**Resumo sobre a Lei Geral de Proteção de Dados (LGPD)**

**Os requisitos para o tratamento de dados pessoais são os seguintes:**

1. Consentimento do titular dos dados.
2. Cumprimento de obrigação legal ou regulatória pelo controlador.
3. Tratamento realizado pela administração pública para políticas públicas.
4. Realização de estudos por órgãos de pesquisa, garantindo a anonimização dos dados.
5. Execução de contrato ou procedimentos preliminares a pedido do titular dos dados.
6. Exercício regular de direitos em processos judiciais, administrativos ou arbitrais.
7. Proteção da vida ou incolumidade física do titular ou de terceiros.
8. Tutela da saúde em procedimentos realizados por profissionais de saúde ou autoridades sanitárias.
9. Atendimento a interesses legítimos do controlador ou terceiros, desde que não prevaleçam direitos e liberdades fundamentais do titular.
10. Proteção do crédito.

Além disso, a lei estabelece requisitos adicionais relacionados ao consentimento, acesso às informações, mudanças de finalidade e tratamento baseado em legítimo interesse do controlador. A autoridade nacional também pode solicitar relatórios de impacto à proteção de dados em determinados casos.

**O tratamento de dados pessoais sensíveis só é permitido nas seguintes situações:**

1. Consentimento específico e destacado do titular ou seu responsável legal para finalidades específicas.
2. Cumprimento de obrigações legais ou regulatórias pelo controlador.
3. Tratamento compartilhado de dados necessários para a execução de políticas públicas ou estudos por órgãos de pesquisa, garantindo, quando possível, a anonimização dos dados.
4. Exercício regular de direitos, inclusive em contratos, processos judiciais e administrativos, ou arbitrais.
5. Proteção da vida ou da integridade física do titular ou de terceiros.
6. Tutela da saúde, exclusivamente em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridades sanitárias.
7. Garantia da prevenção à fraude e à segurança do titular em processos de identificação e autenticação de cadastros em sistemas eletrônicos, resguardados os direitos mencionados na Lei de Proteção de Dados.

Além disso, o tratamento de dados pessoais sensíveis deve ser vedado ou regulamentado quando há comunicação ou compartilhamento de dados entre controladores com o objetivo de obter vantagem econômica, exceto em casos de prestação de serviços de saúde e outros mencionados na lei.

Os dados anonimizados não são considerados dados pessoais, a menos que possam ser revertidos de forma razoável. A pseudonimização também é permitida, desde que os dados percam a possibilidade de associação direta ou indireta a um indivíduo, exceto por informações adicionais mantidas separadamente pelo controlador em ambiente seguro.

No contexto de estudos em saúde pública, os órgãos de pesquisa podem acessar bases de dados pessoais para fins de estudos e pesquisas, desde que os dados sejam tratados exclusivamente dentro do órgão, em ambiente controlado e seguro, garantindo a anonimização ou pseudonimização dos dados e respeitando os padrões éticos relacionados a estudos e pesquisas. A divulgação dos resultados desses estudos não deve revelar dados pessoais e o acesso aos dados é regulamentado pelas autoridades competentes.

**O tratamento de dados pessoais de crianças e adolescentes deve:**

Ser realizado no melhor interesse deles e de acordo com a legislação aplicável. Para crianças, é necessário obter o consentimento específico e destacado de pelo menos um dos pais ou responsável legal. Os controladores de dados devem tornar públicas informações sobre os tipos de dados coletados, sua utilização e os procedimentos para exercer os direitos relacionados. A coleta de dados pessoais de crianças sem consentimento é permitida apenas em situações específicas, como para entrar em contato com os pais ou responsável legal, sendo proibida a sua divulgação a terceiros sem consentimento. Os controladores não devem exigir informações pessoais além das estritamente necessárias para a participação em atividades online. Devem ser feitos esforços razoáveis para verificar o consentimento dado pelo responsável, levando em consideração as tecnologias disponíveis. As informações sobre o tratamento de dados devem ser fornecidas de forma simples, clara e acessível, levando em conta as características das crianças.

**O tratamento de dados pessoais termina nas seguintes situações:**

1. Quando a finalidade do tratamento é alcançada, ou quando os dados não são mais necessários para atingir a finalidade específica desejada;
2. No fim do período de tratamento estabelecido;
3. Após a comunicação do titular, inclusive quando ele revoga seu consentimento, desde que não haja interesse público;
4. Quando há determinação da autoridade nacional devido a violação da lei.

Após o término do tratamento, os dados pessoais devem ser eliminados, mas podem ser mantidos para as seguintes finalidades:

1. Cumprimento de obrigações legais ou regulatórias pelo controlador;
2. Uso em estudos por órgãos de pesquisa, com a garantia de anonimização dos dados, sempre que possível;
3. Transferência a terceiros, desde que respeitados os requisitos de tratamento de dados estabelecidos na lei;
4. Uso exclusivo pelo controlador, com os dados anonimizados e vedado o acesso por terceiros.

**Os direitos do titular de dados pessoais, de acordo com a legislação mencionada, incluem:**

1. Titularidade dos dados pessoais.
2. Direitos fundamentais de liberdade, intimidade e privacidade.
3. Confirmação da existência de tratamento.
4. Acesso aos dados.
5. Correção de dados incompletos, inexatos ou desatualizados.
6. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei.
7. Portabilidade dos dados para outro fornecedor de serviço ou produto.
8. Eliminação dos dados pessoais tratados com consentimento, exceto em casos previstos por lei.
9. Informação sobre compartilhamento de dados com entidades públicas e privadas.
10. Informação sobre a possibilidade de não fornecer consentimento e suas consequências.
11. Revogação do consentimento.
12. Peticionar perante a autoridade nacional em relação aos dados pessoais.
13. Opor-se ao tratamento realizado com base em dispensa de consentimento.
14. Exercer os direitos mediante requerimento expresso ao agente de tratamento.
15. Receber resposta do controlador sobre a adoção imediata de providências ou indicação do agente de tratamento.
16. Exercer os direitos sem custos para o titular, conforme regulamentação.
17. Notificar os agentes de tratamento sobre a correção, eliminação, anonimização ou bloqueio dos dados compartilhados.
18. Portabilidade não inclui dados já anonimizados pelo controlador.
19. Exercer o direito perante os organismos de defesa do consumidor.
20. Obter confirmação de existência ou acesso aos dados pessoais de forma simplificada ou por declaração completa.
21. Armazenamento dos dados pessoais em formato que facilite o acesso.
22. Fornecimento das informações e dados em formato eletrônico ou impresso.
23. Solicitar cópia eletrônica integral dos dados pessoais tratados com base no consentimento ou contrato.
24. Revisar decisões automatizadas que afetem seus interesses.
25. Receber informações claras sobre os critérios e procedimentos das decisões automatizadas.
26. Possibilidade de auditoria em tratamentos automatizados de dados pessoais.
27. Dados pessoais referentes ao exercício regular de direitos não podem ser utilizados em prejuízo do titular.
28. Defesa dos interesses e direitos do titular em juízo, individual ou coletivamente.

Esses são os direitos básicos do titular de dados pessoais conforme expressos na legislação mencionada.

**As regras referem-se ao tratamento de dados pessoais pelas pessoas jurídicas de direito público e empresas públicas e sociedades de economia mista têm como principais regras:**

1. O tratamento de dados pessoais deve ser realizado para o cumprimento de finalidades públicas, no interesse público e de acordo com as competências legais ou atribuições do serviço público.
2. As pessoas jurídicas devem informar claramente as hipóteses em que realizam o tratamento de dados, fornecendo informações atualizadas sobre a previsão legal, finalidade, procedimentos e práticas utilizadas.
3. Deve ser designado um encarregado para operações de tratamento de dados pessoais.
4. As operações de tratamento de dados devem ser publicizadas de acordo com as disposições da autoridade nacional.
5. As empresas públicas e sociedades de economia mista devem seguir as mesmas regras aplicáveis às pessoas jurídicas de direito privado.
6. Os dados devem ser mantidos em formato interoperável e estruturado para o uso compartilhado, visando a execução de políticas públicas, prestação de serviços públicos e disseminação de informações.
7. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuições legais, respeitando os princípios de proteção de dados.
8. O Poder Público não pode transferir dados pessoais a entidades privadas, exceto em casos específicos previstos na lei.
9. A comunicação ou uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado requer informação à autoridade nacional e consentimento do titular, exceto em casos previstos na lei.
10. A autoridade nacional pode solicitar informações aos órgãos e entidades do poder público e emitir parecer técnico para garantir o cumprimento da lei.
11. A autoridade nacional pode estabelecer normas complementares para as atividades de comunicação e uso compartilhado de dados pessoais.

**As responsabilidades descritas nos artigos mencionados são:**

1. A Autoridade Nacional de Proteção de Dados (ANPD) tem a responsabilidade de enviar um informe com medidas cabíveis para fazer cessar a violação da Lei de Proteção de Dados Pessoais quando ocorrer uma infração por órgãos públicos.
2. A ANPD pode solicitar aos agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e boas práticas para o tratamento de dados pessoais pelo Poder Público.

**A transferência internacional de dados pessoais só é permitida nos seguintes casos:**

1. Para países ou organizações internacionais que ofereçam um nível adequado de proteção de dados pessoais.
2. Quando o controlador oferecer garantias de cumprimento dos princípios e direitos do titular, conforme estabelecido na lei, através de cláusulas contratuais específicas, cláusulas-padrão contratuais, normas corporativas globais, selos, certificados ou códigos de conduta regularmente emitidos.
3. Quando a transferência for necessária para cooperação jurídica internacional entre órgãos públicos de inteligência, investigação e persecução, de acordo com instrumentos de direito internacional.
4. Quando a transferência for necessária para a proteção da vida ou da integridade física do titular ou de terceiros.
5. Quando autorizada pela autoridade nacional.
6. Quando resultar de compromissos assumidos em acordos de cooperação internacional.
7. Quando necessária para a execução de política pública ou atribuição legal do serviço público, com publicidade adequada.
8. Quando o titular fornecer consentimento específico e destacado para a transferência, com informação prévia sobre a natureza internacional da operação.
9. Quando necessário para atender às hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

A avaliação do nível de proteção de dados do país estrangeiro ou organismo internacional é realizada pela autoridade nacional, considerando normas, natureza dos dados, princípios de proteção de dados, medidas de segurança, garantias judiciais e institucionais, e outras circunstâncias específicas relativas à transferência.

A definição de cláusulas-padrão contratuais e verificação de garantias contratuais específicas são feitas pela autoridade nacional, que pode solicitar informações adicionais e realizar diligências de verificação. A autoridade nacional pode designar organismos de certificação para realizar essas tarefas, e seus atos podem ser revisados ou anulados pela autoridade nacional. As garantias de observância dos princípios de proteção e direitos do titular também são analisadas com base nas medidas técnicas e organizacionais adotadas pelo operador.

Quaisquer alterações nas garantias apresentadas devem ser comunicadas à autoridade nacional.

**Os controladores e operadores de dados pessoais devem:**

Manter registros das operações de tratamento de dados, inclusive com base no legítimo interesse. A autoridade nacional pode exigir que o controlador elabore um relatório de impacto à proteção de dados pessoais, contendo informações sobre os tipos de dados coletados, metodologia de coleta e segurança, além das medidas adotadas para mitigação de riscos. O operador deve tratar os dados de acordo com as instruções do controlador, que deve verificar o cumprimento das instruções e das normas aplicáveis. A autoridade nacional pode estabelecer padrões de interoperabilidade, portabilidade, acesso aos dados e tempo de guarda dos registros, levando em consideração a necessidade e a transparência.

**O encarregado pelo tratamento de dados pessoais é:**

Uma figura estabelecida pelo Artigo 41 desta lei e deve este controlador de dados designar um encarregado, cuja identidade e informações de contato devem ser divulgadas publicamente. As responsabilidades do encarregado incluem receber reclamações e comunicações dos titulares dos dados, lidar com comunicações da autoridade nacional, orientar funcionários sobre práticas de proteção de dados e executar outras atribuições determinadas pelo controlador. A autoridade nacional pode estabelecer normas complementares relacionadas à definição e atribuições do encarregado.

**O controlador ou operador de dados pessoais é:**

Responsável por reparar os danos patrimoniais, morais, individuais ou coletivos causados a terceiros em violação à legislação de proteção de dados pessoais. O operador pode ser responsabilizado solidariamente com o controlador quando descumprir as obrigações legais ou não seguir as instruções lícitas do controlador. Os controladores diretamente envolvidos no tratamento dos dados também podem ser responsabilizados solidariamente. O ônus da prova pode ser invertido a favor do titular dos dados quando for verossímil sua alegação ou quando a produção de prova for excessivamente onerosa para ele. Ações de reparação por danos coletivos podem ser exercidas coletivamente em juízo. Aquele que reparar o dano tem direito de regresso contra os demais responsáveis. Os agentes de tratamento não serão responsabilizados se provarem que não realizaram o tratamento atribuído, que não houve violação à legislação de proteção de dados ou que o dano foi decorrente de culpa exclusiva do titular dos dados ou de terceiro. O tratamento de dados será considerado irregular quando não observar a legislação ou não fornecer a segurança esperada pelo titular dos dados, e o controlador ou operador que deixar de adotar as medidas de segurança previstas na lei será responsável pelos danos decorrentes da violação da segurança dos dados. As violações do direito do titular no âmbito das relações de consumo seguem as regras de responsabilidade da legislação aplicável.

**Os agentes de tratamento de dados devem:**

Adotar medidas de segurança para proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado. A autoridade nacional pode estabelecer padrões técnicos mínimos para garantir a segurança dos dados, considerando a natureza das informações, o tipo de tratamento e o estado atual da tecnologia. As medidas de segurança devem ser implementadas desde a concepção do produto ou serviço até a sua execução. Os agentes de tratamento e qualquer pessoa envolvida no processo devem garantir a segurança da informação mesmo após o término do tratamento. O controlador deve comunicar à autoridade nacional e ao titular qualquer incidente de segurança que possa causar risco ou dano relevante aos titulares, fornecendo informações sobre o incidente, as medidas de segurança utilizadas, os riscos relacionados e as ações tomadas para mitigar os efeitos. A autoridade nacional pode determinar medidas adicionais, como divulgação do incidente e ações para reverter ou mitigar seus efeitos. Os sistemas utilizados no tratamento de dados pessoais devem atender aos requisitos de segurança, boas práticas, governança e princípios gerais estabelecidos na Lei.

**As sanções administrativas previstas no texto são as seguintes:**

1. Advertência, com prazo para adoção de medidas corretivas.
2. Multa simples, de até 2% do faturamento da pessoa jurídica, limitada a R$ 50.000.000,00 por infração.
3. Multa diária, observado o limite total da multa simples.
4. Publicização da infração após confirmação.
5. Bloqueio dos dados pessoais até regularização.
6. Eliminação dos dados pessoais.
7. Suspensão parcial do funcionamento do banco de dados por até 6 meses, prorrogável.
8. Suspensão do exercício da atividade de tratamento dos dados pessoais por até 6 meses, prorrogável.
9. Proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados.

As sanções são aplicadas após procedimento administrativo, considerando a gravidade da infração, a boa-fé do infrator, a vantagem obtida pelo infrator, a condição econômica do infrator, entre outros critérios. O valor da multa diária é determinado com base na gravidade da falta e no dano causado, e as metodologias para o cálculo das multas devem ser estabelecidas pela autoridade nacional em regulamento.