acesso à informação necessária à tutela judicial ou administrativa de direitos fundamentais

c) as informações ou documentos que versem sobre condutas que impliquem violação dos direitos humanos praticadas por agentes públicos ou a mando de autoridades públicas não poderão ser objeto de restrição de acesso

d) o disposto na Lei de Acesso à Informação (Lei nº 12.527/2011) não exclui as demais hipóteses de sigilo e de segredo de justiça nem as hipóteses de segredo industrial decorrentes da exploração direta de atividades econômicas pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público

Com relação às informações pessoais, além da Lei de Acesso à Informação, há lei específica que as protege no que se refere ao seu tratamento: Lei n° 13.709/2018 (**Lei Geral de Proteção de Dados Pessoais – LGPD**), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Esta lei se aplica a qualquer operação de tratamento realizada em território nacional, ressalvadas aquelas:

(i) realizadas por pessoa natural para fins exclusivamente particulares e não econômicos;

(ii) realizadas para fins exclusivamente jornalístico, artístico ou acadêmicos, ressalvadas as exceções apresentadas pela lei;

(iii) realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; e

(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 na lei.

O **tratamento** é toda operação realizada com dados pessoais, como 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.

A LGPD traz o conceito de dado pessoal sensível, que é aquele 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.

Os dados pessoais só poderão ser tratados para propósitos legítimos, específicos e informados ao titular, de forma adequada e conforme necessidade, sendo garantida, ao titular, a consulta facilitada e gratuita sobre a forma e a duração do tratamento e sobre a integralidade de seus dados pessoais.

A LGPD estabelece que o tratamento de dados pessoais só pode ser realizado nas seguintes condições:

a) Com o consentimento do titular, que deve ser dado por escrito ou por outro meio que demonstre sua vontade. Este consentimento deve se referir a uma finalidade específica.

b) Para cumprir uma obrigação legal ou regulatória pelo controlador. O controlador é a pessoa física ou jurídica, pública ou privada, que toma as decisões sobre o tratamento de dados pessoais.

c) Pela administração pública, para tratar e compartilhar dados necessários para executar políticas públicas previstas em leis e regulamentos, ou respaldadas em contratos, convênios ou instrumentos semelhantes, sempre observando a lei.

d) Para realizar estudos por órgãos de pesquisa, garantindo sempre que possível, a anonimização dos dados pessoais.

e) Quando necessário para a execução de contratos ou de procedimentos preliminares relacionados a um contrato do qual o titular seja parte, a pedido do titular dos dados.

f) Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, este último nos termos da Lei de Arbitragem (Lei nº 9.307/1996).

g) Para a proteção da vida ou da incolumidade física do titular ou de terceiros.

h) Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

i) Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

j) Para a proteção do crédito. O consentimento é dispensado para os dados tornados manifestamente públicos pelo próprio titular, resguardados seus direitos e os princípios previstos na LGPD. Existem algumas pequenas diferenças nas hipóteses e condições de tratamento quando se trata de dados pessoais sensíveis, conforme o art. 11 da LGPD.

O **tratamento de dados pessoais por pessoas jurídicas de direito público deve ser realizado para atender sua finalidade pública**, na perseguição do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

a) Sejam informadas as hipóteses em que 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 sites.

b) Seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.

O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelo órgão público, respeitando os princípios de proteção de dados pessoais.

É proibido ao Poder Público transferir a entidades privadas dados pessoais constantes de base de dados a que tenha acesso, exceto:

a) Em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observada a Lei de Acesso à Informação.

b) Nos casos em que os dados forem acessíveis publicamente, observadas as disposições da LGPD.

c) Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos semelhantes.

d) Na hipótese de a transferência de dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que seja proibido o tratamento para outras finalidades.

Os contratos e convênios referidos devem ser comunicados ao encarregado de dados, que deverá tomar as providências cabíveis, conforme §2º do art. 26 da LGPD.

A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado também deverá ser comunicada, e dependerá do consentimento do titular, exceto:

a) Nas hipóteses de dispensa de consentimento previstas na legislação.

b) Nos casos de compartilhamento de dados, em que deverá ser dada publicidade.

c) Nas exceções acima referenciadas.

As leis de acesso à informação e de proteção de dados pessoais também trazem normativas sobre a responsabilização de agente que fizer mau uso de informações protegidas.

Para mais informações, é importante consultar a legislação vigente:

a) Lei nº 12.527/2011 – Lei de Acesso à Informação

b) Decreto nº 68.155/2023 – regulamenta, em âmbito estadual, a Lei nº 12.527/2011

c) Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais

d) Decreto nº 65.347/2020 – dispõe sobre a aplicação da Lei nº 13.709/2018 no âmbito do Estado de São Paulo

Em não se tratando de informações sigilosas ou pessoais, as informações devem ser prestadas aos cidadãos, na forma regulamentar.

A Lei de Acesso à Informação determina que devemos dar acesso imediato às informações disponíveis e, na impossibilidade, em prazo não superior a 20 dias, comunicar a data, local e modo de realizar a consulta, efetuar reprodução ou obter certidão, indicar as razões de fato ou de direito da recusa, total ou parcial ao acesso pretendido ou comunicar que não possui a informação, indicando, quando possível, o órgão ou entidade que possa atender a demanda.

Não serão atendidos pedidos de acesso à informação no caso de informações sigilosas ou pessoais, nos termos da legislação vigente, e quando tais pedidos forem:

a) Genéricos, que impossibilitem a identificação e a compreensão da solicitação.

b) Desproporcionais ou que exijam trabalhos adicionais de análise, interpretação ou consolidação, cujo atendimento cause impacto significativo à atividade da unidade.

c) Desarrazoados, demonstrada a gravidade de risco claro e específico ao interesse público associado ao atendimento do pedido.

Assim, o servidor público que, no âmbito de suas atribuições, colete, armazene e/ou utilize informações pessoais, por exemplo, pelo acesso a cadastro de pessoas para participação de conselhos e grupos setoriais, pela realização de eventos e pela venda de ingressos, deve verificar mecanismos de proteção dos dados pessoais, tanto nos sistemas informacionais, como na observância das regras e possibilidades de compartilhamento e divulgação.

No processo de coleta de dados pessoais, a área técnica deverá definir a necessidade de acesso a cada um dos dados e prever métodos de proteção dos dados pessoais no setor, responsabilizando-se por tais dados. Também devem ser observadas, quando do processo de coleta, as regras de armazenamento, utilização, compartilhamento interno no âmbito da Secretaria e divulgação, ou não, das informações pessoais.

Resumo em Perguntas & Respostas:

O que é o acesso à informação e qual é a sua importância? O acesso à informação é um direito fundamental. A publicidade deve ser observada como preceito e o sigilo como exceção. As informações de interesse público devem ser disponibilizadas e publicizadas independentemente de solicitação, favorecendo o controle social da administração pública.

O que são informações sigilosas? As informações sigilosas são aquelas submetidas temporariamente à restrição de acesso público devido à sua imprescindibilidade para a segurança da sociedade e do Estado. Tais informações podem ser classificadas como ultrassecretas, secretas ou reservadas, com prazos máximos de restrição de acesso de 25 anos, 15 anos e 5 anos, respectivamente. Após o prazo de classificação ou verificado o termo final, a informação se torna automaticamente de acesso público.

Quem tem a competência para classificar a informação em um dos graus de sigilo? A classificação de sigilo é de competência das seguintes autoridades:

a) No grau de ultrassecreto: do Governador do Estado, do Vice-Governador do Estado, dos Secretários de Estado, do Controlador-Geral do Estado e do Procurador-Geral do Estado.

b) No grau de secreto: das autoridades acima mencionadas e das autoridades máximas das entidades da Administração Indireta.

c) No grau de reservado: das autoridades acima mencionadas e das que ocupem cargo ou função de coordenador ou de hierarquia equivalente ou superior.

O que é uma informação pessoal? A informação pessoal é aquela relacionada à pessoa natural identificada ou identificável. As informações pessoais, relativas à intimidade, vida privada, honra e imagem, terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 anos a contar da data de sua produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem (titular).

Quais são as condições para o tratamento de dados pessoais? A Lei Geral de Proteção de Dados Pessoais estabelece que o tratamento de dados pessoais só pode ser realizado nas seguintes condições:

a) Com o consentimento do titular, que deve ser dado por escrito ou por outro meio que demonstre sua vontade. Este consentimento deve se referir a uma finalidade específica.

b) Para cumprir uma obrigação legal ou regulatória pelo controlador. O controlador é a pessoa física ou jurídica, pública ou privada, que toma as decisões sobre o tratamento de dados pessoais.

c) Pela administração pública, para tratar e compartilhar dados necessários para executar políticas públicas previstas em leis e regulamentos, ou respaldadas em contratos, convênios ou instrumentos semelhantes, sempre observando a lei.

d) Para realizar estudos por órgãos de pesquisa, garantindo sempre que possível, a anonimização dos dados pessoais.

e) Quando necessário para a execução de contratos ou de procedimentos preliminares relacionados a um contrato do qual o titular seja parte, a pedido do titular dos dados.

f) Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, este último nos termos da Lei de Arbitragem (Lei nº 9.307/1996).

g) Para a proteção da vida ou da incolumidade física do titular ou de terceiro.

h) Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

i) Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

j) Para a proteção do crédito.

Quais são os principais diplomas normativos que regulamentam o acesso à informação e a proteção de dados pessoais? As principais leis que regulamentam o acesso à informação e a proteção de dados pessoais são: Lei nº 12.527/2011 – Lei de Acesso à Informação; Decreto nº 68.155/2023 – regulamenta, em âmbito estadual, a Lei nº 12.527/2011; Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais; Decreto nº 65.347/2020 – dispõe sobre a aplicação da Lei nº 13.709/2018 no âmbito do Estado de São Paulo.