LGPD

O novo mindset de privacidade

#LGPDBoaVista • Somos guardiões dos dados.

BoaVista
privacidade,
proteção
e segurança

BoaVista

Sumário

LGPD - Direitos do Titular

Regulamentação da LGPD

Segurança dos Dados Pessoais

Introdução

O que é privacidade?

É o direito que temos de reserva de informações pessoais e da própria vida pessoal. Na legislação brasileira (Constituição Federal), o direito à privacidade é garantido no art. 5.º:

"Art. 5.º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação."

A privacidade também é considerada um direito universal e está garantida no art. 12 da Declaração Universal dos Direitos Humanos:

"Ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques à sua honra ou à sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências ou ataques."

O que é Proteção de Dados Pessoais?

Significa garantir que os dados pessoais sejam usados apenas para finalidades legítimas, específicas, explícitas e informadas ao titular, fundamentadas em uma ou mais bases legais da LGPD assegurando que os dados pessoais não sejam usados para fins discriminatórios, ilícitos ou diferentes dos acordados.

O que é Segurança da Informação?

É um conjunto de medidas necessárias para garantir que sejam preservadas a confidencialidade, a integridade e a disponibilidade das informações de uma organização ou indivíduo de forma a preservar essa informação de acordo com necessidades específicas. O principal objetivo da Segurança da Informação é proteger os dados e não somente os ativos físicos e tecnológicos por onde passam ou estão armazenados.

Dentro das organizações em geral, existe uma área responsável pela Segurança da Informação que deve garantir acesso seguro e autorizado às informações e também garantir a privacidade dos dados.

Como os dados pessoais são tratados atualmente?

Atualmente, os dados devem ser tratados de acordo com as diretrizes da LGPD. Recomendamos muita atenção ao acessar "joguinhos". Veja bem as políticas de uso, leia e só concorde se estiver ciente do que está sendo coletado e para qual finalidade serão usados seus dados.

LGPD
Aspectos Gerais da Lei

O que é LGPD?

A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018 e suas posteriores alterações), chamada de LGPD, regulamenta o uso de dados pessoais de pessoas físicas (ou pessoas naturais) no Brasil, estabelecendo regras sobre o tratamento desses dados, nos meios físicos e digitais. Estão sujeitas ao cumprimento da lei a pessoa natural (qualquer cidadão) ou a pessoa jurídica (empresa) de direito público ou privado. O objetivo da LGPD é proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade das pessoas naturais.

De maneira geral, a lei foi criada para regulamentar a privacidade das pessoas em operações de tratamento de dados pessoais, dando ao titular dos dados mais controle e possibilidade de saber de forma transparente como são usados seus dados nas operações de tratamento de dados pessoais, possibilitando que ele possa exercer os direitos previstos na LGPD.

As empresas e pessoas físicas que usam os dados pessoais dos titulares para fins de oferta ou fornecimento de bens ou serviços precisam ser transparentes a respeito da finalidade do uso, armazenamento e consumo dos dados utilizados.

Quem é quem na LGPD?

Titular de dados: o “dono” dos dados. Exemplo: você é o titular do número do seu telefone, endereço, e-mail, etc.

Controlador: pessoa ou empresa que toma decisões sobre o tratamento de dados pessoais.

Operador: pessoa ou empresa, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Agentes de tratamento: pessoa ou empresa que é controlador e operador ao mesmo tempo.

As demais legislações continuarão a ter validade com a entrada da LGPD?

Sim, as demais legislações continuam em vigência, a LGPD não revogou nenhuma. Dessa forma, as legislações terão de conviver em harmonia e serão trabalhadas em conjunto. O art. 64 traz isso de forma clara.

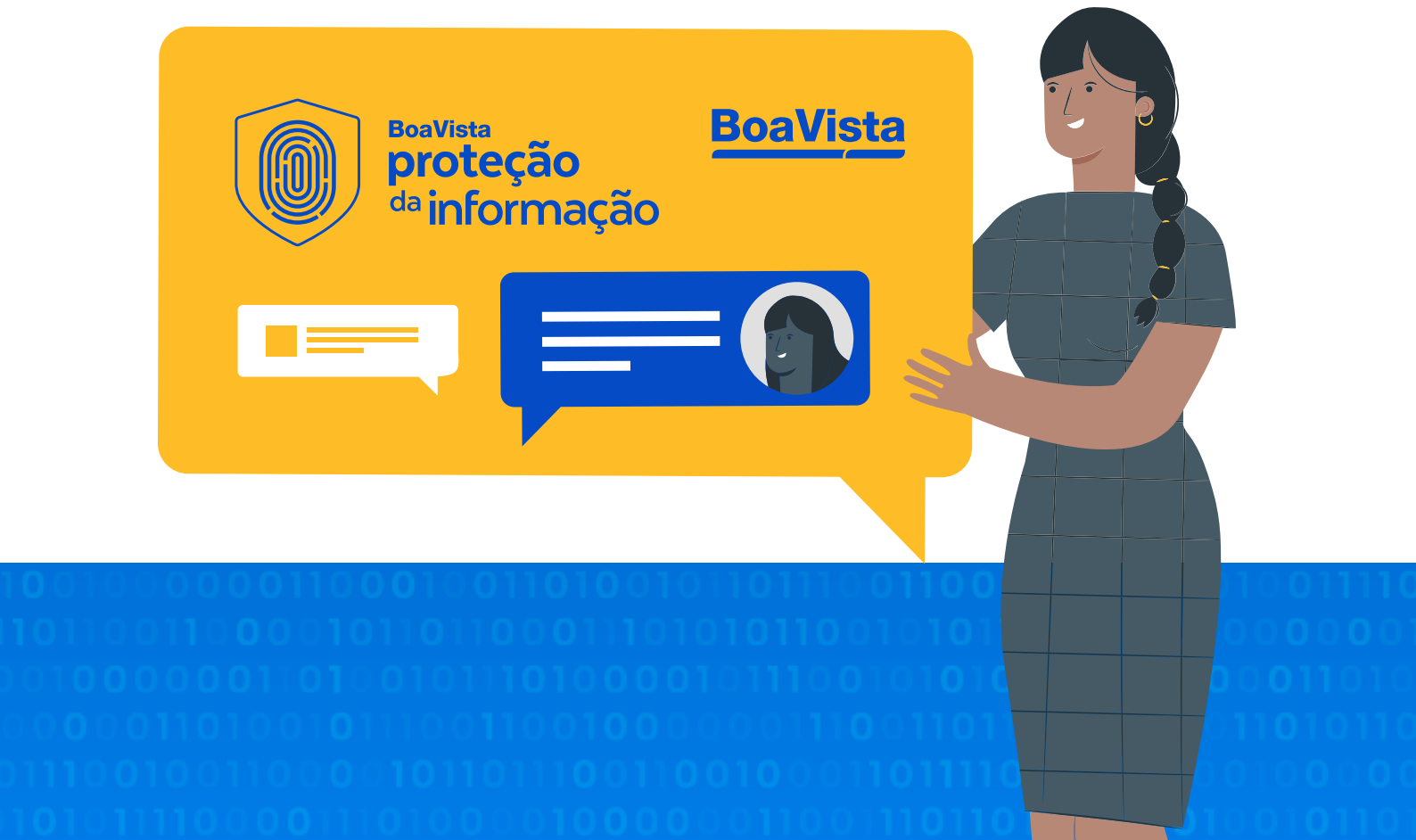
Podemos destacar como um exemplo clássico de que as leis devem conviver em harmonia o disposto no art. 7.º, X, da LGPD, em que se estabelece como base legal para tratamento de dados pessoais a proteção do crédito com a citação expressa de que deve ser observado o disposto na legislação pertinente. Portanto, quando se fala da proteção ao crédito, devemos aplicar as disposições do Código de Defesa do Consumidor, que em seu art. 43 trata dos bancos de dados, e a Lei 12.414/2011, alterada pela Lei Complementar 166/2019, regulamentada pelo Decreto 9.936/2019, que regula o Cadastro Positivo e estabelece as regras relativas aos bancos de dados.

O que é tratamento de dados para a LGPD?

É toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Em resumo, encostou no dado, está tratando o dado.

A lei se aplica apenas para empresas de dados?

Não, a LGPD é para todos! Todo tratamento de dados pessoais deve estar adequado e respeitar as determinações da LGPD.



O que é dado pessoal?

É toda informação que identifica ou que possa tornar identificável uma pessoa. Por exemplo, nome, CPF, RG, endereço, telefone, e-mail.

O que é dado pessoal sensível?

Segundo a LGPD, considera-se dado sensível dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

Quem está sujeito à LGPD?

As novas regras afetam todos os setores da economia, inclusive as relações entre clientes e fornecedores de produtos e serviços, empregado e empregador, e outras relações nas quais dados pessoais são coletados, tanto no ambiente digital quanto fora dele.

Em resumo, todas as operações de tratamento realizadas por pessoas físicas ou jurídicas (públicas ou privadas) estão sujeitas à LGPD, mesmo que os dados não estejam localizados no País. Se os dados pessoais tiverem sido coletados no Brasil ou o tratamento for realizado aqui ou com objetivo de fornecer serviços em território nacional ou para quem esteja no País, estão sujeitos à LGPD.

É importante verificar a aplicabilidade no artigo 3.º da LGPD. O art. 4.º traz as hipóteses em que não se aplica a LGPD.

Quem irá regulamentar?

A Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal integrante da Presidência da República, irá regulamentar a LGPD.

Qual é a diferença entre controlador e operador?

Resumidamente, o controlador é um dos principais responsáveis pelos dados pessoais, isto é, é quem toma as decisões sobre os tratamentos daqueles dados. Já o operador é quem atua sobre os dados, isto é, executa os tratamentos dos dados pessoais de acordo com as definições do controlador. Em alguns processos, a mesma empresa ou pessoa pode executar os papéis de controlador e operador e, com isso, tornar-se o agente de tratamento. Por exemplo, quando a Boa Vista incrementa as bases de dados escolhendo quais dados pessoais devem existir na base, é controladora. Quando, um cliente envia informações sobre negativações, a Boa Vista é operadora, pois só irá executar a negativação em nome do cliente (controlador); mas a partir do momento em que a Boa Vista recebe os dados, integra-os aos seus bancos e fornece os serviços, passa a ser controladora e operadora, o que a torna um agente de tratamento.

Quem é o DPO (Encarregado de Dados)?

Data Protection Officer - DPO (Encarregado de Dados), também conhecido como encarregado pelo tratamento dos dados pessoais, é o responsável pela proteção dos dados pessoais da empresa e estará envolvido nas definições dos tratamentos de dados pessoais. É o responsável por conscientizar a organização sobre proteção de dados pessoais e ser a ponte com a ANPD, o órgão regulador da LGPD.

Quais as principais atividades do DPO?

- Auditar periodicamente as operações de tratamento de dados.
- Monitorar o comportamento e tráfego de informações pessoais.
- Atender às dúvidas dos titulares de dados
- Ser o ponto de contato com a ANPD.
- Ter ciência e garantir conformidade nos tratamentos de dados pessoais na empresa.
- Orientar colaboradores quanto à gestão de privacidade de dados.

Em quais hipóteses os dados pessoais podem ser tratados?

A lei traz 10 hipóteses que autorizam o tratamento de dados pessoais com igual importância, a saber:

1. **Proteção do crédito,** inclusive quanto ao disposto na legislação pertinente.

2. **Cumprimento de obrigação legal ou regulatória** pelo controlador.

3. Quando necessário para a **execução de contrato** ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

4. **Interesses legítimos** do controlador ou de terceiros, para apoio e promoção de atividades do controlador e, ao mesmo tempo, proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitados as legítimas expectativas dele e os direitos e as liberdades fundamentais nos termos da LGPD.

5. Pela **administração pública**, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios e outros.

6. Realização de **estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais.

7. **Exercício regular de direitos** em processo judicial, administrativo ou arbitral.

8. **Proteção da vida** ou da incolumidade física do titular ou de terceiros.

9. **Tutela da saúde.**

10. **Consentimento pelo titular.**

Sempre que tratar um dado pessoal, devo ter uma base legal?

Sim, todo e qualquer tratamento de dados pessoais deve estar fundamentado ao menos em uma das 10 bases legais da LGPD. Nenhum dado pessoal pode ser tratado sem que haja uma correta definição da base legal pelo departamento jurídico. Lembre-se, encostou no dado, está tratando o dado!

Só posso tratar o dado pessoal se tiver consentimento do titular?

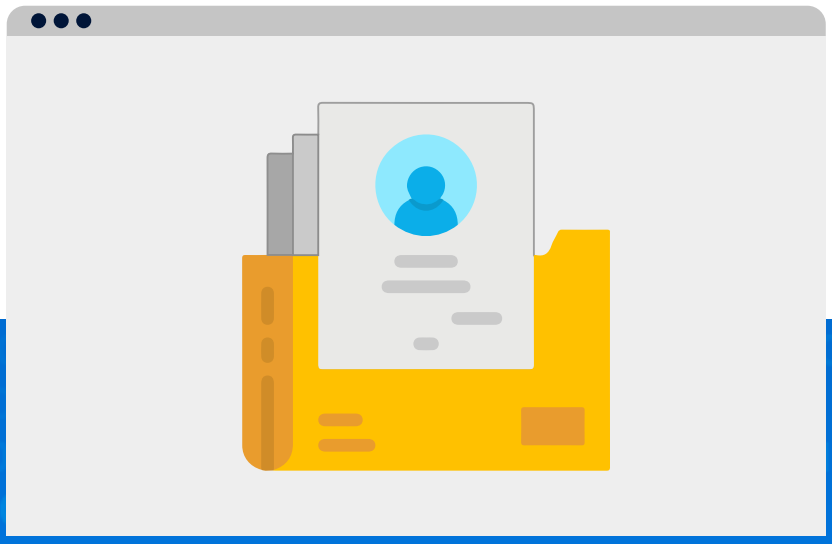
O consentimento é só uma das 10 hipóteses da LGPD para tratamento dos dados pessoais. Não é mais importante que nenhuma outra e nem possui hierarquia entre as bases legais definidas pela LGPD, podendo as bases legais serem utilizadas individualmente ou em conjunto, conforme o caso. Lembrando que, ao utilizar o consentimento, ele deve ser inequívoco e expresso, e ser definida sua finalidade. O titular dos dados deve desejar por sua vontade a coleta e o tratamento dos seus dados que estão sendo fornecidos. Um exemplo de consentimento inequívoco é quando você entra num site e este informa que, para prosseguir com a navegação, é necessário consentir com os Termos de Uso e o titular continua com a navegação sabendo que, com isso, aceitou os termos colocados.

Como existe a base legal de proteção ao crédito, a Boa Vista e os demais GBD estão isentos da LGPD?

Não. Todo tratamento deve ser fundamentado ao menos em uma base legal da LGPD (e não apenas na base legal da proteção do crédito). Todo cuidado e segurança devem ser seguidos para garantir a proteção dos dados pessoais e a privacidade do titular dos dados.

O que é GBD (gestor de banco de dados)?

É uma definição contida na Lei 12.414/2011 e posteriores alterações, na qual, para fins de Cadastro Positivo, GBD é a pessoa jurídica que atende aos requisitos da referida lei, sendo a responsável pela administração de bancos de dados com dados positivos, bem como pela coleta, pelo armazenamento, pela análise e pelo acesso de terceiros aos dados armazenados.



O que é Cadastro Positivo?

Funciona como um boletim escolar que registra os pagamentos que você fez no seu histórico de crédito, transformando esse comportamento em nota (ou pontuação). Por isso, permite uma análise mais justa na hora que você pedir crédito, pois sua capacidade de pagamento também será considerada.

Qual a diferença do Cadastro Positivo com a LGPD?

São duas leis distintas e cada qual tem suas funções. A lei que regula o Cadastro Positivo disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou pessoas jurídicas, para formação de histórico de crédito. A LGPD regulamenta o tratamento de dados pessoais. As duas leis são complementares, pois o Cadastro Positivo trata dados pessoais, e a LGPD, em complementação à Lei do Cadastro Positivo, regulamenta esse tratamento.

Quais são os princípios que devem ser seguidos para utilização e tratamento dos dados pessoais do titular e como a Boa Vista agirá?

A LGPD traz 10 princípios que precisam **obrigatoriamente** ser observados para que os dados do titular possam ser utilizados e tratados, e a Boa Vista seguirá as diretrizes, quais sejam:

Finalidade: fará o tratamento dos dados pessoais dos titulares de dados para fins específicos, legítimos, explícitos e informados. A finalidade deve estar dentro dos limites da lei e expressamente clara para o titular dos dados.

Adequação: o tratamento deve ser compatível com as finalidades que a Boa Vista informou ao titular.

Necessidade: a Boa Vista deverá utilizar apenas os dados pessoais do titular dos dados estritamente necessários para alcançar as finalidades informadas a ele, qualquer que seja a base legal aplicada ao tratamento.

Livre acesso: a pessoa física titular dos dados tem o direito de solicitar para a Boa Vista consulta, de forma simples e gratuita, de todos os dados que a empresa detenha a seu respeito.

Qualidade dos dados: deve ser garantido aos titulares de dados que as informações que a Boa Vista tenha sobre eles sejam verdadeiras e atualizadas. É necessário ter atenção à exatidão, clareza e relevância dos dados de acordo com a necessidade e a finalidade de seu tratamento.

Transparência: todas as informações trafegadas por meio da Boa Vista, em todos os seus meios de comunicação, devem ser claras, precisas e verdadeiras, observados os segredos comercial e industrial.

Segurança: a Boa Vista deve apresentar garantias técnicas e administrativas adequadas para garantir a segurança dos dados pessoais, incluindo a proteção contra seu tratamento não autorizado, ilícito, contra a sua perda, destruição ou danificação acidental, adotando as tecnologias adequadas.

Prevenção: a Boa Vista atuará de forma preventiva e adotará medidas para evitar a ocorrência de eventuais danos em virtude do tratamento de dados pessoais.

Não discriminação: os dados pessoais não serão utilizados para discriminar ilicitamente ou promover abusos contra os titulares de dados.

Responsabilização e prestação de contas: além da preocupação em cumprir integralmente a legislação, a Boa Vista deverá ter provas e evidências de todas as medidas adotadas que demonstrem a boa-fé e a diligência.

Qual a diferença entre as bases legais (hipóteses) e os princípios da lei?

Todo tratamento de dados pessoais deve estar fundamentado ao menos em uma das 10 bases legais, isto é, deve-se verificar qual base legal permite aquele tratamento (proteção ao crédito, legítimo interesse, consentimento, entre outras). Já os 10 princípios (por exemplo, qualidade, livre acesso, finalidades) devem ser seguidos integralmente em todos os tratamentos de dados, norteando as decisões acerca do tratamento de dados pessoais.

Por exemplo, uma padaria pode fazer o cadastro dos seus clientes optando pela base legal Consentimento, fazendo com que cada cliente deva autorizar a coleta dos seus dados. Porém, a padaria não deve coletar todos os dados. Deve-se restringir aos dados pessoais que façam sentido para um cadastro, por exemplo. Então, nome, telefone e e-mail fazem sentido, mas time de futebol e religião, não. Dessa forma, esses últimos dados não devem ser coletados atendendo aos princípios da adequação, finalidade e necessidade. Já o princípio de segurança diz que não se deve deixar os dados pessoais coletados em um papel em cima do balcão, por exemplo. Então, a empresa deverá ter mecanismos de segurança.

No mesmo exemplo, o princípio de qualidade prevê que a padaria mantenha os dados pessoais sempre atualizados. Cada princípio diz algo sobre esse exemplo. E, dessa forma, toda vez que houver um tratamento de dados pessoais, todos esses princípios devem ser observados e atendidos. Então, pensou em coletar dados pessoais, deve-se pensar em como atender a todos os princípios e qual base legal fundamentará essa coleta. Da mesma forma, se for vender um produto que trabalhe com dados pessoais ou desenvolver um sistema ou qualquer outro evento que envolva dados pessoais, deve-se atender a esses princípios sempre relacionando-os a uma base legal. E, com isso, pensar primeiro em privacidade.

O que é *Privacy by Default* e *Privacy by Design*?

A primeira se refere à “cultura da privacidade”, a atitude que precisamos ter constantemente: sempre pensar primeiro na privacidade, principalmente, quando tratamos dados pessoais.

Quando isso é aplicado aos nossos processos produtivos, entra a segunda, *Privacy by Design*, que significa aplicar esse raciocínio de proteção, desde a concepção até a execução dos produtos e serviços, o que envolve todos nós, guardiões dos dados.

Um exemplo é quando um aplicativo pergunta se o usuário permite utilizar a localização. Os desenvolvedores pensaram na privacidade ao permitir a decisão do usuário. Se ele permitir ou não, é uma escolha própria. Mas ele tinha a opção.

Na mesma linha, o celular vem com a opção de usar segurança, como senha ou biometria, ou não usar nenhuma opção segura, mas a possibilidade existe e a escolha é novamente do usuário.

Quais são os pilares do *Privacy by Design*?

Existem sete pilares que auxiliam o entendimento do *Privacy by Design* e, consequentemente, a sua utilização. A saber:

- **Ser proativo e não reativo** – prevenir e não remediar: a metodologia de *Privacy by Design* é caracterizada por ser proativa e não reativa. Dessa forma, antecipa e previne eventos de invasão de privacidade antes de acontecerem. Assim, não espera um risco de privacidade se materializar nem tenta remediar quando infrações de privacidade acontecem. Essa abordagem é executada para prevenir que elas ocorram. Em resumo, *Privacy by Design* acontece antes dos fatos, não depois.

- ***Privacy by Default*** – privacidade por padrão: *Privacy by Design* busca oferecer o mais alto grau de privacidade, garantindo que os dados pessoais estão automaticamente protegidos em qualquer sistema ou prática de negócio. Se um indivíduo não fizer nenhuma ação, sua privacidade permanece intacta. Nenhuma ação é necessária por parte de um indivíduo para proteger sua privacidade. Por padrão, o sistema já é construído para garantir isso.

- **Privacidade incorporada ao projeto** – *Privacy by Design* é inerente ao design e à arquitetura dos sistemas de TI e a todas as práticas de negócio. Não é construído como um add-on (aplicativo instalado ao lado de um programa já existente para aumentar as suas funcionalidades). O resultado é que a privacidade se torna um componente essencial das funcionalidades principais a serem desenvolvidas. A privacidade deve ser integral ao sistema sem diminuir funcionalidades.

- **Funcionalidade total** – "soma-positiva" em vez de "soma-zero": um jogo de soma-positiva é aquele em que todos ganham, diferente do jogo de soma-zero, no qual, para um ganhar, outro precisa perder. A metodologia de *Privacy by Design* busca a proteção dos dados aliada às funcionalidades sem serem necessárias negociações como privacidade versus segurança, garantindo e demonstrando que ambas são possíveis.

- **Segurança de ponta a ponta** – proteção durante todo o ciclo de vida dos dados: *Privacy by Design*, sendo intrínseca ao sistema, mesmo antes da primeira informação ser coletada, garante a segurança durante todo o ciclo de vida dos dados envolvidos. Medidas robustas de segurança são essenciais à privacidade,

do início ao fim.

- **Visibilidade e transparência** – *Privacy by Design* visa garantir que, independentemente dos negócios ou da tecnologia envolvidos, os tratamentos dos dados seguirão as premissas e os objetivos estabelecidos, sujeitos a auditoria.

- **Respeito pela privacidade do usuário** – solução centrada no usuário: este é um dos preceitos básicos do *Privacy by Design*. Toda a arquitetura e operacionalidade do sistema ou da prática de negócio devem ser centradas na privacidade do usuário, pensando sempre na proteção completa dos seus dados pessoais.

LGPD
Direitos do Titular

Quais são os direitos do titular?

Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, intimidade e privacidade. Para garantir todos esses pontos, a LGPD assegura alguns direitos ao titular dos dados:

- Acesso facilitado aos dados.
- Correção ou atualização dos seus dados.
- Anonimização, bloqueio ou eliminação dos seus dados.
- Eliminação de dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD.

- Revogação do consentimento.
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.
- Portabilidade dos dados.
- Informação sobre a existência e finalidade específica do tratamento dos dados, forma e duração, assim como sobre o possível compartilhamento.
- Oposição ao tratamento irregular e à reclamação à autoridade.
- Revisão dos tratamentos de dados baseados em decisões automatizadas.

O que é autodeterminação?

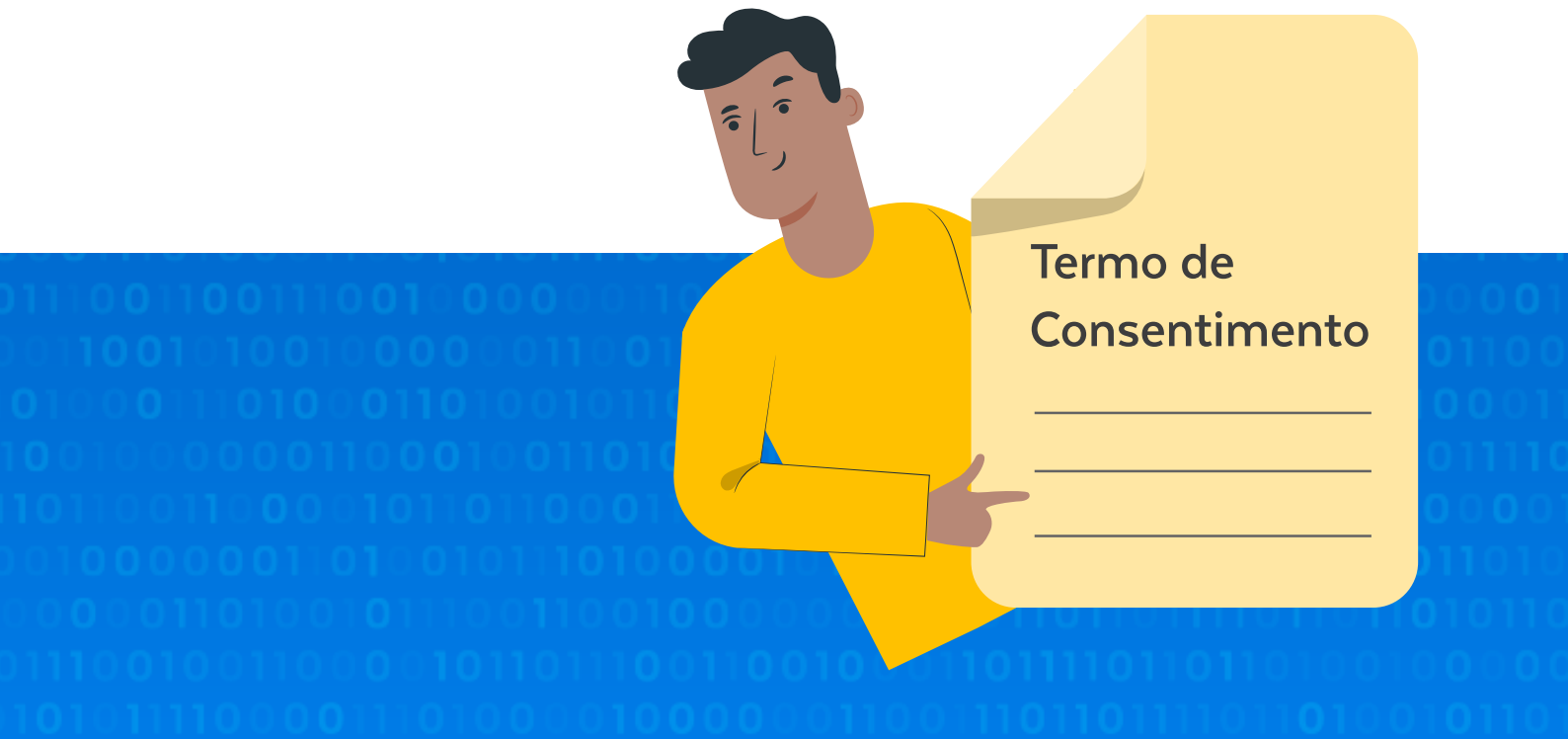
É um direito do titular dos dados assegurado pela LGPD em que se dá controle ao indivíduo sobre o armazenamento e uso de informações a seu respeito, exceto em casos em que a própria disponha de outra forma ou alguma outra legislação permita o uso dos dados pessoais.

Dessa forma, um titular pode impedir que a Boa Vista trate seus dados?

Todo tratamento de dados pessoais deve ser fundamentado em uma base legal e respeitar todos os princípios da LGPD ou estar baseado em alguma outra lei vigente, garantindo dessa forma os direitos do titular. Se o tratamento seguir essas premissas, excetuando-se na hipótese de ser baseado em consentimento, a Boa Vista poderá dar continuidade ao tratamento. Por exemplo, uma pessoa que teve seu nome negativado exige que esse tratamento seja interrompido. Pela LGPD, esse titular dos dados está exercendo o direito de oposição ao tratamento. Porém, esse direito pode ser executado apenas para tratamentos irregulares e abusivos e a negativação segue leis vigentes e a base legal de proteção do crédito da LGPD. Dessa forma, o titular dos dados não pode interferir no tratamento.

Porém, se o tratamento for baseado em consentimento, o titular dos dados pode interromper o tratamento?

Sim, a base legal de consentimento deixa a decisão sobre a existência ou não do mesmo para o titular. O titular dos dados tem o direito de consentir e revogar o consentimento sempre que achar necessário. Quando der o consentimento, tem de ser expresso e inequívoco, isto é, em um website e ele próprio deve marcar a opção que aceita os termos, que não pode já vir preenchida. Além disso, o Termo de Consentimento deve ser bem explicado, de fácil entendimento, descrevendo a finalidade de todos os tratamentos a que o dado pessoal está sujeito, com quem esses dados poderão ser compartilhados e qual a duração do tratamento. Esse consentimento não pode ser condicionado a nenhuma troca. Ele deve ser espontâneo. Da mesma forma, sua revogação deve ser de fácil acesso.



O que é livre acesso?

É o direito do titular dos dados em saber quais dados pessoais uma empresa tem dele. Além disso, o titular pode corrigir os dados errados e pedir para excluir ou bloquear aqueles que acredita serem indevidos ou abusivos e obter informações sobre como seus dados pessoais são tratados.

Da mesma forma, como nem sempre um titular pode impedir um tratamento de dados, ele também não pode solicitar a exclusão e o bloqueio de dados pessoais protegidos por alguma outra lei ou base legal da LGPD. Como exemplo, temos os dados de negativação, que não são do titular, e sim do cliente (credor) que solicita esse tratamento.

Uma empresa poderá, sem prejuízo, recusar-se a prestar atendimento caso o consumidor não queira consentir, mesmo quando a finalidade for explicada?

Depende da situação. Se o consentimento for, por exemplo, para armazenamento de informações cadastrais que visam garantir que o titular dos dados é quem diz ser, e o titular não consentir mesmo após a explicação, a empresa poderá não atender à solicitação, pois não conseguirá garantir a segurança do próprio titular (um impostor pode se passar por ele e não haverá registros desse fato). A lei dá direitos ao titular, porém, tais direitos não se sobrepõem a obrigações como essa em que a empresa tem de fazer a validação evitando que uma pessoa se passe por outra.

O que é portabilidade dos dados?

É o direito do titular de transferir seus dados para outro controlador. Um exemplo é transferir os dados de saúde, como resultados de exames, de um laboratório para outro.

O que é revisão dos tratamentos de dados baseados em decisões automatizadas?

É quando uma empresa utiliza recursos de tecnologia (por exemplo, inteligência artificial) para fazer o tratamento dos dados.

Regulamentação da LGPD

O que é ANPD?

A Autoridade Nacional de Proteção de Dados é o órgão da administração pública federal, integrante da Presidência da República, que irá regulamentar a LGPD.

Quais sanções podem ser aplicadas em caso de descumprimento da LGPD?

- Bloqueio do tratamento.
- Eliminação dos dados.
- Multa diária (mesmo teto).
- Advertência.
- Publicização da infração.
- Multa (até 2% do faturamento) limitada, no total, a R$ 50 MM (cinquenta milhões de reais) por infração.

Essas sanções já são predefinidas?

Não, o órgão regulador levará em consideração as questões abaixo. Dessa forma, devemos sempre fazer o melhor visando garantir segurança e privacidade dos dados pessoais, inclusive documentando os processos e as tecnologias utilizados, mostrando diligência.

- Reincidência.
- Medidas corretivas.
- Condição econômica.
- Proporcionalidade.
- Proteção de dados.
- Boas práticas e governança.
- Cooperação do infrator.
- Grau do dano/gravidade.
- Vantagem obtida ou pretendida.

O que é publicização?

Significa dar publicidade ao fato, isto é, obrigação de assumir publicamente a responsabilidade pelo ocorrido.

O que é responsabilidade solidária?

Dentre as sanções legais que o descumprimento da LGPD pode trazer, há um ponto importante, que precisa ser ressaltado: a responsabilidade e, portanto, a aplicação dessas punições são, na maioria dos casos, compartilhadas entre o controlador e o operador envolvidos.

Na LGPD, existe a “solidariedade”, o que quer dizer que os controladores e operadores respondem pela responsabilidade sobre tratamento de dados pessoais que gere danos ao titular (salvo nos casos de exclusão previstos na Lei).

Segurança dos Dados Pessoais

O que é incidente de privacidade?

É um incidente que fere a privacidade de uma pessoa. Pode ser, por exemplo, acesso não autorizado aos dados pessoais, incidentes ou ilícitos que causem alteração, eliminação, divulgação dos dados pessoais, entre outros. Aqui é claro o exemplo que demos de que é necessária a autenticação do usuário para que alguém não se passe por outro.

Quais as melhores práticas para evitar um incidente?

- Pensar sempre em privacidade (Privacy by Default e Privacy by Design).
- Seguir as recomendações da empresa quanto às senhas seguras.
- Não compartilhar senhas e jamais anotá-las; principalmente, nunca as escrever em cadernos ou post-its.
- Encaminhar arquivos somente por meios seguros homologados pela empresa.
- Copiar somente as pessoas necessárias em e-mails.
- Certificar-se de que os endereços de e-mail estão corretos.
- Conectar-se com frequência à VPN ou à rede da empresa para atualizações sistêmicas.

O que é política de mesa limpa?

É manter a área de trabalho, portanto, mesa e tela do computador livres de informações que possam ser usadas de forma maliciosa ou até ilícita. Dessa forma, minimizam-se os riscos de acesso não autorizado, exibição, perda ou alteração das informações quando não estivermos atentos ao ambiente ou estivermos ausentes.

Quais tecnologias auxiliam a segurança dos dados?

Além de seguir todas as melhores práticas para evitar um incidente de privacidade, é importante contar com a tecnologia para aumentar a segurança. Duas técnicas são muito importantes: criptografia e anonimização dos dados pessoais.

Os dados criptografados são aqueles submetidos a um processo que os torna ininteligíveis. As pessoas só conseguem ler dados criptografados com uma chave que os decodifica.

A diferença para dados anonimizados é que estes não têm a tal chave. A anonimização é irreversível e faz com que os dados não possam ser relacionados a uma pessoa. A LGPD não considera os dados anonimizados como dados pessoais. Portanto, dados anonimizados estão fora do escopo da LGPD.

O que deve ser feito para garantir a segurança?

- Bloquear o computador ao se ausentar.
- Bloquear o celular quando não estiver em uso.
- Trocar as senhas periodicamente.
- Usar senhas complexas.
- Usar senhas diferentes para contas diferentes.
- Não discutir assuntos confidenciais da companhia em lugares públicos.
- Prestar atenção ao descartar informações. Se forem restritas, confidenciais ou contiverem dados pessoais, devem ser descartadas de forma apropriada, como, por exemplo, numa fragmentadora de papel.
- Destruir as informações corretamente quando não forem mais necessárias.
- Usar configurações de privacidade em mídia social para restringir o acesso a informações pessoais.
- Evitar usar redes públicas de wi-fi e nunca utilizar quando estiver trabalhando.
- Informar a Segurança da Informação quando ocorrer algo suspeito.

- Pensar sempre primeiro em privacidade (Privacy by Default e Privacy by Design), seja ao desenvolver um novo produto ou software ou criar um processo, por exemplo.

- Nunca ser abusivo.

- Entender o princípio da minimização: “Menos é mais.”

- Se tiver dúvidas sobre a lei, pergunte às áreas do Jurídico ou de Privacidade.

- Verifique se o tratamento que está executando tem validade jurídica e se está escrito em contrato.

- Sem promessas, mais realidade. Traga o negócio para a realidade.

- Sempre tenha contrato e só execute o que está nele.

- Só faça ativações ou reativações se estiver em contrato.

O que não deve ser feito para garantir a segurança?

- Não clicar em links suspeitos.
- Não abrir e-mails ou anexos suspeitos.
- Não enviar e-mails corporativos para o e-mail pessoal.
- Não usar o e-mail corporativo para fins pessoais.
- Não deixar contratos e documentos à vista.
- Não esquecer armários e gavetas abertos.
- Não compartilhar crachá de identificação nem usá-lo para reservas de mesas em restaurantes, por exemplo.
- Não fornecer informações confidenciais a desconhecidos.
- Não conversar assuntos da empresa em elevadores, restaurantes, nem trabalhar em locais públicos.
- Não salvar senhas no navegador de Internet.
- Não anotar senhas em arquivos ou papéis.

- Não compartilhar senhas.
- Não publicar informações privadas/confidenciais.
- Não instalar programas não autorizados no seu computador de trabalho.
- Não inserir pendrives de origem desconhecida.
- Não deixar dispositivos desacompanhados.
- Não deixar wi-fi ou Bluetooth ligados quando não estiverem em uso.

Considerando que a Boa Vista adota as melhores práticas de mercado, quais certificações possui?

- ABNT NBR ISO/27701:2019 - Técnicas de Segurança para Gestão da Privacidade da Informação
- ABNT NBR ISO 9001:2015 – Sistema de Gestão da Qualidade
- ABNT NBR ISO/IEC 27001:2013 – Sistema de Gestão da Segurança da Informação
- DAMA –Maturidade em Gestão, Governança e Qualidade de Dados e Aplicação

O que é a Certificação ABNT NBR ISO 27701:2019?

A certificação de Sistema de Gestão da Privacidade da Informação – SGPI é um padrão de referência internacional e extensão da ISO/IEC 27001. Uma empresa certificada significa que possui um processo de gerenciamento e mitigação de riscos relacionados a proteção e privacidade envolvidos em todo o ciclo de vida dos dados pessoais.

Ter a Certificação é estar em conformidade com a Lei Geral de Proteção de Dados (LGPD).

O que é a Certificação ABNT NBR ISO 9001:2015?

A Certificação do Sistema de Gestão da Qualidade (SGQ) possui ferramentas de padronização, é um modelo seguro para Gestão da Qualidade, trazendo confiança ao cliente de que os produtos e serviços da empresa serão criados de modo repetitivo e consistente, adquirindo uma qualidade de acordo com aquilo que foi definido pela empresa. Nessa norma, muito se aplica a ferramenta da qualidade: o Ciclo PDCA (Plan-Do-Check-Action), que significa Planejar, Fazer, Checar e Agir.

Princípios de Gestão da Qualidade: Foco no Cliente, Liderança, Abordagem de Processo, Abordagem Sistêmica para a Gestão, Envolvimento das Pessoas, Melhoria Contínua, Abordagem Factual para Tomada de Decisões e Benefícios Mútuos nas Relações com os Fornecedores.

O que é a Certificação ABNT NBR ISO/IEC 27001:2013?

A Certificação de Sistema de Gestão de Segurança da Informação (SGSI) é um padrão de referência internacional. Uma empresa certificada significa que possui um nível de maturidade em seus processos com relação à Segurança da Informação, passando maior credibilidade aos clientes e parceiros de negócios.

Princípios do Sistema de Gestão de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.

O que é a Certificação DAMA?

Selo de Maturidade em Gestão, Governança e Qualidade de Dados e Aplicação em USO Nível 4 conferido pelo Data Management Association (DAMA) e também pela aplicação e uso das melhores práticas contidas no DAMA-DMBOK.

BoaVista
privacidade,
proteção
e segurança

BoaVista