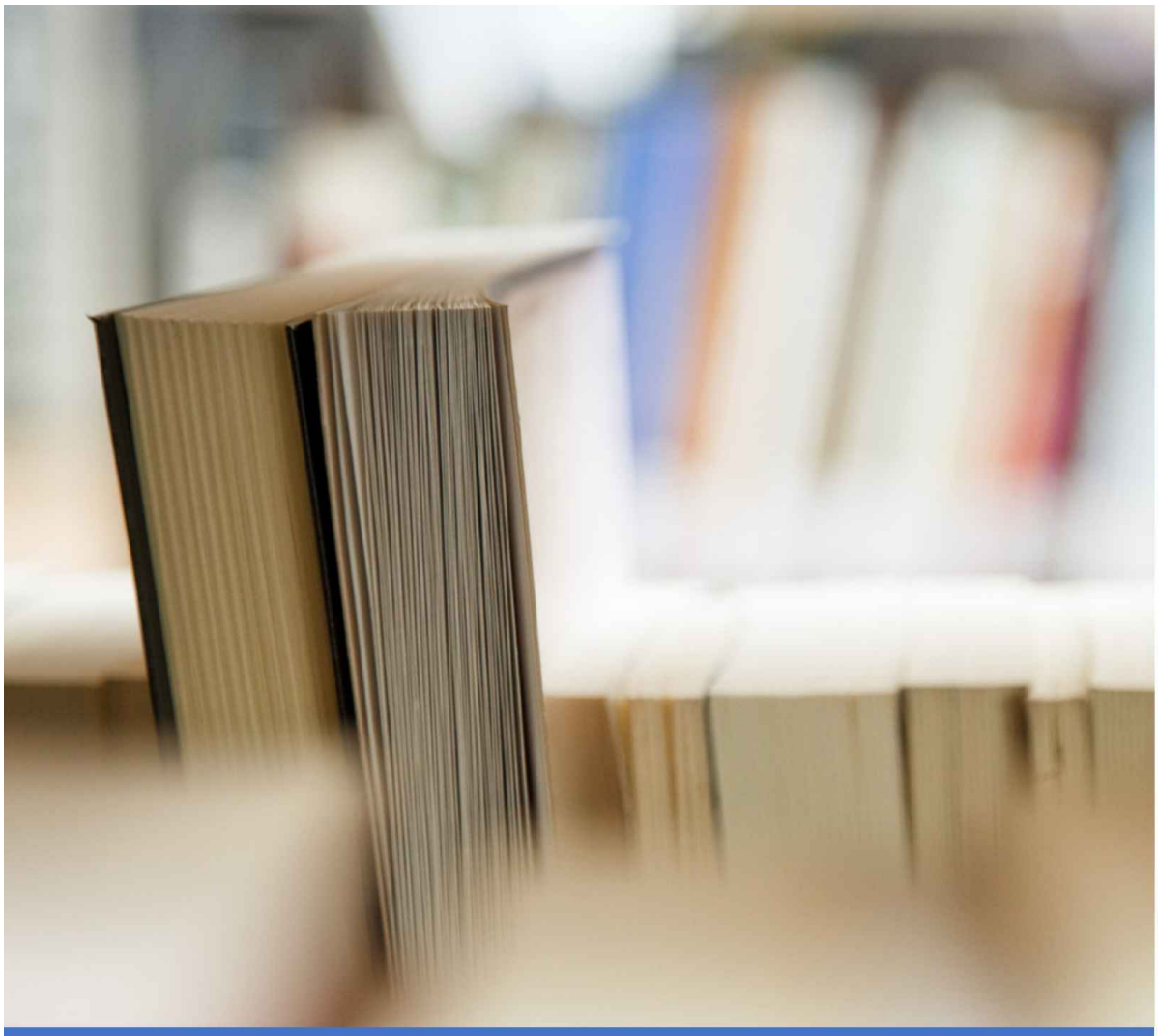
Entendendo Privacidade de Dados Pessoais na LGPD

Sandro Oliveira



Entendendo Privacidade de Dados Pessoais na LGPD

Sandro Lima de Oliveira

PrivacidadeGuru

Privacy by design

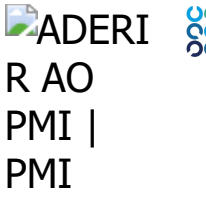
Sobre o autor

Sandro Lima de Oliveira
Pai de família, cristão, musicista e gestor da área de tecnologia.
Linkedin:
https://www.linkedin.com/in/sandro-lima-de-oliveira/

aws CERTIFIED Solutions Architect Associate

CERTIFICATION ITIL

Microsoft CERTIFIED Systems Engineer



Agradecimentos

Como toda jornada na nossa vida começa com um passo, no agradecimento não poderia ser diferente.

Agradeço a minha maravilhosa família pelo apoio e compreensão. Muito obrigado Claudia, Fernanda, Laura e Letícia.

Agradeço ao meu Deus senhor, criador e mantenedor de todas as coisas.

Sumário

Introdução

A cada era ou geração a humanidade inventa meios de facilitar sua vida e como resultado, por muitas vezes estes acabam se fundindo com nossas necessidades mais básicas. Hoje vivemos um momento ímpar, em que a informação passou a ter um valor intrínseco maior do que as grandes empresas do século XX. A informação tornou-se o motor das empresas e dos indivíduos como sociedade.

Cada vez que você compra um produto online, usa um serviço, registra-se para receber e-mail, vai ao seu médico, paga seus impostos e contas, ou celebra qualquer contrato ou solicitação de serviço, você deve fornecer algumas de suas informações pessoais.

Mesmo sem o seu conhecimento explícito, as informações sobre você estão sendo geradas e capturadas por empresas, empresas, organizações de todos os tipos e agências governamentais com as quais você provavelmente nunca interagiu intencionalmente.

A única maneira de os clientes, cidadãos e consumidores confiarem e confiarem no governo e nas empresas é por meio de fortes práticas de proteção de dados, com legislação eficaz para ajudar a minimizar o monitoramento desnecessário por autoridades estaduais e regular a vigilância por empresas.

Desde 1960 e com a expansão das capacidades de tecnologia da informação e comunicação, empresas e organizações governamentais têm armazenado essas informações pessoais em bancos de dados computadorizados.

Agora vivemos a revolução da informação, em que as antigas falsas fronteiras, aos poucos, estão sendo ultrapassadas.

Neste cenário, a manutenção do valor da informação torna-se estratégica e traz em si o dever de sua proteção.

A proteção da informação pode ser aplicada em vários níveis de nossa sociedade. Nosso governo, assim como outros, preocupado com o correto tratamento das informações pela sociedade, elaborou leis e decretos de salvaguarda deste processo.

Muito do que fazemos é baseado em estatutos, padrões, precedência e outras formas de regulamentação.

Convido a você para juntos refletirmos sobre o entendimento de umas das leis mais recentes aplicadas em nosso país, a LGPD.

Leis de segurança

Leis e Projetos de Lei gerais sobre proteção de dados e privacidade em 2018/2019

Nos anos de 2018 e 2019 tivemos:

MODELOS REGULATÓRIOS UNIÃO EUROPEIA

- Diretiva 95/46/CE
- Regulamento Europeu Geral de Proteção de Dados (GDPR)

MODELOS REGULATÓRIOS NOS ESTADOS UNIDOS

- Privacy Act
- Modelo setorial

Características das novas leis de proteção de dados:

1. Não existe dado pessoal insignificante (conceito amplo: "identificado ou identificável")
2. Necessidade de uma base legal para o tratamento de dados
3. Instrumentos de tutela coletiva e preventiva

Globalmente, há um aumento crescente nas leis de proteção de dados, muitas das quais foram modeladas diretrizes ou regulamentos abrangentes, como a Diretiva da UE mencionada acima, ou as Diretrizes da OCDE sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais.

Segundo pesquisa UNCTAD (Conferência das Nações Unidas sobre Comércio e Desenvolvimento, A UNCTAD é Órgão da Assembleia Geral da Organização das Nações Unidas (ONU), mas suas decisões não são obrigatórias. Ela tem sido utilizada pelos países em desenvolvimento como um grupo de pressão.

Mais de cem países em todo o mundo têm agora leis de proteção de dados. Abaixo, encontra-se um resumo de quais países em todo o mundo têm uma legislação de proteção de dados completa ou de rascunho, com base nesse rastreador.

Regionalmente, há esforços para garantir a proteção de dados nos blocos regionais. Por exemplo, a Comunidade de Desenvolvimento da África Austral (SADC) desenvolveu uma lei modelo que harmoniza as políticas para o mercado de TIC na África Subsaariana, que inclui componentes sobre proteção de dados.

Atualmente tanto a Austrália quanto a Nova Zelândia possuem legislação sobre proteção de dados. Na Austrália, o governo alterou a Lei de Privacidade da Austrália de 1988 para incluir requisitos obrigatórios de notificação de violação que exigirão que as organizações denunciem uma "violação de dados elegível" à autoridade de proteção de dados e notifiquem os clientes afetados imediatamente. Na Nova Zelândia, a Lei de Privacidade do país controla como as "agências" coletam, usam, divulgam, armazenam e dão acesso a "informações pessoais".

Regionalmente, o continente tem a Estrutura de Privacidade da Cooperação Econômica da Ásia-Pacífico (APEC), que visa desenvolver um padrão uniforme de lei de proteção de dados em toda a região. Somente China, Hong Kong, Indonésia, Japão, Coréia, Malásia, Filipinas, Cingapura e Vietnã fazem parte deste bloco regional. O sistema de regras de privacidade transfronteiriça da

APEC (CBPR) foi forjado fora dessa estrutura. Ao contrário do GDPR, o sistema CBPR não desloca nem altera as leis e regulamentos nacionais de um país.

Em toda a América do Norte e América Latina, dezessete países (Canadá, EUA, México, Nicarágua, Jamaica, Trinidad e Tobago, Nicarágua, Costa Rica, Colômbia, Peru, Bolívia, Chile, Argentina, Paraguai, Uruguai, Bahamas, República Dominicana) possuem legislação. Quatro estão elaborando o Equador (Honduras, Panamá, Brasil, Jamaica), enquanto os outros não tinham nenhum ou não tinham dados disponíveis para determinar se um estava em vigor.

Fora da legislação específica do seu próprio país, os EUA e a UE adotaram a Estrutura do Escudo de Privacidade UE-EUA. Esta Estrutura foi concebida pelo Departamento de Comércio dos EUA e pela Comissão Europeia para fornecer às empresas dos dois lados do Atlântico um mecanismo para cumprir os requisitos de proteção de dados da UE ao transferir dados pessoais da União Europeia para os Estados Unidos em apoio ao comércio transatlântico.

Os países latino-americanos também fazem parte da Rede Ibero-Americana de Proteção de Dados (RIPD), composta por 22 autoridades de proteção de dados de Andorra, Argentina, Chile, Colômbia, Costa Rica, México, Peru e Uruguai. Na última década, a organização promoveu o desenvolvimento de uma legislação abrangente de proteção de dados e a introdução de autoridades de proteção de dados em toda a América Latina.

Uma pesquisa de 2016 da Consumers International mostrou que na América Latina as preocupações sobre como os dados dos indivíduos são coletados e os temores sobre a perda de privacidade são relativamente altos em comparação com todas as outras regiões. Setenta por cento (70%) dos entrevistados da América Latina e do Caribe afirmaram que os consumidores raramente entendem e controlam como seus dados são coletados, armazenados e usados.

Este ano, a IBM realizou entrevistas com mais de 2.200 profissionais de TI, profissionais de proteção e conformidade de 477 empresas que experimentaram uma violação de dados nos últimos 12 meses. De acordo com os resultados, as violações de dados continuam a ser mais caras e resultam em mais registros de consumidores perdidos ou roubados, ano após ano.

Princípios de cuidado com a privacidade seguidos mundialmente

Melhores práticas na gestão mundial dos dados pessoais: o que é justo e apropriado em todas as leis e regulamentações no serviço do tratamento dos dados pessoais.

A desintermediação digital está virando de ponta cabeça parcerias e cadeias de fornecimento – nossos parceiros de negócios de longa data podem tornar-se nossos maiores concorrentes, se nossos aliados tradicionais começarem a servir diretamente os clientes.

Por estes motivos que regras intercambiáveis no tratamento de dados estão sendo introduzidas nas organizações neste tempo.

Qual o significado de Proteção de Dados?

Os indivíduos, como consumidores, cidadãos, clientes, funcionários, etc., precisam ter os meios para exercer seu direito à privacidade e proteger a si mesmos e a suas informações pessoais de qualquer tipo de abuso.

A proteção de dados significa salvaguardar e proteger o seu direito fundamental à privacidade, que está consagrado nas leis, códigos e convenções nacionais e internacionais.

A proteção de dados é comumente definida como a lei projetada para proteger seus dados pessoais, que são coletados, gerenciados, processados e armazenados por meios informatizados ou

"automatizados" ou destinados a fazer parte de um sistema de arquivamento manual.

Nas sociedades e economias modernas do século 21, para capacitá-lo a controlar suas informações e protegê-lo de abusos, é essencial que as leis de proteção de dados restrinjam e moldem as atividades de empresas, organizações, empresas e governos. Todas essas instituições têm demonstrado repetidamente que, a menos que regras e leis restrinjam suas ações, elas possivelmente se empenharão em coletar dados pessoais, gerenciá-los, mantê-los etc., sem nos dizer absolutamente nada, em muitos e muitos casos.

O RH é fundamental para proporcionar o aculturamento da lei da Privacidade de Dados Pessoais, o que deu errado (sem citar nome) o que deu certo, informar e atualizar procedimentos.

Como funciona a Proteção de Dados Pessoais?

Onde existe uma lei abrangente de proteção de dados, as organizações, públicas ou privadas, que coletam e usam suas informações pessoais têm a obrigação de lidar com esses dados de acordo com a lei de proteção de dados.

Esta lei é baseada em uma série de princípios gerais que exigem que:

1. Deve haver limites para quais dados pessoais são coletados;
2. As informações pessoais devem ser obtidas por meios lícitos e justos, com o consentimento do indivíduo (titular dos dados);
3. As informações pessoais devem ser corretas, relevantes para os fins para os quais são usadas, precisas, completas e atualizadas, etc.

LGPD

A Lei 13.709/18 estabelece que dado pessoal é toda informação relacionada a pessoa natural "identificada" ou "identificável" e determina que o tratamento desses dados deve considerar os dez princípios de privacidade descritos na lei.

Ao segui-los, as organizações demonstrarão que os dados pessoais coletados são necessários, mínimos, corretos, de qualidade, atendem a uma finalidade de negócio válida, dentre outras características.

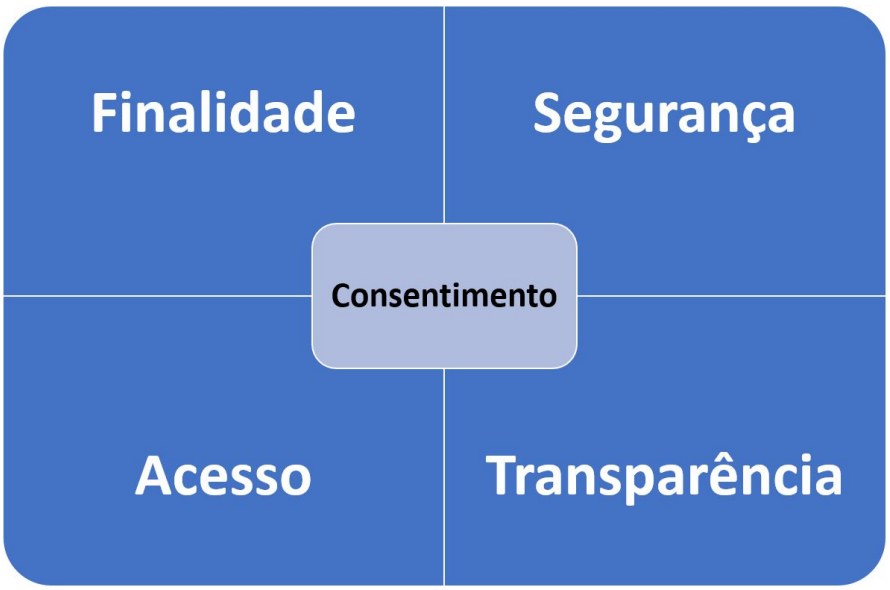
Um dos pilares da transformação digital nas empresas e organizações é a atividade de tratamento dos dados, ou seja, como as empresas produzem, gerenciam e usam a informação.

Até há algum tempo, os dados eram produtos de ações deliberadas a pesquisas de clientes e de inventários físicos, que eram parte dos próprios processos de negócios:

- Fabricação
- Operações
- Vendas
- Marketing

Os dados resultantes eram usados principalmente para previsões, avaliações e tomada de decisões.

Em contrapartida, hoje nos deparamos com um dilúvio de dados. A maioria dos dados que hoje inunda as empresas não é gerada por qualquer planejamento sistemático, como pesquisa de mercado. Em vez disso, é produto da quantidade sem precedentes de conversas, interações ou processos, dentro ou fora das empresas.



O que é Dado Pessoal?

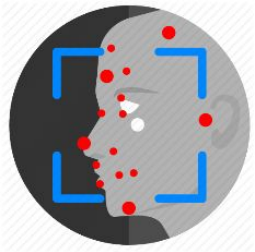
A Lei Geral de Proteção de Dados foi sancionada em agosto de 2018 e é um importante marco normativo brasileiro. Ela foi criada para estabelecer regras mais claras e transparentes ao tratamento de dados pessoais, realizado por pessoa natural ou jurídica, de direito público ou privado, inclusive nos meios digitais.

Mas, afinal, o que é dado pessoal, de acordo com a Lei?

O conceito de dado pessoal é bastante abrangente, sendo definido como a "informação relacionada à pessoa identificada ou identificável". Isso quer dizer que um dado é considerado pessoal quando ele permite a identificação, direta ou indireta, da pessoa natural por trás do dado, como por exemplo: nome, sobrenome, data de nascimento, documentos pessoais (como CPF, RG, CNH, Carteira de Trabalho, Passaporte e Título de Eleitor), endereço residencial ou comercial, telefone, e-mail, cookies e endereço IP.

A Lei traz também a definição de dados pessoais sensíveis, que são aqueles que se referem à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". Por seu maior potencial lesivo, o tratamento desses dados deve observar regras ainda mais rígidas.

Quando temos um dado que não pode identificar, de forma direta ou indireta um indivíduo, temos o que a lei chama de dado



anonimizado.

Por exemplo, quando um instituto de pesquisa vai às ruas e pergunta a religião das pessoas ou em qual candidato elas votarão com o objetivo de identificar um perfil geral, as informações são coletadas de forma anônima ou são anonimizadas posteriormente, a depender do caso.
Essas são as definições que a LGPD traz sobre dados pessoais, e as empresas que, de alguma maneira, lidam com eles, devem estar atentas à forma como estão tratando essas informações, para garantirem que seus processos estão em conformidade com a nova lei.

Em tempos de Big Data, em que os dados, estruturados e não estruturados, vêm das mais variadas fontes e são tratados dentro dos mais diversos sistemas, é essencial que as empresas redobrem a atenção com a segurança e a idoneidade das informações.

Pessoa natural identificável

Conjunto de dados de informações secundárias, onde pode-se identificar uma pessoa natural.

Por exemplo:

- CEP
- Número de telefone
- Triangulação de antenas de celular
- Log de GPS
- Extrato de contas de serviços básicos
- Cookies em web browsers etc.

Tratamento dos dados

O tratamento dos dados envolve várias atividades, que podem estar atuando ligadas ou em separado, dependo do processo e da finalidade da empresa no tratamento de dados pessoais.

Para atender às exigências do LGPD, as empresas, especialmente as que investiram pouco em gestão e segurança de dados nos últimos anos, vão enfrentar uma série de desafios para desenvolver uma estratégia com base nos dados coletados dos usuários e a necessidade de excluí-los quando for a hora.

O primeiro passo para atender essa exigência é ser capaz de identificar e classificar todas as informações de identificação pessoal na rede. Dados da Varonis coletados durante a condução de mais de mil risk assessments para clientes e potenciais clientes em 2017, mostraram que quarenta e sete por cento das empresas têm, no mínimo, mil arquivos sensíveis abertos a todos os funcionários, enquanto vinte e dois por cento das empresas têm mais de 12 mil arquivos nessa mesma situação.

Este cenário, principalmente quando falamos sobre a forma de coletar e gerenciar os dados da internet, estejam estes armazenados em ambientes físicos ou virtuais, deve sofrer mudanças drásticas em pouco tempo. Para isso, vai ser fundamental cuidar das informações de identificação pessoal que estejam armazenadas em ambiente

corporativo, como números de CPF e cartão de crédito, entre outros documentos e dados.

O segundo passo para atender às exigências da LGPD é ter um processo específico para a necessidade de excluir os dados quando não estiverem mais em uso, como a definição de configurações de permissionamento que garantam o armazenamento da menor quantidade possível de informações de identificação pessoal – apenas as que forem realmente necessárias para a empresa – e, ainda assim, com acesso seguro e restrito às pessoas mais indicadas para fazer uso dos dados, eliminando o quanto antes as informações desnecessárias para a prestação de serviços.

Tratamento

Exemplos de Tratamento de Dados:

- Gestão de pessoal e de folhas de pagamentos;
- Acesso/consulta de uma base de dados de contatos que contenha dados pessoais;
- Envio de mensagens de correio eletrônico promocionais;
- Destruição de documentos que contenham dados pessoais;
- Publicação/colocação de uma foto de uma pessoa num sítio web;
- Armazenamento de endereços IP ou endereços MAC;
- Gravação de vídeo (CCTV).

Objetivo da Lei

O objetivo é garantir a privacidade dos dados pessoais das pessoas e permitir um maior controle sobre eles, criando regras claras sobre os processos de coleta, armazenamento e compartilhamento dessas informações, ajudando a promover o desenvolvimento tecnológico na sociedade e a própria defesa do consumidor.

A LGPD e o GDPR garantem o direito à privacidade e a proteção de dados pessoais de indivíduos. Para isso, é preciso existir um controle maior sobre essas informações dos cidadãos, por meio de plataformas transparentes e seguras, apresentando como os dados são coletados, armazenados, tratados e compartilhados. A intenção é garantir os direitos e liberdades fundamentais.

Privacidade refere-se a manter informações confidenciais que sejam pessoalmente identificáveis ou que possam causar danos, constrangimentos ou risco de vida a alguém, se reveladas.

O principal motivo dessas novas regulamentações é manter os dados de usuários e consumidores protegidos, garantindo a segurança de todas as informações armazenadas.

Quando se trata de clientes, garantir que seus dados sejam mantidos com a maior segurança possível, é o mínimo que a maioria deles espera das empresas nas quais investem tempo ou dinheiro.

Os dados que não são mantidos em segurança são muito mais fáceis de acessar por hackers e fontes externas, algo que muitas empresas estão descobrindo devido à proteção de dados que não está à altura ou não está atualizada.

Caso da rede hotéis Mariott:

A violação de dados do Marriott está sendo investigada em vários países, onde a gigante de hotéis e resorts está presente. Na U.E., o Gabinete do Comissário da Informação (ICO) lidera a investigação. É o órgão independente do Reino Unido criado para defender os direitos de informação. As autoridades locais de cada país estão

interessadas em participar como "autoridades de supervisão" no quadro cooperativo do GDPR. De acordo com a OIC, como a investigação está em um estágio inicial, nenhuma atribuição oficial foi feita. Dado que a receita anual global da empresa alcançou US$ 22,89 bilhões em 2017 e a multa mais rígida foi de quatro por cento (no valor de US$ 915 milhões), chegou-se ao montante de US$ 3,5 bilhões, como estimaram inicialmente os analistas alguns dias após o incidente ter sido divulgado. Além disso, é possível que alguns clientes possam tomar medidas legais contra a empresa e reivindicar danos que elevarão ainda mais o custo da violação. Na pior das hipóteses, se for provado que a empresa estava totalmente ciente do ataque dos hackers bem antes de ser revelada, a Comissão de Valores Mobiliários dos Estados Unidos buscará uma ação judicial contra a Marriott, alegando prejuízos sérios para seus investidores.

Com a LGPD, a privacidade para os brasileiros deixa de ser uma noção e passa a ser considerada um direito da sociedade.

Como já sabemos, objetivo da LGPD é fortalecer a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico, além da livre iniciativa, livre concorrência e inovação.

Agentes de tratamento : controlador e o operador – devem pensar em regras e meios técnicos para proteger os dados pessoais e comprovar sua efetividade nas empresas. Seja por criptografia, anonimização dos dados, controle de acesso, procedimentos, políticas de gestão de dados pessoais e treinamentos para equipes que garantam a governança dos dados pessoais e boas práticas.

Estrutura : disposições preliminares, requisitos para tratamento de dados, direitos dos titulares, tratamento de dados pessoais pelo poder público, transferência internacional de dados, agentes de tratamento dos dados (controlador e operador), segurança e boas práticas na proteção dos dados pessoais e fiscalização.

- Manutenção da privacidade no radar de toda corporação.
- Possibilidade de eliminação e retificação.
- Coletar e processar quantidade mínima de dados.

A quem se aplica?

Setores impactados: todos aqueles que tratam de dados, como bancos, corretoras, seguradoras, clínicas médicas, hospitais, varejo, hotéis e companhias aéreas.

Exceções: a lei não se aplica quando o tratamento dos dados é realizado por uma pessoa física para fins exclusivamente particulares/não econômicos, para fins exclusivamente jornalísticos (mantendo a liberdade de imprensa) e artísticos, e para tratamentos realizados para fins de segurança pública e defesa nacional.

Aplica-se ao setor público e privado qualquer tratamento de dados pessoais de pessoas naturais. Por tratamento de dados pessoais entende-se "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".

Transcrevendo a GDPR, a LGPD será aplicável em todos os locais onde existam dados de cidadãos brasileiros.

Independentemente de como será a auditoria, e se ela existirá, o fato é que toda empresa estrangeira que tiver filial no Brasil ou oferecer serviços ao mercado nacional e coletar e tratar dados de cidadãos brasileiros, estará sujeita à lei.

Quais são as referências?

Vários frameworks disponíveis no mercado hoje podem ajudar a adequar a organização para a LGPD.

O Projeto de Lei que resultou na "Lei Carolina Dieckmann" foi diante de situação específica experimentada pela atriz em maio de 2012. Ela teve copiadas de seu computador pessoal 36 fotos em situação íntima, incluindo conversas, que acabaram divulgadas na Internet sem sua autorização.

- ISO 31.000
- GDPR
- 12.737/2012 (Lei Carolina Dieckman)
- Lei nº 4.595/1964, arts. 4º, inciso VIII
- Lei nº 4.728/1965, art. 9º.
- Lei nº 6.099/1974, arts. 7º e 23, "a".
- Lei nº 10.194/2001, art. 1º, inciso II.
- Lei Complementar nº 130/2009, art. 1º
- COBIT

Atenção aos Riscos

Atenção aos Riscos – foco da ISO 31000

ISO 31000 é uma norma da família de gestão de risco criada pela International Organization for Standardization. O objetivo da ISO 31000 é estabelecer princípios e orientações genéricas sobre gestão de riscos. A ISO 31000 estabeleceu um framework universal reconhecido de gestão de processos de tipos específicos de riscos para organizações de qualquer segmento, independentemente do seu tamanho.

Além da segurança digital, os itens incluem danos à reputação ou à marca, risco político e terrorismo. São riscos que organizações privadas e públicas de todos os tipos e tamanhos do mundo devem enfrentar cada vez mais.

A norma fornece diretrizes gerais para gerenciar riscos, em quaisquer atividades, incluindo a tomada de decisão em todos os níveis. Além disso, fornece também uma abordagem comum que pode ser personalizada para cada tipo de organização e seus contextos.

Multas e penalizações

As multas podem variar de 2% do faturamento do ano anterior a R$ 50 milhões, passando por penalidades diárias.

No caso do descumprimento da LGPD, as penalidades incluem advertência formal, obrigatoriedade na divulgação de incidentes, exclusão de dados pessoais, suspensão, proibição parcial ou total das atividades de coleta de informações pessoais. Existe ainda uma multa de até 2% do faturamento da pessoa jurídica, limitada a R$ 50 milhões.

As empresas que violarem os conceitos de privacidade de dados do LGPD ou não forem transparentes em como utilizam essas informações, podem pagar multas de até 2% sobre o volume de negócios global ou 20 milhões de euros.

A maior penalização é com relação a imagem da empresa.

Advertência:

- Multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil limitada, no total, a R$ 50.000.000,00 por infração;
- Multa diária
- Publicização da infração
- Bloqueio de dados pessoais
- Eliminação dos dados pessoais a que se refere a infração

Onde não se aplica?

A nova lei de proteção de dados não é aplicada para casos de Segurança Pública e Defesa Nacional.

As legislações colocam as pessoas no controle sobre seus dados e a tarefa de cumprir esse regulamento recai sobre empresas e organizações. Isso significa que a empresa tem que ser capaz de

provar que o indivíduo concordou com uma determinada ação.

Os negócios que trabalham com dados pessoais devem ter um setor responsável pela proteção de dados para garantir a conformidade com a LGPD.

A LGPD afeta qualquer tipo de serviço que seja oferecido ao cidadão europeu. Dessa forma, se um e-commerce no Brasil vende algum produto em algum país da União Europeia, a empresa precisa se adaptar ao regulamento se quiser fazer negócio com seus clientes estrangeiros.

Como muitos dos serviços online estão disponíveis de forma global, é mais viável alterar toda a plataforma do que segmentar diferentes políticas de acordo com a residência do usuário.

Fica claro que a LGPD não é apenas uma questão de TI. Ela tem implicações abrangentes para toda a empresa, incluindo a forma como lidar com as atividades de marketing por dados e vendas online. Esperamos que este texto tenha reforçado seu conhecimento sobre revolução da internet.

Encarregado de Proteção de Dados (DPO)

Especialista encarregado de administrar todo o fluxo de informações em qualquer empresa, desde sua coleta até seu tratamento. Além disso, servirá como ponte entre uma empresa e a futura Autoridade Nacional de Dados.

Toda empresa responsável por tratamento de dados deverá nomear um Encarregado de Proteção dos dados pessoais.

Segundo a LGPD, este encarregado poderá ser uma pessoa física ou jurídica (no segundo caso, uma empresa especialista na prestação deste serviço). Este profissional deve ter independência de análise e geração de relatórios na organização em que trabalha ou presta serviço.

Dependendo do tamanho da sua organização ou do tipo do negócio, talvez seja necessária (ou não) a contratação de pessoa ou serviço de Encarregado de Proteção de Dados.

Encarregados de Proteção de Dados podem ser recursos dedicados, compartilhados ou até sob demanda, dependo do projeto de sua organização. Mas em todas essas situações, ele deve ocupar uma posição independente de influências estratégicas ou políticas da organização.

O Encarregado de Proteção de Dados será o principal responsável por mostrar as evidências da adequação da Lei perante a Autoridade Nacional de Proteção de Dados.

Esse especialista é um dos responsáveis por avaliar o RIPD (Relatório de Impacto a Proteção de Dados), que toda a organização deverá prover para a ANPD. É recomendado que o Encarregado possua um bom conhecimento técnico e didático das leis de Proteção de Dados nacionais e estrangeiras.

Tarefas e comprometimentos

Avaliação de Processos e Riscos

É o levantamento de quais situações devem ser corrigidas pela empresa para a garantia de que a LGPD seja cumprida em todos os departamentos.

RIPD – Relatório de Impacto a Proteção de Dados

Recomenda-se a geração, análise e correção dos dados do relatório de impacto a proteção de dados de forma recorrente, independentemente do tipo de função da organização.

Antes de realizar o RIPD (Relatório de Impacto a Proteção de Dados), é necessário catalogar todo o tipo de tratamento de dados que a empresa realiza. Feito isso, deve-se verificar quais tratamentos podem ensejar elevado risco aos titulares de dados. A LGPD exige que seja realizada uma análise de impacto específica, para que a

própria empresa busque medidas que minimizem o risco inicialmente diagnosticado. Caso o risco ainda seja alto após a efetivação do RIPD, a Autoridade de Proteção de Dados competente deve ser consultada.

Redução e Exposição a Riscos

É a etapa de implementação das medidas para proteger os dados pessoais na base da empresa (contramedidas). Elas podem ser de segurança, técnicas e administrativas, que evitam, combatem ou minimizam a perda ou indisponibilidade de ativos de informação devido a ameaças que atuam sobre algumas vulnerabilidades.

A redução de risco, ou mitigação de risco, é a implementação de salvaguardas e contramedidas para eliminar vulnerabilidades ou bloquear ameaças. Escolher a contramedida mais econômica ou benéfica faz parte do gerenciamento de risco, mas não é um elemento de avaliação de risco. Na verdade, a seleção de contramedidas é uma avaliação pós-risco ou uma atividade pós-análise de risco. Outra variação potencial da mitigação de risco é a prevenção de risco.

Inúmeras contramedidas podem ajudar a garantir a confidencialidade contra possíveis ameaças. Isso inclui criptografia, preenchimento de tráfego de rede, controle de acesso rigoroso, procedimentos rigorosos de autenticação, classificação de dados e treinamento extensivo de pessoal.

Selecionar uma contramedida ou controle (abreviação de controle de segurança) no âmbito do gerenciamento de risco depende muito dos resultados da análise de custo / benefício. No entanto, você deve considerar vários outros fatores ao avaliar o valor ou a pertinência de um controle de segurança:

- O custo da contramedida deve ser menor que o valor do ativo.
- O custo da contramedida deve ser menor que o benefício da contramedida.
- O resultado da contramedida aplicada deve fazer com que o custo de um ataque seja maior para o perpetrador do que o

benefício derivado de um ataque.

A contramedida deve fornecer uma solução para um risco real sabendo-se que a segurança deve ser projetada para suportar e ativar tarefas e funções de negócios. Assim, contramedidas e salvaguardas precisam ser avaliadas no contexto de uma tarefa de negócios.

Adoção do Privacy by Design

Aborda a proteção desde a concepção do produto ou sistema, sendo incorporada diretamente às estruturas tecnológicas, ao modelo de negócio e à infraestrutura física. Ou seja, a privacidade está presente na própria arquitetura, permitindo que o próprio usuário seja capaz de preservar e gerenciar a coleta e o tratamento de seus dados pessoais.

De acordo com o LGPD, a proteção de dados por design significa que você deve adotar medidas técnicas e organizacionais nas fases iniciais do projeto das operações de processamento. Desse modo, os princípios de privacidade e proteção de dados são protegidos desde o início.

O termo "Privacidade por Design" significa simplesmente "proteção de dados por meio de design de tecnologia".

Por trás disso está o pensamento de que a proteção dos dados nos procedimentos de gestão da informação é melhor adotada quando já está integrada à tecnologia.

A autenticação do usuário e a implementação técnica do direito ao objeto devem ser consideradas. Além disso, com precauções, pode-se usar outros padrões, como os padrões ISO. Em casos individuais, deve-se assegurar que o estado da arte, bem como os custos de implementação razoáveis, seja incluído.

Além dos critérios nomeados, o tipo, o escopo, as circunstâncias e o propósito do processamento devem ser considerados. Isso deve ser contrastado com as várias probabilidades de ocorrência e a gravidade dos riscos associados ao processamento. O texto da lei leva a concluir que, muitas vezes, várias medidas de proteção devem

ser usadas entre si para satisfazer os requisitos estatutários. Na prática, essa consideração já é executada em uma fase inicial de desenvolvimento ao definir decisões sobre tecnologia. A certificação reconhecida pode servir como um indicador para as autoridades de que os responsáveis cumpriram os requisitos legais de "Privacidade por projeto".

Perguntas a serem inseridas em todos os projetos da organização:

- Quais são os requerimentos que nós precisamos cumprir ou seguir?
- Qual será o custo para aplicar este requisito ao nosso produto ou serviço?
- Quando esta regulação precisará estar aplicada?

Procedimentos de política de privacidade

A política de segurança da informação nada mais é que um conjunto de práticas e controles adequados, formada por diretrizes, normas e procedimentos, com objetivo de minimizar os riscos com perdas e violações de qualquer bem. Se aplicada de forma correta ajuda a proteger as informações que são consideradas como um ativo importante dentro da organização.

Entender como os dados são capturados e manipulados pela empresa é fundamental para as próximas etapas e, durante essa análise, também é importante conhecer as práticas adotadas para a guarda desses dados.

Após entender os processos de negócio e como os dados são consumidos, inicia-se a etapa de descoberta e análise das entidades que precisam ter acesso às informações a serem protegidas. Aqui normalmente são encontradas as primeiras dificuldades relativas ao tema proteção de dados, pois geralmente são descobertas entidades com acessos questionáveis ou até indevidos, como também as deficiências em controlar esses acessos.

A ação adequada neste ponto é investir em tecnologia e processos destinados a controlar de forma mais efetiva credenciais que possibilitem o acesso aos repositórios de dados. Sem uma

ferramenta para a gestão das credenciais de acesso bem estruturada e adequadamente implantada, além de processos para a governança destas credenciais bem definidos, corre-se sério risco em permitir acessos indevidos. Isso é Política de Privacidade.

Interfaces

Marco Civil da Internet

O Marco Civil da Internet, oficialmente chamado de Lei N° 12.965/14, é a lei que regula o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado.

O marco civil da internet não garante a privacidade e a proteção de dados de forma abrangente, completa e estruturada. Nem todas as disposições sobre proteção de dados são de natureza protetiva

O marco civil da internet não é uma normativa geral sobre proteção de dados pessoais. Art. 3º a disciplina do uso da internet no brasil tem os seguintes princípios:

ii - proteção da privacidade;
iii - proteção dos dados pessoais, na forma da lei;
art. 7º o acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
i - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
ii - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
iii - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
vii - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
...
ix - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
viii - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
justifiquem sua coleta;
b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

ANPD

Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.

Com a MP 869, a lei está vigente desde 28/12/2018 no que se refere à criação da ANPD e estará vigente a partir de agosto de 2020 em relação aos seus demais aspectos.

Uma das atribuições é fiscalizar, e, se necessário, aplicar multa às empresas que lidam com dados pessoais.

Caberá à autoridade garantir o cumprimento da Lei Geral de Proteção de Dados.

- **Zelar**

- **Implementar**
- **Fiscalizar**

De um ponto de vista prático, as empresas e o poder público ganharam seis meses para se adaptar ao texto legal, e o novo governo, recém-empossado, deverá se movimentar para criar, de fato, a ANPD.

No entanto, o que realmente chama a atenção na MP 869 são as alterações que potencialmente podem expor os titulares de dados pessoais e reduzir a sua proteção. Um exemplo disso está na modificação do artigo 11 da LGPD, que trata das hipóteses legais para tratamento de dados sensíveis.

A MP 869 passou a permitir expressamente o compartilhamento de dados sensíveis quando houver "necessidade de comunicação para a adequada prestação de serviços de saúde suplementar". Essa modificação permitirá que planos e seguros privados de assistência médica tenham acesso a informações referentes à origem racial, étnica, de convicção religiosa, de opinião política, de saúde, genéticos ou biométricos.

Essa exposição, potencialmente, pode permitir a discriminação de usuários, sendo fundamental que haja, ao menos, uma regulamentação que especifique claramente quais informações (e sob que circunstâncias) podem ser compartilhadas.

Também foi modificado o artigo 20 da LGPD, que estabelece o direito do titular dos dados de solicitar a revisão, por uma pessoa natural, de decisões tomadas exclusivamente com base em tratamento automatizado de dados (ou seja, sem interferência humana) que afetem seus interesses (como as decisões referentes a perfis pessoais, profissionais, de consumo e de crédito).

BACEN 4.658

Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem. Esses requisitos deverão ser observados pelas instituições financeiras e

demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Subcontratantes

A LGPD estende-se também aos subcontratantes de uma empresa, como fornecedores e parceiros de tecnologia. Eles também ficam sujeitos às obrigações e podem realizar pagamentos de indenização.

Ferramentas auxiliares

CSIRTs

Grupos de Resposta a Incidentes de Segurança em Computadores.

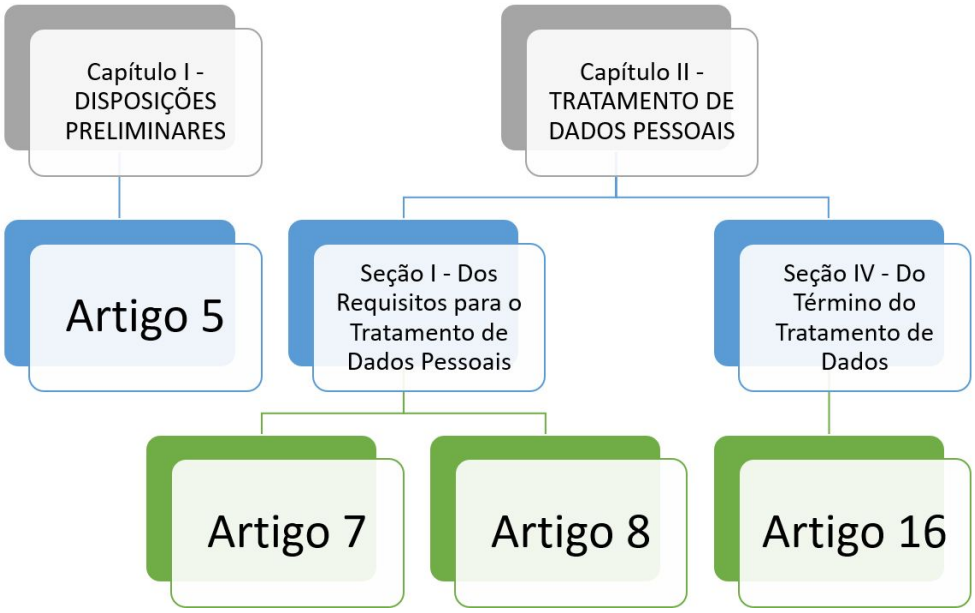
Um "Computer Security Incident Response Team (CSIRT)", ou Grupo de Resposta a Incidentes de Segurança, é uma organização responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores. Um CSIRT normalmente presta serviços para uma comunidade bem definida, que pode ser a entidade que o mantém, como uma empresa, um órgão governamental ou uma organização acadêmica. Um CSIRT também pode prestar serviços a uma comunidade maior, como um país, uma rede de pesquisa ou clientes que pagam por seus serviços.

Um CSIRT pode ser um grupo formal ou um grupo "ad hoc". Um grupo formal tem no trabalho de resposta a incidentes a sua principal função. Um grupo "ad hoc" é reunido quando há um incidente de segurança em andamento ou para responder a um incidente, quando necessário.

Parceiros

Um parceiro especializado pode auxiliar nesse período de transição, possibilitando um maior conhecimento e aplicação de medidas eficientes para o cumprimento da lei.

Artigo 5



I - Dado Pessoal

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

Informação que identifica uma pessoa diretamente ou indiretamente fazendo referência, por exemplo, a nome, número de identidade, endereço IP, um ou mais fatores específicos sobre forma física, psicológica, genética, mental, econômica, cultural ou social. Ou seja, qualquer informação relativa a uma pessoa singular identificada ou identificável (titular de dados). Uma pessoa singular identificável é aquela que pode ser identificada, direta ou indiretamente, por referência a um identificador como um nome, número de identificação, dados de localização, identificador on-line ou a mais fatores específicos da física, fisiologia, identidade genética, mental, econômica, cultural ou social dessa pessoa.

II - Dado Pessoal Sensível

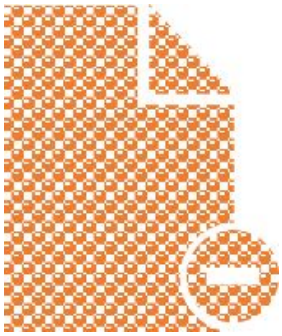
Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Um dado sensível é aquele que não só possui informações que você não gostaria que fossem compartilhadas, como também que pode causar um alto risco de exposição tanto na sua vida social quanto profissional.

No âmbito do LGPD, para que um dado sensível possa ser tratado, o consentimento há de ser livre (dado sem nenhum tipo de pressão ou coação); inequívoco (sem deixar dúvidas de que o titular consentiu com o tratamento); informado (deixando claro o que é tratamento de dados e as implicações do tratamento); expresso (apresentando indicação clara e objetiva de que o titular concorda com o tratamento dos dados e suas implicações); e específico (explicando para o titular o exato propósito do tratamento).

Portanto, empresas farmacêuticas, de diagnósticos e da área de saúde devem ficar particularmente atentas a tais exigências, pois é normal que estas empresas coletem e processem uma colossal quantidade de dados sensíveis.

III – Dado Anonimizado



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

Processo da retirada dos identificadores, mas mantendo a informações explicitamente necessárias para o processamento.

- Neste processo os dados que possam identificar uma pessoa são excluídos ou invalidados.
- *Impossibilidade de reversão.*
- Se forem utilizados para a formação do perfil comportamental de uma determinada pessoa natural, ainda que não identificada. Órgão competente poderá dispor sobre padrões e técnicas utilizadas em processo de anonimização.

Por exemplo:

Numa pesquisa sobre uma localidade, em que o nome das pessoas é anonimizado (tornado anônimo) e é levado em conta somente o fluxo de movimentação dos moradores, para fins de otimização de transporte.

Um processo de remoção de informações pessoalmente identificáveis de um conjunto de dados para tornar impossível ou, pelo menos, mais difícil identificar uma determinada pessoa.

Pseudonimização

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.

IV – Banco de Dados

Segundo o entendimento da LGPD é um conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Bancos de dados ou bases de dados são conjuntos de arquivos relacionados entre si com registros sobre pessoas, lugares ou coisas. São coleções organizadas de dados que se relacionam de forma a criar algum sentido e dá mais eficiência durante uma pesquisa ou estudo.

V – Titular

Segundo a LGPD, Titular é uma pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

VI – Controlador

Segundo a LGPD, Controlador é uma pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

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.

VII – Operador

Segundo a LGPD, Operador caracteriza-se uma pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Esta é uma atividade operacional e prática.

VIII – Encarregado

Segundo a LGPD, Encarregado é uma pessoa indicada pelo controlador para atuar como canal de comunicação entre o

controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;

IX – Agentes de Tratamento

Agentes de tratamento: o controlador e o operador

O controlador de dados determina as finalidades para as quais e os meios pelos quais os dados pessoais são processados. Portanto, numa empresa ou organização a tarefa de decidir "por que" e "como" os dados pessoais devem ser processados, é do controlador de dados. Os funcionários que processam dados pessoais em sua organização, o fazem para cumprir suas tarefas como controlador de dados.

A sua empresa ou organização é um controlador conjunto quando, em conjunto com uma ou mais organizações, determina em conjunto "por que" e "como" os dados pessoais devem ser processados. Os controladores conjuntos devem entrar em um acordo estabelecendo suas respectivas responsabilidades para cumprir as regras da LGPD. Os principais aspectos do acordo devem ser comunicados aos indivíduos cujos dados estão sendo processados.

O operador processa dados pessoais somente em nome do controlador. O processador de dados geralmente é um terceiro externo à empresa. No entanto, no caso de grupos de empresas, uma empresa pode atuar como processador para outra empresa.

Os deveres do Operador em relação ao controlador devem ser especificados em um contrato ou outro ato legal. Por exemplo, o contrato deve indicar o que acontece com os dados pessoais após o término do contrato. Uma atividade típica de operadores é oferecer soluções de TI, incluindo armazenamento em nuvem. O operador de dados só pode subcontratar uma parte de sua tarefa para outro operador ou nomear um outro quando tiver recebido autorização prévia por escrito do controlador de dados.

X – Tratamento

Tratamento

Segundo a LGPD, Tratamento é 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

Segundo a LGPD, a Anonimização é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Anonimização é a transformação de dados para que eles não sejam mais identificáveis como associados a uma determinada pessoa.

Para que a anonimização seja efetiva, a identificação da pessoa associada aos dados não pode ser mais possível, mesmo com a adição de outros conhecimentos sobre os dados anônimos. O problema para controladores de dados e operadores de dados com a maioria dos casos de anonimização perfeita é que os dados também são inúteis para qualquer outra análise. Mesmo assim, no entanto, dados anônimos ainda podem ser úteis para desenvolvimento e teste de casos de uso.

XII – Consentimento

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

O consentimento deve ser dado livremente, específico, informado e não ambíguo. Para obter o consentimento livre, deve ser dado voluntariamente. O elemento "livre" implica uma escolha real pelo titular dos dados. Qualquer elemento de pressão ou influência inadequada que possa afetar o resultado dessa escolha torna o consentimento inválido. Ao fazê-lo, o texto legal leva em consideração um certo desequilíbrio entre o responsável pelo tratamento e o assunto dos dados. Por exemplo, em uma relação empregador-empregado: O funcionário pode se preocupar que sua recusa ao consentimento possa ter consequências negativas graves em sua relação de trabalho, portanto, o consentimento só pode ser uma base legal para o processamento em algumas circunstâncias excepcionais. Além disso, a chamada "proibição de acoplamento" ou "proibição de acoplamento ou amarração" se aplica. Assim, a execução de um contrato não pode depender do consentimento para processar outros dados pessoais, o que não é necessário para a execução desse contrato.

XIII – Bloqueio

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

XIV – Eliminação

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

De acordo com isto, os dados pessoais devem ser imediatamente apagados quando os dados já não são necessários para o seu propósito original de processamento, ou o titular dos dados retirou o seu consentimento e não existe outro motivo legal para processamento, o titular dos dados contestou e não existem motivos legítimos para o processamento.

O controlador está, por um lado, sujeito automaticamente a obrigações de apagamento legais e deve, por outro lado, cumprir o direito de apagamento do sujeito dos dados. A lei não descreve como os dados devem ser apagados em casos individuais. O elemento determinante é que, como resultado, não é mais possível discernir dados pessoais sem esforço desproporcional.

É suficiente se a mídia de dados tiver sido fisicamente destruída ou se os dados forem permanentemente sobrescritos com o uso de softwares específicos.

XV – Transferência Internacional de Dados

Transferência internacional de dados: transferência de dados pessoais para outro país ou organismo internacional do qual o país seja membro;

Fluxos de dados pessoais de e para países fora do Brasil e organizações internacionais são necessários para a expansão do comércio internacional e a cooperação internacional.

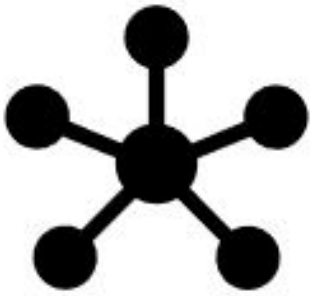
O aumento desses fluxos levantou novos desafios e preocupações com relação à proteção de dados pessoais.

No entanto, quando os dados pessoais são transferidos do Brasil para controladores, operadores ou outros destinatários em países terceiros ou para organizações internacionais; o nível de proteção das pessoas singulares assegurada no Brasil por esta Lei não deve ser comprometido, inclusive nos casos de frente Transferências de dados pessoais do país terceiro ou organização internacional para controladores, operadores no mesmo ou noutro país terceiro ou organização internacional.

Em qualquer caso, as transferências para países terceiros e organizações internacionais só podem ser efetuadas em plena conformidade com o presente regulamento.

Uma transferência só pode ocorrer se, sem prejuízo das outras disposições da LGPD, as condições estabelecidas nas disposições do presente regulamento relativas à transferência de dados pessoais para países terceiros ou organizações internacionais forem cumpridas pelo responsável pelo tratamento ou pelo subcontratante.

XVI – Uso Compartilhado dos Dados



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;

Lembre-se de que essas restrições e condições só se aplicam quando o compartilhamento envolve dados pessoais - ou seja, informações sobre indivíduos vivos identificáveis. Portanto, o compartilhamento de dados completamente anonimizados não está sujeito a nenhuma restrição.

Atividades:

- Identifique outros Controladores com quem você compartilha Dados Pessoais ou é um Controlador de Dados conjunto.
- Identifique os Operadores de Dados.
- Determine onde os contratos com cláusulas apropriadas são necessários para terceiros e inicie.
- Assegure-se de que um contrato ou acordo de compartilhamento de informações esteja em vigor, quando necessário.
- Desenvolver e gerenciar processos locais para garantir a conformidade com a orientação de contratos.
- Configure e implemente um processo para monitorar a conformidade de seus terceiros.

XVII – Relatório de Impacto à Proteção de Dados Pessoais

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.

Basicamente, uma avaliação de impacto de proteção de dados sempre deve ser realizada quando o processamento pode resultar em um alto risco aos direitos e liberdades das pessoas físicas.

A Autoridade Nacional deve estabelecer e publicar uma lista de operações de processamento que sempre exigem uma avaliação de impacto de proteção de dados em sua jurisdição (lista legra). A autoridade também pode publicar uma lista de atividades de processamento que especificamente não exigem uma avaliação de impacto de privacidade (whitelist). Se uma empresa nomeou um Encarregado de Proteção de Dados, seu conselho deve ser levado em consideração ao conduzir um RIPD. Como e por que critérios as consequências e riscos para os titulares de dados são avaliados, permanece em grande parte sem resposta

Exemplos:

RIPD requerido

Um banco exibindo seus clientes em um banco de dados de referência de crédito; um hospital prestes a implementar um novo banco de dados de informações de saúde com dados de saúde dos pacientes; um operador de ônibus prestes a implementar câmeras on-board para monitorar o comportamento dos motoristas e passageiros.

RIPD não é obrigatório

Um médico processando dados pessoais de seus pacientes. Nesse caso, não há necessidade de um DPIA, pois o processamento pelos médicos não é feito em grande escala nos casos em que o número de pacientes é limitado.

XVIII – Órgão de pesquisa

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

Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei. O governo anunciou no dia 28 de dezembro de 2018 a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por acompanhar e aplicar sanções descritas na Lei Geral de Proteção de Dados (LGPD), sancionada em agosto deste ano.

A criação foi feita por medida provisória (MP 869/18) assinada pelo presidente Michel Temer nesta semana. A ANPD era para ter sido aprovada em agosto, junto com o texto da Lei Geral de Proteção de Dados. Contudo, o presidente vetou o texto sob o argumento de "vício de iniciativa". Isso porque o órgão estaria vinculado ao Ministério da Justiça.

O texto aprovado na última semana prevê que a ANPD vai ter autonomia técnica, mas será vinculada à Presidência da República. Assim, será composta por um conselho-diretor formado por cinco diretores, que serão nomeados pelo presidente, e os membros do conselho terão mandatos de quatro anos.

De acordo com o texto assinado por Temer, entre as atribuições da Autoridade Nacional de Proteção de Dados (ANPD) estão:

- Zelar pela proteção de dados pessoais;
- Editar normas e procedimentos sobre o tema;
- Aplicar sanções em caso de descumprimento de regras.

Artigo 6

II – Adequação

Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento. Caso seja necessária alguma inclusão de metadados, redução de dados coletados ou anonimização que possam facilitar o processamento, de acordo com a finalidade concedida.

Adequação no formato para transferência internacional dos dados.

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.

Dados coletados para fins específicos, explícitos e legítimos e não processadas posteriormente de maneira incompatível com esses objetivos, adequados, relevantes e limitados ao necessário em relação aos fins para os quais são tratados (minimização de dados);

preciso e, quando necessário, atualizado; todas as medidas razoáveis devem ser tomadas para garantir que os dados pessoais que são imprecisos, tendo em conta as finalidades para as quais são processados, sejam apagados ou retificados sem demora ("precisão");

O excesso de informação, além de ser prejudicial para o trabalho de tratamento de dados, aumenta o risco da revelação não autorizada.

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.

Em suma, o direito de acesso significa que os controladores de dados devem fornecer uma cópia dos dados pessoais processados mediante solicitação.

V – Qualidade dos Dados

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;

Os dados têm um tremendo impacto na trajetória de uma organização no que se refere à previsão de comportamentos e padrões de compra do cliente, auxiliando com o gerenciamento eficaz do produto, fornecendo informações competitivas às organizações e muito mais.

No entanto, se os seus dados não forem precisos, completos e consistentes, podem levar a grandes erros ao tomar decisões de negócios.

O Instituto de pesquisas empresariais Gartner estima que o impacto financeiro médio da má qualidade dos dados nas empresas é de US $ 15 milhões por ano, o que significa que você não pode deixar de dar prioridade à gestão da qualidade de dados, especialmente agora que os padrões da LGPD estão prestes a serem implementados.

Com a LGPD, a maneira pela qual as organizações podem usar seus dados agora vem com restrições. Para garantir a conformidade, o gerenciamento da qualidade de dados deve ser implementado nas organizações para operar corretamente e usar os dados de acordo com as regulamentações.

Aqui estão alguns fatores que causam dados incorretos:

- Silos de informação - No mundo do bigdata, as informações vêm de várias fontes e sistemas.
- Diversas tecnologias - Dada a variedade de tecnologias que as empresas utilizam, os dados são apresentados em diversos formatos.
- Dados inconsistentes - Como os dados são provenientes de várias fontes, pode haver discrepâncias neles. Por exemplo, os sistemas de marketing e vendas podem ter registros diferentes do número de celular de um cliente.

Antes que a conformidade com a LGPD possa ser alcançada, os dados precisam ser catalogados para registrar quais dados são armazenados, onde e por quê; seja estruturado ou não estruturado e se é armazenado digitalmente ou em formato analógico. Este é mais um exercício consultivo do que um processo de TI.

A minimização de dados é fundamental para muitos dos requisitos da LGPD, portanto, é necessário tomar decisões sobre quais dados pessoais são necessários, sob quais bases estão sendo coletadas e o que pode ser excluído. Ao mesmo tempo, a qualidade dos dados restantes precisará ser melhorada: as duplicatas devem ser encontradas e resolvidas, e os dados conflitantes devem ser validados em relação a fontes confiáveis para garantir a precisão.

Essa fase requer um sistema que permita que os dados sejam consultados e subsequentemente entregues, excluídos, corrigidos ou portados quando solicitados. O truque aqui é acessar esses dados em tempo real quando necessário.

Estabelecer o modelo de governança certo desde o início é absolutamente crítico. Deve haver um corpo interno, não apenas com autoridade para orquestrar as fases acima, mas também com a missão de mudar os processos e supervisionar sua implementação. Parte desse processo pode ser designar o encarregado de proteção de dados, conforme descrito na própria LGPD.

O controlador precisa ter mecanismos que assegurem a qualidade dos dados para o correto tratamento.

VI – Transparência

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.

Uma das formas de garantir a transparência no tratamento dos dados é a implementação de serviços de Atendimento ao Cliente, Ouvidoria e planos de Auditorias Externas.

Princípios da transparência:

1. O princípio da transparência exige que qualquer informação dirigida ao público ou à pessoa em causa seja concisa, facilmente acessível e fácil de entender, e que seja utilizada uma linguagem clara e simples e, adicionalmente, quando apropriado, a visualização.
2. Tais informações podem ser fornecidas em formato eletrônico, por exemplo, quando endereçadas ao público, por meio de um site.
3. Isso é particularmente relevante em situações em que a proliferação de atores e a complexidade tecnológica da prática dificultam que o titular de dados conheça e compreenda se, por quem e com que finalidade os dados pessoais relativos a ele ou ela está sendo coletada, como no caso da publicidade online.
4. Dado que as crianças merecem proteção específica, qualquer informação e comunicação, onde o processamento é dirigido a uma criança, deve estar em uma linguagem tão clara e clara que a criança possa compreender facilmente.

VII – Segurança

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;

Segundo as melhores práticas a segurança baseia-se na tríade Confidencialidade, Integridade e Disponibilidade.

Confidencialidade é sobre privacidade e garantir que a informação seja acessível somente para aqueles com uma necessidade comprovada de vê-la. Seria inaceitável para um estranho ser capaz de acessar informações confidenciais de um laptop simplesmente levantando a tampa e ligando-a. É por isso que um laptop deve ser protegido por senha e os dados nele criptografados quando desligados.

A integridade refere-se às informações armazenadas em um banco de dados que são consistentes e não modificadas. Os sistemas devem ser projetados de forma que a entrada e o gerenciamento de informações não sejam propensos a erros humanos e que o fluxo de informações não resulte em perda ou alteração

A disponibilidade diz respeito a informações que estão presentes quando são necessárias para dar suporte aos cuidados. O projeto do sistema deve incluir controles e verificações de acesso apropriados para que as informações no sistema tenham consistência e precisão, sejam confiáveis e corretas e possam ser confiáveis ao fornecer assistência ou saúde.

VIII – Prevenção

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Impedir o manuseio inadequado dos dados com foco em:

- Armazenamento
- Transmissão
- Processamento de informação

A proteção de confidencialidade fornece um meio para usuários autorizados acessarem e interagirem com recursos, mas previne que usuários não autorizados façam isso.

Os sistemas de comunicação são vulneráveis a ataques da mesma maneira que qualquer outro aspecto da infraestrutura de TI é vulnerável. Entender as ameaças e possíveis contramedidas é uma parte importante da proteção de um ambiente. Qualquer atividade ou condição que possa causar danos a dados, recursos ou pessoal deve ser

abordada e mitigada, se possível. Tenha em mente que o dano inclui mais do que apenas destruição ou dano; também inclui divulgação, atraso no acesso, negação de acesso, fraude, desperdício de recursos, abuso de recursos e perdas. Ameaças comuns contra a segurança do sistema de comunicação incluem negação de serviço, espionagem, representação, reprodução e modificação.

IX – Não Discriminação

Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

Alusão ao artigo 5 da Constituição Federal, que garante o direito de que todos são iguais pela lei.

As novas salvaguardas da lei são particularmente importantes para os direitos humanos na era digital. Escândalos recentes envolvendo o Facebook com a Cambridge Analytica e a preocupação pública com violações de dados digitais, publicidade direcionada e perfil do setor privado levaram a pedidos por maiores controles sobre como os dados pessoais são coletados e usados.

Na era digital, tudo o que uma pessoa faz online gera ou implica dados que podem ser altamente reveladores sobre sua vida privada. A LGPD fornece novas maneiras pelas quais as pessoas podem proteger seus dados pessoais e, por extensão, sua privacidade e outros direitos humanos. Ele oferece a todos mais controle e exige que empresas, governos e outras organizações divulguem mais sobre suas práticas de dados e regulam a maneira como coletam, processam e armazenam dados das pessoas.

Proteções especiais se aplicam a informações confidenciais. O processamento de determinadas categorias especiais de dados sensíveis é rigorosamente regulamentado. Estes incluem informações revelando a origem racial ou étnica de alguém, opiniões políticas, crenças religiosas ou filosóficas, ou filiação sindical, bem como dados sobre genética, saúde e biometria (por exemplo, impressões digitais, reconhecimento facial e outras medidas corporais)

Depois que os dados são coletados, as empresas precisam ser mais transparentes sobre como elas são compartilhadas com outras pessoas. Em teoria, isso significa que os usuários podem aprender mais sobre como as empresas abordam as parcerias de criação de perfil e de segmentação de anúncios on-line, especialmente aquelas que oferecem serviços de análise da Web, publicidade ou mídia social.

Sistemas que incorporam decisões algorítmicas ou outras formas de criação de perfil podem levar à discriminação baseada em raça, sexo, religião, nacionalidade ou outro status. Mesmo se os indivíduos consentirem, eles ainda têm o direito de analisar os resultados significativos de sistemas automatizados de tomada de decisão. À medida que governos e empresas usam algoritmos para tomar decisões importantes sobre a vida das pessoas, como se uma pessoa recebe benefícios públicos, seguro de saúde, crédito ou emprego, essas proteções prometem um grau de transparência e responsabilidade e protegem contra a discriminação que afeta a pessoa. direitos humanos.

X – Responsabilização e Prestação de Contas

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.

- *Não repúdio.*

O não-repúdio garante que o assunto de uma atividade ou quem causou um evento não pode negar que o evento ocorreu. O não-repúdio impede que um sujeito afirme não ter enviado uma mensagem, não ter executado uma ação ou não ter sido a causa de um evento.

Isso é possível por meio de identificação, autenticação, autorização, responsabilidade e auditoria. O não-repúdio pode ser estabelecido usando certificados digitais, identificadores de sessão, logs de transação e vários outros mecanismos de controle de acesso e transações.

Um sistema construído sem a aplicação adequada de não-repúdio não fornece verificação de que uma entidade realizou uma determinada ação. O não-repúdio é uma parte essencial da responsabilidade. Um suspeito não pode ser responsabilizado se puder repudiar a reclamação contra ele.

Artigos 7 e 8

Consentimento

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

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.

O titular dos dados deve pelo menos ser notificado sobre a identidade do controlador, que tipo de dados será processado, como será usado e a finalidade das operações de processamento como uma proteção contra a "fluência de função". O titular dos dados também deve ser informado sobre o seu direito de retirar o consentimento a qualquer momento. A retirada deve ser tão fácil quanto dar consentimento. Quando relevante, o controlador também deve informar sobre o uso dos dados para tomada de decisões automatizada, os possíveis riscos de transferência de dados devido à ausência de uma decisão de adequação ou outras salvaguardas apropriadas.

O consentimento deve estar vinculado a um ou vários propósitos especificados, que devem ser suficientemente explicados. Se o consentimento deve legitimar o processamento de categorias especiais de dados pessoais, as informações para o titular dos dados devem referir-se expressamente a isso.

Deve sempre haver uma clara distinção entre as informações necessárias para o consentimento informado e as informações sobre outros assuntos contratuais.

Por último, mas não menos importante, o consentimento deve ser inequívoco , o que significa que requer uma declaração ou um claro ato afirmativo. O consentimento não pode ser implícito e deve ser sempre dado por meio de um opt-in, uma declaração ou uma moção ativa, para que não haja mal-entendido que o titular dos dados tenha consentido com o processamento específico. Dito isto, não há exigência de formulário para consentimento, mesmo que seja recomendado o consentimento por escrito devido à responsabilidade do responsável pelo tratamento. Pode, portanto, também ser dado em formato eletrônico. Nesse sentido, o consentimento de crianças e adolescentes em relação aos serviços da sociedade da informação é um caso especial.

Como se pode ver, o consentimento não é uma bala de prata quando se trata do processamento de dados pessoais. Especialmente considerando que lei de proteção de dados deixaram claro que “se

um controlador escolhe confiar no consentimento para qualquer parte do processamento, ele deve estar preparado para respeitar essa escolha e interromper essa parte do processamento se um indivíduo retirar o consentimento. "Estritamente interpretado, isso significa que o controlador não está autorizado a mudar do consentimento da base legal para o interesse legítimo, uma vez que o titular dos dados retira o seu consentimento. Isso se aplica mesmo que um interesse legítimo válido existisse inicialmente. Portanto, o consentimento deve ser sempre escolhido como última opção para o processamento de dados pessoais.

O consentimento deve ser fornecido se você acredita que seu processamento é legal e caso necessário o controlador pode comprovar o uso.

O texto da solicitação do consentimento deverá ser claro em sua finalidade, tipo de tratamento e data de expiração. Deve ser uma forma inteligível e de fácil acesso em linguagem clara e clara.

Caso contrário, o consentimento não conta e seu processamento pode ser considerado ilegal:

- O titular precisa conceder
- O controlador precisa provar que possui
- Precisa ser de claro e fácil entendimento
- Uma vez concedido, precisar ter a informação da duração do tempo do tratamento

Marco Civil da Internet, art 7º

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

IX - Consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais

Lei 13.709/2018 Art. 5º

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

Interesse legítimo

Um controlador determina os propósitos e meios de processar dados pessoais. Um processador é responsável pelo processamento de dados pessoais em nome de um controlador. Se você é um processador, a LGPD coloca obrigações legais específicas em você; por exemplo, você é obrigado a manter registros de dados pessoais e atividades de processamento.

Você terá responsabilidade legal em caso de ato ou incidente de violação. No entanto, se você for um controlador, não ficará desobrigado de suas falhas onde um processador está envolvido – a LGPD coloca mais obrigações para garantir que seus contratos com operadores estejam em conformidade com a lei.

Artigo 16

Eliminação dos Dados

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:

- A destruição pode ser designada por um período de retenção aplicado a uma data de criação de dados ou registros.
- Uma solicitação de um titular ou a conclusão de uma destruição de transação pode resultar na exclusão de arquivos de

Os registros de um banco de dados ou a remoção de dados de um arquivo, deve ser aplicada ao plano de gerenciamento de registros de uma organização para garantir remoção apropriada de dados.

Simplesmente declarar que os dados devem ser destruídos nem sempre é suficiente. Deve haver diretrizes claras sobre como destruir os dados com base em seu tipo.

Vamos debater sobre conteúdo digital:

- A destruição da maioria dos conteúdos digitais é simplesmente uma questão de excluir os dados ou os arquivos que contêm os dados.
- É preciso ter cuidado ao excluir dados de uma mídia off-site manipuladas por terceiros.
- Nas tecnologias atuais, a exclusão é feita removendo-se somente os cabeçalhos usando comandos padrão do sistema operacional para excluir arquivos, normalmente exclui apenas as informações de cabeçalho e deixa o conteúdo dos arquivos intactos.

Formatar a mídia inteira é a melhor maneira de garantir que os dados sejam removidos do disco. A formatação adequada é importante porque o uso da formatação padrão limpará somente os cabeçalhos de cada arquivo e, mais uma vez, deixará os dados intactos no disco.

O gerenciamento de direitos digitais ou DRM é outro método de remover o acesso a conteúdo digital por meio de meios programáticos, definindo um período de expiração no conteúdo.

Quando um dispositivo não está conectado à rede da organização, a execução de rotinas de exclusão em relação à hora de dados, ao realizar uma exclusão manual, é impossível.

O treinamento e os lembretes adequados são a melhor maneira de manter os funcionários cientes da necessidade de excluir dados expirados de copiadoras e máquinas de fax de impressoras de mídia portáteis.

Muitas impressoras copiadoras e aparelhos de fax contêm discos mecânicos ou sólidos que são usados para armazenar uma cópia do material impresso que é apresentado a eles. Isso pode ser uma fonte de risco quando as máquinas são devolvidas após o período de locação ou descartadas antes que as máquinas sejam removidas.

Os dispositivos de armazenamento devem ter as informações a serem eliminadas destruídas. Alguns fabricantes desses dispositivos automaticamente limpam os discos rígidos após o uso.

Destruir documentos em papel em uma organização é uma tarefa extremamente difícil. Não por causa do processo, mas por causa da dificuldade em determinar quais documentos precisam ser destruídos. Os documentos em papel raramente têm uma data de exclusão, pois normalmente são impressões de arquivos que não possuem datas de exclusão incorporadas.

Muitos documentos recebem uma classificação de dados que pode ajudar a determinar uma data de destruição. Desde que os funcionários sejam devidamente treinados sobre o significado da classificação de dados e como eles aplicam as políticas de retenção, é uma boa prática colocar uma data de destruição no papel.

Se o papel foi impresso de um arquivo que não tem uma data de destruição, o documento deve ser destruído quando não for mais necessário e usado a cópia digital para necessidades futuras.

Para muitas empresas, pode ser mais eficiente contratar uma empresa de destruição de pessoas para destruir documentos vencidos.

O desenvolvimento e a execução de um programa de ciclo de vida informativo ajudam as organizações a garantir que estão coletando os dados certos, fornecendo transparência adequada para a coleta processando-a adequadamente e destruindo os dados, uma vez que não há mais necessidade de negócios para isso.

Ter um programa de ciclo de vida informativo em vigor é importante para minimizar o risco para as organizações e os titulares de dados aos quais os dados pertencem.

Princípios

1. Legalidade, justiça e transparência - mantenha-a legal e justo; diga o que você vai fazer com os dados em termos claros

2. Limitação de finalidade - não faça mais com os dados do que você disse que faria

3. Minimização de dados - não colete mais dados do que o necessário

4. Precisão - mantenha dos dados atualizados e lide com imprecisões o mais rápido possível

5. Limitação de armazenamento - não mantenha os dados por mais tempo do que o necessário

6. Integridade e confidencialidade - mantenha os dados seguros enquanto você os possui

7. Responsabilidade - mostre que você está cumprindo os princípios acima

Legalidade

Para que o processamento de dados pessoais seja legal, ele deve atender aos critérios da lei e estabelecer claramente qual dos discernimentos se aplica a qualquer situação.

Em essência, os critérios a serem escolhidos em relação à legalidade do processamento são os seguintes:

1. O titular dos dados consentiu

2. É necessário estabelecer um contrato entre sua organização e os dados a serem tratados

3. Você legalmente tem que fazer isso

4. Você está protegendo os interesses vitais do titular dos dados

5. Deve ser do interesse público

6. É para seus interesses legítimos - desde que não afete os direitos e liberdades do sujeito

Portanto, embora o consentimento seja um aspecto importante do LGPD, não é a única maneira de que coletar e processar dados pessoais pode ser legal. De fato, você pode encontrar que uma proporção significativa dos dados pessoais que sua organização possui e processos não requerem consentimento; em vez disso, é necessário para fins legais, como suporte aos clientes (contratuais), ou lidar com a autoridade tributária (legal). O processo de obter e manter o consentimento pode envolver alterações nos processos de negócios de sistemas.

Consentimento

Se você acredita que seu processamento é legal porque possui o consentimento do titular dos dados, você deve poder comprová-lo. Você não pode ocultar o termo de consentimento entre outras divagações contratuais e pode fugir disso.

Uma vez dado, o consentimento pode ser retirado a qualquer momento pelo titular dos dados, e isso deve ser tão fácil quanto antes.

Direitos do titular dos dados

A LGPD estabelece um conjunto de direitos que o titular dos dados pode exercer e ao qual o controlador que possui seus dados pessoais deve reagir e responder, geralmente em um mês.

- O direito de ser informado. O ser informado de quais dados serão coletados, porque, por quem, para que finalidade e para onde os dados irão.
- O direito de acesso. A garantia de ver dados pessoais mantidos.
- O direito à retificação. A garantia da correção dos dados se estiverem errados ou imprecisos.
- O direito de remoção. A garantia de remover dados pessoais quando não forem mais necessários
- O direito de restringir o processamento. A garantia de interromper o processamento dos dados, se houver motivos para fazê-lo

- O direito à portabilidade de dados. A garantia de obter os dados de forma transportável e movê-los para um processador alternativo
- O direito de impedimento. A garantia de impedir que os dados sejam processados.

Esses direitos seguem os princípios que discutimos anteriormente e visam garantir que os dados pessoais sejam processados de forma justa e transparente e que o titular dos dados possa fazer algo a respeito se isso não acontecer.

Oficial de proteção de dados

Dependendo da sua organização e do que ela faz com os dados pessoais, você pode ou não precisar de um responsável pela proteção de dados.

Você terá que designar um se:

- Você é uma autoridade ou órgão público
- Você monitora os titulares dos dados em larga escala
- Grandes volumes de dados de categorias especiais estão envolvidos

Os responsáveis pela proteção de dados podem ser de meio período, podem ser compartilhados entre organizações e podem ser recursos ou serviços externos. Eles devem permanecer independentes e seus detalhes de contato devem estar disponíveis gratuitamente, especialmente para os titulares dos dados.

O responsável pela proteção de dados é o principal contato com a autoridade supervisora e provavelmente se envolverá quando os principais problemas de privacidade e proteção de dados forem abordados na organização, como durante as avaliações de impacto na proteção de dados.

O responsável pela proteção de dados precisará ter pleno conhecimento da lei de proteção de dados para cumprir a função.

Avaliações de impacto na proteção de dados

Para estabelecer uma cultura em que a privacidade dos dados seja incorporada a novos processos e sistemas, em vez de acrescentada como uma reflexão tardia, a LGPD exige que sejam realizadas avaliações de impacto na proteção de dados onde os riscos envolvidos para os titulares de dados sejam razoavelmente sentidos estar alto. Esse processo envolve a compreensão dos dados pessoais envolvidos e a abordagem de riscos prováveis através do uso de controles apropriados, para que a proatividade, e não a reatividade, esteja na ordem do dia.

Transferências internacionais

O envio de dados pessoais de cidadãos brasileiros levanta questões sobre a proteção dos dados e impõe restrições sobre como isso pode ser feito. Para ser útil, a ANPD decidirá regularmente em quais países teremos relação de confiança para cuidar dos dados pessoais dos brasileiros e publicará uma lista daqueles considerados aceitáveis. Outras maneiras de obter aprovação são:

- Um acordo juridicamente vinculativo (apenas organismos públicos).
- Regras corporativas vinculativas.
- Usando cláusulas padrão em seu contrato.
- Assinatura de um código de conduta ou esquema de certificação aprovado.

7 passos para estar de acordo com a LGPD

1. Compromisso de gerenciamento da segurança

Antes de iniciar um projeto para alcançar a conformidade com a LGPD, é muito importante garantir o compromisso da alta gerência. Esse é provavelmente o fator mais significativo neste projeto.

2. Definir funções e responsabilidades

É importante estabelecer desde o início quem fará o que, tanto no seu projeto inicial para cumprir a LGPD, quanto para a proteção a longo prazo dos dados pessoais que você possui. O documento Responsabilidades e Autoridades de Funções da LGPD define várias funções, incluindo um grupo diretor de segurança da informação para supervisionar a maneira como a proteção de dados é controlada, um gerente de segurança da informação e, mais importante, a informação dos proprietários com o maior envolvimento diário com os dados em questão. Se ainda não estiver alocado, é necessário tomar decisões sobre quem cumprirá essas funções, incluindo o potencial recrutamento.

A única função que é explicitamente mandatada na LGPD é a do DPO (Encarregado ou Data Protection Officer). Como mencionamos, você pode ou não precisar nomear um deles. Se você é um órgão público, não há decisão a ser tomada; caso contrário, pode ser necessário obter visualizações de diferentes perspectivas da empresa sobre se você manipula dados pessoais em uma escala que pode ser considerada grande.

Se você precisar de um DPO, precisará decidir se deve nomear internamente, compartilhar um recurso com uma ou mais organizações similares ou contratar um serviço de terceiros.

3. Comunicação, conscientização e treinamento

Depois de iniciar seu projeto e definir quem desempenhará qual papel, há muito valor em aumentar a conscientização geral sobre a LGPD e a segurança da informação em geral, para que as pessoas saibam o que é e por que é importante.

O público-alvo incluirá várias partes interessadas, como fornecedores e contratados, além de funcionários, e é útil criar um programa gerenciado de comunicação para que isso aconteça regularmente.

Você também precisa identificar as necessidades de treinamento das pessoas que estão assumindo as várias funções envolvidas na obtenção da conformidade de forma contínua. Isso pode ser feito definindo quais competências são necessárias e, em seguida, conduzindo um exercício de comparação por questionário para encontrar as lacunas; estes podem ser preenchidos através de uma combinação de treinamento formal e informal, incluindo cursos, seminários on-line, seminários, livros e, é claro, a leitura do próprio regulamento. Normalmente, é necessário treinamento em áreas como mapeamento de dados, impacto na proteção de dados, avaliações e gerenciamento de incidentes.

Documentos / modelos necessários:

- Programa de Comunicação LGPD.
- Apresentação do LGPD.
- Procedimento de Desenvolvimento de Competências LGPD.
- Questionário de desenvolvimento de competências do LGPD.
- Treinamento de conscientização sobre segurança da informação.
- Atas de Reunião.

4. Inventário de dados pessoais

Quando o seu time estiver pronto, a próxima etapa é fazer uma análise da maneira como os dados pessoais são coletados, armazenados, processados, transferidos e descartados na sua organização. Existem muitas maneiras de representar isso, mas a maioria se resume a desenhar diagramas do fluxo e registrar as informações relevantes em uma planilha.

Você precisará envolver as pessoas responsáveis por coletar e processar os dados diariamente para garantir que seja obtida uma

imagem o mais completa possível. Você pode fazer isso organizando oficinas e usando quadros brancos e notas autoadesivas, ou pode enviar uma planilha para eles e pedir que eles a concluam, ou você pode fazer as duas coisas; o que se encaixa na cultura da sua organização.

O importante aqui é entender os principais fatos, como os itens de dados que estão sendo coletados, para qual finalidade, por qual método (por exemplo, no site, pessoalmente, em papel), onde, como e por quanto tempo os dados são coletados, armazenados e para onde são enviados. Isso ajudará a identificar quaisquer controles adicionais que precisam ser aplicados a ele (como criptografia, por exemplo) e a estabelecer a base legal sob a qual podem ser coletados e processados (por exemplo, consentimento contratual).

A abordagem geral que você decide adotar em relação à retenção de dados pode ser refletida na Política de Retenção e Proteção de Registros.

5. Avaliações de impacto na proteção de dados

Esta é uma área relativamente nova para muitas organizações, mas claramente definida pela LGPD. Novos projetos e mudanças significativas nos processos existentes precisarão considerar cuidadosamente o impacto nos dados pessoais como parte de sua avaliação e planejamento, com controles apropriados, com base em uma avaliação justa dos riscos. Se você tiver um processo de projetos, será necessário avaliá-lo com relação a Lei; a LGPD declara que isso é necessário apenas onde houver um risco alto, mas você pode achar que é uma boa ideia realizar essas avaliações como uma questão de curso para cada projeto.

Documentos / modelos necessários ter:

- Processo de avaliação de impacto na proteção de dados
- Questionário de Avaliação de Impacto na Proteção de Dados

- Pasta de trabalho de avaliação de impacto na proteção de dados
- Relatório de Avaliação de Impacto na Proteção de Dados
- Procedimento de avaliação da LGPD do fornecedor
- Formulário de Avaliação da LGPD do Fornecedor

6. Preparar para violações de dados pessoais

Atualmente, o consenso no setor de segurança da informação não é se uma organização sofrerá uma violação de segurança, mas quando; e isso já pode ter acontecido, mas você simplesmente não sabe. Portanto, ter um GUIA DE IMPLEMENTAÇÃO da LGPD e um procedimento de gerenciamento de incidentes é obrigatório. A LGPD exige em que sua autoridade supervisora seja informada sobre violações conhecidas que representam um alto risco para os titulares de dados e é específica sobre os prazos e as informações que devem ser fornecidas.

Documentos:

- Procedimento de resposta a incidentes de segurança da informação
- Procedimento de notificação de violação de dados pessoais
- Formulário de notificação de violação de dados pessoais
- Registro de Violação de Dados Pessoais

7. Analisar transferências internacionais

Além de proteger os dados pessoais em sua própria organização, você também precisa pensar para onde mais os envia e como estão protegidos lá. Esta é uma área envolvida e pode ser um assunto longo e prolongado ou simples e oportuno, dependendo de como os requisitos da LGPD sejam compreendidos. O primeiro passo é saber quais dados você envia para onde e por quê. Você tem várias opções disponíveis para aplicar à transferência, dependendo de fatores

como o destino, tipo de dados e finalidade. Transferências internacionais de dados pessoais para ajudá-lo a escolher seu caminho e entender o que precisa ser feito.

Anexos

O que é DLP (data leak prevention)?

Qualquer vazamento de dados causa impacto negativo nas empresas. As abordagens tradicionais de segurança, como firewalls, não podem proteger os dados contra vazamentos. Os sistemas de prevenção de vazamento / perda de dados (DLP) são soluções que protegem os dados confidenciais de estar em mãos não confiáveis.

Dados sensíveis e confidenciais são um requisito para a maioria das empresas, portanto, a proteção desses dados é muito solicitada pelos principais gerentes, administradores e gerentes de TI da empresa. As abordagens tradicionais de segurança, como firewalls, não podem proteger os dados contra vazamentos. Os sistemas de prevenção de vazamento / perda de dados (DLP) são soluções que protegem os dados confidenciais de estar em mãos não confiáveis.

A prevenção de vazamento de dados (DLP, data leak prevention) é um conjunto de tecnologias voltadas para a perda de informações confidenciais que ocorrem em empresas em todo o mundo. Concentrando-se na localização, classificação e monitoramento de informações em repouso, em uso e em movimento, essa solução pode ajudar muito uma empresa a identificar as informações que possui e impedir os inúmeros vazamentos de informações que ocorrem a cada dia. O DLP não é uma solução plug-and-play. A implementação bem-sucedida desta tecnologia requer preparação significativa e manutenção contínua diligente. As empresas que buscam integrar e implementar o DLP devem estar preparadas para um esforço significativo que, se feito corretamente, pode reduzir

significativamente o risco para a organização. Aqueles que implementam a solução devem adotar uma abordagem estratégica que aborde riscos, impactos e medidas de mitigação, juntamente com medidas apropriadas de governança e garantia.

CPF não se vende em farmácia!

Como podemos hoje em plena vigência da LGPD permitirmos o engano do desconto baseado na troca dos nossos dados pessoais?

Se os nossos dados não tivessem valor, não existiria uma lei específica para protegê-los, logo nossa sociedade precisa se conscientizar disso, pois de nada adianta um Lei para proteger uma sociedade conivente com a transgressão da coleta dos dados sem a informação da finalidade e o devido consentimento.

Nossos dados pessoais valem muito. Várias empresas estão logrando êxito em seus negócios trabalhando com os dados pessoais e infelizmente outras não estão tendo o zelo correto no tratamento permitindo e assumindo o risco de violação de dados.

Estamos agora no Brasil com uma das maiores suspeitas de violação de dados pessoais dos nossos cidadãos e precisamos cobrar dos controladores, processadores e operadores que implementem o conceito de que a privacidade dos dados deve ser o padrão de toda a linha de negócio e não podemos nos eximir de nossa responsabilidade na cobrança das autoridades da garantia do uso correto de nosso valor mais íntimo.

Cada vez que você adquire um produto online, usa um serviço, registra-se para receber e-mail, vai ao seu médico, compra medicamentos na farmácia, paga seus impostos e contas, ou celebra qualquer contrato ou solicitação de serviço, você deve fornecer algumas de suas informações pessoais.

Mesmo sem o seu conhecimento explícito, as informações sobre você estão sendo geradas e capturadas por empresas, empresas,

organizações de todos os tipos e agências governamentais com as quais você provavelmente nunca interagiu intencionalmente.

A única maneira dos clientes, cidadãos e consumidores confiarem em si mesmos e confiarem no governo e nas empresas é por meio de fortes práticas de proteção de dados como a nossa LGPD, com uma legislação eficaz para ajudar a minimizar o monitoramento desnecessário por autoridades estaduais e regular a vigilância por empresas.

Globalmente, há um aumento crescente nas leis de proteção de dados, muitas das quais foram modeladas diretrizes ou regulamentos abrangentes, como a Diretiva da UE mencionada acima, ou as Diretrizes da OCDE sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais.

Não se venda! Não troque suas informações pessoais por balas, descontos ou afiliações inexistentes. Questione sempre qual é a finalidade da coleta, tratamento e descarte de seus dados pessoais.

Há dois agentes em cada extremidade destes questionamentos: Organizações e Pessoas.

As organizações estão coletando as informações pessoais das pessoas, mas não estão informando qual será o Tratamento destas informações. Mas segundo a LGPD todo cidadão brasileiro tem a garantia de ceder ou não uma informação pessoal, chamada Dados, e todo brasileiro tem o direito que questionar a organização para que informe qual será o Tratamento dos dados que foram informados.

Sabemos que os Dados são um dos principais insumos da transformação digital nas organizações; e, como organizações, sabemos que precisamos dar o tratamento adequado aos dados custodiados para o Tratamento.

Até algum tempo atrás os dados eram produtos de ações deliberadas a pesquisas de clientes e de inventários físicos, que

erma parte de processos de negócios: fabricação, operações, vendas e marketing. Os dados resultantes eram usados principalmente para previsões, avaliações e tomada de decisões.

Em contraste, hoje nos deparamos com um dilúvio de dados, onde a maioria que é gerada ou Tratada nas organizações não é gerara por qualquer planejamento sistemático. Por isso, usa-se cada vez mais produtos de IoT, IA e BigData para o tratamento.

Mas os dados preciosos são os dados pessoais, pois eles têm o poder de alavancar lucros em empresas ou mitigar prejuízos. Entretanto, iniciou-se uma verdadeira corrida do ouro pelas informações pessoais das pessoas, e para regulamentar as posições do cidadão brasileiro e as organizações, é que foi criada a LGPD, similar a GDPR.

A Lei 13.709/18 estabelece que dado pessoal é toda informação relacionada a pessoa natural "identificada" ou "identificável" e determina que o tratamento desses dados deve considerar os 10 princípios de privacidade descritos na lei.

Ao segui-los as organizações demonstrarão que os dados pessoais coletados são necessários, mínimos, corretos, de qualidade, atendem uma finalidade de negócio válida dentre outras características.

O Brasil e a UE não são os únicos países ou uniões de países que possuem leis como esta. Outros países como África do Sul, Madagascar, Austrália, Nova Zelândia, Canadá, Estados Unidos, Argentina, Butão, Índia, entre outros, já possuem leis semelhantes.

Ou seja, é mundial a percepção de que as informações pessoais precisam ser protegidas de abusos.

No Brasil as organizações já precisam estar aderentes com a LGPD e talvez seja por isso que hoje estamos presenciando esta corrida do ouro.