inloco

Descomplicando Privacy by Design

Um guia prático para implementar os 7 princípios fundamentais na sua empresa

Introdução

As principais legislações em matéria de proteção de dados ao redor do mundo exigem que as organizações implementem medidas técnicas e administrativas para proteger a privacidade desde a concepção (no inglês, *"by design"*) de um produto ou serviço até a sua efetiva entrega. Mas o que isso significa na prática? Como implementar cada um dos sete princípios fundamentais de *Privacy by Design* com medidas técnicas e organizacionais? O objetivo deste ebook é exatamente responder a essas perguntas de modo a otimizar os esforços de sua organização na adequação legal, com alguns exemplos de como a In Loco já implementou tais princípios para ilustrar e tornar mais tangível sua aplicação.

Expediente

Autoria
Raissa Moura, Daniela Cabella e Lara Ferraz

Designer
Victor Gomes

Revisão
Lana Pinheiro

In Loco
São Paulo, 28 de janeiro de 2020.

Por que sua empresa deve se importar com proteção de dados e privacidade?

Por que sua empresa deve se importar com proteção de dados e privacidade?

Privacidade é um dos temas mais quentes do momento. Na última edição da maior feira mundial de tecnologia voltada para os consumidores, a Consumer Electronic Show (CES) em Las Vegas (EUA), o evento que mais chamou a atenção foi uma mesa redonda sobre privacidade com representantes de algumas das maiores empresas de tecnologia do mundo. A sala de quinhentos lugares ficou lotada, e outras pessoas ainda precisaram ser acomodadas em uma nova sala para acompanhar a discussão por vídeo. Mas por que esse tema é tão importante para as empresas e por onde começar os trabalhos internos nesse assunto?

Estamos vivendo um momento de transição para uma nova cultura no mercado, semelhante ao que vivemos com a entrada em vigor do Código de Defesa do Consumidor (CDC): os próprios consumidores estão exigindo que as empresas sejam mais transparentes e lhes deem maior controle. No caso do CDC, os consumidores passaram a poder exigir maior transparência com relação aos seus direitos e a exigir que as empresas os respeitem de forma integral e eficaz. Com relação à privacidade, as pessoas físicas (usuárias da internet) estão também exigindo maior transparência com relação a quais informações suas são coletadas, como são utilizadas pelas empresas, além de exigirem meios de poder exercer certos direitos.

De acordo com pesquisa realizada e consolidada pelo relatório da Consumer Pulse 2019[1], mais de 75% dos consumidores não estão confortáveis com a coleta de dados via microfone ou assistente de voz e 51% dizem que o número de anúncios invasivos está crescendo. *"Quase um terço dos consumidores conhece alguma marca que foi "longe demais" e*

---

1 Disponível em: https://www.accenture.com/_acnmedia/PDF-110/Accenture-See-People-Not-Patterns.pdf. Acesso em: 19 janeiro de 2020

2 Disponível em: https://noomis.febraban.org.br/especialista/noomisblog/84-das-empresas-nao-estao-prontas-para-proteger-dados-pessoais. Acesso em 19 janeiro de 2020.

69% deles deixariam de fazer negócios ou repensaria seu relacionamento com uma marca por causa disso."[2] Vê-se, portanto, que os consumidores estão atentos e demandam um cuidado maior com o que é feito com seus dados pessoais pelas empresas e como isso pode afetar sua privacidade.

Além dos consumidores, as próprias autoridades públicas também estão bastante atentas. No Brasil, antes mesmo da entrada em vigor da Lei Geral de Proteção de Dados (LGPD) - prevista para agosto de 2020 -, as autoridades já notificaram diversas empresas tanto pelo uso indevido dos dados de consumidores ou simplesmente para entender se esses dados estão sendo tratados corretamente, embasando-se em princípios e preceitos da legislação em vigor. A proteção à privacidade é um direito já previsto na Constituição Federal (promulgada em 1988), reforçado pelo Código Civil de 2002 e que dialoga fortemente com o CDC (1990) e o Marco Civil da Internet (2014). O tema, portanto, não é novo, mas sua fiscalização tem sido mais forte recentemente. Nos dois últimos anos, o Ministério Público do Distrito Federal e Territórios (MPDFT) aplicou multas milionárias a diversas empresas que não aplicam medidas de proteção aos dados pessoais e privacidade dos consumidores, e ainda firmou Termos de Ajustamento de Conduta (TACs) com outros. Em maio de 2019, por exemplo, o MPDFT pediu indenização de R$ 10 milhões a empresa operadora de bitcoins pelo vazamento de dados, e, em dezembro de 2018, uma rede de drogarias foi multada em quase R$ 8 milhões por falta de transparência com relação ao cadastro e uso de informações pessoais dos consumidores.

Essa tendência não é apenas no Brasil, mas global - as autoridades estrangeiras, inclusive, têm imposto multas altíssimas: uma plataforma de rede social envolvida em escândalo relacionado ao processo democrático das eleições nos EUA e em outros países pelo mundo foi multada, em julho de 2019, em US$ 5,5 bilhões pela falta de transparência e uso indevido das informações pessoais de seus usuários. Em outro caso, uma companhia aérea foi multada em US$ 230 milhões por ter sofrido um *cyber* ataque e não ter aplicado medidas de proteção de dados para evitar que as informações de cartões bancários de seus clientes fossem acessadas por terceiros não autorizados.

Para evitar que haja esse tipo de condenação pelas autoridades públicas, e também para contribuir com a fidelização de seus clientes (que se fidelizam às marcas nas quais confiam), a chave é aplicar os princípios da **“privacidade desde a concepção”**, ou, no inglês, ***“Privacy by Design”***, a todos os processos, sistemas, ferramentas, produtos e serviços de suas empresa.

O que é ***Privacy by Design*?**

O que é *Privacy by Design*?

O *Privacy by Design* é um princípio geral, composto por 7 princípios fundamentais mais específicos, que tem como objetivo antecipar as situações que podem ferir a privacidade das pessoas e evitar que elas aconteçam. O conceito foi desenvolvido por Ann Cavoukian, especialista em privacidade e proteção de dados e *"Information and Privacy Commissioner"* da província de Ontário, Canadá, entre 1997 e 2014. Essas informações foram publicadas no documento denominado "Privacy by Design: os 7 princípios fundamentais". Esse documento foi adotado em 2010 pela *International Assembly of Privacy Commissioners and Data Protection Authorities* e difundido no mundo todo.

Os princípios ajudam organizações a utilizar os dados pessoais de forma segura e devem ser aplicados em novas tecnologias (inclusive no uso de algoritmos, big data e inteligência artificial), ferramentas, processos, sistemas, produtos ou serviços, de qualquer segmento de negócio. Por meio deles, é possível garantir o desenvolvimento tecnológico e a inovação com respeito aos direitos humanos e liberdades fundamentais.

A In Loco desenvolve seus produtos e serviços respeitando a privacidade desde a concepção *(by design)* e acredita que, ao contribuir para que outras organizações também apliquem esses mesmos princípios exigidos pelas legislações de proteção de dados (com destaque para LGPD e GDPR), o mercado de forma geral ganha ao conquistar maior confiança dos seus consumidores e parceiros de negócios (ambos têm maior propensão a se fidelizarem a marcas nas quais confiam) e das autoridades fiscalizadoras.

Dessa forma, vê-se que nunca foi tão importante implementar os 7 princípios fundamentais do Privacy by Design!

Vejamos, a seguir, a definição de cada um desses 7 princípios e como implementá-los, com alguns exemplos práticos da própria In Loco.

Os 7 princípios fundamentais do ***Privacy by Design***

01 Princípio

Proativo e não reativo; preventivo e não corretivo

O Privacy by Design, também referido por meio de sua sigla “PbD”, tem por objetivo antecipar as situações que podem ferir a privacidade das pessoas antes mesmo de elas ocorrerem. O PbD não espera que os riscos à privacidade se materializem, ao contrário: visa impedir que eles ocorram. Isso pode ser feito por meio de medidas técnicas e organizacionais, conforme os exemplos a seguir:

Medida organizacional

Garantir que os diretores e acionistas da sua organização estejam comprometidos em adotar os mais altos padrões de privacidade. Isso significa não apenas buscar a conformidade com as regulamentações em matéria de proteção de dados, mas também proativamente prevenir qualquer prática ou decisão de negócio que possa gerar impactos negativos na privacidade dos usuários de seus produtos e serviços.

Medida técnica

Empregar os melhores esforços preventivos para que os problemas relacionados à privacidade sejam identificados e corrigidos na fase do design (planejamento), antes do desenvolvimento e lançamento de um produto, por exemplo, mediante avaliação sistemática e adoção de alternativas inovadoras e mais protetivas à privacidade.

Como funciona na In Loco?

Privacidade é o framework para tomada de decisões. Estabelecemos uma cultura organizacional voltada para a privacidade tão forte que todos os diretores e acionistas estão dispostos a ir além da conformidade com as leis de proteção de dados. Entendemos que compliance é obrigação e que cumprir os requisitos legais após uma coleta ou compartilhamento de dados que poderia ser evitado, por exemplo, não é sinônimo de privacidade. Asseguramos, portanto, que todos estejam alinhados com essa visão

da empresa e neguem qualquer proposta que contrarie nossa missão de entregar conveniência e privacidade através da computação ubíqua.

Nossa tecnologia foi criada para proteger a identidade das pessoas e impedir o acesso a informações que possam rastrear ou identificar diretamente um indivíduo. Assim, a In Loco não acessa os identificadores estáticos e únicos dos dispositivos (IMEI e MAC) nem contas associadas ao dispositivo (e-mail e telefone). Embora não fosse obrigação legal, com esta medida resguardamos as pessoas de eventuais riscos em caso de incidentes envolvendo dados pessoais.

Também aplicamos técnicas avançadas para pseudonimizar, ou anonimizar (sempre que possível), os dados de identificação indireta, como o Mobile Advertising ID. Agimos também para aprimorar continuamente os nossos esforços com investimento em pesquisa e desenvolvimento em anonimização, mantendo equipe exclusiva para estudar e prototipar técnicas no estado da arte como privacidade diferencial e criptografia homomórfica.

02 Princípio

Privacidade como padrão (by default)

Os dados pessoais devem ser automaticamente protegidos em qualquer sistema de tecnologia da informação (TI) ou prática de negócio de modo que as pessoas não precisem fazer esforços para ter a sua privacidade garantida. Assim, nenhuma ação é necessária por parte do indivíduo para proteger sua privacidade - ela é embutida no sistema, por padrão. Isso pode ser feito por meio de medidas técnicas e organizacionais, conforme os exemplos a seguir:

Medida organizacional

Especificar a finalidade para a coleta, uso, armazenamento e compartilhamento dos dados pessoais antes mesmo de coletá-los. Esse princípio de PbD tem, portanto, estrita relação com o princípio da finalidade, previsto no artigo 6º, inciso I, da LGPD. Se não há propósito legítimo para o tratamento do dado, por padrão deve-se evitar coletá-lo.

Medidas técnicas

(i)

Limitar a coleta apenas àquelas informações estritamente necessárias para as finalidades específicas e relacionadas ao serviço ou produto utilizado pelo usuário. Essa medida está relacionada com princípio da necessidade, consagrado pelo artigo 6º, inciso III, da LGPD.

(ii)

Coletar o mínimo de informação possível e fazer o máximo esforço para não identificar individualmente o titular de dados, coletando apenas os dados relevantes e essenciais ao cumprimento das suas finalidades legítimas. Essa prática tem ligação direta como princípio da minimização previsto no artigo 5, 1, c, do GDPR.

(iii)

Limitar o uso, retenção e divulgação de informações pessoais aos propósitos relevantes identificados e para os quais o indivíduo prévia e expressamente consentiu, quando necessária sua autorização para esses tipos de operações.

Como funciona na In Loco?

Especificamos com clareza qual a finalidade do tratamento das informações pessoais em nossa Política de Privacidade e não coletamos dados sem a permissão prévia e expressa do usuário. Esse consentimento é solicitado antes da coleta de dados - portanto, não há coleta sem o consentimento.

Outro ponto que vale ressaltar é a garantia de efetividade do princípio da necessidade (artigo 6º, inciso III, da LGPD) ou minimização (artigo 5, item 1, alínea c, do GDPR) também por parte dos nossos clientes pois, ao utilizar a tecnologia da In Loco, os apps parceiros não precisam tratar dados de localização - atendendo ao princípio da necessidade e minimização -, e podem focar em seu negócio principal enquanto utilizam tecnologia avançada e se beneficiam da expertise da In Loco para tratar os dados de localização de forma segura e com garantia de privacidade.

Por fim, coletamos o mínimo de informações possível e fazemos o máximo esforço para não identificar individualmente o titular do dado, utilizando apenas os dados relevantes e essenciais ao comprimento das finalidades legítimas autorizadas pelo titular. A In Loco adota técnicas que limitam a coleta de dados a uma média de 2,5 visitas diárias por usuário, e somente se o usuário ativar e mantiver ativada sua geolocalização. A In Loco também impede o processamento de visitas a locais sensíveis - como templos religiosos, hospitais e creches. Portanto, minimizamos o tratamento de dados, garantindo que não haja intrusão nem rastreabilidade dos indivíduos. Os dados pessoais são retidos apenas pelo tempo necessário para cumprir os propósitos declarados e depois destruídos com segurança. Essas são práticas têm por padrão a maior proteção à privacidade.

03 Princípio

Privacidade incorporada ao Design

A privacidade deve ser um componente essencial da funcionalidade de um produto ou serviço disponibilizado para a sociedade e deve ser incorporada nas tecnologias de maneira holística, segura e criativa. Isso pode ser feito da seguinte forma:

Medida organizacional

Adotar uma abordagem sistemática de Privacy by Design baseada em padrões e frameworks reconhecidos, passíveis de revisões e auditorias externas. É importante realizar, sempre que possível, avaliações detalhadas de impacto e risco à privacidade com documentação clara das técnicas de PbD empregadas, medidas tomadas para mitigação de riscos, utilizando métricas objetivas para avaliar o impacto e risco à privacidade.

Medida técnica

Incorporar privacidade ao design dos produtos e serviços, minimizando o impacto da tecnologia na privacidade das pessoas, de forma que as configurações de privacidade não sejam facilmente degradadas por meio de uso, configuração indevida ou erro dos sistemas.

Como funciona na In Loco?

Incorporamos privacidade às nossas tecnologias, operações e arquitetura de informação de maneira holística, integrada e criativa, facilitando a criação de experiências customizadas e humanizadas, voltadas para os usuários de aplicativos. Isso possibilita que os indivíduos (i) recebam ofertas e benefícios que lhes sejam relevantes, no momento certo, e (ii) sejam auxiliados na desburocratização do processo de realização de cadastros, tudo isso sem identificar as pessoas e com total proteção da sua identidade. Sabemos que incorporar privacidade significa, muitas vezes, reinventar as opções existentes, porque as

alternativas não são aceitáveis. É para solucionar esse desafio que o nosso time trabalha todos os dias. O resultado é que a privacidade se tornou um componente essencial da funcionalidade principal dos produtos da In Loco. A privacidade é parte integrante do sistema, sem diminuir a sua funcionalidade – exatamente como afirma Ann Cavoukian, pois a In Loco consegue entregar resultados relevantes para os indivíduos e para a sociedade mantendo os padrões mais elevados de privacidade e proteção de dados.

04 Princípio

Funcionalidade total

O Privacy by Design busca acomodar todos os objetivos e interesses legítimos de uma maneira positiva, com "ganhos em dobro" para os indivíduos e sociedade. Portanto, rejeita abordagens antiquadas que coloquem a privacidade como um cálculo de resultado zero e destaca que, traçando objetivos legítimos, é possível inovar respeitando a privacidade, o que resultará em uma soma positiva. Esse princípio pode ser colocado em prática por meio das seguintes medidas:

Medida organizacional

Acomodar todos os interesses legítimos e positivos, evitando falsas dicotomias, como privacidade x segurança, demonstrando que é possível e muito mais desejável ter ambos. É importante documentar: (i) as decisões e processos que foram rejeitados por ter uma soma zero; (ii) como foi possível atender aos objetivos legítimos que não têm relação com a privacidade, e (iii) quais foram as soluções encontradas para atender esses objetivos com respeito à privacidade.

Medida técnica

Desenvolver tecnologias inovadoras que alcancem resultados reais de soma positiva, onde é possível atender múltiplos interesses além da privacidade. Ann Cavoukian ressalta que as organizações que conseguem superar as escolhas de soma zero, sem comprometer a funcionalidade dos produtos e serviços, conquistam a liderança global em privacidade.

Como funciona na In Loco?

Abraçamos esse princípio e rejeitamos qualquer tipo de dicotomia falsa como "privacidade x segurança", ou "privacidade x receita", pois nossa tecnologia é prova de que é possível garantir os objetivos dos nossos clientes, fomentando o desenvolvimento econômico e a inovação, os objetivos da própria empresa, e, principalmente, entregando os benefícios da tecnologia para as pessoas com respeito aos seus direitos e liberdades individuais, ao incorporar privacidade em nosso modelo de negócio.

05 Princípio

Segurança de ponta-a-ponta e proteção durante todo o ciclo de vida dos dados

O Privacy by Design garante o gerenciamento seguro das informações durante todo o ciclo de vida dos dados. Não deve haver lacuna na proteção dos dados nem na prestação de contas. Isso pode ser garantido com a aplicação das medidas abaixo:

Medida organizacional

Assumir a responsabilidade pela segurança dos dados pessoais durante todo seu ciclo de vida, adotando uma política robusta de Segurança da Informação, bem como as melhores técnicas disponíveis no mercado e os padrões desenvolvidos por organismos reconhecidos.

Medida técnica

Garantir a confidencialidade, integridade e disponibilidade dos dados pessoais durante todo seu ciclo de vida, observando, dentre outras técnicas, criptografia forte, métodos apropriados de controle de acesso e registro de operações envolvendo dados pessoais, além da destruição segura.

Como funciona na In Loco?

Partimos do pressuposto de que não é possível ter privacidade sem segurança, e implementamos as melhores práticas para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais durante todo o seu ciclo de vida.

Dentre outros métodos utilizados na In Loco, aplicamos técnica avançada de pseudonimização do Advertising ID (identificador de publicidade) dos usuários, sendo que o dado original é removido da base e substituído por dados criptografados e hasheados, como descrito na Política de Privacidade.

Esses dois identificadores (hashed

ID e o ID encriptado) são suficientes para suprir os serviços da In Loco e não permitem a identificação dos titulares dos dados. Eles também reduzem, ou até mesmo eliminam, o risco de o Mobile Advertising ID ser capaz de identificar qualquer titular de dados no caso de eventual acesso a esses dados e cruzamento com base de dados de terceiros que contenha o mesmo ID atrelado a outros dados pessoais, como CPF, e-mail, dentre outros.

Assim, na hipótese de qualquer acesso não autorizado ao hashed ID e ao ID encriptado, não será possível o terceiro associar diretamente qualquer titular a tais dados, evitando-se os riscos de danos aos usuários titulares dos dados. A In Loco também aplica técnicas de assinatura criptográfica, que permitem a detecção de quaisquer alterações realizadas nos dados que compõem a sua base.

06 Princípio

Visibilidade e transparência

No PbD, a transparência, diligência e o compliance são fundamentais para estabelecer a responsabilidade e confiança, garantindo aos interessados que a organização está operando de acordo com suas declarações e objetivos e que suas promessas são passíveis de verificação. Esse princípio pode ser colocado em prática da seguinte forma:

Medidas organizacionais

Documentar e disponibilizar as políticas e procedimentos relacionados à privacidade e disponibilizar canal de comunicação para facilitar petições de titulares, parceiros e autoridades públicas. Também é importante estabelecer uma metodologia de auditar terceiros sempre que necessária a transferência de dados pessoais a eles, para verificar se empregam os requisitos de segurança adequados e estabelecer cláusulas contratuais de proteção de dados.

Medidas técnicas

Estabelecer medidas técnicas capazes de monitorar e avaliar continuamente a conformidade com as políticas e procedimentos de proteção de dados.

Como funciona na In Loco?

Prezamos pela transparência, diligência e pelo *compliance*. Nossos sistemas estão sujeitos à verificação independente e temos um time focado exclusivamente em proteção de dados, com orçamento próprio, que conta com a participação de advogados especializados para garantir que todas as normas vigentes e obrigações legais estejam sendo atendidas na prática com monitoramento e melhorias contínuas.

Mantemos informações sobre políticas e práticas relacionadas à proteção de dados pessoais à plena e imediata disposição dos nossos

colaboradores, clientes, parceiros, autoridades e titulares de dados, além de disponibilizarmos canal de comunicação pelo endereço de e-mail **“dpo@inloco.com.br”** para facilitar qualquer requisição.

07 Princípio

Respeito pela privacidade do usuário

Acima de tudo, o *Privacy by Design* exige que as organizações prezem ao máximo pelos interesses do indivíduo, mantendo o usuário no controle dos seus dados pessoais. Os melhores resultados de PbD são aqueles projetados para atender as necessidades dos titulares dos dados, colocando-os em primeiro lugar. As medidas abaixo explicam como isso pode ser feito.

Medidas organizacionais

Capacitar os titulares dos dados a gerenciar ativamente os seus dados pessoais, evitando abuso e uso indevido de seus dados.

Medidas técnicas

Estabelecer padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular de dados a exercer, de forma efetiva, todos os seus direitos assegurados por lei, e que lhes deem absoluto controle sobre os seus dados pessoais.

Como funciona na In Loco?

Empregamos padrões fortes de privacidade, muito acima dos padrões adotados por outras empresas do setor

Além disso, nós da In Loco estamos desenvolvendo um novo portal onde os titulares de dados poderão consultar quais aplicativos têm a tecnologia de localização da In Loco, e conseguirão gerenciar seus próprios dados, o que viabilizará, por meio de avisos apropriados e interfaces amigáveis, o exercício efetivo de seus direitos previstos na LGPD.

Conclusão

Conclusão

Os 7 princípios fundamentais que formam o *Privacy by Design* devem permear toda a tecnologia, processos, cultura e governança da empresa. Em outras palavras: deve ser parte indissociável do seu DNA.

Em um momento de crescente valorização do direito humano à privacidade e de crescente fiscalização na matéria de proteção de dados, as organizações que desejam conquistar a confiança dos seus consumidores e parceiros, além de se destacar de suas concorrentes, devem investir na implementação de medidas técnicas e organizacionais que cubram todos os aspectos do PbD.

Sobre este e-book

Sobre este e-book

Este e-Book faz parte das iniciativas da In Loco para disseminação de uma cultura nacional de proteção de dados e da privacidade. A In Loco busca inserir o Brasil no mapa global da inovação com condições de concorrer com gigantes da economia digital com respeito à privacidade, atendendo ao disposto no artigo 2º, inciso V, da LGPD, que reconhece o desenvolvimento econômico, tecnológico e a inovação como fundamentos da Lei Geral de Proteção de Dados.

Existimos para facilitar a vida das pessoas.

Somos uma empresa de tecnologia que fornece inteligência a partir de dados de localização respeitando a privacidade do consumidor. Para nós, privacidade e conveniência para as pessoas significam mais resultados para as marcas.

Atualmente estamos distribuídos entre Recife, São Paulo, Nova York e São Francisco.

Conheça nossas soluções →

inloco

Conveniência + Privacidade