Estratégia Concursos

Aula 16

Banco do Brasil (Escriturário - Agente de Tecnologia) Passo Estratégico de Conhecimentos Bancários - 2023 (Pós-Edital)

Autor:
Alexandre Violato Peyerl

09 de Fevereiro de 2023

Índice

LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): LEI Nº 13.709/2018. SEGURANÇA CIBERNÉTICA: RESOLUÇÃO CMN Nº 4.893/2021

ROTEIRO DE REVISÃO E PONTOS DO ASSUNTO QUE MERECEM DESTAQUE

Lei Geral de Proteção de Dados (LGPD): Lei nº 13.709, de 14 de agosto de 2018 e suas alterações.

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

São fundamentos da proteção de dados pessoais:

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A 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;

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

A 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:
    - jornalístico e artísticos; ou
    - acadêmicos;
- III - realizado para fins exclusivos de:
    - segurança pública;
    - defesa nacional;
    - segurança do Estado; ou
    - atividades de investigação e repressão de infrações penais;
        - *nesses casos, o tratamento será regido por legislação específica.*
- 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.

Conceitos:

- **Dado pessoal**: informação relacionada a pessoa natural identificada ou identificável.
- **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.
- **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.
- **Banco de dados**: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
- **Titular**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- **Controlador**: pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais.

- **Operador**: pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.
- **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).
- **Agentes de tratamento**: o controlador e o operador.
- **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.
- **Anonimização**: utilização de meios técnicos por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
- **Consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
- **Bloqueio**: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.
- **Eliminação**: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.
- **Transferência internacional de dados**: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.
- **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 órgãos e entidades públicos e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos; ou
    - entre entes privados.
- **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.
- **Órgão de pesquisa**: órgão ou entidade da administração pública ou pessoa jurídica de direito privado sem fins lucrativos, 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.

- **Autoridade nacional**: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Princípios a serem observados nas atividades de tratamento de dados pessoais:

- **Finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
- **Adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
- **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.
- **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.
- **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.
- **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.
- **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.
- **Prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
- **Não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
- **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.

Tratamento de dados pessoais

O tratamento de dados pessoais só pode ser realizado nas seguintes hipóteses:

- mediante o fornecimento de consentimento pelo titular;
    - 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.
- para o cumprimento de obrigação legal ou regulatória pelo controlador;
- pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas;
- para a realização de estudos por órgão de pesquisa;
    - nesse caso, sempre que possível, deve ser garantida a anonimização dos dados pessoais.
- quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular;
- para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
- para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- 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;
- para a proteção do crédito.

É dispensada a exigência de consentimento para os dados tornados manifestamente públicos pelo titular.

Na hipótese em que o consentimento é requerido:

- Esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
- Se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular deve ser informado com destaque sobre esse fato.

Tratamento de Dados Pessoais Sensíveis

Somente poderá ocorrer nas seguintes hipóteses:

- I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas.
- II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
    - cumprimento de obrigação legal ou regulatória pelo controlador;
    - tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
    - realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
    - exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
    - proteção da vida ou da incolumidade física do titular ou de terceiro;
    - tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
    - garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:

- I - a portabilidade de dados quando solicitada pelo titular; ou
- II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços.

É **vedado** às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de **seleção de riscos na contratação** de qualquer modalidade, assim como na **contratação e exclusão de beneficiários**.

Os dados anonimizados não são considerados dados pessoais para os fins da Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

Podem ser considerados como dados pessoais os utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

Na realização de estudos em **saúde pública**:

- Os órgãos de pesquisa podem ter acesso a bases de dados pessoais, que são tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança que incluam, sempre que possível, a anonimização ou pseudonimização dos dados.
    - Pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, salvo pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
- A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa em nenhuma hipótese poderá revelar dados pessoais.
- O órgão de pesquisa é o responsável pela segurança da informação, não permitida a transferência dos dados a terceiro.

Tratamento de Dados Pessoais de Crianças e de Adolescentes

- O tratamento de dados pessoais de crianças deve ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
    - Podem ser coletados dados pessoais de crianças sem o consentimento acima quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento.
- Os controladores não devem condicionar a participação de crianças em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

Término do Tratamento de Dados

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, resguardado o interesse público; ou
- IV - determinação da autoridade nacional, quando houver violação ao disposto na Lei.

Os dados pessoais devem ser eliminados após o término de seu tratamento, 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; ou

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

Direitos do titular

Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade.

O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

- I - confirmação da existência de tratamento;
- II - acesso aos dados;
- III - correção de dados incompletos, inexatos ou desatualizados;
- IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade a Lei;
- V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses em que é autorizada a conservação;
- VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- IX - revogação do consentimento.

Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Tratamento de dados pessoais pelo poder público

O tratamento de dados pessoais pelas pessoas jurídicas de direito público 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:

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

Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas de direito público.

As empresas públicas e as sociedades de economia mista:

- Que atuam em regime de **concorrência** terão o mesmo tratamento dispensado às pessoas jurídicas de **direito privado** particulares.
- Quando estiverem operacionalizando **políticas públicas** e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público.

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.

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.

É vedado ao Poder Público transferir a entidades privadas 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;
- nos casos em que os dados forem acessíveis publicamente;
- quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou
- 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.

Agentes de tratamento de dados pessoais

Controlador e Operador

- Devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.
- O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verifica a observância das próprias instruções e das normas sobre a matéria.

Encarregado pelo Tratamento de Dados Pessoais

- O controlador deve indicar encarregado pelo tratamento de dados pessoais.
- A identidade e as informações de contato do encarregado devem ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no site do controlador.
- Atividades do encarregado:
    - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
    - receber comunicações da autoridade nacional e adotar providências;
    - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
    - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Responsabilidade e Ressarcimento de Danos

- O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
- A fim de assegurar a efetiva indenização ao titular dos dados:
    - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador.
    - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente.
- O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
    - Ou seja, nesses casos, ao invés do titular provar que houve mal uso dos seus dados, cabe ao operador ou controlador comprovar que não houve.
- As ações de reparação por danos coletivos podem ser exercidas coletivamente em juízo.
- Os agentes de tratamento só não serão responsabilizados quando provarem:
    - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

- que, embora tenham realizado o tratamento de dados pessoais, não houve violação à legislação de proteção de dados; ou
- que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Segurança e do Sigilo de Dados

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.

Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação em relação aos dados pessoais, mesmo após o seu término.

O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, devendo mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Sanções Administrativas

Sanções administrativas aplicáveis pela autoridade nacional:

- **Advertência** com indicação de prazo para adoção de medidas corretivas.
- **Multa:**
  - Simples - Até 2% do faturamento da pessoa jurídica de direito privado no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 por infração.
  - Diária - observado o limite total acima.

- **Publicização** da infração após devidamente apurada e confirmada a sua ocorrência.
- **Bloqueio dos dados** pessoais a que se refere a infração até a sua regularização.
- **Eliminação** dos dados pessoais a que se refere a infração.
- **Suspensão parcial do funcionamento do banco de dados** a que se refere a infração pelo período máximo de 6 meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador.
- **Suspensão do exercício da atividade de tratamento dos dados pessoais** a que se refere a infração pelo período máximo de 6 meses, prorrogável por igual período.
- **Proibição parcial ou total** do exercício de atividades relacionadas a tratamento de dados.

Com exceção das multas, as sanções acima podem ser aplicadas às entidades e aos órgãos públicos.

A aplicação das sanções compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.

As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

- I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
- II - a boa-fé do infrator;
- III - a vantagem auferida ou pretendida pelo infrator;
- IV - a condição econômica do infrator;
- V - a reincidência;
- VI - o grau do dano;
- VII - a cooperação do infrator;
- VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados;
- IX - a adoção de política de boas práticas e governança;
- X - a pronta adoção de medidas corretivas; e
- XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Autoridade Nacional de Proteção de Dados (ANPD)

- É autarquia de natureza especial da administração pública federal, integrante da Presidência da República.
- A ANPD tem autonomia técnica e decisória, possuindo patrimônio próprio.
- É composta de:
    - Conselho Diretor, órgão máximo de direção;
    - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;
    - Corregedoria;
    - Ouvidoria;
    - Procuradoria; e
    - unidades administrativas e unidades especializadas.
- O Conselho Diretor é composto de 5 diretores, incluído o Diretor-Presidente.
    - Os membros do Conselho Diretor são escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados.
    - O mandato dos membros do é de 4 anos.
    - Somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar.
- Principais competências da ANPD:
    - zelar pela proteção dos dados pessoais;
    - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações;
    - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
    - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação;
    - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
    - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

- editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade;
- celebrar compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos;
- comunicar às autoridades competentes as infrações penais das quais tiver conhecimento.

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

- Composto de 23 representantes de diversos órgãos.
- A participação no Conselho é considerada prestação de serviço público relevante, não remunerada.
- Competências:
  - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD;
  - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;
  - sugerir ações a serem realizadas pela ANPD;
  - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade;
  - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.

Segurança Cibernética: Resolução CMN nº 4.893/2021

A RESOLUÇÃO CMN Nº 4.893/2021 dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil (BCB), não incluídas as instituições de pagamento, que seguem outra regulamentação do BCB.

As instituições devem implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a **confidencialidade**, a **integridade** e a **disponibilidade** dos dados e dos sistemas de informação utilizados.

A política mencionada no caput deve ser compatível com:

- I - o porte, o perfil de risco e o modelo de negócio da instituição;
- II - a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da instituição; e
- III - a sensibilidade dos dados e das informações sob responsabilidade da instituição.

Pode ser adotada política de segurança cibernética única por:

- I - conglomerado prudencial; e
- II - sistema cooperativo de crédito.

A política de segurança cibernética deve contemplar, no mínimo:

- I - os objetivos de segurança cibernética da instituição;
- II - os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética;
    - Esses procedimentos e controles devem abranger, no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.
- III - os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;

- IV - o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição;
    - os quais devem abranger inclusive informações recebidas das empresas prestadoras de serviços a terceiros.
- V - as diretrizes para:
    - a) a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios;
    - b) a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição;
    - c) a classificação dos dados e das informações quanto à relevância; e
    - d) a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes;
- VI - os mecanismos para disseminação da cultura de segurança cibernética na instituição, incluindo:
    - a) a implementação de programas de capacitação e de avaliação periódica de pessoal;
    - b) a prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros; e
    - c) o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética;
- VII - as iniciativas para compartilhamento de informações sobre os incidentes relevantes com as demais instituições.

As instituições devem estabelecer plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética, o qual deve abranger, no mínimo:

- I - as ações a serem desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;
- II - as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética; e
- III - a área responsável pelo registro e controle dos efeitos de incidentes relevantes.

As instituições devem designar diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes, o qual pode desempenhar outras funções na instituição, desde que não haja conflito de interesses.

Deve ser elaborado relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro, o qual deve abordar, no mínimo:

- I - a efetividade da implementação das ações;
- II - o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- III - os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e
- IV - os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

A política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser **documentados e revisados, no mínimo, anualmente**.

As políticas, estratégias e estruturas para gerenciamento de riscos, especificamente no tocante aos critérios de decisão quanto à terceirização de serviços, devem contemplar a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no País ou no exterior.

Previamente à contratação desses serviços, as instituições devem adotar procedimentos que contemplem:

- I - a adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e
- II - a verificação da capacidade do potencial prestador de serviço de assegurar:
    - a) o cumprimento da legislação e da regulamentação em vigor;
    - b) o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
    - c) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
    - d) a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;

- e) o acesso da instituição contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
- f) o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- g) a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos; e
- h) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

Os serviços de computação em nuvem abrangem a disponibilidade à instituição contratante, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

- I - processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;
- II - implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou
- III - execução, por meio da internet, de aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

As instituições devem assegurar que suas políticas para gerenciamento de riscos previstas na regulamentação em vigor disponham, no tocante à continuidade de negócios, sobre:

- I - o tratamento dos incidentes relevantes relacionados com o ambiente cibernético das atividades da instituição;
- II - os procedimentos a serem seguidos no caso da interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a substituição da empresa contratada e o reestabelecimento da operação normal da instituição; e
- III - os cenários de incidentes considerados nos testes de continuidade de negócios.

Os procedimentos adotados pelas instituições para gerenciamento de riscos previstos na regulamentação em vigor devem contemplar, no tocante à continuidade de negócios:

- I - o tratamento previsto para mitigar os efeitos dos incidentes relevantes e da interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados;
- II - o prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos; e
- III - a comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes que configurem uma situação de crise pela instituição financeira, bem como das providências para o reinício das suas atividades.

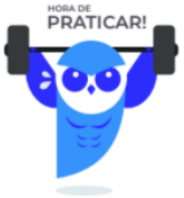
O Banco Central do Brasil pode vetar ou impor restrições para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem quando constatar, a qualquer tempo, a inobservância do disposto na Resolução, bem como a limitação à atuação do Banco Central do Brasil, estabelecendo prazo para a adequação dos referidos serviços.

APOSTA ESTRATÉGICA

Dos temas que abordamos, certamente a LGPD tem maiores chances de cobrança. Acredito que o conhecimento dos conceitos trazidos pela lei pode lhe ajudar a interpretar uma questão contextualizada, portanto, acho importante você conhecer os seguintes:

- **Dado pessoal**: informação relacionada a pessoa natural identificada ou identificável.
- **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.
- **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.
- **Controlador**: pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais.
- **Operador**: pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.
- **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).
- **Agentes de tratamento**: o controlador e o operador.
- **Anonimização**: utilização de meios técnicos por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

QUESTÕES ESTRATÉGICAS



1. (Cesgranrio/2021/Banco do Brasil/Escriturário)

Um determinado banco programou uma campanha de empréstimos a juros baixos, com o escopo de angariar clientes para sua carteira de mutuários. Após ampla campanha de divulgação, vários pretendentes compareceram às agências bancárias, onde receberam informações de que deveriam subscrever fichas com informações pessoais e autorizar que o banco as divulgasse sempre que julgasse necessário e sem que houvesse necessidade de essa divulgação ser previamente comunicada à clientela. Nos termos da Lei nº 13.709, de 14 de agosto de 2018, a cláusula de divulgação deve obedecer ao princípio da

a) negociação

b) taxação

c) menção

d) referência

e) transparência

Comentários:

Questão sobre a LGPD. A cláusula citada no enunciado diz respeito à permissão do tratamento e utilização dos dados pessoais por parte da instituição financeira, portanto, ela deverá atender ao princípio da transparência, que, de acordo com a LGPD, diz respeito à "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".

Gabarito: E

---

2. (Cesgranrio/2021/Banco do Brasil/Escriturário)

Ao realizar a matrícula do seu curso, o estudante preencheu uma ficha cadastral com os seguintes dados: nome, endereço, telefone, religião, estado civil, raça, nome dos pais, número de filhos e sindicato ao qual era filiado. Segundo a Lei Geral de Proteção de Dados (LGPD), consideram-se sensíveis os seguintes dados solicitados:

a) religião, raça e filiação a sindicato

b) religião, estado civil e filiação a sindicato

c) religião, estado civil e raça

d) número de filhos, raça e religião

e) número de filhos, raça e estado civil

Comentários:

A LGPD considera como 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;*"

Portanto, dentre os dados trazidos pelo enunciado, são dados sensíveis:

~~nome~~, ~~endereço~~, ~~telefone~~, **religião**, ~~estado civil~~, **raça**, ~~nome dos pais~~, ~~número de filhos~~ e **sindicato ao qual era filiado.**

Gabarito: A

---

3. (IADES/2019/BRB/Escriturário)

Considere que, em um órgão público, foi detectada a necessidade da atribuição de responsáveis para manterem registro das operações de tratamento de dados pessoais. De acordo com a Lei nº 13.709/2018, quem devem ser esses responsáveis?

a) Os agentes de tratamento de dados e o conselho diretor.

b) O controlador e o operador.

c) O presidente da República e o controlador.

d) A autoridade nacional e o operador.

e) O governante e a autoridade nacional.

Comentários

Conforme vimos no roteiro de revisão, os responsáveis por manterem registro das operações de tratamento de dados pessoais são o controlador e o operador, sendo a letra B o gabarito.

Relembrando:

Controlador: pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais.

Operador: pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

Gabarito: B

---

4. (Cebraspe/2021/Serpro/Cientista de Dados)

Para fins de aplicação da LGPD, dado pessoal é o que permite identificar ou tornar identificável, de forma inequívoca, um indivíduo.

Comentários

Correto. Conceito legal:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

Gabarito: Certo

---

5. (Cebraspe/2021/Serpro/Cientista de Dados)

A anonimização impossibilita que um dado seja associado, direta ou indiretamente, a um indivíduo.

Comentários

Correto! Com a anonimização um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Um dado anonimizado é o relativo a titular que não possa ser identificado.

Gabarito: Certo

---

6. (Cebraspe/2021/Serpro/Cientista de Dados)

O tratamento dos dados regulados deve atender ao princípio da adequação, o qual limita o tratamento ao mínimo necessário para a atividade.

Comentários

Questão errada, pois o princípio da adequação afirma que deve haver compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

É o princípio da necessidade que limita o tratamento ao mínimo necessário para as suas finalidades.

Gabarito: Errado

---

7. (Cebraspe/2021/Serpro/Cientista de Dados)

Consentimento é a manifestação do titular – pessoa natural ou jurídica – sobre o tratamento de seus dados para uma finalidade específica.

Comentários

Pegadinha: Consentimento é a manifestação do titular – pessoa natural ~~ou jurídica~~ – sobre o tratamento de seus dados para uma finalidade específica.

A Lei trata sobre dados pessoais, portanto, as pessoas jurídicas não estão incluídas no conceito de "titular".

> Art. 5º Para os fins desta Lei, considera-se:
>
> V - **titular**: **pessoa natural** a quem se referem os dados pessoais que são objeto de tratamento;
>
> XII - **consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o **tratamento de seus dados pessoais** para uma finalidade determinada;

Gabarito: Errado

---

8. (Cebraspe/2020/TJ PA/Analista de Sistemas)

De acordo com a Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), as atividades de tratamento de dados pessoais devem observar a boa-fé e o princípio

a) de dado pessoal, segundo o qual a informação é relacionada à pessoa natural identificada ou identificável.

b) de banco de dados, como um conjunto estruturado de dados pessoais estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

c) da anonimização, com a 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.

d) da prevenção, com a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

e) da eliminação, que é a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Comentários

A única alternativa que traz um princípio é a letra D, que trata do princípio da prevenção. Todas as demais trazem conceitos relacionados à aplicação da LGPD.

Gabarito: D

---

9. (Cebraspe/2020/Ministério da Economia/TI)

Entre os fundamentos que disciplinam a proteção de dados pessoais no Brasil, estão o respeito à privacidade, a autodeterminação informativa e a liberdade de expressão, de informação, de comunicação e de opinião.

Comentários

Questão correta. Todos os fundamentos trazidos no enunciado estão previstos na Lei.

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I - **o respeito à privacidade**;
>
> II - **a autodeterminação informativa**;
>
> III - **a liberdade de expressão, de informação, de comunicação e de opinião**;
>
> IV - a inviolabilidade da intimidade, da honra e da imagem;
>
> V - o desenvolvimento econômico e tecnológico e a inovação;
>
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Gabarito: Certo

10.(Cebraspe/2020/Ministério da Economia/TI)

A referida lei não se aplica ao tratamento de dados pessoais realizado por pessoa natural para fins econômicos.

Comentários

Está errado, pois não se aplica ao tratamento de dados pessoas realizado por pessoa natural para fins **não** econômicos.

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
>
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

Gabarito: Errado

11.(Cebraspe/2021/Serpro/Cientista de Dados)

É indispensável o consentimento do titular ao uso dos seus dados pessoais em pesquisas estatísticas que necessitem de tais informações, mesmo que as pesquisas sejam de evidente interesse público ou geral.

Comentários

A questão está errada, pois nesse caso é dispensável o consentimento do titular. Todavia, na medida do possível, deverá ser garantida a anonimização dos dados.

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

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

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

Gabarito: Errado

12.(Cebraspe/2021/Apex/Analista TI)

No seu processo de cadastramento de usuários, um site na Web obteve dados pessoais sensíveis de um usuário.

Nessa situação hipotética, de acordo com a Lei n.º 13.709/2018, o tratamento dos referidos dados pelo site poderá ser feito sem o consentimento do titular se

a) for indispensável para a proteção da vida.

b) houver demanda para a realização de estudos por órgão de pesquisa reconhecido pelo governo federal, sendo desnecessária, nesse caso, a anonimização dos dados.

c) for necessário para promover exclusivamente ações de marketing.

d) houver a necessidade de disponibilizar os dados para uma empresa parceira.

Comentários

As hipóteses de tratamento de dados pessoais sensíveis estão no art. 11 da LGPD. Vejamos seus incisos:

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - **sem fornecimento de consentimento do titular**, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da *Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)* ;

e) **proteção da vida ou da incolumidade física do titular ou de terceiro**;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Gabarito: A

13.(Cebraspe/2021/Serpro/Cientista de Dados)

O tratamento de dados pessoais previsto na LGPD poderá ser feito quando necessário para o atendimento dos interesses legítimos do controlador, exceto nas situações em que prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Comentários

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

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

Gabarito: Certo

14.(Cebraspe/2021/Serpro/Cientista de Dados)

O tratamento de dados pessoais poderá ser realizado a pedido do próprio titular dos dados quando for necessário para a execução de contrato do qual ele seja parte.

Comentários

Questão correta:

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

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;

Gabarito: Certo

15.(Cebraspe/2020/Ministério da Economia/TI)

Os dados pessoais serão eliminados após o término de seu tratamento, sendo autorizada a sua conservação para a finalidade de estudo por órgão de pesquisa, sendo garantida, sempre que possível, a anonimização desses dados.

Comentários

Correto! Previsão legal:

> 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.

Gabarito: Certo

16.(Cebraspe/2021/Serpro/Cientista de Dados)

Em caso de infração à LGPD cometida por agente de tratamento de dados, um dos critérios para a aplicação da sanção administrativa ao infrator é a sua condição econômica.

Comentários

Questão correta, pois a condição econômica do infrator é um dos critérios considerados na definição da sanção.

> Art. 52. § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
>
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
>
> II - a boa-fé do infrator;
>
> III - a vantagem auferida ou pretendida pelo infrator;
>
> **IV - a condição econômica do infrator;**
>
> V - a reincidência;
>
> VI - o grau do dano;

> VII - a cooperação do infrator;
>
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
>
> IX - a adoção de política de boas práticas e governança;
>
> X - a pronta adoção de medidas corretivas; e
>
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Gabarito: Certo

17.(Instituto AOCP/2020/Ministério da Justiça/Cientista de Dados)

Considerando o que dispõe a Lei nº 13.709/2018, de Proteção de Dados, assinale a alternativa correta.

a) O término do tratamento de dados pessoais ocorrerá, dentre outras hipóteses, quando se verificar que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada.

b) O titular dos dados pessoais não tem direito de obter do controlador, em relação aos dados do titular por ele tratados, a confirmação da existência de tratamento.

c) A portabilidade dos dados pessoais a outro fornecedor de serviço ou produto, prevista na Lei nº 13.709/2018, inclui dados que já tenham sido anonimizados pelo controlador.

d) O titular dos dados pessoais não tem direito de obter do controlador, em relação aos dados do titular por ele tratados, informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

e) Ao titular dos dados pessoais não é dado o direito de peticionar em relação aos seus dados, perante a autoridade nacional, contra o controlador.

Comentários

A – Certa. Trata-se de uma das hipóteses de término do tratamento de dados pessoais:

> 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.

B – Errada. Tem direito sim.

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> I - confirmação da existência de tratamento;

C – Errada. Os dados que já tenham sido anonimizados pelo controlador não são incluídos na portabilidade.

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
>
> § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

D – Errada. O titular tem esse direito.

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

E – Errada. É garantido ao titular o direito de peticionar à ANPD.

> Art. 55-J. Compete à ANPD:
>
> V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;

Gabarito: A

18.(Cesgranrio/2021/CEF/Técnico Bancário)

A Resolução CMN nº 4.893, de 26 de fevereiro de 2021, dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

Essa Resolução determina que a política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser, no mínimo, documentados e revisados

a) trimestralmente

b) semestralmente

c) anualmente

d) bienalmente

e) trienalmente

Comentários

Conforme a Resolução CMN 4.893/2021:

> *Art. 10. A política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser* ***documentados e revisados, no mínimo, anualmente***.

Gabarito: C

QUESTIONÁRIO DE REVISÃO E APERFEIÇOAMENTO

Perguntas

1) O que é um dado anonomizado?

2) Nos termos da LGPD, quem é o controlador e quem é o operador?

3) No âmbito das atividades de tratamento de dados pessoais, o que significa o princípio da necessidade?

4) No âmbito das atividades de tratamento de dados pessoais, o que significa o princípio da adequação?

5) Pode ser realizado tratamento de dados pessoais para fins de proteção de crédito?

6) É possível realizar o tratamento de dados pessoais sensíveis sem o consentimento do titular?

7) As operadoras de planos privados de assistência à saúde podem realizar o tratamento de dados de saúde para a prática de seleção de riscos na contratação?

8) Qual o período máximo pelo qual a ANPD pode suspender o exercício da atividade de tratamento de dados a que se refere a infração?

9) Qual o limite da multa aplicável pela ANPD?

10) Caso um banco contrate uma empresa para prestar serviços de implantação e execução do seu aplicativo, de quem é a responsabilidade pela integridade e pelo sigilo dos dados?

11) A política de segurança cibernética deve ser formulada com base e princípios que busquem assegurar o que?

12) Em que documento devem estar as rotinas e procedimentos a serem utilizados na prevenção e na resposta de incidentes?

13) O diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes pode desempenhar outra função dentro da instituição?

14) A política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser documentados e revisados com que periodicidade?

15) A execução, por meio da internet, de aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços, é considerada que tipo de serviços de computação?

Perguntas com respostas

1) O que é um dado anonomizado?

É um dado relativo a titular que não possa ser identificado.

2) Nos termos da LGPD, quem é o controlador e quem é o operador?

Controlador é a pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais. O operador, por sua vez, é a pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

3) No âmbito das atividades de tratamento de dados pessoais, o que significa o princípio da necessidade?

Que o tratamento dos dados deve ser limitado ao mínimo necessário para a realização de sua finalidade.

4) No âmbito das atividades de tratamento de dados pessoais, o que significa o princípio da adequação?

Que deve haver compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

5) Pode ser realizado tratamento de dados pessoais para fins de proteção de crédito?

Sim, trata-se de uma das hipóteses em que a LGPD expressamente permite a realização de tratamento de dados pessoais.

6) É possível realizar o tratamento de dados pessoais sensíveis sem o consentimento do titular?

Sim, mas apenas nas hipóteses admitidas pela LGPD, como o cumprimento de obrigação legal ou regulatória pelo controlador, a realização de estudos por órgão de pesquisa, o exercício regular de direito e a proteção da vida.

7) As operadoras de planos privados de assistência à saúde podem realizar o tratamento de dados de saúde para a prática de seleção de riscos na contratação?

Não. É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

8) Qual o período máximo pelo qual a ANPD pode suspender o exercício da atividade de tratamento de dados a que se refere a infração?

6 meses, prorrogáveis por igual período.

9) Qual o limite da multa aplicável pela ANPD?

Até 2% do faturamento do último exercício, excluídos os tributos, limitada, no total, a R$ 50 milhões por infração.

10) Caso um banco contrate uma empresa para prestar serviços de implantação e execução do seu aplicativo, de quem é a responsabilidade pela integridade e pelo sigilo dos dados?

A responsabilidade é do banco.

11) A política de segurança cibernética deve ser formulada com base e princípios que busquem assegurar o que?

A confidencialidade, a integralidade e a disponibilidade dos dados e dos sistemas de informações utilizados.

12) Em que documento devem estar as rotinas e procedimentos a serem utilizados na prevenção e na resposta de incidentes?

No plano de ação e de resposta a incidentes.

13) O diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes pode desempenhar outra função dentro da instituição?

Sim, desde que não haja conflito de interesses.

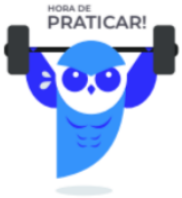
14) A política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser documentados e revisados com que periodicidade?

No mínimo anualmente.

15) A execução, por meio da internet, de aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços, é considerada que tipo de serviços de computação?

Serviço de computação em nuvem.

LISTA DE QUESTÕES ESTRATÉGICAS



1. (Cesgranrio/2021/Banco do Brasil/Escriturário)

Um determinado banco programou uma campanha de empréstimos a juros baixos, com o escopo de angariar clientes para sua carteira de mutuários. Após ampla campanha de divulgação, vários pretendentes compareceram às agências bancárias, onde receberam informações de que deveriam subscrever fichas com informações pessoais e autorizar que o banco as divulgasse sempre que julgasse necessário e sem que houvesse necessidade de essa divulgação ser previamente comunicada à clientela. Nos termos da Lei nº 13.709, de 14 de agosto de 2018, a cláusula de divulgação deve obedecer ao princípio da

a) negociação

b) taxação

c) menção

d) referência

e) transparência

2. (Cesgranrio/2021/Banco do Brasil/Escriturário)

Ao realizar a matrícula do seu curso, o estudante preencheu uma ficha cadastral com os seguintes dados: nome, endereço, telefone, religião, estado civil, raça, nome dos pais, número de filhos e sindicato ao qual era filiado. Segundo a Lei Geral de Proteção de Dados (LGPD), consideram-se sensíveis os seguintes dados solicitados:

a) religião, raça e filiação a sindicato

b) religião, estado civil e filiação a sindicato

c) religião, estado civil e raça

d) número de filhos, raça e religião

e) número de filhos, raça e estado civil

3. (IADES/2019/BRB/Escriturário)

Considere que, em um órgão público, foi detectada a necessidade da atribuição de responsáveis para manterem registro das operações de tratamento de dados pessoais. De acordo com a Lei nº 13.709/2018, quem devem ser esses responsáveis?

a) Os agentes de tratamento de dados e o conselho diretor.

b) O controlador e o operador.

c) O presidente da República e o controlador.

d) A autoridade nacional e o operador.

e) O governante e a autoridade nacional.

4. (Cebraspe/2021/Serpro/Cientista de Dados)

Para fins de aplicação da LGPD, dado pessoal é o que permite identificar ou tornar identificável, de forma inequívoca, um indivíduo.

5. (Cebraspe/2021/Serpro/Cientista de Dados)

A anonimização impossibilita que um dado seja associado, direta ou indiretamente, a um indivíduo.

6. (Cebraspe/2021/Serpro/Cientista de Dados)

O tratamento dos dados regulados deve atender ao princípio da adequação, o qual limita o tratamento ao mínimo necessário para a atividade.

7. (Cebraspe/2021/Serpro/Cientista de Dados)

Consentimento é a manifestação do titular – pessoa natural ou jurídica – sobre o tratamento de seus dados para uma finalidade específica.

8. (Cebraspe/2020/TJ PA/Analista de Sistemas)

De acordo com a Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), as atividades de tratamento de dados pessoais devem observar a boa-fé e o princípio

a) de dado pessoal, segundo o qual a informação é relacionada à pessoa natural identificada ou identificável.

b) de banco de dados, como um conjunto estruturado de dados pessoais estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

c) da anonimização, com a 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.

d) da prevenção, com a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

e) da eliminação, que é a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

9. (Cebraspe/2020/Ministério da Economia/TI)

Entre os fundamentos que disciplinam a proteção de dados pessoais no Brasil, estão o respeito à privacidade, a autodeterminação informativa e a liberdade de expressão, de informação, de comunicação e de opinião.

10.(Cebraspe/2020/Ministério da Economia/TI)

A referida lei não se aplica ao tratamento de dados pessoais realizado por pessoa natural para fins econômicos.

11.(Cebraspe/2021/Serpro/Cientista de Dados)

É indispensável o consentimento do titular ao uso dos seus dados pessoais em pesquisas estatísticas que necessitem de tais informações, mesmo que as pesquisas sejam de evidente interesse público ou geral.

12.(Cebraspe/2021/Apex/Analista TI)

No seu processo de cadastramento de usuários, um site na Web obteve dados pessoais sensíveis de um usuário.

Nessa situação hipotética, de acordo com a Lei n.º 13.709/2018, o tratamento dos referidos dados pelo site poderá ser feito sem o consentimento do titular se

a) for indispensável para a proteção da vida.

b) houver demanda para a realização de estudos por órgão de pesquisa reconhecido pelo governo federal, sendo desnecessária, nesse caso, a anonimização dos dados.

c) for necessário para promover exclusivamente ações de marketing.

d) houver a necessidade de disponibilizar os dados para uma empresa parceira.

13.(Cebraspe/2021/Serpro/Cientista de Dados)

O tratamento de dados pessoais previsto na LGPD poderá ser feito quando necessário para o atendimento dos interesses legítimos do controlador, exceto nas situações em que prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

14.(Cebraspe/2021/Serpro/Cientista de Dados)

O tratamento de dados pessoais poderá ser realizado a pedido do próprio titular dos dados quando for necessário para a execução de contrato do qual ele seja parte.

15.(Cebraspe/2020/Ministério da Economia/TI)

Os dados pessoais serão eliminados após o término de seu tratamento, sendo autorizada a sua conservação para a finalidade de estudo por órgão de pesquisa, sendo garantida, sempre que possível, a anonimização desses dados.

16.(Cebraspe/2021/Serpro/Cientista de Dados)

Em caso de infração à LGPD cometida por agente de tratamento de dados, um dos critérios para a aplicação da sanção administrativa ao infrator é a sua condição econômica.

17.(Instituto AOCP/2020/Ministério da Justiça/Cientista de Dados)

Considerando o que dispõe a Lei nº 13.709/2018, de Proteção de Dados, assinale a alternativa correta.

a) O término do tratamento de dados pessoais ocorrerá, dentre outras hipóteses, quando se verificar que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada.

b) O titular dos dados pessoais não tem direito de obter do controlador, em relação aos dados do titular por ele tratados, a confirmação da existência de tratamento.

c) A portabilidade dos dados pessoais a outro fornecedor de serviço ou produto, prevista na Lei nº 13.709/2018, inclui dados que já tenham sido anonimizados pelo controlador.

d) O titular dos dados pessoais não tem direito de obter do controlador, em relação aos dados do titular por ele tratados, informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

e) Ao titular dos dados pessoais não é dado o direito de peticionar em relação aos seus dados, perante a autoridade nacional, contra o controlador.

18.(Cesgranrio/2021/CEF/Técnico Bancário)

A Resolução CMN nº 4.893, de 26 de fevereiro de 2021, dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

Essa Resolução determina que a política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser, no mínimo, documentados e revisados

a) trimestralmente

b) semestralmente

c) anualmente

d) bienalmente

e) trienalmente

GABARITO

1. E
2. A
3. B
4. Certo
5. Certo
6. Errado
7. Errado
8. D
9. Certo
10. Errado
11. Errado
12. A
13. Certo
14. Certo
15. Certo
16. Certo
17. A
18. C

REFERÊNCIAS BIBLIOGRÁFICAS

Lei 13.709/2018 (LGPD)

Resolução CMN 4.893/2021 (Segurança Cibernética)

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.

Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.