LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

Prefeitura de
JACAREÍ

PREFEITURA MUNICIPAL DE JACAREÍ
SECRETARIA DE GOVERNO E PLANEJAMENTO
DIRETORIA DE GOVERNANÇA E TRANSPARÊNCIA 2021

Izaías Santana
Prefeito Municipal

CelsoFlorênciodeSouza
Secretáriode Governoe Planejamento

Anderson Ulisses de Araújo Santiago
Diretorde Governança e Transparência

1. O QUE É A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD?

A Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709, aprovada em 14 de agosto de 2018, dispõe sobre o tratamento de dados pessoais em âmbito nacional, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e a livre formação da personalidade de cada indivíduo. Seu principal foco é oferecer ao titular dos dados maior conhecimento, controle e transparência na coleta, processamento, uso e compartilhamento de suas informações pessoais, tanto aquelas armazenadas em bancos de dados das instituições privadas e de órgãos públicos, tanto de forma digital, quanto aquelas disponíveis em meios físicos.

O que são dados pessoais?

São informações relacionadas à pessoa natural identificada ou identificável como nome, data de nascimento, filiação, apelido, CPF, RG, foto, endereço residencial, endereço de e-mail, ende reço IP, cookies, hábitos de navegação, posição geolocacional (GPS), formulários cadastrais, números de documentos, enfim, aquilo que permita identificar uma pessoa física, é um dado pessoal.

O que é tratamento de dados, conforme a LGPD?

Tratamento é qualquer operação efetuada sobre dados pessoais, por meios manuais ou automatizados, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Desta feita, a Administração, ao tratar os dados dos usuários, deve ponderar a real necessidade da solicitação de alguma informação específica para viabilizar a oferta do produto ou serviço. Por exemplo, não se recomenda a solicitação do CPF para a aquisição de um medicamento em drogaria, sem que se esclareça previamente o titular e se comprove a necessidade de tal informação.

De igual forma, deve-se ponderar a necessidade de solicitar informações sobre religião, opinião política, filosófica, política do usuário para a prestação de serviço, pois quanto mais dados são coletados, maior a responsabilidade do Poder Público acerca da segurança da informação sob sua guarda.

A LGPD estabelece, também, que alguns dados pessoais estão sujeitos a cuidados ainda mais específicos, como os “dados sensíveis” e os dados sobre “crianças eadolescentes”.

O que são dados sensíveis?

São informações 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 (prontuários e exames) ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Esses dados poderiam expor o indivíduo, social ou profissionalmente, de forma indesejada, dando margem a uma possível discriminação. Em razão disso, os dados sensíveis exigem um tratamento ainda mais delicado, com a adoção, pelas entidades controlado ras, de medidas de segurança mais rígidas, como, por exemplo, a anonimização desses dados e cama das de proteção mais extensas.

2.QUANDO A LGPD ENTRA EM VIGOR?

A LGPD entrou em vigor em 14 de agosto de 2020, contudo, as penalidades previstas na Lei somente passaram a valer a partir de 01 de agosto de 2021.

3. QUAIS SÃO OS FUNDAMENTOS DA LGPD?

- Respeito à privacidade - ao assegurar os direitos fundamentais de inviolabilidade da intimidade, da honra, da imagem e da vida privada.
- Autodeterminação informativa - ao expressar o direito do cidadão ao controle, e assim, à proteção de seus dados pessoais e íntimos.
- Liberdade de expressão, de informação, de comunicação e de opinião, que são direitos previstos na Constituição brasileira.
- Desenvolvimento econômico e tecnológico e a inovação - a partir da criação de um cenário de segurança jurídica em todo o país.
- Livre iniciativa, livre concorrência e a defesa do consumidor - por meio de regras claras e válidas para todo o setor público e privado.
- Direitos humanos - o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas.

4. PORQUE A PREFEITURA MUNICIPAL DE JACAREÍ DEVE FAZER O CONTROLE DE DADOS PESSOAIS?

- A Prefeitura pode tratar dados pessoais a todo momento – pode receber ser guardiã de um grande volume de dados pessoais, dos cidadãos e dos próprios servidores, no âmbito dos diversos órgãos municipais.
- Para evitar o uso indevido de dados pessoais, que podem ser do cidadão ou seus agentes públicos.
- Para tomada de decisões no setor público.
- Para evitar que ocorram vazamento de dados ou compartilhamentos indevidos e assim, afastar eventuais responsabilizações previstas na LGPD.

5. PARA QUAIS TIPOS DE DADOS PESSOAIS NÃO SE APLICA A LGPD?

Àqueles usados para fins exclusivamente particulares e não econômicos jornalísticos ou artísticos, para fins acadêmicos, para investigações, repressão de crimes, ou em casos de segurança pública e defesa nacional.

6. QUEM SÃO CONSIDERADOS AGENTES DE TRATAMENTO?

O “controlador” (pessoa física ou jurídica, de direito público ou privado, responsável pelas decisões referentes ao tratamento de dados pessoais) e o “operador” (pessoa física ou jurídica que realiza o tratamento de dados pessoais em nome do controlador).

O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. A qualquer momento pode ser necessária a demonstração clara dessas operações, podendo os mesmos ser responsabilizados por eventual infração à LGPD.

7. QUEM É O TITULAR DOS DADOS?

A pessoa natural a quem se referem esses dados, como os cidadãos usuários dos serviços públicos da PMJ, os agentes públicos e políticos, os servidores estatutários, celetistas, temporários, ocupantes de cargo em comissão. O dono do dado é a própria pessoa ao qual este dado se refere.

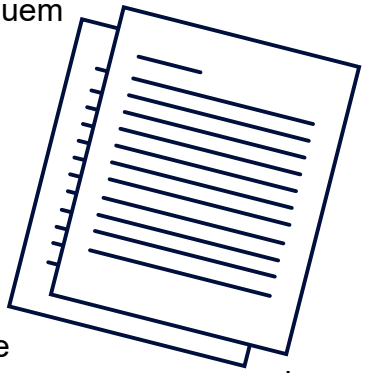
Envolve tanto dados corporativos, dos próprios servidores e contratados como, é claro, do público externo com o qual o cada órgão se relaciona.

8. QUAIS SÃO OS DIREITOS DO TITULAR?

- Acesso facilitado às informações sobre o tratamento de seus dados. Esses dados deverão ser disponibilizados de forma clara, adequada e ostensiva, principalmente no que se refere à confirmação da existência de tratamento e, em caso positivo, sua finalidade, forma, duração. Assim, a Secretaria X deve informar as hipóteses em que, no exercício de suas competências previstas em lei, realizão 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.
- Acesso e correção de dados incompletos, inexatos ou desatualizados.
- Anonimização, bloqueio ou eliminação de dados desnecessários.
- Portabilidade de seus dados.
- Revogação do consentimento/eliminação dos dados, sendo assegurado o direito de petição à autoridade nacional.
- Informação sobre com quem os dados foram compartilhados.
- Informação sobre o poder de não consentir e suas consequências.
- Identificação do controlador e seu contato.

9. QUEM É O CONTROLADOR?

Pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais, sendo as responsáveis pela definição das medidas de segurança que serão aplicadas no tratamento desses dados, como secretários e diretores-presidentes de entidades da Administração Indireta.



10. QUEM É O OPERADOR?

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Exemplo: sistemas utilizados pleas Secretarias, nos quis são inseridos os dados pessoais, para fins de buscar, arquivar, controlar informações de outras pessoas.

11. QUEM É O ENCARREGADO OU DATA PROTECTION OFFICER - DPO?

É um profissional de conhecimento ímpar e multidisciplinar que figura como protagonista para que os órgãos e entidades estejam em conformidade com a LGPD, sendo indicado pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados - ANPD. É recomendável que o DPO tenha conhecimentos de governança, compliance, direito, segurança da informação, ferramentas de segurança e processos de segurança, possuindo habilidades de gerenciamento e capacidade de interação com a equipe interna da entidade controladora, terceiros, titulares de dados e órgãos oficiais.

A identificação e informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva no sítio eletrônico do controlador. No caso da Administração Pública, é indicado um Encarregado de Dados,que contará com o suporte de outras pessoas para a gestão dessas informações, considerando o volume de dados tratados pela Prefeitura.

12. O QUE É O RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS?

Documentação do controlador que contém a descrição das fases de tratamento dos dados pessoais, a identificação de quem acessa esses dados pessoais, bem como quais são os mecanismos de privacidade, segurança e mitigação de risco, cujo prazo de envio ainda será regulamentado pela ANPD.

13. O QUE É O CONSENTIMENTO DO TITULAR?

É a concordância e autorização do titular quanto ao tratamento de seus dados pessoais. Deve ocorrer de forma livre, informada, inequívoca e para uma finalidade determinada, por escrito (neste caso, de maneira destacada das demais cláusulas) ou por outro meio que demonstre a manifestação de vontade do titular. Autorizações/consentimentos genéricos para tratamento de dados serão nulos,bem como se o dado for utilizado para finalidade diversa da inicialmente consentida.

ATENÇÃO: A administração pública pode tratar dados sem o consentimento em atividades de interesse público determinadas em lei, desde que informe ao titular quando, como, para que e com base em qual artigo de lei.

14. COMO DEVERÁ SER OBTIDO O CONSENTIMENTO DO TITULAR?

Por escrito ou por outro meio que demonstre a livre e inequívoca manifestação de sua vontade. O titular deve concordar não só com o tratamento, mas com a finalidade daquele tratamento. Quando o tratamento de dados envolver o compartilhamento destes com algum outro controlador, deve haver consentimento específico para que possa haver tal compartilhamento, ressalvadas as hipóteses legais dedispensa de consentimento, respeitados, sempre, os princípios de proteção dosdados pessoais elencados no art. 6º da LGPD.

15. QUAIS SÃO AS HIPÓTESES EM QUE PODE OCORRER TRATAMENTO SEM CONSENTIMENTO?

- Para o cumprimento de obrigação legal ou regulatória pelo controlador.
- Quando houver a necessidade, por parte da Administração Púbica, de compartilhar dados que sejam necessários para executar políticas públicas previstas em leis ou regulamentos.
- Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.
- Para a proteção da vida ou da incolumidade física do titular ou de terceiro.
- Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por autoridade sanitárias, por exemplo, informações de saúde que são anotadas no prontuário do paciente e compartilhadas com os médicos e enfermeiros que estão cuidando do caso.
- 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.
- 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).
- Para a proteção da vida ou da incolumidade física do titular ou de terceiro.
- Quando o dado pessoal for utilizado para fins de prevenção à fraude, com ações voltadas à segurança do titular, normalmente aplicada nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.
- Para a proteção do crédito,inclusive quanto ao disposto na legislação pertinente.

16. COMO OS DADOS PODERÃO SER TRATADOS?

O titular do dado deverá assinar um termo de consentimento, que deverá ter redação clara, indicando a finalidade específica do tratamento.

A PMJ poderá tratar e compartilhar os dados necessários à execução de políticas públicas previstas em lei e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, independentemente do consentimento do titular dos dados, desde que sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

17. O TITULAR PODE REVOGAR O CONSENTIMENTO?

Sim, a qualquer tempo o titular pode revogar seu consentimento, exceto quando o consentimento for dispensável. Essa revogação poderá ser requerida mediante manifestação expressa do titular, por procedimento gratuito e facilitado.

Além disso, o cidadão pode solicitar que seus dados sejam apagados, ou pode solicitar transferir dados para outro fornecedor de serviços (esta opção não é usual no serviço público, uma vez que, de um modo geral não há opção de prestador). O controlador, entretanto, poderá se opor à exclusão dos dados solicitados pelo titular, apresentando razões fundamentadas acerca da continuidade/guarda das informações. Por exemplo, na área da saúde, não é possível excluir dados de prontuários médicos, ainda que solicitados pelo paciente, haja vista a obrigação legal imposta pela Lei nº 13.787/18, que determina a guarda do prontuário pela institui-ção de saúde pelo prazo mínimo de 20 anos.

18. HÁ ALGUMA ESPECIFICIDADE PARA O TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES?

Sim. Esse tratamento deverá ser realizado com o consentimento específico, e em destaque, dado por, pelo menos, um dos pais ou responsável legal. Órgãos sujeitos a tratamento de crianças e adolescentes deverão tomar a medida necessária para manter controle desse consentimento, uma vez que podem ser demandados, a qualquer momento, a demonstrar quais dados foram tratados, de que forma, e quais são os respectivos responsáveis. Sem o consentimento, só se pode coletar dados de crianças e adolescentes se for para urgências relacionadas a entrar em contato com os pais ou responsáveis e/ou para proteção da criança e do adolescente.

19. O QUE É DADO ANONIMIZADO?

É aquele que, originariamente, era relativo a uma pessoa, mas que passou por etapas que garantiram sua desvinculação com essa pessoa, não permitindo que, via meios técnicos e outros, se reconstrua o caminho para descobrir quem era a pessoa titular do dado. Se um dado for anonimizado, então a LGPD não se aplicará a ele.

20. QUAL É A AUTORIDADE MÁXIMA DA ESTRUTURA DE IMPLANTAÇÃO DA LGPD NO BRASIL?

A fiscalização e a regulação da LGPD ficarão a cargo da Autoridade Nacional de Proteção de Dados Pessoais (ANPD), que será um elo entre sociedade e governo, permitindo que as pessoas enviem dúvidas, sugestões, denúncias ligadas à LGPD para apuração. A ANPD, que está em processo de formação, será vinculada à Presidência da República, e com autonomia técnica garantida pela lei. A proposta da ANPP é orientar, preventivamente. Após isso, fiscalizar, advertir e, somente após tudo isso, penalizar, se a LGPD continuar sendo descumprida.

21. O PODER PÚBLICO TAMBÉM ESTÁ SUJEITO ÀS DISPOSIÇÕES DA LGPD?

Sim, os dados pessoais tratados pelo Poder Público também estão sujeitos à LGPD. Porém, o Poder Público pode tratar dados pessoais sem pedir o consentimento do titular sempre que for necessário para a execução de políticas públicas. O Poder Público também poderá tratar dados pessoais, fora do escopo da lei, no caso de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, que serão tratados de acordo com legislação específica, que contenha medidas proporcionais e necessárias para que o tratamento de dados pessoais atenda ao interesse público. Para a criação das normas específicas para esses casos, a Autoridade Nacional de Proteção de Dados Pessoais - ANPD emitirá recomendações e opiniões técnicas.

22. É POSSÍVEL O USO COMPARTILHADO DE DADOS ENTRE DIFERENTES ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA?

A Lei permite o uso compartilhado de dados pessoais entre entes do poder público, desde que atenda a finalidades específicas de execução de políticas públicas e a atribuição legal desses órgãos, respeitados os princípios do art. 6º. O inciso III do art. 7º assegura, como uma de suas dez bases legais para o tratamento de dados, o tratamento e uso compartilhado pela Administração Pública de dados necessários à execução de políticas públicas previstas em leis, regulamentos ou ainda respaldadas em contratos, convênios ou instrumentos congêneres, nos termos do Capítulo IV.

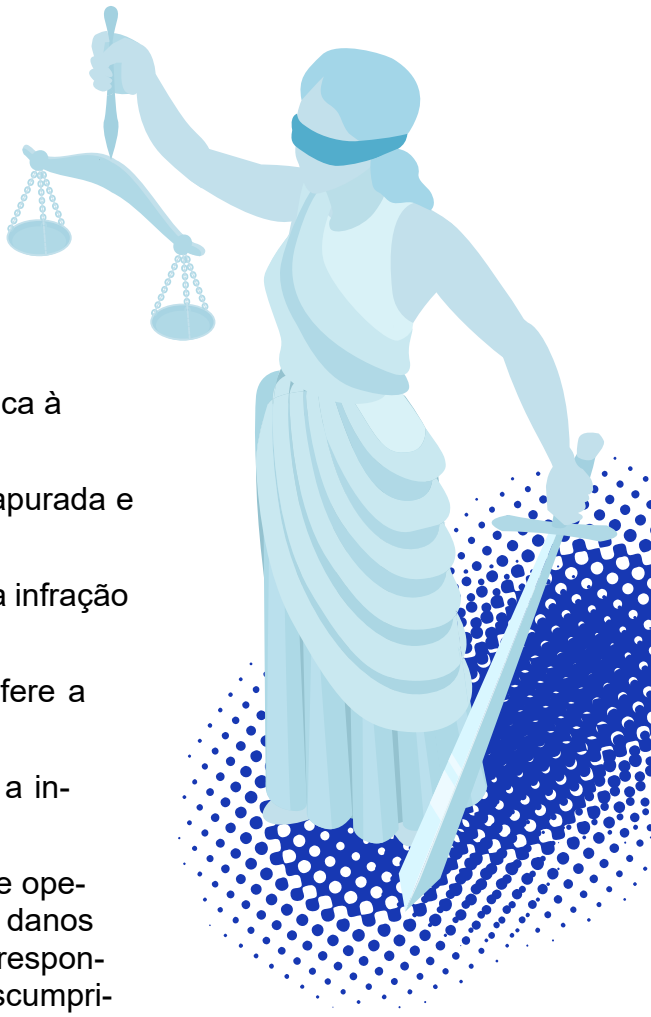
23. A LGPD DISPÕE SOBRE A TRANSFERÊNCIA DE DADOS ENTRE O PODER PÚBLICO E INSTITUIÇÕES DO SETOR PRIVADO?

O artigo 26 prevê que 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 da Lei.

Veta a transferência dos dados pessoais constantes de bases de dados a que tenha acesso, exceto:

- Em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
- Em casos em que os dados forem acessíveis publicamente;
- Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres;
- Para prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados.

24. QUAIS SÃO AS PENALIDADES E SANÇÕES CABÍVEIS A QUEM DESCUMPRIR A LGPD?



- Advertência, com indicação de prazo para adoção de medidas corretivas.
- Multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, limitada, no total, a R$ 50.000.000,00 por infração (não se aplica à Administração Direta da PBH).
- Multa diária limitada a esse valor (não se aplica à Administração Direta da PMJ).
- Publicização da infração após devidamente apurada e confirmada a sua ocorrência.
- Bloqueio dos dados pessoaisa que se refere a infração até a sua regularização.
- Eliminação dos dados pessoais a que se refere a infração.
- Bloqueio dosdados pessoaisa que se refere a infração até a sua regularização.

Quanto aos agentes de tratamento (controlador e operador), estes responderão solidariamente pelos danos que causarem no exercício de suas atividades, respondendo civil e administrativamente em caso de descumprimento da LGPD.

Quanto a órgãos da Administração Indireta, se estes estiverem na operacionalização de políticas públicas, terão o mesmo tratamento destinado às demais entidades públicas. Assim, a penalidade de multa não será aplicável.

Documento elaborado por: DIRETORIA DE GOVERNANÇA E TRANSPARÊNCIA
JACAREÍ – 2020.

Última atualização em: Setembro/2021

GLOSSÁRIO LGPD - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Este glossário visa facilitar o entendimento dos principais termos da Lei Geral de Proteção de Dados Pessoais - LGPD, Lei nº 13.709/18, aprovada em 14 de agosto de 2018. Foi elaborado tendo como fonte a própria Lei, além de orientações disponíveis no site do Governo Federal, sob a coordenação do Serviço Federal de Processamento de Dados – SERPRO.

1. Agentes de Tratamento: o Controlador e o Operador.

2. 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.

3. Autoridade Nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

4. Banco de Dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

5. Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

6. Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Se elaborado de uma forma muito genérica, sem especificação, poderá ser considerado nulo. O consentimento pode ser revogado pelo titular. Quando tratar dados pessoais for condição para fornecimento de produto ou serviço ou para exercício de um direito, você deve ser avisado sobre isso e sobre os meios pelos quais pode exercer seus direitos como titular. A administração pública poderá tratar e compartilhar os dados necessários à execução de políticas públicas previstas em lei e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, independentemente do consentimento do titular dos dados, desde que sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

7. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

8. Criptografia: arte de proteção da informação através de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem.

9. 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.

10. Dado Pessoal: informação relacionada à privacidade de uma pessoa naturalidentificada ou identificável. Alguns exemplos de dados pessoais são: nome, endereço, e-mail, idade, números de documentos de identificação (RG, CPF, CNH, título de eleitor), estado civil, informações relativas à localização geográfica, número de IP, dentre outros.

11. Dado Pessoal de Criança e de Adolescente: o Estatuto da Criança e do Adolescente (ECA) considera criança a pessoa até 12 anos de idade incompletos e adolescente aquela entre 12 e 18 anos de idade. Em especial, a LGPD determina que as informações sobre o tratamento de dados pessoais de crianças e de adolescentes deverão ser fornecidas de maneira simples, clara e acessível, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança. Deverá ser coletado o consentimento dos pais ou responsáveis para efetuar tratamento de dados de criança ou adolescente.

12. Dado Pessoal Sensível: dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Diz respeito à intimidade de um indivíduo. Merecem proteção especial, uma vez que pode ser usado para fins de discriminação.

13. Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

14. Encarregado: também denominado como Data Protection Officer (DPO), o encarregado é a 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).

15.Garantia da Segurança da Informação: capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. A Política Nacional de Segurança da Informação (PNSI) dispõe sobre a governança da segurança da informação aos órgãos e às entidades da administração pública federal em seu âmbito de atuação.

16. Garantia da Segurança de Dados: ver garantia da segurança da informação

17. Interoperabilidade: capacidade de sistemas e organizações operarem entre-si, trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, além dos padrões de interoperabilidade de governo eletrônico (ePING)

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

19. 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.

20. Pseudonimização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

21. Relatório de Impacto à Proteção de Dados Pessoais: documentação emitida pelo 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.

22. Titular: pessoa natural a quem se referem os dados pessoais que são objetode tratamento.

23. Transferência Internacional de Dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

24. Tratamento: qualquer operação efetuada sobre dados pessoais, por meios manuais ou automatizados, como 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 mera visualização de dados por um servidor caracteriza tratamento. Pode ser considerado tratamento toda operação realizada com dados pessoais, como as que se referem a:

- acesso - possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc., visando receber, fornecer ou eliminar dados;
- armazenamento - ação ou resultado de manter ou conservar em repositório um dado;
- arquivamento - ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotada a sua vigência;
- avaliação - ato ou efeito de calcular valor sobre um ou mais dados;
- classificação - maneira de ordenar os dados conforme algum critério estabelecido;
- coleta - recolhimento de dados com finalidade específica;
- comunicação - transmitir informações pertinentes a políticas de ação sobre os dados;
- controle - ação ou poder de regular, determinar ou monitorar as ações sobre o dado;
- difusão - ato ou efeito de divulgação, propagação, multiplicação dos dados;
- distribuição - ato ou efeito de dispor de dados de acordo com algum critério estabelecido;
- eliminação - ato ou efeito de excluir ou destruir dado do repositório;
- extração - ato de copiar ou retirar dados do repositório em que se encontrava;
- modificação - ato ou efeito de alteração do dado;
- processamento - ato ou efeito de processar dados;
- produção - criação de bens e de serviços a partir do tratamento de dados;
- recepção - ato de receber os dados ao final da transmissão;
- reprodução - cópia de dado preexistente obtido por meio de qualquer processo;
- transferência - mudança de dados de uma área de armazenamento para outra, ou para terceiro;
- transmissão - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc;
- utilização - ato ou efeito do aproveitamento dos dados.

25. Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas 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.

26. Vazamento de dados: transmissão não autorizada de dados de dentro de uma organização para um destino ou recipiente externo. Os dados podem ser transferidos eletronicamente ou fisicamente, de forma acidental ou intencional (pela ação de agentes internos, pela ação de agentes externos ou pelo uso de software malicioso).

Documento elaborado por: DIRETORIA DE GOVERNANÇA E TRANSPARÊNCIA

JACAREÍ – 2020.

Última atualização em: Setembro/2021