INCOGNIA

Aplicando o ***Privacy by Design***

Introdução

As leis de proteção de dados em todo o mundo exigem que as organizações implementem medidas administrativas para proteger a privacidade dos usuários. Mas o que isso significa na prática? Como uma empresa pode implementar cada um dos sete princípios fundamentais *Privacy by Design* através de medidas técnicas e organizacionais? Neste e-book, respondemos a estas questões utilizando a Incognia como modelo de implementação do *Privacy by Design*.

Autoras:
Raissa Moura
Ex Head of Privacy, Incognia

Lara Ferraz
Ex Privacy Associate, Incognia

Atualizado por:
Dayana Caroline Costa
Head of Privacy e DPO, Incognia

Designer:
Evandro Truzzi

Incognia
Palo Alto, Outubro, 2023

O que é a *Privacy by Design*?

O que é a *Privacy by Design*?

Privacy by Design é uma abordagem à engenharia de sistemas que dá prioridade à privacidade. É composta por 7 princípios fundamentais cujo objetivo é garantir que a privacidade seja incorporada nos produtos e serviços por padrão. A ideia foi desenvolvida por Ann Cavoukian, uma especialista em privacidade e proteção de dados e antiga Comissária de Privacidade e Informação da província de Ontário, no Canadá, entre 1997 e 2014. Ela publicou este framework no artigo intitulado **"*Privacy by Design*: os 7 princípios fundamentais".**

Estes princípios ajudam as organizações a proteger os dados pessoais e a garantir que a privacidade seja incorporada em todas as ferramentas, processos, sistemas, produtos e serviços de qualquer organização. Graças a estes princípios, o desenvolvimento tecnológico e a inovação podem ser garantidos enquanto os direitos humanos e as liberdades fundamentais são respeitados.

Na Incognia, consideramos fundamental garantir a privacidade dos usuários e a proteção de seus dados. **Um dos valores principais da nossa empresa é respeitar e colocar a privacidade do usuário em primeiro lugar.**

Coletar, armazenar e trabalhar com dados de localização levanta considerações importantes sobre a privacidade do usuário. A Incognia segue os 7 princípios fundamentais da ***Privacy by Design*** para garantir que a privacidade seja incorporada aos seus produtos por padrão, e não como uma reflexão tardia ou uma caixa de seleção de conformidade.

Os 7 princípios fundamentais do *Privacy by Design*

01 Princípio

Princípio Proativo e não Reativo; Preventivo e não Corretivo

O ***Privacy by Design***, ou PbD, visa adotar uma abordagem proativa e preventiva da privacidade. PbD significa que não se deve esperar que ocorram violações da privacidade para agir; pelo contrário, o objetivo é evitar que ocorram. Isto deve ser feito através da adoção de medidas técnicas e organizacionais, como se descreve na seção seguinte.

Medidas organizacionais

Assegure-se de que a diretoria e a liderança da sua organização estão empenhados em manter os mais elevados padrões de privacidade. Isto significa não só o cumprimento dos regulamentos de proteção de dados, mas também a prevenção proativa de qualquer prática ou decisão comercial que possa ter um impacto negativo na privacidade dos usuários dos seus produtos e serviços.

Medidas técnicas

Utilizar os melhores métodos preventivos para que os problemas de privacidade sejam identificados e corrigidos na fase de concepção, antes de qualquer produto ser desenvolvido e lançado. O objetivo é avaliar e implementar sistematicamente alternativas que sejam simultaneamente inovadoras e mais protetoras da privacidade.

Implementação
na Incognia

Privacy by Design
Princípio 01

Um dos nossos principais valores na Incognia é respeitar e colocar a privacidade do usuário em primeiro lugar. A privacidade é a base para nossa tomada de decisões. Estabelecemos uma cultura organizacional focada em respeitar e proteger a privacidade do usuário. Consideramos o cumprimento dos regulamentos governamentais como uma obrigação legal, mas reconhecemos que o cumprimento dos regulamentos não garante necessariamente a privacidade do usuário. Enquanto empresa, estamos dispostos a adotar medidas que vão muito além da conformidade para garantir a privacidade do usuário.

A nossa tecnologia foi concebida para proteger a identidade das pessoas e impedir o acesso a informações que possam localizar ou identificar diretamente um indivíduo. Concentramo-nos em encriptar e proteger os dados pessoais que coletamos e, intencionalmente, não coletamos dados pessoais de identificação direta. Ademais, é incrivelmente difícil tornar totalmente anônimo um conjunto de dados de localização preciso, mas estamos muito perto disso. É importante identificar que dados são capazes de reidentificar um usuário e aplicar-lhes técnicas criptográficas, como a encriptação e o hash.

O nosso objetivo é transformar os dados de localização numa versão ilegível de si próprios, para que ainda possam ser utilizados, com técnicas como a zero knowledge proof, mas que não possam ser lidos sem uma chave de encriptação ou, em certos casos, não possam ser lidos de qualquer forma. Outras técnicas, incluindo a estrutura de conjuntos probabilísticos, a privacidade diferencial e o k-anonimato, aproximam os dados do anonimato total, tornando quase impossível identificar um utilizador individual a partir do conjunto de dados de localização.

02 Princípio

Privacy by default

Os dados pessoais devem ser automaticamente protegidos em qualquer sistema de tecnologias da informação (TI) ou prática comercial, de modo a que as pessoas não precisem fazer qualquer esforço para terem a sua privacidade garantida. Como tal, **não é necessária qualquer ação por parte do indivíduo para proteger a sua privacidade - esta é integrada no sistema por padrão.** Isto pode ser feito através de medidas técnicas e organizacionais, de acordo com os exemplos que se seguem:

Medida organizacional

Especificar a finalidade da coleta, utilização, armazenamento e compartilhamento de dados pessoais, mesmo antes de os coletar. Este princípio de PbD está, portanto, estritamente relacionado com o princípio da finalidade, previsto no Artigo 6, I, da LGPD. Se não existir uma finalidade legítima para o tratamento dos dados, este deve ser evitado por padrão.

Medidas técnicas

(i) Limitar a coleta apenas às informações estritamente necessárias para os fins específicos e relacionados com o serviço ou produto utilizado pelo usuário. Esta medida está relacionada com o princípio da finalidade, estabelecido pelo Artigo 6°, I, da LGPD.

(ii) Coletar a menor quantidade de informação possível e fazer o máximo para não identificar individualmente o titular dos dados, recolhendo apenas os dados relevantes e essenciais para o cumprimento das suas finalidades legítimas. Esta prática está diretamente relacionada com o princípio da necessidade previsto no artigo 6°, III, da LGPD.

(iii) Limitar o uso, armazenamento e divulgação de dados pessoais às finalidades relevantes identificadas e apenas processar dados pessoais de forma lícita, justa e transparente

Implementação na Incognia

Privacy by Design
Princípio 02

Especificamos claramente a finalidade do tratamento dos dados pessoais na nossa Política de Privacidade e a operação de tratamento é lícita, leal e transparente. Também vale a pena mencionar que a Incognia cumpre a garantia de eficácia do princípio da finalidade (artigo 6º, I, da LGPD) e necessidade ou minimização (artigo 6º, III, da LGPD) em nome dos nossos clientes. Ao utilizar a tecnologia Incognia, os clientes não precisam tratar os dados de localização - cumprindo o princípio da necessidade e da minimização - e podem concentrar-se na sua atividade principal, beneficiando da experiência da Incognia para tratar os dados de localização de forma segura e com garantia de privacidade.

Por fim, coletamos o mínimo de informação possível e fazemos todos os esforços razoáveis para não identificar o titular dos dados individualmente, utilizando apenas os dados que são relevantes e essenciais para o cumprimento das finalidades legítimas informadas ao titular dos dados. Os dados pessoais são armazenados apenas durante o tempo necessário para cumprir as finalidades declaradas e depois são eliminados de forma segura. Estas práticas constituem, por padrão, os mais elevados padrões de proteção da privacidade.

03 Princípio

Privacidade incorporada ao design

A privacidade deve ser um componente essencial da funcionalidade de um produto ou serviço disponibilizado à sociedade e deve ser incorporada nas tecnologias de uma forma **holística, segura e criativa.** Isto pode ser feito da seguinte forma:

Medida organizacional

Implementação de uma abordagem sistemática à privacidade, baseada em normas e frameworks reconhecidos, sujeita a revisões e auditorias externas. É importante realizar, sempre que possível, avaliações pormenorizadas do impacto e do risco para a privacidade, com documentação clara das técnicas de privacidade aplicadas, medidas adotadas para mitigação de riscos e uso de métricas objetivas para avaliar o impacto e o risco para a privacidade.

Medidas técnicas

Incorporar a privacidade no design de produtos e serviços, minimizando o impacto da tecnologia na privacidade das pessoas, de modo que as definições de privacidade não sejam facilmente degradadas pela utilização, configuração incorreta ou erro do sistema.

Implementação na Incognia

Privacy by Design
Princípio 03

Incorporamos a privacidade nas nossas tecnologias, operações e arquitetura de uma forma holística, integrada e criativa, facilitando a criação de experiências personalizadas e humanizadas para os usuários dos aplicativos. Isto permite que os indivíduos sejam assistidos na criação de novas contas e na automatização do processo de cadastro, sem identificar pessoas e com total proteção da sua identidade. Sabemos que incorporar a privacidade significa muitas vezes reinventar as opções existentes, porque as alternativas não são aceitáveis. A nossa equipe trabalha todos os dias para resolver este desafio. Como resultado, **a privacidade tornou-se um componente essencial da funcionalidade central dos produtos da Incognia**. A privacidade é uma parte intrínseca dos nossos sistemas, sem diminuir a sua funcionalidade - exatamente como Ann Cavoukian afirmou, porque a Incognia é capaz de fornecer resultados relevantes para os indivíduos e para a sociedade, mantendo os mais elevados padrões de privacidade e proteção de dados.

04 Princípio

Funcionalidade total

O ***Privacy by Design*** procura acomodar todos os objetivos e interesses legítimos de uma forma positiva, com "benefícios duplos" para os indivíduos e a sociedade. Por conseguinte, rejeita abordagens antiquadas que colocam a privacidade como um cálculo de soma zero e salienta que, ao definir objetivos legítimos, é possível inovar respeitando a privacidade, o que resultará em saldo positivo. Este princípio pode ser posto em prática através das seguintes medidas:

Medida Organizacional

Acomodar todos os interesses legítimos e positivos, evitando falsas dicotomias, como privacidade x segurança, demonstrando que é possível e mais desejável ter ambos. É importante registrar: **(i)** as decisões e processos que foram rejeitados por terem um resultado de soma nula; **(ii)** como foi possível cumprir objetivos legítimos que não estão relacionados com a privacidade, e **(iii)** que soluções foram encontradas para cumprir esses objetivos com respeito pela privacidade.

Medidas técnicas

Desenvolver tecnologias inovadoras que alcancem resultados positivos reais, em que possam ser satisfeitos múltiplos interesses para além da privacidade. Ann Cavoukian salienta que as organizações que conseguem ultrapassar as escolhas de soma nula sem comprometer a funcionalidade dos produtos e serviços, alcançaram a liderança global em matéria de privacidade.

Implementação na Incognia

Privacy by Design
Princípio 04

Adotamos este princípio e rejeitamos qualquer tipo de falsa dicotomia como "privacidade x segurança", ou "privacidade x receita", porque a nossa tecnologia é a prova de que é possível garantir os objetivos dos nossos clientes, fomentando o desenvolvimento econômico e a inovação, os objetivos da própria empresa e, acima de tudo, proporcionando os benefícios da tecnologia às pessoas com respeito pelos seus direitos e liberdades individuais, incorporando a privacidade no nosso modelo de negócio.

05 Princípio

Segurança e proteção de ponta-a-ponta

O ***Privacy by Design*** garante a gestão segura da informação ao longo de todo o ciclo de vida dos dados. Não deve haver qualquer lacuna na proteção dos dados ou na responsabilização. Isto é algo que pode ser garantido através da implementação das medidas abaixo:

Medida Organizacional

Aceitar a responsabilidade pela segurança dos dados pessoais ao longo do seu ciclo de vida, adotando uma Política de Segurança da Informação forte, bem como as melhores técnicas disponíveis no mercado e as normas desenvolvidas por organizações reconhecidas.

Medidas Técnicas

Assegurar a confidencialidade, integridade e disponibilidade dos dados pessoais ao longo do seu ciclo de vida, utilizando, entre outras técnicas, uma encriptação forte, métodos adequados de controle de acesso e de registo de operações que envolvam dados pessoais, bem como sua deleção de forma segura.

Implementação na Incognia

Privacy by Design
Princípio 05

Baseamos a nossa abordagem no pressuposto de que a privacidade não é possível sem segurança e implementamos as melhores práticas para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais ao longo do seu ciclo de vida. Entre outros métodos utilizados na Incognia, aplicamos uma técnica avançada para pseudonimizar IDs e substituí-los por dados encriptados e com hash, tal como descrito na nossa Política de Privacidade.

Os IDs hasheados são suficientes para fornecer os serviços da Incognia e não permitem a identificação dos titulares dos dados. Assim, no caso de qualquer acesso não autorizado a nossa base de dados, não será possível ao terceiro associar diretamente qualquer usuário a esses dados.

A Incognia também aplica uma técnica avançada para pseudonimizar os dados de localização. O nosso objetivo é transformar os dados de localização numa versão ilegível de si mesmos, para que ainda possam ser utilizados, com técnicas como zero *knowledge proof*, mas não possam ser lidos sem uma chave de encriptação ou, em certos casos, não possam ser lidos de qualquer forma. Outras técnicas, incluindo a estrutura de conjuntos probabilísticos, a privacidade diferencial e o k-anonimato, aproximam os dados da anonimização total, tornando quase impossível identificar um usuário individual a partir do conjunto de dados de localização. Por fim, é importante ressaltar que a Incognia segue as melhores práticas internacionais de segurança e é auditada anualmente para conformidade com os padrões da SOC 2, tipo II.

06 Princípio

Visibilidade e transparência

Em PbD, a transparência, a diligência e a conformidade são fundamentais para estabelecer a responsabilidade e a confiança, assegurando às partes interessadas que a organização está operando de acordo com as suas declarações e objetivos e que as suas promessas podem ser verificadas. Este princípio pode ser posto em prática da seguinte forma:

Medida Organizacional
Documentar e disponibilizar políticas e procedimentos relacionados com a privacidade e disponibilizar um canal de comunicação para facilitar requisições de titulares de dados, parceiros e autoridades públicas. É também importante estabelecer um procedimento de auditoria a terceiros sempre que seja necessária a transferência de dados pessoais, para verificar se estes 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 o cumprimento dos requisitos de segurança.

Implementação na Incognia

Privacy by Design
Princípio 06

Temos orgulho da nossa transparência, diligência e conformidade. Os nossos sistemas estão sujeitos a verificações independentes e temos uma equipe focada exclusivamente na proteção de dados, que conta com a participação de advogados especializados para garantir que todos os regulamentos e obrigações legais em vigor sejam cumpridos na prática com monitoramento e melhoria contínua. Mantemos informações sobre políticas e práticas relacionadas à proteção de dados pessoais à plena e imediata disposição de nossos colaboradores, clientes, parceiros, autoridades e titulares de dados, bem como disponibilizamos um canal de comunicação através de endereço de e-mail.

07 Princípio

Respeito pela privacidade do utilizador Princípio

Acima de tudo, o ***Privacy by Design*** exige que as organizações valorizem os interesses dos indivíduos, mantendo o usuário no controle de seus dados. Os melhores resultados de ***Privacy by Design*** são os concebidos para satisfazer as necessidades dos titulares dos dados, colocando-os em primeiro lugar. As medidas abaixo explicam como isto pode ser feito.

Medida organizacional

Permitir que os titulares dos dados façam uma gestão ativa dos seus dados pessoais, evitando abusos e utilizações indevidas dos mesmos.

Medidas técnicas

Estabelecer procedimentos e políticas de proteção de dados fortes, avisos adequados e interfaces de fácil utilização que permitam ao titular dos dados exercer adequadamente todos os seus direitos assegurados por lei e que lhe dêem controle real sobre os seus dados pessoais.

Implementação na Incognia

Privacy by Design
Princípio 07

Utilizamos procedimentos e políticas de privacidade fortes, muito acima dos padrões adotados por outras empresas do setor. Aplicamos ***privacy by design*** olhando sempre para os interesses do indivíduo.

Acreditamos que o valor da tecnologia é servir à humanidade e que as pessoas não devem abdicar da sua privacidade para ter comodidade, por isso respeitamos e colocamos a privacidade do usuário em primeiro lugar. Não queremos saber quem é o nosso usuário e não coletamos quaisquer dados que possam identificar diretamente o usuário.

Conclusão

Os 7 princípios fundamentais que moldam a *Privacy by Design* devem estar presentes em toda a tecnologia, processos, cultura e governança de uma empresa. Em outras palavras, o PbD deve ser uma parte intrínseca do seu DNA.

Neste momento de crescente valorização do direito humano à privacidade e de crescente vigilância em matéria de proteção de dados, as organizações que pretendam ganhar a confiança dos seus consumidores e parceiros, para além de se destacarem dos seus concorrentes, devem investir na implementação de medidas técnicas e organizacionais que abranjam todos os aspectos do PbD.

A Incognia coloca a privacidade do usuário em primeiro lugar e incorporou a ***Privacy by Design*** na base da empresa e dos seus produtos.

Sobre este e-book

Este e-Book faz parte das iniciativas da Incognia para promover a proteção de dados e a privacidade.

Colocamos a privacidade do usuário em primeiro lugar

A **Incognia** é uma empresa de identidade baseada em geolocalização com soluções para verificação de usuários e segurança de contas em toda a jornada digital, desde a abertura até autenticação e validação de eventos sensíveis. Com mais de uma década de experiência em tecnologia de geolocalização, a nova abordagem da Incognia combina a inteligência dos dispositivos e análise do comportamento de localização para proporcionar uma experiência de uso sem fricção. A Incognia entrega avaliações de risco personalizáveis e acionáveis desde o dia um para potencializar a estratégia de empresas na prevenção de fraudes, otimização de receita, proteção de usuários e construção de confiança com seus consumidores. Estamos sediados em Palo Alto, nos Estados Unidos, com equipes na área da Baía de São Francisco, Nova York e Brasil.

A missão da Incognia é facilitar experiências digitais através da combinação inigualável de segurança, privacidade e conveniência, por isso somos uma empresa *Privacy by Design.* Para saber mais, acesse nossas políticas.

Saiba mais sobre nossas soluções ⟶