Move Forward with Confidence

BUREAU VERITAS CERTIFICATION

Norma Técnica
TS-BVCBr0001
Versão 2

Proteção de Dados Pessoais
Novembro/2019

Nota: É proibida a reprodução deste material, por qualquer meio, sem a prévia autorização do BUREAU VERITAS DO BRASIL.

Av. Alfredo Egídio de Souza Aranha ,100 - Vila Cruzeiro - São Paulo - SP - CEP: 04726-170
Telefone: 11 2655-9000 - Site: www.bureauveritas.com.br

Todas as informações apresentadas neste documento são protegidas por direitos autorais e são de propriedade da BUREAU VERITAS CERTIFICATION HOLDING, salvo indicação em contrário por escrito. Nenhuma parte do documento pode ser reproduzida, copiada, transmitida a qualquer pessoa, de qualquer forma e por qualquer meio, sem o prévio consentimento por escrito da BUREAU VERITAS CERTIFICATION HOLDING.

"BUREAU VERITAS" e o BUREAU VERITAS 1828 são marcas registradas e de propriedade da BUREAU VERITAS SA.

Nenhuma licença ou direito explícito ou implícito de qualquer tipo é concedido em relação a quaisquer marcas registradas ou outros direitos de propriedade intelectual da BUREAU VERITAS CERTIFICATION HOLDING ou BUREAU VERITAS SA.

É estritamente proibido oferecer e/ou executar serviços de certificação e/ou verificação, incluindo a emissão de certificados, total ou parcialmente com base e/ou em conformidade com este documento, sem custos ou encargos, sem prévia autorização da BUREAU VERITAS CERTIFICATION HOLDING por escrito.

A BUREAU VERITAS CERTIFICATION HOLDING renúncia toda garantia e garantias, expressas ou implícitas, incluindo qualquer garantia de comercialidade ou adequação a uma finalidade ou uso específico, ou a não violação de direitos de terceiros com relação ao documento fornecido.

Em nenhuma hipótese a BUREAU VERITAS CERTIFICATION HOLDING e a BUREAU VERITAS SA, seus agentes, consultores e subcontratantes, serão responsáveis por danos especiais, indiretos ou consequentes, decorrentes ou decorrentes do uso deste documento e seu conteúdo, incluindo, sem limitação, a perda de dados, perda de lucro, perda de contratos ou interrupções de negócios ou consequentes, decorrentes ou decorrentes do uso deste documento e seu conteúdo, incluindo, sem limitação, a perda de dados, perda de lucro, perda de contratos ou interrupções de negócios.

Sumário

© Copyright - 30/11/2019

Norma Técnica TS-BVCBr0001

Proteção de Dados Pessoais em conformidade com o regulamento (UE) 2016/679, Lei nº 13.709/2018 e Lei nº 13.853/2019

Introdução

O Regulamento (UE) 2016-679 que trata da proteção e da livre circulação de dados pessoais (referido a seguir como "Regulamento") foi adotado em 27 de abril de 2016 e publicado posteriormente no Jornal Oficial da União Europeia (OJEU) em 4 de maio de 2016.

Desde a publicação da Diretiva da Comunidade Europeia em 24 de outubro de 1995 que trata do processamento e livre movimentação de dados pessoais, a evolução das tecnologias de informação e da comunicação levou a um crescimento exponencial do processamento e compartilhamento de dados pessoais.

O Regulamento (UE) 2016-679 foi publicado como uma resposta a essa evolução tecnológica no marco de modernização da abordagem europeia para a proteção de dados pessoais.

O Regulamento, que passou a vigorar a partir de 25 de maio de 2018, tem como principal objetivo reduzir as discrepâncias jurídicas entre as diferentes legislações dos Estados-Membros da União Europeia quanto a proteção de dados pessoais.

No Brasil, a lei Geral de Proteção de Dados Pessoais (Lei nº 13.709) publicada em 14 de agosto de 2018 e alterada em 08 de julho de 2019 pela Lei nº 13.853, detalha os requisitos da proteção de dados pessoais para assim assegurar maior proteção dos direitos pessoais. A LGPD, que passa a vigorar em agosto de 2020, altera de forma expressiva como as organizações públicas e privadas devem processar e armazenar dados pessoais e impõe multas expressivas para aquelas organizações que não aderirem e cumprirem com o estabelecido.

Nessa perspectiva e dentro da estrutura da sua política de conformidade, as empresas devem incluir nas estratégias e processos de seus negócios as obrigações decorrentes do Regulamento ou da LGPD e implementar ações para atender a esses novos requisitos dentro dos prazos estabelecidos.

Tanto o Regulamento como a LGPD exigem que as organizações assumam total responsabilidade quanto aos dados que controlam ou processam, para assim estabelecer processos e alocar recursos internos e competências para garantir a plena responsabilidade e proteção de dados pessoais.

Evidenciar que o tratamento realizado por controladores, operadores, subcontratados e fornecedores de serviços atende o estabelecido na LGPD ou no Regulamento, representa um desafio fundamental para a reputação, imagem e competividade das empresas.

Desde essa perspectiva, o esquema de certificação, materializado nesta Norma Técnica, foi idealizado para permitir que as empresas evidenciem a conformidade com essas novas obrigações.

O objetivo desta Norma Técnica de certificação é o de estabelecer as disposições técnicas, organizacionais e da documentação vinculadas ao atendimento das obrigações legais, conforme definido no Regulamento e na LGPD. O pleno atndimento das obrigações legais é um novo princípio que exige que as empresas estejam aptas a justificar toda a sistemática de controle e monitoramento implantada para garantir a conformidade da proteção de dados pessoais.

A norma técnica de certificação abrange a obrigação de documentar os requisitos impostos tanto pelo Regulamento como a LGPD, implantar mecanismos técnicos e organizacionais que assegurem a conformidade e a manutenção das condições operacionais, para assim evidenciar o pleno atendimento do estabelecido.

© Copyright - 30/11/2019

1. Escopo

De acordo com o Regulamento (UE) 2016/679 e a LGPD, a adesão a códigos de conduta (Artigo 40 e artigo 50 respectivamente) ou mecanismos de certificação aprovados (GDPR Artigo 42) pode ser utilizada para evidenciar a conformidade com as obrigações de controladores e operadores.

Além da adesão de controladores e operadores afetados pelo Regulamento ou a LGPD, mecanismos de certificação podem ser criados para evidenciar a existência de salvaguardas adequadas dadas por controladores ou operadores, no âmbito da transferência de dados pessoais para organizações internacionais ou países terceiros, que não estejam sujeitos ao Regulamento ou a LGPD.

Qualquer certificação relativa a este esquema não reduz a responsabilidade do controlador e operador de cumprir com o estabelecido no Regulamento (UE) 2016/679, ou a Lei 13.709/2018 e a Lei nº 13.853/2019 e não interfere com as funções e os poderes das autoridades nacionais de supervisão (Autoridades de Proteção de Dados).

O esquema de certificação especifica os requisitos vinculados à proteção de dados pessoais que uma organização pode implantar para estar em conformidade com o Regulamento (UE) 2016/679 ou a Lei nº 13.709 de 14/08/2018 e a Lei nº 13.853 de 08/07/2019.

O esquema de certificação aplica-se a qualquer organização - independentemente do porte, tipo e natureza - e aplica-se às atividades, produtos e serviços referidos ao tratamento de dados pessoais que podem ser controlados ou influenciados desde a perspectiva do ciclo de vida.

Especificamente, o esquema é aplicável a qualquer controlador e operador, independentemente da natureza, escopo, contexto ou finalidades do tratamento de dados pessoais.

Para os operadores, algumas cláusulas do esquema podem não se aplicar (consulte o apêndice 3). No caso de a cláusula ser aplicável tanto para o controlador quanto para o operador, é utilizado o termo organização.

As seguintes formas verbais são usadas no documento: "deve" se refere a um requisito a ser atendido; "convém que" refere-se a uma recomendação; "pode" refere-se a uma factibilidade ou capacidade de ação.

Informação indicada como “NOTA” serve como orientação para esclarecer a respeito do entendimento ou utilização de um determinado requisito ou cláusula.

© Copyright - 30/11/2019

2. Referências

Os seguintes documentos, na sua totalidade ou em parte, foram utilizados como as principais referências do esquema de certificação. Para referências datadas, somente a edição citada se aplica. Para referências sem data, aplica-se a última edição do documento referenciado (incluindo quaisquer alterações).

- Lei nº 13853 de 08 de julho de 2019 altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências;
- Lei 13.709 de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais (Lei Geral de Proteção de Dados Pessoais – LGDP);
- Regulamento (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016, referente à proteção das pessoas naturais no que tange ao tratamento de dados pessoais e a livre circulação desses dados, que revoga a Diretiva 95/46 / CE (General Data Protection Regulation - GDPR);
- WP29 - Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679;
- WP29 - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation
- 2016/679;
- WP29 - Guidelines on Personal data breach notification under Regulation 2016/679;
- WP29 - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679;
- WP29 - Guidelines on Data Protection Officers (‘DPOs’);
- WP29 - Guidelines for identifying a controller or processor’s lead supervisory authority;
- WP29 - Guidelines on the right to data portability;
- WP29 - Guidelines on consent under Regulation 2016/679;
- WP29 - Guidelines on the right to «data portability»;
- WP29 - Guidelines on transparency under Regulation 2016/679;
- ISO 27001:2013, Information technology -- Security techniques -- Information security management systems -- Requirements;
- ISO/IEC 29100:2011, Information technology -- Security techniques -- Privacy;
- ISO/IEC 29101:2013, Information technology -- Security techniques -- Privacy architecture framework;
- ISO 9001:2015, Quality management systems - Requirements;

Os seguintes documentos, na sua totalidade ou em parte, foram utilizados para assegurar a conformidade com requisitos de acreditação:

- EDPB - Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679;
- ISO 17065:2012 - Conformity assessment - Requirements for bodies certifying products, processes and services;
- EA 1/22 A:2016 - EA Procedure and Criteria for the Evaluation of Conformity Assessment Schemes by EA Accreditation Body Member.

© Copyright - 30/11/2019

3. Termos e definições

Para os propósitos deste documento, aplicam-se os seguintes termos e definições.

3.1 Sistema de Gestão

Conjunto de elementos que interagem para formalizar o estabelecimento de políticas, consecução de objetivos e realização de processos numa organização.

3.2 Organização

Pessoa ou grupo de pessoas que com funções, responsabilidades e autoridade estabelecem relacionamentos para atingir seus objetivos.

3.3 Alta Direção

Pessoa ou grupo de pessoas que dirige e controla uma organização no mais alto nível.

3.4 Direitos da pessoa

Consulte: Lei 13.709 de 14/08/2018, Artigo 9, Artigo 17 e Artigo18.

NOTA: Para o GDPR os artigos 12 a 23 (capítulo III: direitos dos titulares dos dados) do Regulamento (UE) 2016/679 trazem essa definição.

3.5 Obrigações de conformidade

Requisitos legais que uma organização (3.2) deve atender e outros requisitos que a organização deve ou pode escolher cumprir. As obrigações de conformidade estão vinculadas à proteção dados pessoais de acordo com a Lei 13.709 de 14/08/2018.

NOTA: Para atendimento ao Regulamento (UE) 2016/679, a organização deve obrigatoriamente atendê-lo.

3.6 Processo

Conjunto de atividades inter-relacionadas ou interativas que entregam resultados pretendidos.

3.7 Dados pessoais

Qualquer informação relativa a uma pessoa natural identificada ou identificável. Pessoa natural identificável é aquela que pode ser identificada, direta ou indiretamente mediante um identificador como o nome, número de identificação, dados de localização, identificador “on-line” ou por um ou mais fatores específicos referentes a características físicas, fisiológicas, sexo, atributos mentais, condição econômica, cultural ou social dessa pessoa.

3.8 Dados pessoais sensíveis

Qualquer informação pessoal relacionada ao indivíduo referida a:

- origem étnica ou racial;
- opiniões políticas;
- religião ou crenças filosóficas;
- filiação sindical ou a organização de caráter religioso, filosófico e político;
- dados genéticos;
- condição de saúde;
- dados genéticos ou biométricos utilizados para fins de identificação ou autenticação única de uma pessoa natural;

© Copyright - 30/11/2019

- opção sexual;
- condenações criminais ou medidas associadas que tratem da segurança.

NOTA: Consultar a Lei 13.709 de 14/08/2018, Artigo 5.

3.9 Dado pessoal de alto risco

Dados pessoais de alto risco podem incluir:

- dados pessoais sensíveis (3.8);
- dados de pessoas naturais vulneráveis, em particular, de crianças;
- aspectos pessoais avaliados, em particular, na análise ou previsão quanto ao desempenho no trabalho, situação econômica, saúde, preferências ou interesses pessoais, confiabilidade ou comportamento, localização ou movimentos utilizados na criação de perfis pessoais;
- tratamento de grande quantidade de dados pessoais que afetam número elevado de titulares.

A possibilidade e a gravidade do risco para os direitos e liberdades do titular devem ser estabelecidas mediante referência à natureza, âmbito, contexto e finalidades de tratamento dos dados. O risco deve ser avaliado desde a perspectiva de uma postura objetiva, mediante a qual é estabelecido se as operações de tratamento envolvem um risco ou um alto risco.

3.10 Tratamento

Qualquer operação ou conjunto de operações realizadas sobre dados (3.7) ou conjuntos de dados pessoais. Essas operações podem ser automatizadas e incluem: coleta, gravação, organização, estruturação, armazenamento, adaptação, alteração, recuperação, consulta, uso, divulgação mediante transmissão, difusão ou disponibilização, alinhamento ou combinação, restrição, exclusão ou destruição.

3.11 Controlador

Pessoa física ou jurídica, autoridade pública, agência ou outro organismo que, individualmente ou em conjunto com outros, define os propósitos e os meios de tratamento de dados pessoais. A nomeação do controlador, por meio dos critérios específicos, pode ser estabelecida por legislação da EU ou do Brasil.

NOTA: Consultar a Lei 13.709 de 14/08/2018, Artigo 5º - VI.

3.12 Operador

Pessoa física ou jurídica, autoridade pública, agência ou qualquer outra organização que processa dados pessoais em nome ou a mando de um controlador (3.11).

NOTA: Consultar a Lei 13.709 de 14/08/2018, Artigo 5 - VII.

3.13 Destinatário

Pessoa física ou jurídica, autoridade pública, agência governamental ou outro organismo para o qual os dados pessoais são divulgados, seja terceiro ou não**.**

NOTA: Consultar o artigo 23 da LGPD que detalha as regras do tratamento de dados pessoais pelo poder público.

3.14 Consentimento do titular dos dados

Qualquer manifestação dada livremente, de forma específica, informada e inequívoca dos desejos do titular pela qual, ele ou ela, mediante declaração ou por clara ação afirmativa indica a aprovação da realização de um tratamento de dados pessoais relativos a ele ou ela para uma finalidade determinada e informada.

© Copyright - 30/11/2019

NOTA: Consultar Lei 13.709 de 14/08/2018, Artigo 5º XII

3.15 Violação de dados pessoais

Se caracteriza pela quebra de segurança que leva à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais transmitidos, armazenados ou processados.

3.16 Autoridade Nacional de Proteção de Dados (ANPD)

É uma autoridade pública, denominada como Autoridade Nacional nos termos da Lei nº 13.709 de 14/08/2018 (Art.5º XIX) e no artigo 55 da Lei nº 13853 de 08 de julho de 2019.

NOTA:

Nos países da EU é uma autoridade pública independente constituída por um Estado-Membro nos termos do artigo 51º do Regulamento Europeu 2016/679.

3.17 Responsabilização

Processo permanente e dinâmico que consiste na obrigação de prestar contas quanto ao cumprimento de requisitos estatutários e regulamentares e de um mecanismo capaz de evidenciar a eficiência das medidas adotadas e a eficácia da proteção de dados.

NOTA: Consultar Lei 13.709 de 14/08/2018, Artigo 6º X.

3.18 Avaliação de Impacto à Proteção de Dados Pessoais

A Avaliação de Impacto da Proteção de Dados Pessoais é um processo que auxilia as organizações (controladores) na identificação, avaliação e mitigação de riscos (vinculados aos direitos e liberdades dos titulares) de produtos ou serviços de tratamento de dados a serem realizados.

3.19 Proteção de dados desde a concepção

Cada novo serviço ou processo de negócios que faz uso de dados pessoais deve levar em consideração a proteção desses dados. Uma organização deve evidenciar que implantou mecanismos adequados de segurança e que a conformidade dessas medidas é monitorada. Na prática, isso significa que dados pessoais serão levados em consideração durante todo o ciclo de vida de um sistema computacional ou desenvolvimento de um processo.

3.20 Proteção de dados como padrão

A organização deve garantir que (como padrão) as funcionalidades de arquivos e aplicativos de dados pessoais asseguram um elevado nível de proteção dos mesmos, ou seja: as mais rígidas configurações de privacidade aplicam-se automaticamente quando um cliente adquire um novo produto ou serviço. Em outras palavras, nenhuma alteração manual das configurações de privacidade deve ser necessária por parte do usuário. Há também um aspecto temporal para este princípio, visto que os dados e informações pessoais devem ser mantidos apenas pelo tempo necessário para fornecer o produto ou serviço.

3.21 Regras Corporativas Vinculantes

São políticas de proteção de dados pessoais que devem ser respeitadas por um controlador ou operador, estabelecido na EU ou no Brasil, para realizar transferências especificas ou para transferir conjuntos de dados pessoais para um país terceiro, ou para um grupo de empreendimentos ou de empresas que participam em conjunto de uma atividade econômica.

© Copyright - 30/11/2019

3.22 Ciclo de vida

Etapas consecutivas e interligadas de um sistema vinculado a produtos ou serviços, desde a concepção até o descarte final.

3.23 Infraestrutura

Instalações físicas, equipamentos e serviços necessários para o funcionamento de uma organização.

© Copyright - 30/11/2019

4. Organização e Estrutura

4.1 Liderança e comprometimento

A alta Direção deve demonstrar que está totalmente comprometida com a implementação dos requisitos deste esquema de certificação e a processos que asseguram a conformidade do tratamento de dados com a Lei 13.709 de 14/08/2018 (Brasil) e/ou Regulamento (UE) 2016/679, conforme aplicabilidade no país e adoção do requisito legal pela organização.

A Alta Direção deverá implementar medidas técnica e organizacionais para assegurar e evidenciar que o tratamento de dados está em conformidade com os princípios do tratamento de dados pessoais conforme a Lei 13.709 de 14/08/2018 (Brasil) Artigo 6º e/ou no artigo 5 do Regulamento (UE) 2016/679, conforme aplicabilidade no país.

Em particular, essas medidas devem:

a) estar vinculadas à natureza, escopo, contexto e finalidades do tratamento;

b) ser adaptadas aos riscos da possibilidade e gravidade dos direitos e liberdades das pessoas naturais;

c) ser aplicadas a todas as atividades de tratamento ao longo do ciclo de vida de produtos ou serviços, a partir do desenvolvimento dos produtos e/ou serviços que compreendem o tratamento de dados pessoais.

Essas medidas devem ser avaliadas de forma regular e atualizadas, quando necessário.

4.2 Política

4.2.1 Estabelecer a política de proteção de dados pessoais

A Alta Direção deve estabelecer, documentar, implementar e manter uma política que declare seu compromisso de fornecer produtos e/ou serviços que envolvam o tratamento de dados pessoais em conformidade com a Lei 13.709 de 14/08/2018 e/ou Regulamento (UE) 2016/679 e sua responsabilidade no cumprimento de obrigações legais junto a clientes e titulares dos dados.

Essa política deve incluir um compromisso

a) à proteção de dados pessoais, incluindo a prevenção de violações de dados pessoais;

b) cumprir suas obrigações legais (ver 5.2);

c) implementar medidas técnicas e organizacionais dentro da organização para assegurar o cumprimento da Lei 13.709 de 14/08/2018 e/ou Regulamento (UE) 2016/679, conforme aplicável.

4.2.2 Comunicando a política de proteção de dados pessoais

Essa política deve estar:

- disponível, comunicado, entendida e aplicado dentro da organização, incluindo subcontratados e fornecedores de serviços, quando necessário;
- disponível para as partes interessadas relevantes, conforme apropriado.

© Copyright - 30/11/2019

4.3 Funções organizacionais, responsabilidades e autoridades

4.3.1 Organização e responsabilidades

A organização deve possuir uma estrutura organizacional documentada para garantir a conformidade com a Lei 13.709 de 14/08/2018 ou com o Regulamento (UE) 2016/679 (ver 5.2), conforme a aplicabilidade.

As responsabilidades e autoridades vinculadas com o tratamento de dados pessoais devem ser identificadas, atribuídas e entendidas. Os recursos requeridos devem ser identificados e alocados.

4.3.2 Encarregado de Proteção de Dados

Um Encarregado da Proteção de Dados deve ser nomeado para garantir a conformidade dos processos vinculados à proteção de dados pessoais.

O Encarregado de Proteção de Dados deve ser designado com base nas competências profissionais, na experiência e no conhecimento das leis e práticas da proteção de dados.

A organização deve assegurar que o Encarregado da Proteção de Dados participe de todas as questões relacionadas à proteção de dados pessoais, e deve alocar os recursos e orçamento necessários para assegurar a realização de todas as tarefas inerentes a função.

O Encarregado da Proteção de Dados deve reportar ao mais alto nível da organização.

A organização deve assegurar que o Encarregado da Proteção de Dados possa exercer suas tarefas com a necessária independência e confidencialidade. Caso o Encarregado da Proteção de Dados for encarregado de outras tarefas, deve ser assegurado a ausência de conflito de interesse.

O Encarregado da Proteção de Dados é responsável das seguintes atividades:

a) informar e aconselhar a organização e os funcionários que realizam o tratamento de dados quanto a suas obrigações (ver 5.2);

b) monitorar a conformidade da organização com o cumprimento das obrigações legais (ver 5.2) e com políticas e disposições internas, incluindo a atribuição de responsabilidades, conscientização e capacitação do pessoal que atua nas operações de tratamento e das auditorias relacionadas;

c) organizar a realização de revisões periódicas do conjunto de medidas técnicas e organizacionais relacionadas à proteção de dados pessoais (ver 6.7);

d) assessorar, quando solicitado, sobre a Avaliação de Impacto à Proteção de Dados Pessoais e monitorar seu desempenho;

e) cooperar com a Autoridade Nacional de Proteção de Dados (ANPD);

f) atuar, quando necessário, como ponto de contato junto a Autoridade Nacional de Proteção de Dados (ANPD) a respeito de questões relacionadas com dados.

A organização deve comunicar os detalhes de contato do Diretor de Proteção de Dados à Autoridade Nacional de Proteção de Dados (ANPD), titulares e outras partes interessadas sempre que necessário.

NOTA 1: O Encarregado da Proteção de Dados pode ser um funcionário ou uma pessoa contratada. Habilidades profissionais e experiência abrangem tanto habilidades de gestão, Tecnologia da Informação, Segurança da Informação e conhecimento dos produtos e serviços da organização.

NOTA 2: As diretrizes encontradas no WP29 “Guidelines on Data Protection Officers” pode ser utilizado para identificar e mitigar situações potenciais de conflito de interesse.

© Copyright - 30/11/2019

5. Gestão de Riscos de Dados Pessoais

5.1 Geral

A organização deve implementar um plano eficaz para a proteção de dados pessoais, que considere a natureza, o escopo, contexto e as finalidades do tratamento e dos riscos associados.

Esse plano de ação deve abordar:

a) conformidade com as obrigações legais (ver 5.2);

b) resultados de Avaliações de Impacto de Proteção de Dados (ver 5.3);

c) medidas para monitorar e controlar a eficácia.

Ao planejar essas ações, a organização deve:

- considerar o estado da arte tecnológico e seus requisitos financeiros, operacionais e de negócios;
- avaliar a eficácia dessas ações, mediante a adoção de técnicas apropriadas aos riscos identificados.

5.2 Atendimento aos requisitos legais e outros requisitos

A organização deve identificar todas os requisitos legais e outros requisitos relacionados às operações de tratamento de dados pessoais, incluindo:

a) Requisitos regulamentares: Lei 13709 de 14/08/2018 e quaisquer outras disposições em matéria de proteção de dados estabelecidos na legislação nacional;

b) Códigos de conduta impostos ou regras corporativas obrigatórias;

c) Políticas específicas e requisitos do controlador ou do cliente relacionadas com a proteção de dados pessoais.

A organização deve levar em conta esses requisitos ao estabelecer, implementar, manter e melhorar continuamente seu conjunto de medidas técnicas e organizacionais e manter informações documentadas quanto suas obrigações legais e da conformidade.

NOTA: quando o atendimento à legislação da Comunidade Europeia for um requisito, o Regulamento (UE) 2016/679 e quaisquer outras disposições em matéria de proteção de dados da União ou dos Estados-Membros devem ser incluído na alínea “a” deste requisito;

5.3 Avaliação de Impacto à Proteção de Dados Pessoais

O controlador deve estabelecer as atividades, produtos e serviços vinculados ao tratamento de dados pessoais que podem afetar a confidencialidade e integridade dos dados pessoais e as possíveis situações de violações de dados pessoais, dentro da perspectiva de ciclo de vida (ver 7.3).

O controlador deve definir um procedimento e critérios para a realização da Avaliação de Impacto à Proteção de Dados Pessoais. Esses critérios devem considerar o estado da arte tecnológico e a natureza, âmbito, contexto e finalidades do tratamento que resultem num elevado risco para os direitos e liberdades das pessoas naturais (ver nota 1).

O controlador com o apoio dos operadores deve considerar:

a) descrição sistemática das operações de tratamento e finalidades do tratamento (ver 7.3);

b) uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos propósitos estabelecidos;

© Copyright - 30/11/2019

c) uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados;

d) a categorização de risco dos dados pessoais;

e) condições anormais e situações razoavelmente previsíveis que podem levar a violações de dados pessoais;

f) As medidas destinadas à abordagem dos riscos, incluindo garantias, medidas de segurança e mecanismos para assegurar a proteção dos dados pessoais e para demonstrar a conformidade regulatória, levando conta os direitos e os interesses legítimos das pessoas em causa e de outras pessoas envolvidas;

g) qualquer alteração do risco representado pelas operações de tratamento, incluindo o desenvolvimento ou modificação de novas atividades, produtos e serviços.

A Avaliação de Impacto à Proteção de Dados Pessoais deve ser realizada e gerenciado mediante uma abordagem multidisciplinar que inclui marketing, desenvolvimento comercial ou de negócios, operações, tecnologia da informação e segurança, o jurídico e outras funções relevantes, incluindo as percepções dos titulares dos dados e seus representantes, quando apropriado. O apoio específico do Encarregado de Proteção de Dados deve ser solicitado.

A Avaliação de Impacto à Proteção de Dados Pessoais deve ser documentada, incluindo as situações potenciais de violações de dados pessoais.

O controlador deve comunicar os resultados da Avaliação de Impacto à Proteção de Dados Pessoais aos níveis e funções relevantes da organização, incluindo os operadores de dados, conforme apropriado.

NOTA 1

Os procedimentos e critérios para avaliação para a realização da Avaliação de Impacto sobre a Proteção de Dados Pessoais devem atender as recomendações da Autoridade Nacional de Proteção de Dados (ANPD) estabelecido na Lei nº 13.853/2019.

NOTA 2

Para as organizações que adotaram adicionalmente a legislação da comunidade Europeia, a Avaliação deve ser realizada conforme estabelecido no artigo 35 do Regulamento (UE) 2016/679.

5.4 Gerenciamento de violações de dados pessoais

A organização deve estabelecer, implementar e manter o(s) processo(s) necessário(s) para se preparar e responder a potenciais situações de violação de dados pessoais (ver 5.3).

Objetivamente, a organização deve:

a) preparar-se para responder planejando ações para prevenir ou mitigar adequadamente as violações de dados pessoais e suas consequências em função da magnitude das violações e seu impacto potencial;

b) responder a situações manifestadas de violação de dados;

c) testar periodicamente, onde possível, as ações de resposta planejadas;

d) revisar e rever periodicamente o(s) processo(s) e ações de resposta planejadas, especialmente após a ocorrência de situações ou testes de violação de dados pessoais;

e) fornecer informações relevantes e treinamento relacionado à preparação e resposta à violação de dados pessoais, conforme apropriado, às partes interessadas relevantes, incluindo as pessoas que trabalhem sob seu controle.

O operador deve notificar o controlador, sem atraso indevido, após tomar conhecimento de uma violação de dados pessoais.

© Copyright - 30/11/2019

Quando a violação de dados pessoais resulte em um alto risco para os direitos e liberdades das pessoas naturais, o controlador deve comunicar prontamente essa violação à pessoa natural afetada.

Adicionalmente, quando da violação de dados pessoais, o controlador deve notificar, sem demora, a Autoridade Supervisora sobre a violação de dados pessoais, exceto quando essa violação não resulte em um risco para os direitos e liberdades da pessoa natural.

A comunicação à pessoa em causa e/ou à Autoridade Nacional de Proteção de Dados (ANPD) deve cumprir os requisitos expressos no artigo 48º da Lei 13.709 de 14/08/2018 (ver Nota).

A organização deve manter registros de quaisquer violações de dados, incluindo os fatos relacionados à violação de dados pessoais, seus efeitos e as ações corretivas realizadas. Estes registros serão disponibilizados à ANPD, quando solicitado.

NOTA: Quando o atendimento ao Regulamento (UE) 2016/679 for um requisito, a organização deve efetuar a comunicação atendendo os artigos 33º e 34º do Regulamento (UE) 2016/679.

© Copyright - 30/11/2019

6. Sistema de Gestão

6.1 Manual e procedimentos

A organização deve estabelecer, implementar, manter e melhorar continuamente um conjunto de processos e procedimentos ("Sistema de Gestão") de acordo com os seguintes elementos desta norma de certificação, que assegurem a correta implementação e manutenção de processos relacionados a dados pessoais.

O "Sistema de Gestão" deve ser adequado ao tipo, abrangência e volume de produtos e/ou serviços que envolvam o tratamento de dados pessoais e aos riscos associados à probabilidade e gravidade para os direitos e liberdade das pessoas naturais.

Esse "Sistema de Gestão" deve dar suporte aos processos de negócios da organização e suas interações, mediante a utilização de medidas técnicas ou organizacionais apropriadas ('integridade e confidencialidade') e garantir que os dados pessoais sejam coletados, armazenados e arquivados em conformidade, incluindo a adequada segurança dos dados pessoais, assegurando a proteção contra tratamento não autorizado ou ilegal e contra perdas acidentais, perda, destruição ou danificação.

NOTA: A norma ISO 9001:2015 (Sistema de gestão da qualidade) ou a norma ISO 27001:2013 (Sistema de Gestão de Segurança da Informação) podem ser utilizadas para atender os requisitos mínimos do sistema de gestão definidos neste esquema de certificação.

6.2 Informação documentada

O "sistema de gestão" da organização deve incluir informação documentada relacionada com o tratamento de dados e processos de proteção de dados pessoais.

A organização deve ter um procedimento para gerenciar informações documentadas, que contemple:

- a identificação, descrição, revisão e aprovação;
- a distribuição, acesso, retificação, exclusão e uso;
- o armazenamento e preservação;
- o controle de mudanças;
- a retenção e descarte.

A organização deve manter registros para evidenciar o controle efetivo da conformidade de produtos e/ou serviços.

Os registros devem ser legíveis, mantidos em boas condições, recuperáveis e retidos por um período definido, levando em consideração as exigências relevantes legais ou dos clientes.

6.3 Avaliação de desempenho

A organização deve determinar:

a) o que precisa ser controlado e monitorado e quando;

b) os métodos de monitoramento, medição, análise e avaliação;

c) os critérios de desempenho e indicadores apropriados.

Adicionalmente, a organização deve estabelecer, implementar e manter o(s) processo(s) necessário(s) para avaliar os requisitos de conformidade (ver 5.2).

© Copyright - 30/11/2019

A organização deve reter informação documentada como evidência do monitoramento e conformidade de suas operações.

6.4 Auditoria Interna

A organização deve realizar auditorias internas pelo menos uma vez por ano, de todos os requisitos desta norma de certificação para fornecer informação a respeito:

- da conformidade com os requisitos;
- a efetiva implementação e manutenção.

O escopo e a frequência das auditorias devem contemplar os riscos para os processos e atividades de dados pessoais e o desempenho de auditorias anteriores.

As auditorias internas devem ser realizadas por auditores competentes, devidamente treinados. A imparcialidade dos auditores deve ser assegurada.

Os relatórios de auditoria devem detalhar qualquer desvio significativo dos requisitos desta norma. Em particular, os relatórios de auditoria devem identificar questões relacionadas à tecnologia ou processos que possam afetar a conformidade (ver 5.2).

6.5 Não conformidade e ação corretiva

A organização deve determinar oportunidades de melhoria e implantar as ações necessárias para atender as obrigações legais (ver 5.2) e evitar recorrências.

Quando ocorrer uma não-conformidade, a organização deve:

a) tomar medidas imediatas para resolver a questão;

b) avaliar ações cabíveis mediante a identificação da causa raiz da não-conformidade para evitar a recorrência;

c) implementar o plano de ação e verificar se as correções foram efetivamente implementadas.

A organização deve reter informações documentadas como evidência da natureza das não-conformidades e das ações corretivas relacionadas.

6.6 Reclamações

A organização deve garantir que as reclamações de clientes e partes interessadas sejam efetivamente gerenciadas.

A organização deve comunicar publicamente o processo utilizado para a gestão de reclamações.

Após o recebimento de uma reclamação, a organização deve:

a) comunicar ao reclamante o recebimento da reclamação;

b) reunir e verificar todas as informações necessárias para validar a reclamação e tomar uma decisão;

c) comunicar formalmente ao reclamante a decisão sobre a reclamação;

d) assegurar que quaisquer ações corretivas e preventivas sejam tomadas.

© Copyright - 30/11/2019

6.7 Análise crítica pela Direção

O Encarregado de Proteção de Dados deve organizar a análise crítica com a participação da Alta Direção em intervalos planejados apropriados, no mínimo anualmente, para revisar o desempenho da organização em relação à proteção de dados pessoais.

A análise crítica pela Direção deve incluir os seguintes assuntos, conforme apropriado:

- status de planos de ação resultantes de Análises Críticas anteriores;
- resultados de auditorias internas e externas;
- satisfação do cliente e/ou feedback das partes interessadas, incluindo reclamações;
- incidentes, violações, não conformidades e ações corretivas associadas;
- a eficácia das ações realizadas para tratar resultados da Avaliação de Impacto da Proteção de Dados; resultados de monitoramento e supervisão;
- desempenho de fornecedores e prestadores de serviços;
- qualquer alteração nos requisitos legais e outros requisitos.

Os resultados da análise crítica pela Direção devem incluir:

- oportunidades de melhoria;
- um plano de ação que inclua necessidades de recursos;
- ações de melhoria, se necessário, quando a conformidade com a proteção de dados não foi alcançada;
- qualquer implicação para a política de proteção de dados pessoais da organização.

A conclusão das análises críticas e os planos de ação associados devem ser efetivamente comunicados ao pessoal apropriado e implementados. Os registros das análises críticas devem ser documentados.

6.8 Comunicação

6.8.1 Geral

Ao estabelecer seu (s) processo (s) de comunicação, a organização deve:

a) levar em consideração os requisitos legais e outros requisitos (ver 5.2);

b) garantir que as informações comunicadas relacionadas à proteção de dados pessoais sejam consistentes e confiáveis com os requisitos desta norma.

A organização deve reter informações documentadas como evidência de sua comunicação, onde apropriado.

6.8.2 Comunicação interna

A organização deve:

a) comunicar internamente informações relevantes ao sistema de gestão de proteção de dados entre os vários níveis e funções da organização, incluindo mudanças no sistema de gestão, conforme apropriado;

b) garantir que o (s) seu (s) processo (s) de comunicação possibilite (m) que as pessoas que trabalhem sob o controle da organização contribuam para a melhoria contínua.

© Copyright - 30/11/2019

A organização deve assegurar que quaisquer políticas ou requisitos específicos do cliente, códigos de conduta, obrigações, regras corporativas vinculantes, etc. são entendidos, implementados e comunicados claramente ao pessoal relevante e, quando apropriado, a fornecedores e prestadores de serviços.

6.8.3 Comunicação externa

A organização deve comunicar externamente as informações relevantes para a proteção de dados pessoais, conforme estabelecido pelo (s) processo (s) de comunicação da organização e conforme exigido por suas obrigações de conformidade (ver 5.2).

Em particular, os controladores, com o apoio dos operadores, devem adotar as medidas necessárias para fornecer informações relativas aos direitos e liberdades das pessoas naturais, nos termos dos artigos 9º e 48º da Lei 13.709 de 14/08/2018.

NOTA:

Quando o atendimento ao Regulamento (UE) 2016/679 for um requisito, as medidas para fornecer informações relativas aos direitos e liberdades das pessoas naturais, a comunicação deve estar em conformidade com os artigos 12º a 23º (capítulo III: direitos dos titulares de dados) do Regulamento (UE) 2016/679.

© Copyright - 30/11/2019

7. Controle de produto e/ou serviço

7.1 Requisitos para produtos e serviços

A organização deve assegurar que os requisitos para produtos e/ou serviços sejam definidos, incluindo:

a) Atendimento aos requisitos legais e outros requisitos (ver 5.2)

b) requisitos internos considerados necessários pela organização ou impostos por códigos de conduta ou regras corporativas vinculantes.

A organização deve conduzir uma revisão de sua capacidade de atender aos requisitos de produtos e/ou serviços a serem oferecidos aos clientes.

A organização deve reter informação documentada, onde aplicável, sobre os resultados dessa revisão. Essa revisão deve ser atualizada quando houver qualquer mudança de requisitos para os produtos e/ou serviços.

7.2 Projeto e desenvolvimento de produtos e/ou serviços

O controlador deve estabelecer, implementar e manter um processo de projeto e desenvolvimento que garanta a conformidade contínua do tratamento de dados, ao longo de todo o ciclo de vida, incluindo o tratamento de fim da vida útil e descarte final de seus produtos e/ou serviços.

O controlador com o apoio dos operadores deve implementar medidas técnicas e organizacionais apropriadas para assegurar que:

- os requisitos para produtos e serviços são levados em consideração no projeto e desenvolvimento;
- o tratamento de dados pessoais está em conformidade com os princípios relativos ao tratamento de dados pessoais, conforme expresso nos artigos 2º e 6º da Lei 13709 de 14/08/2018. Quando o atendimento a regulamentação da Comunidade Europeia for um requisito, o artigo 5º do Regulamento (UE) 2016/679 deve ser aplicado;
- o tratamento está em conformidade com os interesses ou direitos e liberdades fundamentais da pessoa natural ou com qualquer pessoa natural e, em particular, de pessoas vulneráveis e crianças:
- as adequadas medidas de segurança relacionadas com dados pessoais são definidas em conformidade com o artigo 46º da Lei 13709 de 14/08/2018, e, quando aplicável, o artigo 32º do Regulamento (UE) 2016/679;
- os resultados da respectiva Avaliação de Impacto à Proteção de Dados Pessoais foram levados em consideração e, em particular, as consequências de falha devido à natureza dos produtos e serviços (ver 5.3);
- por padrão ou definição, apenas dados pessoais que são necessários para cada finalidade específica do tratamento sejam processados. Essa obrigação aplica-se ao volume de dados pessoais coletados, à extensão do tratamento realizado e ao período de armazenamento e acessibilidade;
- o pedido de consentimento deve ser apresentado numa forma claramente distinguível, inteligível e de fácil acesso, usando uma linguagem simples e objetiva.

O controlador deve controlar o processo de projeto e desenvolvimento para garantir que os produtos e serviços resultantes atendam aos requisitos para a aplicação especificada ou uso pretendido.

O projeto e o desenvolvimento de produtos ou serviços somente será validado após uma revisão do apropriado fechamento de não conformidades relacionadas à proteção de dados pessoais.

© Copyright - 30/11/2019

O controlador deve reter informação documentada relacionada com as atividades de projeto e desenvolvimento.

NOTA 1: Os direitos e liberdades das pessoas naturais estão expressos nos artigos 17º a 22º (Capítulo III – Direitos do Titular) da Lei 13.709 de 14/08/2018.

NOTA 2: No Regulamento (UE) 2016/679 – Capítulo III: direitos dos titulares dos dados, artigos 12 a 23 estabelecem os direitos e liberdades das pessoas naturais.

7.3 Liberação de produtos e/ou serviços

Quando produtos e/ou serviços resultantes do tratamento de dados pessoais necessitarem de aprovação positiva de liberação ("positive release"), deverão ser adotados procedimentos para assegurar que a liberação não ocorra até que todos os requisitos sejam finalizados e a liberação (de fato) autorizada.

Em conformidade com o artigo 37º e 40º da Lei 13.709 de 14/08/2018 (ver Nota), a organização deve manter registos das atividades de tratamento sob a sua responsabilidade em formatos físicos ou eletrônicos.

Esses registros devem conter as seguintes informações (no nível do controlador):

a) nome e dados de contato do controlador e do Encarregado de Proteção de Dados;

b) os propósitos do tratamento;

c) uma descrição das categorias de titulares de dados e das categorias de dados pessoais;

d) as categorias de destinatários;

e) quando aplicável, transferências de dados pessoais para um país terceiro ou uma organização internacional;

f) sempre que possível, os prazos previstos para a eliminação das diferentes categorias de dados;

g) sempre que possível, uma descrição geral das medidas técnicas e organizacionais associadas à segurança dos dados pessoais.

Esses registros devem conter as seguintes informações (no nível do operador):

a) nome e detalhes de contato do operador;

b) as categorias de tratamento realizadas em nome de cada controlador;

c) quando aplicável, transferências de dados pessoais para um país terceiro ou uma organização internacional;

d) sempre que possível, uma descrição geral das medidas técnicas e organizacionais associadas à segurança dos dados pessoais.

A organização deve disponibilizar os registos à Autoridade Nacional de Proteção de Dados (ANPD), quando solicitado.

NOTA: O artigo 30º do Regulamento (UE) 2016/679 e o artigo 37º da Lei 13.709 de 14/08/2018 estabelecem as obrigatoriedades em relação ao registro das atividades de tratamento de dados.

© Copyright - 30/11/2019

8. Controle operacional

A organização deve desenvolver, implementar e manter procedimentos documentados e/ou instruções que assegurem a conformidade de suas operações de tratamento de dados, inclusive na sua cadeia de fornecimento.

8.1 Controle do Tratamento de dados

Os dados pessoais devem ser

a) tratados de forma legal, justa e transparente em relação ao titular dos dados;

b) precisos e, quando necessário, mantidos atualizados;

c) mantidos numa forma que permita a identificação dos titulares dos dados por um período não superior ao necessário para os fins estabelecidos;

d) processados de maneira a segurança apropriada dos dados pessoais é garantida.

O tratamento de dados de pessoal deve ocorrer em conformidade com os direitos e liberdades das pessoas naturais expressas nos artigos 17º a 22º da Lei 13.709 de 14/08/2018 (ver Nota), em particular os direitos relacionados com:

- informação e acesso a dados pessoais;
- direito de acesso pelo titular dos dados;
- direito de retificação;
- direito de eliminação ou de “ser esquecido”;
- direito à portabilidade de dados;
- direito de oposição.

Levando-se em consideração a natureza, escopo, contexto e propósito do tratamento, bem como os riscos de variação de probabilidade e gravidade para os direitos e liberdades das pessoas naturais, a organização deverá implementar medidas técnicas e organizacionais adequadas para controlar o tratamento e para ser capaz de evidenciar que o tratamento é realizado de acordo com os requisitos legais aplicáveis (ver 5.2).

Devem estar disponíveis procedimentos e/ou instruções que especificam como os dados pessoais são processados para atender aos princípios expressos nos artigos 2º e 6º da Lei 13.709 de 14/08/2018. Para as organizações que adotarem o Regulamento (UE) 2016/679, estes princípios estão expressos no artigo 5º.

O controlador deve assegurar que as ações de mitigação dos riscos resultante do tratamento da Avaliação de Impacto da Proteção de Dados sejam efetivamente implementadas.

De forma consistente com a perspectiva de ciclo de vida, a organização deve manter informações documentadas para evidenciar que os processos foram executados conforme o planejado e demonstrar a conformidade dos produtos e/ou serviços com seus requisitos (ver 7.3).

A ocorrência de qualquer evento durante operações de tratamento que viole os direitos da pessoa natural deve ser registrada como uma não conformidade e dado início a uma ação corretiva.

NOTA:

Para atendimento à legislação da Comunidade Europeia, os direitos e liberdades a serem considerados no tratamento de dados estão expressos nos artigos 12º a 23º (capítulo III: direitos dos titulares de dados) do Regulamento (UE) 2016/679.

© Copyright - 30/11/2019

8.2 Controle de subcontratados e Fornecedores de serviços

A organização deve assegurar que os processos de terceirização sejam controlados de acordo com o artigo 39º da Lei 13.709 de 14/08/2018 (ver Nota) e assegurar a proteção dos direitos do titular dos dados.

O tipo e abrangência do controle ou da influência a ser exercida devem ser definidos tendo em conta a natureza, escopo, contexto e finalidades do tratamento que resultem num risco elevado para com os direitos e liberdades das pessoas naturais.

Em particular:

- a organização deve utilizar fornecedores que forneçam garantias suficientes para implementar medidas técnicas e organizacionais apropriadas que o tratamento de dados cumpra as obrigações de conformidade (ver 5.2) e assegure a proteção dos direitos do titular dos dados;
- o tratamento por um fornecedor externo será gerido por um contrato que define o objeto e a duração do tratamento, a natureza e a finalidade do tratamento, o tipo de dados pessoais e categorias de titulares de dados e os dados e os direitos do controlador.

Esse contrato deve estipular, em especial, que o prestador externo:

(a) trate os dados pessoais seguindo apenas as instruções documentadas do controlador, incluindo no que diz respeito a transferências de dados pessoais para um país terceiro ou uma organização internacional;

b) garanta que as pessoas autorizadas a tratar os dados pessoais se comprometeram com a confidencialidade;

c) adote todas as medidas especificadas relacionadas com a segurança de dados pessoais;

d) assista o controlador através de medidas técnicas e organizativas adaptadas à natureza do tratamento;

(e) auxilie o controlador a garantir o cumprimento da conformidade com as obrigações estabelecidas nos artigos 46º a 50º e 37º a 39º da Lei 13.709 de 14/08/2018, considerando-se a natureza do tratamento. Se a organização adotou o Regulamento (UE) 2016/679 as obrigações estabelecidas encontram-se nos artigos 32º a 36º;

(f) na escolha do controlador de dados, exclua ou devolva os dados pessoais à organização após o término da prestação de serviços relacionados ao tratamento;

(g) coloque à disposição da organização toda a informação necessária para demonstrar a conformidade com as obrigações legais e contribua para auditorias, incluindo inspeções, conduzidas pela organização ou outro auditor, conforme determinado pela organização;

(h) não contrate outro operador e/ou prestador de serviços sem autorização prévia específica ou geral por escrito do controlador de dados;

(i) notifique o controlador sem demora, após ter tomado conhecimento de uma violação de dados pessoais e de qualquer infração a Lei 13.709 e 14/08/2018 ou do Regulamento (UE) 2016/679, quando este for aplicável.

Um controlador ou operador somente pode transferir dados pessoais para um país terceiro ou uma organização internacional se a transferência estiver em conformidade com uma das disposições expressas no Capítulo V (“Da Transferência Internacional de Dados) artigos 33º a 36º da Lei 13.709 de14/08/2018 (ver Nota).

© Copyright - 30/11/2019

NOTA:

Se o atendimento do Regulamento (UE) 2016/679 for uma obrigação adicional de conformidade, a organização deve-se assegurar que os processos de terceirização sejam controlados de acordo com os artigos 27 e 28 do Regulamento (UE) 2016/679. Adicionalmente, a transferência de dados para um país terceiro deve estar em conformidade com os artigos 27º, 44º, 45º e 46º do Regulamento (UE) 2016/679.

© Copyright - 30/11/2019

9. Recursos

A organização deve determinar e providenciar medidas organizacionais para garantir a conformidade com os requisitos de proteção de dados pessoais.

9.1 Infraestrutura

A organização deve implementar medidas técnicas e organizacionais projetadas para atender os princípios da proteção de dados de maneira eficaz e integrar, quando apropriado, as salvaguardas necessárias no tratamento considerando-se o tipo e a natureza do tratamento e os resultados da Avaliação de Impacto de Proteção de Dados

Em particular, tais medidas devem assegurar que, por definição, os dados pessoais não sejam acessíveis a um número indefinido de pessoas naturais sem a intervenção do titular dos dados.

Quando proporcional ao tratamento, as medidas referidas acima incluirão a implementação de políticas adequadas de proteção de dados por parte da organização. Essas medidas devem especificar os controles apropriados de segurança ao longo das diferentes etapas de coleta, armazenamento, manuseio e transferência de dados.

A organização deve implementar procedimentos que garantam que o acesso às informações pessoais seja restrito exclusivamente ao pessoal que precisa ter tal acesso.

A organização deve implementar o processo apropriado para testes regulares, avaliando e analisando a eficácia de medidas técnicas e organizacionais implantadas para garantir a segurança do tratamento.

NOTA 1:

Quando apropriado, a organização pode considerar a conformidade com a ISO/IEC 27001.

NOTA 1:

A norma ISO/IEC 27002:2013 pode ser utilizada como guia para a identificação de medidas apropriadas a serem implementadas.

NOTA 3:

Deve ser dada especial atenção ao armazenamento de dados pessoais em dispositivos ou equipamentos portáteis.

9.2 Pessoal

9.2.1 Competência

A organização deve:

a) determinar a competência necessária da (s) pessoa (s) que executam o trabalho que afeta a proteção de dados pessoais e sua capacidade de cumprir com as obrigações de conformidade, incluindo a comunicação;

b) assegurar que essas pessoas sejam competentes com base em educação, treinamento ou experiência apropriados;

c) determinar as necessidades de treinamento associadas à Avaliação de Impacto à Proteção de Dados Pessoais, conforme apropriado;

d) manter as competências de seu pessoal envolvido na proteção de dados pessoais, considerando-se mudanças em tecnologias e práticas; e,

e) quando aplicável, adotar medidas para adquirir a competência necessária e avaliar a eficácia das ações tomadas.

© Copyright - 30/11/2019

Em particular, a pessoa responsável pela implementação do "sistema de gestão" dentro da organização deve ter recebido capacitação sobre a Lei 13.709 de 14/08/2018, e quando aplicável, do Regulamento (UE) 2016/679.

Registros de todos os treinamentos devem estar disponíveis. Isto deve incluir, no mínimo:

a) nome do treinando e confirmação de presença;

b) a data e a duração do treinamento;

c) o título ou conteúdo do curso, conforme apropriado;

d) o fornecedor de treinamento.

9.2.2 Conscientização

A organização deve assegurar que todo o pessoal relevante esteja ciente de:

a) as políticas e procedimentos de proteção de dados pessoais;

b) as violações de dados pessoais atuais ou potenciais, associadas ao seu trabalho;

c) as implicações da não conformidade com a política de proteção de dados pessoais e as obrigações de conformidade da organização.

© Copyright - 30/11/2019

Anexo 1 – Introdução

0.1 Geral

Os potenciais benefícios para uma organização que implemente um "sistema de gestão" vinculado à proteção de dados pessoais baseados nesta Norma Técnica são:

a) a capacidade de fornecer consistentemente produtos e serviços que atendam aos requisitos estatutários e regulatórios aplicáveis;

b) abordar os riscos e oportunidades associados ao seu contexto e objetivos;

c) a capacidade de demonstrar conformidade com os requisitos regulatórios.

A norma utiliza uma abordagem de processo baseada no ciclo PDCA (Plan-Do-Check-Act) e um pensamento baseado em riscos. No particular, a norma inclui:

- a adoção de regras internas;
- a retenção de registros de qualquer tratamento realizado sob a responsabilidade do controlador ou subcontratado, ou seja, uma descrição de cada operação de tratamento implementada;
- a implementação de uma avaliação de impacto para os processos que apresentem riscos particulares no que diz respeito aos direitos e liberdades das pessoas naturais;
- respeito pelo princípio da transparência nas transações decisivas relacionadas com a proteção de dados pessoais;
- a implementação das abordagens de “proteção de dados desde a concepção” e “proteção de dados como definição ou padrão” em projetos;
- a nomeação do Encarregado de Proteção de Dados;
- documentação e registro das ações de conformidade.

0.2 Objetivo deste esquema de certificação

O objetivo desta norma de certificação é o de dar uma resposta aos avanços das comunicações e das tecnologias de informação e fornecer um marco referencial das medidas organizacionais e de processos que viabilizem o atendimento do Regulamento (UE) 2016/679 ou da Lei 13.709 de 14/08/2018 referente à proteção de dados pessoais.

Uma abordagem sistêmica para a gestão da proteção de dados pessoais pode fornecer à Alta Direção de informações para ações bem sucedidas de longo prazo e criar condições para atingir a conformidade no que se refere à:

- proteção de dados pessoais, mediante a prevenção ou mitigação de violações de dados pessoais;
- auxiliar a organização no atendimento das suas obrigações de responsabilidade legal;
- controlar ou influenciar a maneira como os produtos e serviços da organização são concebidos, desenvolvidos, processados e descartados usando uma perspectiva de ciclo de vida que possa prevenir violações da proteção de dados pessoais;
- comunicar informações apropriadas às partes interessadas relevantes.

© Copyright - 30/11/2019

0.3 Abordagem de processo

0.3.1 Geral

1 **Princípio da responsabilidade objetiva**. Este é um princípio geral de responsabilidade para o controlador por qualquer tratamento de dados pessoais que ele próprio realize ou que seja realizado em seu nome.

2 Consequentemente, esta obrigação exige que o controlador implemente medidas técnicas e organizacionais apropriadas para realizar o tratamento em conformidade com os requisitos do regulamento.

3 **Regras Internas**. Para cumprir com esta obrigação, o controlador deve descrever pormenorizadamente as conformidades requeridas para dar cumprimento ao Regulamento ou a Lei 13.709 e fornecer provas especificas, decorrentes das regras e mecanismos internos adotados.

4 O controlador deve adotar uma abordagem proativa, para evidenciar que é capaz de demonstrar a conformidade sem esperar que irregularidades sejam relatadas e informadas. O controlador deve adotar regras internas e implantar medidas destinadas a assegurar que o tratamento dos dados é efetuado em conformidade com o Regulamento ou a Lei 13.709.

5 O escopo dessas obrigações leva em consideração:

- o objetivo das operações de tratamento;
- os riscos de infringir os direitos e liberdades das pessoas naturais.

6 Dependendo dos riscos associados aos tipos de dados processados, as medidas a serem tomadas abrangem desde a documentação até a implantação de processos específicos de segurança e da implementação de uma avaliação de impacto.

7 **Transparência**. O controlador está sujeito a uma obrigação de transparência e rastreabilidade dos documentos, a fim de poder ser responsabilizado. Deve ser sempre capaz de identificar e documentar as medidas tomadas para cumprir com os requisitos do Regulamento ou da Lei 13.709 e demonstrar que cumpriu suas obrigações com a proteção de dados pessoais. Todas as ações da Política de Proteção de Dados devem ser documentadas para demonstrar sua implementação à Autoridade Nacional de Proteção de Dados (ANPD).

8 **Proteção de dados desde a concepção**. O princípio de "proteção de dados desde a concepção" exige que as organizações levem em consideração a proteção de dados desde o início do projeto de produtos, serviços e sistemas de informação que utilizem dados pessoais.

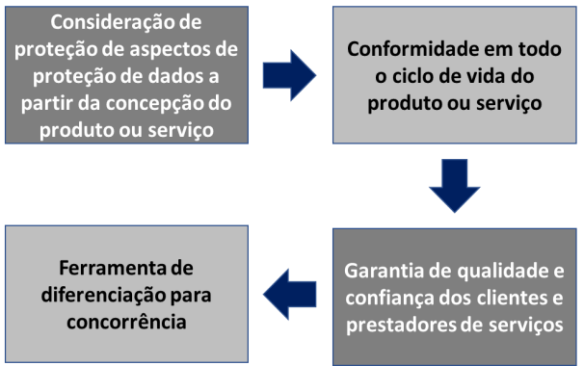

Figura 1: Proteção desde a Concepção (“Design”)

9 **Proteção de dados por definição ou padrão.** O princípio "proteção de dados por definição ou padrão" exige que as organizações possuam um sistema de informação que garanta um alto nível de proteção de dados em todos as etapas (registro, operação, administração, integridade e atualização). A segurança do sistema de informação deve ser assegurada em

© Copyright - 30/11/2019

todos os seus elementos físicos ou lógicos. Esta regra implica que o status de segurança do sistema de informação deve ser monitorado em relação às especificações do fabricante, aspectos vulneráveis e atualizações.

O contexto de aplicação do Regulamento e da Lei 13.709 pode ser visualizada da seguinte forma:

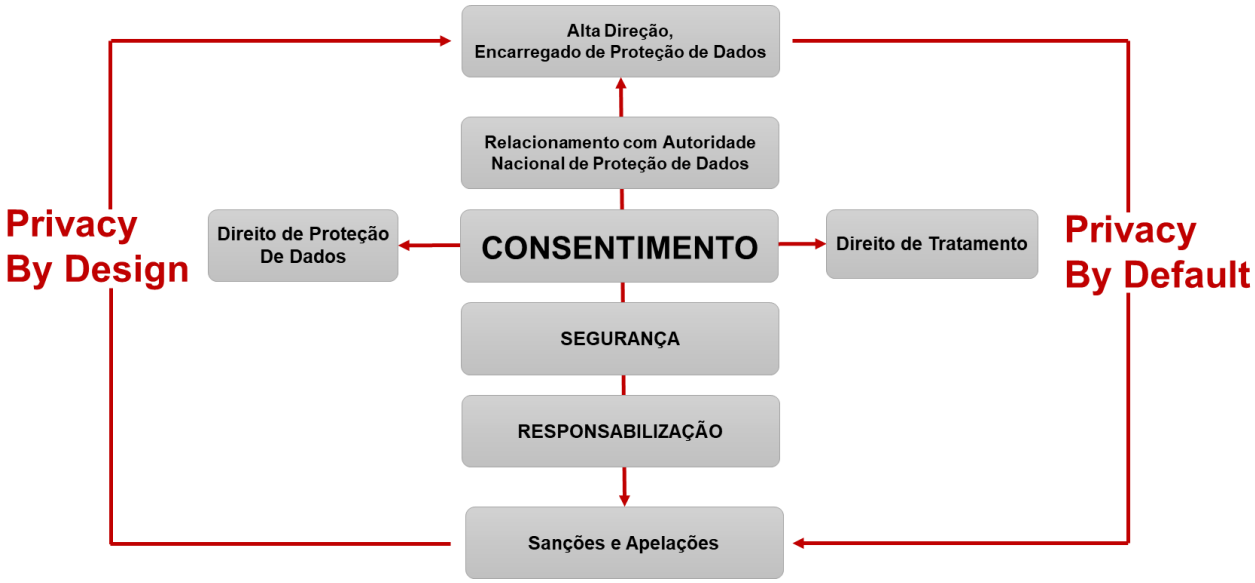

Figura 2: Proteção desde a Concepção (“Design”)

Anexo 2 – Matriz de Referência Cruzada

Norma Técnica TS-BVCBr0001 Proteção de Dados Pessoais
Regulamento (UE) de 2016/679 (GDPR), Lei nº 13.709 (LGPD) de 14/08/2018, Lei nº 13.853 de 08/07/2019

NORMA TÉCNICA TS-BVCBr0001	GDPR	Lei nº 13.709	Lei nº 13.853
0 Prefácio			
1 Escopo	Article 2; Article 3	Artigo 1	
2 Referências			
3 Termos e definições	Article 4	Artigo 5	
4 Organização e Estrutura			
4.1 Liderança e comprometimento	Article 24	Artigo 50	
4.2 Política			
4.2.1 Estabelecer a política de proteção de dados pessoais			
4.2.2 Comunicando a política de proteção de dados pessoais			
4.3 Funções organizacionais, responsabilidades e autoridades	Article 24; Article 28; Article 37; Article 38; Article 39	Artigo 5; Artigo 41; Artigo 42 Artigo 43; Artigo 44	Artigo 5 (VIII), Artigo 55
4.3.1 Organização e responsabilidades			
4.3.2 Encarregado de Proteção de Dados			
5 Gestão de Riscos de Dados Pessoais	Article 24; Article 28	Artigo 38; Artigo 44; Artigo 46	
5.1 Geral			
5.2 Atendimento a requisitos legais e outros requisitos	Article 6; Article 8; Article 24; Article 28	Artigo 37; Artigo 39; Artigo 50	Artigo 55
5.3 Avaliação de Impacto à Proteção de Dados Pessoais	Article 35, Article 36	Artigo 5; Artigo 38; Artigo 39	
5.4 Gerenciamento das violações de dados pessoais	Article 33; Article 34	Artigo 48; Artigo 50	Artigo 48; Artigo 50; Artigo 55

© Copyright - 30/11/2019

NORMA TÉCNICA TS-BVCBr0001	GDPR	Lei nº 13.709	Lei nº 13.853
6 Sistema de Gestão			
6.1 Manual e procedimentos	Article 5	Artigo 50	
6.2 Informação documentada	Article 30 (register), Article 35 (DPIA)	Artigo 40; Artigo 50	
6.3 Avaliação de desempenho	Article 24	Artigo 50	
6.4 Auditoria Interna	Article 24	Artigo 50	Artigo 55
6.5 Não conformidade e ação corretiva			
6.6 Reclamações		Artigo 41; Artigo 50	Artigo 55
6.7 Análise crítica pela Direção	Article 24	Artigo 50	
6.8 Comunicação			
6.8.1 Geral			
6.8.2 Comunicação Interna	Article 41; Article 47		
6.8.3 Comunicação Externa	Article 6; Article 7; Article 12; Article 13; Article 14; Article 15; Article 16; Article 17; Article 18; Article 19; Article 20; Article 21; Article 22; Article 23; Article 34	Artigo 9; Artigo 48	Artigo 55
7 Controle de produto e/ou serviço			
7.1 Requisitos para produtos e serviços	Article 47		
7.2 Projeto e desenvolvimento de produtos e/ou serviços	Article 5; Article 7; Article 12 a 23; Article 25; Article 32; Article 36; Article 41; Article 47	Artigo 46	Artigo 55
7.3 Liberação de produtos e/ou serviços	Article 30; Article 47	Artigo 37	
8 Controle operacional			
8.1 Controle de Tratamento de dados	Article 5; Article 24; Article 12 ao 23; Article 32; Article 36	Artigo 7 ao 16; Artigo 42	
8.2 Controle de subcontratados e fornecedores de serviços	Article 27; Article 28; Article 44; Article 45; Article 46	Artigo 37, Artigo 39	Artigo 55
9 Recursos			

NORMA TÉCNICA TS-BVCBr0001	GDPR	Lei nº 13.709	Lei nº 13.853
9.1 Infraestrutura	Article 24 (2); Article 25 (1) (2); Article 28; Article 32 (1d)	Artigo 46	
9.2 Pessoal			
9.2.1 Competência	Article 24; Article 25; Article 37	Artigo 50	
9.2.2 Conscientização	Article 32(4)	Artigo 50	
8.1 Controle de Tratamento	Article 5; Article 24; Article 12 a 23; Article 32; Article 36	Artigo 42	
8.2 Controle de subcontratados e fornecedores de serviços	Article 27; Article 28; Article 44; Article 45; Article 46	Artigo 3	
9 Recursos			
9.1 Infraestrutura	Article 24 (2); Article 25 (1) (2); Article 28; Article 32 (1d)	Artigo 46	
9.2 Pessoal			
9.2.1 Competência	Article 24; Article 25; Article 37	Artigo 50	
9.2.2 Conscientização	Article 32(4)	Artigo 50	

© Copyright - 30/11/2019

Anexo 3 – Aplicabilidade ao Operador

NORMA TÉCNICA TS-BVCBr0001	LGPD
0 Prefácio	Totalmente Aplicável
1 Escopo	Totalmente Aplicável
2 Referências	Totalmente Aplicável
3 Termos e definições	Totalmente Aplicável
4 Organização e Estrutura	Totalmente Aplicável
4.1 Liderança e comprometimento	Totalmente Aplicável
4.2 Política	Totalmente Aplicável
4.2.1 Estabelecer a política de proteção de dados pessoais	Totalmente Aplicável
4.2.2 Comunicando a política de proteção de dados pessoais	Totalmente Aplicável
4.3 Funções organizacionais, responsabilidades e autoridades	Totalmente Aplicável
4.3.1 Organização e responsabilidades	Totalmente Aplicável
4.3.2 Encarregado de Proteção de Dados	Totalmente Aplicável
5 Gerenciamento de Risco de Dados Pessoais	-:-
5.1 Geral	Aplicável quanto ao apoio a ser dado ao controlador e resultados do Relatório de Impacto à Proteção de Dados Pessoais
5.2 Cumprimento das obrigações legais e da conformidade	Brindar apoio ao controlador
5.3 Avaliação do Impacto à Proteção de Dados Pessoais	Totalmente Aplicável
5.4 Gerenciando violações de dados pessoais	Totalmente aplicável. Requer coordenação com o controlador a respeito da notificação / comunicação.
6 Sistema e Gestão	-:-
6.1 Manual e procedimentos	Totalmente Aplicável
6.2 Informação documentada	Totalmente Aplicável
6.3 Avaliação de desempenho	Totalmente Aplicável
6.4 Auditoria Interna	Totalmente Aplicável

© Copyright - 30/11/2019

NORMA TÉCNICA TS-BVCBr0001	LGPD
6.5 Não conformidade e ação corretiva	Totalmente Aplicável
6.6 Reclamações	Totalmente Aplicável
6.7 Análise crítica pela Direção	Coordenar com o controlador a respeito da eficácia das ações tomadas para tratar os resultados do Relatório de Impacto à Proteção de Dados Pessoais
6.8 Communicação	Totalmente Aplicável
6.8.1 Geral	Totalmente Aplicável
6.8.2 Comunicação Interna	Totalmente Aplicável
6.8.3 Comunicação Externa	Parcialmente aplicável. Requer o apoio ao controlador.
7 Controle de produto e/ou serviço	-:-
7.1 Requisitos para produtos e serviços	Totalmente Aplicável
7.2 Projeto e desenvolvimento de produtos e/ou serviços	Brindar apoio ao controlador
7.3 Liberação de produtos e/ou serviços	Requisitos específicos do registro
8 Controle operacional	Totalmente Aplicável
8.1 Controle de Processamento	Parcialmente aplicável. Requer apoio ao controlador.
8.2 Controle de subcontratados e fornecedores de serviços	Aplicável. Refere-se ao contrato.
9 Recursos	-:-
9.1 Infraestrutura	Totalmente aplicável. Requer coordenação com o controlador a respeito dos resultados do Relatório de Impacto à Proteção de Dados Pessoais.
9.2 Pessoal	Totalmente aplicável. Requer coordenação com o controlador a respeito dos resultados do Relatório de Impacto à Proteção de Dados Pessoais.
9.2.1 Competência	Totalmente Aplicável
9.2.2 Conscientização	Totalmente Aplicável

© Copyright - 30/11/2019