Valideinfo Web

O Poder da Informação ao seu Alcance

ValideInfo, *Compliance* LGPD

CNPJ: 13.342.264/0001-75

www.valideinfoweb.com.br

2020

ValideInfo

Serviço de Tecnologia da Informações e Soluções do Dado desde 2009 no mercado, nos destacamos pela solidez de nossa relação com nossos clientes e pela constante preocupação em inovar e fornece ferramentas seguras, e com a preocupação em auxiliar os nossos Clientes na redução de custos com serviços de informações.

Plataforma Multifuncional para todos os Segmentos, agregamos na operação e negócio, informações e soluções 'online_realtime' através de fontes oficiais e públicas com a finalidade de auxiliar e oferecer segurança para as Empresas nos processos como tomada de decisão, fraude, risco, validação cadastral e fiscal, jurídico, compliance, cobrança entre outros, em conformidade com a nova Lei do Dado.

Módulos oficiais e públicas com informações de pessoas físicas - pessoas jurídicas – veicular, auxiliando as Empresas nos processos como cadastro, localização, identificação, validação, crédito, fraude, cobrança, compliance, jurídico, RH, MKT, comercial, entre outros... *Tudo em um único lugar!*

Objetivo: Agregar e auxiliar as Empresas na redução dos gastos com informações, trazendo os dados oficiais e públicos '*online_realtime'* com a automação dos nossos serviços em sua ferramenta.

Realizamos processos via *web* e *webservice* e/ou lote, através de fontes e links oficiais trazendo todo cadastro de pessoas jurídicas, pessoas físicas e veicular. Temos protesto nacional '*sem custo'*, outros registros provenientes de fontes públicas e oficiais, score de crédito, informações pertinentes para detecção de intenção de golpes ou operações fraudulentas - alertas, monitoramento de carteira de clientes e /ou fornecedores, enriquecimento de base de dados, enriquecimento por telefone, prospecções qualificada *'nacional'*, disparo de E-mails e SMS, APIs, e muito mais...

Somos uma empresa de tecnologia da informação do dado: Agregando e auxiliando as empresas a explorar novas e melhores abordagens comerciais focando em melhores resultados. Trabalhamos para que o seu sucesso aconteça, gerando ações que promovam resultados a curto, médio e longo prazo. Plataforma que agrega informações de todos os tipos, livrando sua empresa da preocupação sobre como capturar e estruturar dados espalhados pelo mundo. Sempre seremos à favor dos negócios...

Missão: Oferecer produtos para gerar e potencializar resultados, desempenhar um atendimento rápido e eficaz contribuindo com o desenvolvimento de nossos clientes e colaboradores, desenvolver e inovar processos e produtos para que nossos clientes/parceiros obtenham sucesso em suas ações.

Visão: Impactar profundamente a precisão de geração de resultados e vantagens competitivas das empresas no mercado global.

Importante:

- Não somos bureau de informação e sim uma Empresa de informação do dado,
- Totalmente customizados *(sem custo)*, fornecendo toda documentação técnica *(webservice)* gratuitamente,
- Dentro da conformidade da nova Lei do Dado,

Acessos: Via Web / Webservice / Lote.

Tecnicamente:

Seguro através do Servidor na UNDER (Data Center Tier 3).
Temos um Cloud Windows com Sistema Operacional Windows Server 2012 R2 - 64 bits, IIS8, com Banco de Dados MongoDB. Banco de dados via Under, não possui acesso externo, evitando assim conexões indevidas.

Características Servidor Under:

- Servidor:
Cloud com Datacenter TIER 3 (máximo de uptime nos Datacenters em São Paulo)
Proteção ANTI DDoS
10 Cores com processadores Xeon de 2.30GHz
20GB de memória RAM
700GB SSD

1 Plataforma com 100GB de Backup
100GB de Storage NAS
10TB de transferência
2GB de link entrada/saída

- Conectividade:
Conexão redundante à internet
Peering com a maioria das nuvens que estão no Brasil
Proteção anti ddos (incluso até 1Gbps)
Roteamento e rede 100% Juniper
Projetamos nossa rede para ter um alto uptime

- Datacenter:
Ambiente projetado para ficar operando continuamente
A Under escolheu um excelente fornecedor e datacenter, neste quesito estamos tranquilos que estamos com o melhor produto
Colocation gerenciado

Toda gestão dos hardwares, instalação física e de seu cabeamento é incluso

O cliente não precisa ter técnicos para fazer estes serviços localmente

Nosso serviço de colocation é pensado para o cliente gerenciar remotamente, de qualquer lugar do mundo

Menos custos para gestão da TI, pois a princípio não precisa de técnicos locais em São Paulo ou Rio de Janeiro

Monitoramento do hardware via NOC e acompanhamento da correção junto a garantia do fabricante incluso em caso de falhas de hardware.

Carta de Conformidade

Valide

CARTA DE CONFORMIDADE COM A LEI 13.709/2018

ValideInfo Serviço de Informações e Soluções em Banco de Dados Ltda (ValideInfo Web), pessoa jurídica de direito privado, inscrita no CNPJ sob o n.º 13.342.264/0001-75, com sede na Rua Barão do Rio Branco, 330 – Cj. 71 – Vila Costa – Cidade Suzano/SP – 08675-030e com escritório comercial na Av. Paulista, n.º 2073 – Horsa II – 17º andar, Conj. 1702 – Cerqueira Cesar – Cidade de São Paulo – 01311-300, declara para todos os fins, que os seus programas e, sistemas encontram-se adequados e em conformidade com a **LEI 13.709/2018 (Lei de Proteção de Dados Pessoais).**

Isto posto, não há qualquer prejuízo ou, desconformidade na utilização de seus sistemas e programas, por parte de qualquer cliente contratante.

Por fim, informa que todas as adequações legais à referida lei de Proteção de Dados Pessoais, são de inteira responsabilidade à empresa **ValideInfo Serviço de Informações e Soluções em Banco de Dados Ltda.**

VALIDEINFO SERVIÇOS DE INFORMAÇÕES E SOLUÇÕES EM BANCO DE DADOS LTDA
CNPJ: 13.342.264/0001-75

São Paulo, 18 de abril de 2019.

VALIDEINFO WEB

CNPJ SOB O N.º 13.342.264/0001-75

Principais Conceitos

- Dado Pessoal: Qualquer informação relacionada a uma pessoa natural(física)que possa ser identificada a partir dos dados coletados. É um conceito central da LGPD, que busca proteger a privacidade dos titulares de dados pessoais
que sejam objeto de tratamento (art. 5o, I).
- Titular: Pessoa natural (física) a quem se referem os dados pessoais que são objeto de tratamento (art. 5°,V).
- Tratamento: Toda operação realizada com dados pessoais, como coleta, utilização, processamento, armazenamento e eliminação (art. 5o,X).
- **Controlador:** Pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5o, VI).
Direitos do Titular: A nova legislação estabelece os seguintes direitos dos titulares (art. 18):
• Confirmar a existência de tratamento de seus dados pessoais;
• Acessar seus dados pessoais;
• Corrigir dados pessoais incompletos, inexatos ou desatualizados;
• Anonimização, bloqueio ou eliminação de dados pessoais desnecessários, excessivos ou tratados em desconformidade com a LPD;
• Portabilidade de dados pessoais a outro fornecedor de produto ou serviço;
• Eliminação de dados tratados como seu consentimento;
• Obtenção de informações sobre as entidades públicas e privadas com asquais o controlador realizouo compartilhamentode dados pessoais;
• Obtenção de informações sobre a possibilidade de não consentir com o tratamento de dados pessoais e sobre as consequências da negativa; e
• Revogação do consentimento dado para o tratamento de dados pessoais.
Transparência Internacional de Dados: Permitida somente nas hipóteses previstas na LPD (art. 33), entre elas:
• Para países que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD;
• Quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;ou
• Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência.
Principais Objetivos: Assegurar o direito à privacidade e à proteção de dados pessoais dos cidadãos, por meio de práticas:
- Privacidade: transparentes e seguras, garantindo direitos e liberdades fundamentais.
- Ttransparêcia: Estabelecer regras claras sobre tratamento de dados pessoais por empresas.
- Desenvolvimento: Fomentar o desenvolvimento econômico e tecnológico.
- Padronização: Estabelecimento de regras únicas e harmônicas sobre tratamento de dados pessoais, independentemente do setor da economia, facilitando as relações comerciais e reduzindo custos decorrentes de incompatibilidades sistêmicas de tratamentos feitos por agentes diversos.
- Proteção do Mercado: Fortalecer a segurança das relações jurídicas e a confiança do titular no tratamento de dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo.
- Concorrência: Promover a concorrência no mercado, facilitando a portabilidade.

- ValideInfo e a LGPD: Com previsão expressa em contrato, a ValideInfo presta as devidas informações com relação à sua atuação no mercado dentro da legalidade prevista na LGPD;
- 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;
- § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
- § 4º 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.
A VALIDEINFO é uma empresa que serve como facilitadora na pesquisa de dados totalmente públicos encontrados em sites e plataformas digitais de órgãos públicos, com isso, demonstra-se a finalidade totalmente idônea da VALIDEINFO, bem como a boa-fé notratamento dos dados pessoais públicos e em total acordo com o interesse público que justifica a publicidade de tais dados como forma de transparência e de se buscar equilíbrio e justiça na sociedade.

Código de Ética

1- Introdução

O Valideinfo Serviço de Tecnologia da Informações e Soluções do Dado, é uma Empresa que atua no segmento dos dados de pessoas físicas, pessoas jurídicas e veicular em fontes públicas e oficiais online e realtime, visando o seu crescimento, dentro de princípios éticos e a satisfação dos seus clientes e instituições congêneres, buscando sempre manter sólida reputação, com a consciência de sua responsabilidade social e ambiental. Suas atividades devem sempre se pautar pela integridade, confiança e lealdade, bem como pelo respeito e valorização do ser humano e sua privacidade, individualidade e dignidade, sem quaisquer preconceitos e formas de discriminação.

2- Objetivo

Este Código de Ética tem como finalidade dirimir questões relacionadas: (i) ao cumprimento de regras de convivência no ambiente de trabalho, sem distinção de hierarquia, áreas ou funções exercidas; (ii) a transparência das operações em geral; (iii) a segurança das atividades dos profissionais envolvidos; e (iv) a segurança e o sigilo das informações que devem ser protegidas pela confidencialidade.

3- Abrangência

O Código de Ética contempla diretrizes de conduta baseadas em padrões éticos e morais que servirão de referencial para o comportamento de todos os colaboradores, internos e externos, cabendo a sua aplicação a todos os integrantes do quadro funcional da [nome da empresa], no exercício de suas funções, inclusive prestadores de serviços, fornecedores e parceiros de negócios que se vinculam à instituição.

4- Divulgação

Este Código de Ética ficará publicamente disponível no *WEBSITE* da Empresa no endereço http://www.valideinfoweb.com.br para consulta de colaboradores a qualquer momento, cabendo ao Representante Legal da Empresa: (i) assegurar o cumprimento deste Código de Ética; (ii) dar ciência aos novos colaboradores sobre o Código de Ética, mantendo registro da ciência e concordância dos mesmos; (iii) promover a ampla divulgação do Código e suas atualizações ao corpo funcional da Empresa, clientes, prestadores de serviços e fornecedores; (iv) esclarecer dúvidas e verificar o entendimento quanto ao conteúdo e aplicação.

5- Valores

• Respeito às pessoas • Responsabilidade social e cidadania. • Integridade profissional e pessoal. • Transparência nos processos. • Orgulho de trabalhar na [nome da empresa]. • Gosto por desafios. • Equidade de Gênero e Raça. • Compromisso com resultados. • Competência técnica. • Confiança e credibilidade. • Confidencialidade e segurança das informações.

6- Princípios Éticos

Os dirigentes e os colaboradores do ValideInfo pautam suas ações pelos seguintes princípios, no relacionamento com os diversos setores da sociedade, assegurando:

6.1. Aos Clientes

6.1.1. O profissionalismo, a confiança e a transparência;

6.1.2. A disponibilidade de soluções que agreguem valor aos negócios de seus clientes, investindo, permanentemente, na busca de tecnologias adequadas e no aprimoramento das estratégias empresariais;

6.1.3. A valorização e o respeito ao cumprimento dos acordos e contratos, bem como aos direitos dos seus clientes;

6.1.4. A valorização das oportunidades de negócios e parcerias construídas com seus clientes, visando resultados em benefício da sociedade; e

6.1.5. A identificação, proposição e viabilização de soluções inovadoras e integradas que contribuem como reforço à legitimidade e sustentação de seus clientes.

6.2. Aos Órgãos Governamentais

6.2.1. O reconhecimento do papel e apoio à atuação dos órgãos controladores, prestando-lhes informações pertinentes e confiáveis no tempo adequado;

6.3. Às Pessoas

6.3.1. A manutenção de um ambiente de trabalho onde o relacionamento é baseado no profissionalismo, confiança, cooperação, integração, respeito às diferenças individuais e urbanidade;

6.3.2. O compartilhamento de seus conhecimentos e experiências, buscando o aprimoramento da capacitação técnica, dos métodos e dos processos, de maneira a atingir melhor resultado global da Empresa;

6.3.3. A valorização das pessoas, contribuindo para o seu desenvolvimento pessoal, técnico e profissional;

6.3.4. O zelo, permanente, pela utilização adequada e econômica dos recursos materiais, técnicos e financeiros da Empresa;

6.3.5. A preservação e respeito à imagem, ao patrimônio e aos interesses da Empresa;

6.3.6. O reconhecimento e valorização do capital intelectual da Empresa e o estímulo ao surgimento de novas lideranças; e

6.3.7. A valorização e o estímulo à conduta ética individual e coletiva.

6.4. Aos Fornecedores e Empresas de Terceirização de Serviços

6.4.1. A legalidade, a impessoalidade, a moralidade, a publicidade e a eficiência em todos os atos praticados;

6.4.2. A manutenção de um relacionamento pautado no respeito mútuo, preservação e confidencialidade das informações pertinentes à Empresa e seus clientes;

6.4.3. Relacionamento com fornecedores e parceiros que possuem práticas harmônicas ao padrão ético adotado pelo ValideInfo e à moral social;

6.4.4. O estabelecimento de parcerias, desde que preservados a imagem e os interesses do ValideInfo; e

6.4.5. A rejeição às disposições contratuais que afrontem ou minimizem a dignidade, a qualidade de vida e o bem-estar social dos empregados terceirizados.

6.5. À Representação dos Empregados, Associações e Instituições

6.5.1. O reconhecimento à legitimidade e manutenção de um diálogo permanente com as instituições representativas dos trabalhadores, legalmente constituídas, mantendo canais de diálogo pautados no respeito mútuo, seriedade, responsabilidade e transparência nas relações;

6.5.2. A negociação como instrumento adequado para buscar a integração e a convergência; e

6.5.3. O cumprimento das determinações explicitadas nos instrumentos que regulam a relação da Empresa com seus empregados.

6.6. À Comunidade

6.6.1. O estabelecimento de relações justas e equilibradas com a comunidade por meio do incentivo, promoção, apoio e participação em ações de responsabilidade social e cidadania;

6.6.2. O incentivo, apoio e participação em ações governamentais voltadas para o desenvolvimento social e o combate à pobreza; e

6.6.3. O estímulo às iniciativas socioculturais e esportivas de seus empregados.

7- Código de Conduta Empresarial

Os dirigentes e empregados do ValideInfo devem pautar seu comportamento por este Código de Conduta Empresarial, nos termos enumerados a seguir.

7.1. Condutas aceitáveis aos dirigentes e empregados do ValideInfo:

7.1.1. Preservar e cultivar a imagem positiva da Empresa;

7.1.2. Comercializar, nas dependências da Empresa, apenas os produtos e serviços de propriedade e de interesse do ValideInfo;

7.1.3. Desenvolver condições propícias ao estabelecimento de um clima produtivo e agradável no ambiente de trabalho;

7.1.4. Tratar as pessoas e suas ideias com dignidade e respeito;

7.1.5. Proceder com lealdade, justiça e franqueza nas relações do trabalho;

7.1.6. Preservar o bem-estar da coletividade, respeitando as características pessoais, a liberdade de opinião e a privacidade de cada um;

7.1.7. Agir com clareza e lealdade na defesa dos interesses do ValideInfo;

7.1.8. Apresentar-se de forma adequada para o desempenho de suas funções e atividades na Empresa;

7.1.9. Abster-se de utilizar influências internas ou externas, para a obtenção de vantagens pessoais e funcionais;

7.1.10. Eximir-se de fazer uso do cargo, da função de confiança ocupada ou da condição de empregado do ValideInfo para obter vantagens para si ou para terceiros;

7.1.11. Utilizar os recursos do ValideInfo apenas para finalidades de interesse da Empresa;

7.1.12. Contribuir para o bom funcionamento de toda a Empresa, abstendo-se de atos e atitudes que impeçam, dificultem ou tumultuem a prestação de serviços;

7.1.13. Recusar de pessoas físicas e/ou jurídicas que mantenham relações comerciais com o ValideInfo presentes e/ou brindes de valor superior a R$ 100,00 *(cem reais)*.

7.1.14. Não elaborar e apresentar informações que reflitam reais posições e resultados econômicos, financeiros, operacionais, logísticos e quaisquer outros que afetem o desempenho da Empresa;

7.1.15. Priorizar e preservar os interesses do ValideInfo junto a clientes, órgãos governamentais, instituições financeiras, fornecedores, entidades e outras empresas com as quais mantenha relacionamento comercial;

7.1.16. Estar acompanhado, de outro empregado ou da chefia ou de um par, ao manter qualquer relacionamento com fornecedor ou parceiro que resulte ou que possa resultar em contratação que atenda a interesse ou necessidade do ValideInfo;

7.1.17. Prestar estrita anuência com as diretrizes e a condução estratégica empresarial ao assumir função de confiança da Empresa; e,

7.1.18. Renunciar ao exercício da função de confiança para a qual tenha sido designado, quando houver dissonância com as diretrizes e orientações estratégicas empresariais.

7.2. Condutas inaceitáveis aos dirigentes e aos empregados do ValideInfo:

7.2.1. Reivindicar benefícios ou vantagens pessoais para si próprio ou para terceiros, em decorrência de relacionamento comercial ou financeiro firmado em nome do ValideInfo com clientes, órgãos governamentais, instituições financeiras, fornecedores, entidades e outras empresas com as quais a [nome da empresa] mantenha este relacionamento;

7.2.2. Ser conivente ou omisso em relação a erros e infrações a este Código de Ética e às disposições legais e regulamentares vigentes;

7.2.3. Exercer outras atividades profissionais durante o expediente, com ou sem fins lucrativos, ou ainda, independentemente da compatibilidade de horários, exercer atividades que constituam prejuízo, concorrência direta ou indireta com as atividades do ValideInfo;

7.2.4. Exercer qualquer tipo de discriminação a pessoas por motivos de natureza econômica, social, política, religiosa, de cor, de raça ou de sexo;

7.2.5. Permitir que perseguições, simpatias, antipatias, caprichos, paixões ou interesses de ordem pessoal interfiram nas suas relações profissionais;

7.2.6. Prejudicar deliberadamente a reputação de empregado da Empresa ou de qualquer outro profissional com quem o ValideInfo mantenha relacionamento comercial;

7.2.7. Prejudicar deliberadamente a reputação dos clientes, órgãos governamentais, fornecedores, entidades e outras empresas com as quais o ValideInfo mantenha relacionamento comercial;

7.2.8. Pleitear, solicitar ou receber presentes, ou vantagens de qualquer espécie, para si ou para terceiros, além da mera insinuação ou provocação para o benefício que se dê, em troca de concessões ou privilégios de qualquer natureza junto o ValideInfo;

7.2.9. Priorizar e preservar interesses pessoais, de clientes, órgãos governamentais, instituições financeiras, fornecedores, entidades e outras empresas, em detrimento dos interesses do ValideInfo;

7.2.10. Obter vantagens, para si ou para terceiros, decorrente do acesso privilegiado a informações do ValideInfo, mesmo que não acarretem prejuízo para a Empresa;

7.2.11. Utilizar em benefício próprio ou repassar a terceiros, documentos, trabalhos, metodologias, produtos, ferramentas, serviços e informações de propriedade do ValideInfo ou de seus clientes e fornecedores, salvo por determinação legal ou judicial;

7.2.12. Manifestar-se em nome da Empresa, por qualquer meio de divulgação pública, quando não autorizado ou habilitado para tal;

7.2.13. Fazer uso inadequado e antieconômico dos recursos materiais, técnicos e financeiros da Empresa;

7.2.14. Impedir ou dificultar a apuração de irregularidades cometidas na Empresa;

7.2.15. Alterar ou deturpar o teor de qualquer documento, informação ou dado de responsabilidade da Empresa ou de terceiros;

7.2.16. Facilitar ações de terceiros que resultem em prejuízo ou dano para a Empresa;

7.2.17. Gerar qualquer tipo de confusão patrimonial entre os bens da Empresa e seus próprios bens, independentemente de advirem vantagens pecuniárias dessa confusão; e

7.2.18. Manter-se no exercício da função de confiança para a qual tenha sido designado, quando houver dissonância com as diretrizes e orientações estratégicas empresariais.

8- Cumprimento do Código de Ética

Em caso de dúvidas sobre qual deve ser a conduta correta a adotar, o colaborador deve procurar ajuda de forma sincera e transparente.

Deve ser comunicada imediata e formalmente ao Representante Legal da Empresa, qualquer situação que possa caracterizar conflito de interesses, ou fatos que possam prejudicar a Empresa ou que contrariem os princípios deste Código.

A Empresa assegura a confidencialidade na condução destes assuntos e o compromisso de apuração dos casos relatados.

Situações que, porventura, não estejam aqui explicitadas, serão tratadas como exceção e encaminhadas ao Representante Legal da Empresa que analisará e decidirá dentro dos princípios deste Código.

Este Código de Ética reflete os valores e a cultura da [nome da empresa] e o seu cumprimento revelam o compromisso de profissionalismo e transparência em todas as nossas ações no trabalho.

O desrespeito ao Código de Ética sujeitará os colaboradores às ações disciplinares, podendo resultar inclusive na sua demissão por justa causa e em processo legal.

Todos que se relacionam de forma direta ou indireta com o ValideInfo, devem conhecer e zelar pelo cumprimento deste Código, tendo os mesmos compromissos éticos, indistintamente do cargo que ocupam.

A não observância de quaisquer das práticas e/ou procedimentos aqui descritos pode infl uir na credibilidade da imagem institucional do ValideInfo, perante os clientes, mercado, órgãos supervisores e regulamentadores, governo e a sociedade em geral.

Este Código entra em vigor a partir da data de sua divulgação.

Política de Gestão dos Serviços Terceirizados

1- Introdução

O Valideinfo Serviço de Tecnologia da Informações e Soluções do Dado, utiliza-se da terceirização, onde algumas de suas atividades são repassadas à prestadores de serviços, com os quais estabelece uma relação de parceria, para que o Cliente mantenha seu foco no SEU SEGMENTO DE ATUAÇÃO. Desta forma, optou por instituir a Política de Gestão dos Serviços Terceirizados com o objetivo principal de parametrizar a contratação e a gestão dos prestadores de serviços.

2- Objetivo

Esta Política de Gestão dos Serviços Terceirizados tem como objetivo estabelecer os critérios, responsabilidades, competências e orientar quanto aos procedimentos a serem adotados nos processos de contratação, gestão e avaliação do desempenho de empresas prestadoras de serviços, com segurança operacional e jurídica.

3- Critérios para o Processo de Terceirização

A decisão de terceirizar deve ser precedida de análise de Risco, Custo, Oportunidade e Conveniência, dentre outros, considerando:

• Importância e criticidade da atividade para os processos da empresa e as consequências de deixar de executá-la internamente.

• Riscos de inadimplemento das obrigações legais.

• Capacidade de reação em eventuais emergências pela empresa.

• Custos de execução por terceiros, em relação ao custo de execução interna.

• Existência de prestadores de serviços capacitados.

• Cumprimento das Políticas da empresa.

• As empresas prestadoras de serviços deverão ser legalmente constituídas e ter comprovada sua idoneidade e capacidade técnica e administrativo-trabalhista, para a assunção das responsabilidades contratuais.

• A formalização do contrato se dará mediante a assinatura dos representantes legais da contratante e contratada, com o respectivo reconhecimento de firma em cartório, em documento que contenha no mínimo:

I – denominação, sede e representantes da contratante;

II – denominação, sede e representantes da contratada;

III – objeto do contrato;

IV – Obrigações e direitos;

V – Vigência;

VI – Honorários, forma de pagamento, índice de reajuste e periodicidade;

VII – cláusula anticorrupção;

VIII - foro para dirimir eventuais conflitos.

• Existindo algum grau de parentesco entre funcionários com a empresa contratada ou o prestador de serviços, ficará impedida a contratação do serviço.

• Fica vedada a terceirização de atividades com pessoas físicas ou firma individual, salvo quando tratar-se de profissional com alto grau de especialização técnica, inclusive consultores técnicos, por prazo determinado.

• É expressamente proibida a utilização, por parte do prestador de serviço/empresa contratada, de mão-de-obra de menores de idade no desempenho de serviços contratados.

• As empresas contratadas/prestadoras de serviços não poderão em nenhuma hipótese subcontratar a totalidade dos serviços.

4- Princípios

• Os empregados de prestadores de serviço não devem ter subordinação direta a empregados da empresa.

• A contratação deverá ser efetuada pelo serviço a ser executado, e não pela mão de obra, exceto no caso de mão de obra temporária.

• Garantir que toda comunicação de execução do serviço ocorra por meio de prepostos.

• Na execução do serviço não poderá haver pessoalidade (estabelecer a execução do serviço por um determinado empregado da contratada).

• Manter a gestão estratégica nas atividades vinculadas ao negócio.

• Garantir qualidade e produtividade por meio da especialização;

• Garantir o cumprimento das obrigações legais e de responsabilidade social.

• As atividades terceirizadas não poderão constar no rol de atividades efetuadas por empregados da empresa no local de prestação de serviço.

• As atividades terceirizadas devem constar no objeto social da contratada.

5- Considerações Finais

Esta política deve ser acompanhada pela Diretoria do ValideInfo, no que tange à aplicação dos procedimentos de acompanhamento e ao controle de suas diretrizes.

As exceções, eventuais violações e casos omissos devem ser analisadas individualmente.

Política de TI

A Política de Tecnologia da Informação é o documento que orienta e estabelece as diretrizes corporativas do Valideinfo Serviços de Informações e Soluções do Dado, para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

Objetivo

Estabelecer diretrizes que permitam aos colaboradores seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações do Valideinfo quanto à:

• Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

• Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

• Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Abrangência

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Das Responsabilidades:

Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar o ValideInfo e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da política.

Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações do ValideInfo. Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Da Área de Tecnologia da Informação

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta política.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o ValideInfo.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

> os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.

> os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

• uso da capacidade instalada da rede e dos equipamentos;

• tempo de resposta no acesso à internet e aos sistemas críticos;

• períodos de indisponibilidade no acesso à internet e aos sistemas críticos;

• incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);

• atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

Do Monitoramento e da Auditoria do Ambiente

Para garantir as regras mencionadas nesta política o ValideInfo poderá:

• implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

• tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação da Diretoria;

• realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

• instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

Correio eletrônico

É proibido aos colaboradores o uso do correio eletrônico do ValideInfo:

• enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

• enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o ValideInfo vulneráveis a ações civis ou criminais;

• divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

• falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

• apagar mensagens pertinentes de correio eletrônico quando o ValideInfo estiver sujeita a algum tipo de investigação.

• produzir, transmitir ou divulgar mensagem que:

> vise vigiar secretamente ou assediar outro usuário;

> vise acessar informações confidenciais sem explícita autorização do proprietário;

> vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

> inclua imagens criptografadas ou de qualquer forma mascaradas;

> tenha conteúdo considerado impróprio, obsceno ou ilegal.

Internet

Todas as regras atuais do ValideInfo visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio

ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

Ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

Identificação

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados no ValideInfo, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 30 dias, não podendo ser repetidas as 03 *(três)* últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 30 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer à área técnica responsável para cadastrar uma nova.

Disposições Gerais

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do ValideInfo. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

Política de Gestão de Riscos

1- Introdução

A Política define um conjunto de princípios e diretrizes para a Gestão de Riscos Corporativos do ValideInfo. Desta forma, tais diretrizes foram estabelecidas com o objetivo de assegurar que sejam formalmente gerenciados os potenciais impactos adversos que influenciam a execução dos objetivos da [nome da empresa].

2- Obejetivo

O objetivo desta Política é estabelecer as diretrizes que regulamentam a Gestão baseada em Riscos, suficientes para propiciar ao ValideInfo capacidade de cumprir com a sua missão bem como seus objetivos estratégicos sem violar o perfil de risco do planejamento estratégico da empresa, tendo como pressupostos:

a) Manter a estrutura apropriada de governança de risco;

b) Estabelecer critérios e parâmetros para identificação, avaliação, monitoramento e controle dos riscos relevantes da entidade;

c) Divulgar e conscientizar os funcionários quanto aos riscos relacionados a seus planos de benefícios;

d) Disseminar a cultura de Gestão baseada em Riscos, especificando o perfil de risco adotado, introduzindo uma linguagem comum para o assunto "riscos" em todos os níveis da organização.

e) Garantir que os processos e procedimentos relacionados ao Gerenciamento de Riscos do ValideInfo atendam aos requerimentos regulatórios vigentes, bem como às melhores práticas internacionais.

Alcance

Essa política é feita para todos os colaboradores do ValideInfo.

Atualização

A Política de Gestão de Riscos Corporativos deve ser revisada sempre que se fizer necessário, não excedendo o período máximo de 06 meses.

A formulação de propostas de alteração desta Política é de competência do comitê de Gestão de Riscos e serão encaminhadas para aprovação da alçada competente pela gerência coordenadora do comitê.

Como Tratar os Riscos

Evitar o risco: não iniciando ou descontinuando a atividade que dá origem ao risco.

Eliminar o risco: removendo a respectiva fonte causadora.

Reduzir o risco: Implantando controles que diminuam a probabilidade de ocorrência do risco ou suas consequências.

Aceitar o risco: assumindo o risco, por uma escolha consciente e justificada formalmente, podendo implementar sistemática de monitoramento.

Compartilhar o risco: com outras partes interessadas.

Aumentar o risco: com vistas a aproveitar uma oportunidade.

Prazos para lidar com os Riscos

Médio e longo prazo: quando a avaliação realizada indicar risco estratégico, orçamentário ou de imagem classificado como risco baixo.

Curto prazo: quando a avaliação realizada indicar risco estratégico, orçamentário ou de imagem classificado como risco médio, ou, em caso de risco negativo, quando a continuidade ou repetição das vulnerabilidades tiver potencial para transformá-lo em risco médio

Imediato: quando a avaliação realizada indicar risco estratégico, orçamentário ou de imagem classificado como risco alto ou extremo, ou, em caso de risco negativo, quando a continuidade ou repetição das vulnerabilidades tiver potencial para transformá-lo em risco alto ou extremo

Níveis de Riscos

Extremo: Aqueles caracterizados por riscos associados à paralisação de operações, atividades, projetos, programas ou processos do ValideInfo, causando IMPACTOS IRREVERSÍVEIS nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas.

- Alto: Aqueles caracterizados por riscos associados à interrupção de operações, atividades, projetos, programas ou processos do ValideInfo, causando IMPACTOS DE REVERSÃO MUITO DIFÍCIL nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas.

- Médio: Aqueles caracterizados por riscos associados à interrupção de operações ou atividades do ValideInfo, de projetos, programas ou processos, causando IMPACTOS SIGNIFICATIVOS nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas, porém recuperáveis.

- Baixo: Aqueles caracterizados por riscos associados à degradação de operações, atividades, projetos, programas ou processos do ValideInfo, causando IMPACTOS PEQUENOS nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas.

- Muito Baixo: Aqueles caracterizados por riscos associados à degradação de operações, atividades, projetos, programas ou processos do ValideInfo, porém causando IMPACTOS MÍNIMOS nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas.

Ciclo da Gestão baseada em Riscos

O ciclo de Gestão Baseada em Riscos corresponde à descrição das diversas atividades que são desenvolvidas para que o perfil de riscos seja gerado e comunicado para as diversas partes interessadas. Esse ciclo deve estar interligado aos demais processos do ValideInfo bem como às Políticas e Diretrizes de investimentos vigentes. Trata-se da efetiva aplicação das ações de identificação, avaliação, mitigação, comunicação e monitoramento das diferentes categorias de riscos existentes nos processos do ValideInfo, realizados periodicamente.

Identificação | Avaliação e Mensuração | Resposta | Comunicação e Monitoramento

Considerações Finais

Esta política deve ser acompanhada pelos Diretores do ValideInfo, no que tange à aplicação dos procedimentos de acompanhamento e ao controle de suas diretrizes.

As exceções, eventuais violações e casos omissos à Política de Riscos Corporativos devem ser analisadas individualmente.

Política de Compras e Contratações de Serviços

Declaração da Política

Apresentamos nesta política orientações institucionais para a contratação de serviços de terceiros (Compras), tanto para serviços como para produtos. O ValideInfo reconhece a importância de ter a capacidade de promover processos de compras e contratações que garantam competitividade, integridade e transparência.

A Política de Compras presente neste documento deve ser vista como instrumento de execução e acompanhamento de projetos, sendo conhecida e entendida por todos os funcionários e aprimorada sempre que possível. Somente as empresas homologadas, técnica e administrativamente, são selecionadas a apresentar suas

condições comerciais, diante de um produto ou serviço previamente identificado, quantificado, especificado com período definido ao seu cumprimento, para que os participantes possam planejar a formação de seu preço com base em premissas claras e disponíveis a todos os envolvidos.

Esta política tem por objetivo construir e qualificar o conjunto de procedimentos administrativos e financeiros institucionais, bem como ampliar sua transparência e facilitar seu cumprimento. Para salvaguardar direitos das partes, o ValideInfo adota a formalização da compra por meio de contrato padrão, com base em seu Código de Ética e foco na legislação em vigor, nas condições operacionais, técnicas e comerciais, e na sustentabilidade dos negócios.

O cumprimento das orientações a seguir é fundamental, sob risco da não liberação de recursos institucionais para pagamento dos serviços, em caso de descumprimento. O processo de compras deverá obedecer a princípios rígidos de equidade e transparência.

Diretrizes

As diretrizes para contratação de serviços e aquisição de bens são as seguintes:

a) Sempre buscar fornecedores que implementem boas práticas sociais e ambientais;

b) Procurar alcançar economias sem perder qualidade e eficiência;

c) Prezar pela transparência nos processos, não compactuando com comportamentos antiéticos, excluindo fornecedores que não procedam de forma semelhante;

d) A seleção de propostas deve ser feita mediante julgamento objetivo, com critérios estabelecidos em cada processo e que sejam de conhecimento geral.

Código de Conduta Ética

O ValideInfo exerce controle de fraude a partir das seguintes práticas:

a) Checagem e comparação de dados contidos nas propostas, tais como: formatação, endereço, telefone, e-mail;

b) Formação de comissões de avaliação técnica de propostas;

c) Revisão, por pelo menos outro funcionário do ValideInfo, de todos os processos;

d) Segregação de funções entre solicitante, responsável pela elaboração de contratos e pagamento.

É obrigação do solicitante da compra:

a) Fazer sempre três cotações. Os concorrentes devem receber exatamente a mesma solicitação (mesmo e-mail);

b) Ao final do processo, todos os concorrentes devem receber retorno sobre sua finalização, mesmo quando a resposta for a opção por outro concorrente;

c) Os envolvidos direta ou indiretamente no processo de compra ou contratação não podem receber quaisquer vantagens ou benefícios pessoais provenientes de empresas fornecedoras ou participantes de processo de compra ou contratação;

d) A confidencialidade das informações técnicas e comerciais dos processos de compra ou contratação deve ser assegurada, restringindo a divulgação de dados dos proprietários apenas para uso interno.

Conduta do Contratante

PROCEDIMENTOS

O ValideInfo definiu como política de contratação a escolha de seus fornecedores por meio de concorrência. Também é nosso compromisso que as políticas e normas sejam orientadas pelas seguintes diretrizes:

a) É obrigatório aos colaboradores envolvidos em processo de compras ou contratação assegurar-se de que os fornecedores ou prestadores de serviço do ValideInfo cumpram a legislação, mediante todos os mecanismos de consultas pertinentes.

b) Assegurar-se de que os fornecedores ou prestadores não constem no Cadastro de Empregadores, na denominada “Lista Suja” do Trabalho Escravo, nem no Cadastro de Empresas Inidôneas e Suspensas (CEIS), da Controladoria-Geral da União. Informar a fornecedores ou prestadores de serviço de que estes deverão assinar contratos, quando aplicável, com cláusulas específicas contra relações de trabalho escravo, infantil e outras formas de trabalho degradante sob sua responsabilidade.

O critério primordial para escolha do fornecedor será o menor preço. Em casos excepcionais em que um fornecedor mais caro esteja sendo contratado, deverá ser explicitada justificativa com os outros critérios (menor impacto ambiental, prazo, qualidade, prestadores de serviço local ou da economia solidária).

Dispensa de Cotação

Não haverá exigência de concorrência com três cotações nos casos de compras e contratações: para valores inferiores a R$ 100,00 *(cem reais)*; quando já houver um contrato guarda-chuva; nos casos de especialidade; e nos casos de compras e contratações emergenciais. Esses casos são explicitados a seguir.

a) Valores inferiores a R$ 100,00 *(cem reais)*: Compras e contratações de valores inferiores a R$ 100,00 *(cem reais)* são dispensadas de concorrência desde que os pagamentos não se refiram a parcelas de um mesmo serviço.

b) Contrato guarda-chuva: Para prestadores de serviços recorrentes, não será necessário realizar concorrência a cada contratação ou compra. O processo para o estabelecimento do contrato guarda-chuva também requer três cotações. Caso não haja contrato guarda-chuva para o serviço procurado, contatar a área financeira e/ou a administrativa para análise da necessidade de elaboração de contrato que será responsabilidade da área demandante.

c) Especialidade: Poderão ser contratados fornecedores com a justificativa de especialidade nas seguintes situações:

1) Para aquisição de materiais, equipamentos ou gêneros que só possam ser fornecidos por produtor, empresa ou representante comercial exclusivo;

2) Para contratação de profissional ou empresa com notória especialização, ou seja, aqueles cujo conceito no campo de sua especialidade, estudos, experiências, organização, aparelhamento, equipe técnica ou de outros requisitos relacionados com suas atividades, permita inferir que o seu trabalho é essencial e indiscutivelmente o mais adequado à plena satisfação do objeto do contrato.

d) Emergência: entende-se por emergência a urgência de atendimento de situação que possa ocasionar prejuízo ou comprometer o trabalho e que não pôde ser prevista antecipadamente. Nesses casos, serão necessárias a

explicitação detalhada da razão pela qual a situação está sendo caracterizada como tal, no próprio formulário de contratação.

Contratos

Este deve ser o fluxo a ser seguido para compras e contratações não dispensados de concorrência:

a) Obter o número mínimo de três cotações;

b) Solicitar certidões para o escolhido;

c) Preencher e imprimir a solicitação de pagamentos com as três cotações anexadas;

d) Obter aprovação da solicitação de pagamento;

e) Fazer o contrato, caso necessário, e obter as assinaturas;

f) Na finalização dos pagamentos parcelados, o funcionário responsável por Contas a Pagar deve verificar com o coordenador do projeto se o serviço foi finalizado ou se o produto foi entregue.

Em caso de conhecimento de violações a esta política, assim como quaisquer informações acerca de eventual descumprimento de dispositivos legais e normativos aplicáveis ao ValideInfo e fornecedores, podem e devem ser manifestas e denunciadas por meio [dos canais adequados para denúncias na empresa].

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 15/08/2018 | Edição: 157 | Seção: 1 | Página: 59

Órgão: Atos do Poder Legislativo

LEI NO 13.709, DE 14 DE AGOSTO DE 2018

Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

O PRESIDENTE DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei 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.

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.

Art. 3º Esta 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 tenha sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do **caput** do art. 4º desta Lei.

Art. 4º Esta 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:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do **caput** deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do **caput** deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do **caput** deste artigo poderá ser tratada por pessoa de direito privado.

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - 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;

III - dado anonimizados: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;

IX - agentes de tratamento: o controlador e o operador;

X - 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;

XI - 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;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - 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 esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - 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;

XVIII - 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;

XIX - autoridade nacional: órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CAPÍTULO II

DO TRATAMENTO DE DADOS PESSOAIS

Seção I

Dos Requisitos para o Tratamento de Dados Pessoais

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

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

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

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

§ 1º Nos casos de aplicação do disposto nos incisos II e III do **caput** deste artigo e excetuadas as hipóteses previstas no art. 4º desta Lei, o titular será informado das hipóteses em que será admitido o tratamento de seus dados.

§ 2º A forma de disponibilização das informações previstas no § 1º e no inciso I do **caput** do art. 23 desta Lei poderá ser especificada pela autoridade nacional.

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º 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.

§ 5º O controlador que obteve o consentimento referido no inciso I do **caput** deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do **caput** do art. 18 desta Lei.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º 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.

§ 2º Na hipótese em que o consentimento é requerido, 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.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Seção II

Do Tratamento de Dados Pessoais Sensíveis

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, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; 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.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do **caput** deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º 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.

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular.

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta 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.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão 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 previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o **caput** deste artigo em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no **caput** deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

§ 4º Para os efeitos deste artigo, a pseudonimização é o 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.

Seção III

Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo 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 de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Seção IV

Do Término do Tratamento de Dados

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.

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.

CAPÍTULO III

DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

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;

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 com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

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, nos termos do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º O responsável deverá informar de maneira imediata aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento.

§ 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.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

II - sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do **caput** deste artigo para os setores específicos.

Art. 20. O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

CAPÍTULO IV

DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I

Das Regras

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II - (VETADO); e

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no **caput** deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no **caput** deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o **caput** deste artigo.

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Art. 25. 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.

Art. 26. 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 desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - 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);

II - (VETADO);

III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do **caput** do art. 23 desta Lei; ou

III - nas exceções constantes do § 1º do art. 26 desta Lei.

Art. 28. (VETADO).

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, às entidades do Poder Público, a realização de operações de tratamento de dados pessoais, informe específico sobre o âmbito e a natureza dos dados e demais detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.

Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Seção II

Da Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

CAPÍTULO V

DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do **caput** do art. 23 desta Lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do **caput** do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do **caput** do art. 33 desta Lei, será realizada pela autoridade nacional.

§ 1º Para a verificação do disposto no **caput** deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.

§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no **caput** deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.

§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no **caput** deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

CAPÍTULO VI

DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Seção I

Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no **caput** deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Seção II

Do Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Seção III

Da Responsabilidade e do Ressarcimento de Danos

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - 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 equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º 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.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do **caput** deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

CAPÍTULO VII

DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I

Da Segurança e do Sigilo de Dados

Art. 46. 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.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no **caput** deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o **caput** deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Art. 48. 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.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá 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.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I - ampla divulgação do fato em meios de comunicação; e

II - medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II

Das Boas Práticas e da Governança

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do **caput** do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

CAPÍTULO VIII

DA FISCALIZAÇÃO

Seção I

Das Sanções Administrativas

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII - suspensão parcial ou total do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período até a regularização da atividade de tratamento pelo controlador;

VIII - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

IX - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

§ 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 - (VETADO);

VIII - (VETADO);

IX - (VETADO);

X - a pronta adoção de medidas corretivas; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.

§ 3º O disposto nos incisos I, IV, V, VI, VII, VIII e IX do **caput** deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa), e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 4º No cálculo do valor da multa de que trata o inciso II do **caput** deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa.

§ 1º As metodologias a que se refere o **caput** deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.

CAPÍTULO IX

DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Seção I

Da Autoridade Nacional de Proteção de Dados (ANPD)

Art. 55. (VETADO).

Art. 56. (VETADO).

Art. 57. (VETADO).

Seção II

Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Art. 58. (VETADO).

Art. 59. (VETADO).

CAPÍTULO X

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações:

"Art. 7º .....

.....

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

....." (NR)

"Art. 16. .....

.....

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais." (NR)

Art. 61. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004.

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 65. Esta Lei entra em vigor após decorridos 18 (dezoito) meses de sua publicação oficial**.**

Brasília, 14 de agosto de 2018; 197oda Independência e 130oda República.

MICHEL TEMER
TORQUATO JARDIM
ALOYSIO NUNES FERREIRA FILHO
EDUARDO REFINETTI GUARDIA
ESTEVES PEDRO COLNAGO JUNIOR
GILBERTO MAGALHÃES OCCHI
GILBERTO KASSAB
WAGNER DE CAMPOS ROSÁRIO
GUSTAVO DO VALE ROCHA
ILAN GOLDFAJN
RAUL JUNGMANN
ELISEU PADILHA