AGILIDADE NA PRIVACIDADE

DICAS PRÁTICAS

ZOOX SMART DATA INCOGNIA™ Sympla

Este ebook foi elaborado pela Zoox Smart Data, Incognia e Sympla, com o objetivo de registrar, de forma mais detalhada, o conteúdo compartilhado no Data Privacy Day 2021 organizado em conjunto pelas três empresas. Também incluímos a participação especial de Michelle Chibba, Pesquisadora Associada do Privacy and Big Data Institute da Ryerson University (Canadá).

Agradecimentos especiais à International Association of Privacy Professionals (IAPP), Exin e Global Institute of Law and Innovation pelo apoio institucional ao evento de Data Privacy Day 2021.

Março, 2021.

01

INTRODUÇÃO

O dia 28 de janeiro, conhecido como Data Privacy Day, é uma data comemorada em mais de 50 países. Foi criada em abril de 2006 pelo Conselho da Europa, sendo que a primeira comemoração oficial ocorreu em janeiro do ano seguinte, como European Data Protection Day (Dia Europeu da Proteção de Dados). Em 2009, os Estados Unidos também adotaram formalmente o dia 28 de janeiro como National Data Protection Day (Dia Nacional da Proteção de Dados). No Brasil, essa data ainda não consta nos calendários oficiais, mas pelo menos desde janeiro de 2018 vem sendo comemorada pela comunidade de proteção de dados, que organiza eventos e ações de conscientização na semana do dia 28.

A escolha do dia 28 de janeiro tem origem na data de assinatura da "Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal" (conhecida como Convenção 108)**, que ocorreu nesse dia no ano de 1981. O objetivo da Convenção é proteger o direito à privacidade considerando o fluxo crescente de processamento automático de dados pessoais em âmbito internacional.**

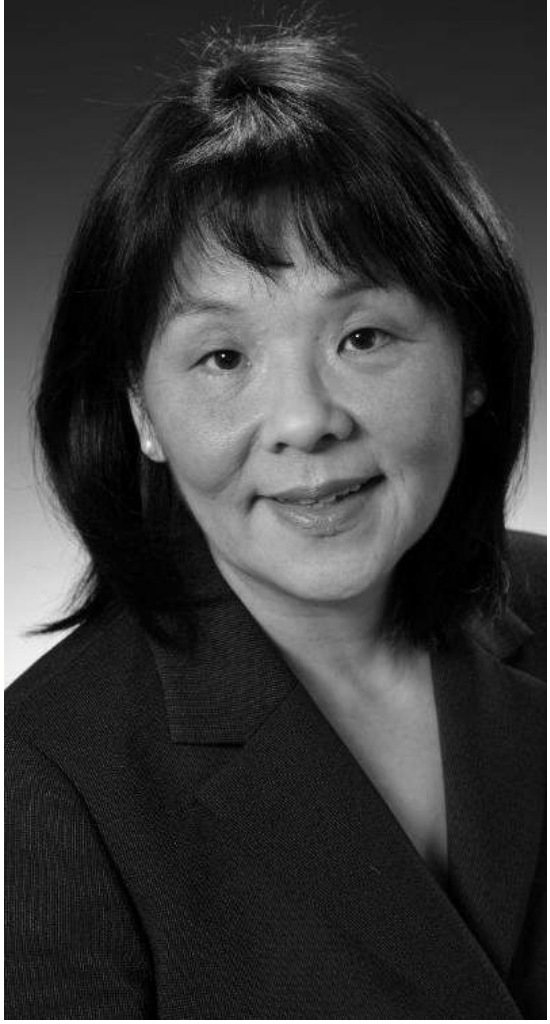
Em um mundo interconectado, essa data tem por objetivo promover a conscientização sobre o tema da privacidade, divulgar e compartilhar melhores práticas e fortalecer a cultura de proteção de dados pessoais - essencial para o desenvolvimento econômico e tecnológico e para a inovação. A Zoox, Incognia e Sympla, empresas de tecnologia e inovação, têm por princípio a colaboração e acreditam que conhecimento e boas práticas em privacidade e proteção de dados devem ser compartilhados. Juntos, podemos elevar o nível de maturidade dos programas de governança em privacidade nas organizações. Os agentes de tratamento ganham e a sociedade também - todo mundo ganha. Vamos juntos!

Zoox - Incognia - Sympla

02

Michelle Chibba

Dia Internacional da Privacidade 2021: uma perspectiva pessoal



De alguma forma, neste ano, o Dia Internacional da Privacidade 2021 ressoa muito mais, dada a pandemia global que enfrentamos. A Dra. Ann Cavoukian fala frequentemente em equiparar privacidade com liberdade e democracia. Embora eu entendesse a perspectiva dela, eu só sabia através de sua narrativa. Nascida e residente no Canadá, felizmente, nunca tive que enfrentar o medo de ter meu direito à privacidade tirado de mim. Seja percebido ou real, foi o "lock down" ou o estado de emergência, e medidas do "fique em casa" que me deram um vislumbre do verdadeiro significado da privacidade.

Quando essas ordens do governo foram introduzidas pela primeira vez em janeiro de 2021 na província de Ontário, Canadá, houve muita confusão em torno da aplicação ("enforcement") dessas ordens pela polícia. As histórias giravam na mídia e nas mídias sociais sobre as invasões extremas em nossas vidas. Alguns exemplos canadenses receberam atenção mundial, como um casal de Montreal que se esforçou muito enquanto caminhava ao mesmo tempo em que "seguia" a lei; outro incidente envolvendo uma reclamação contra uma festa doméstica que acabou em uma briga gravada em vídeo com a polícia local. Embora esses exemplos sejam de uma província diferente, havia perguntas suficientes sendo feitas pelos residentes aqui, o que fez com que o procurador-geral de Ontário saísse com uma declaração de esclarecimento.

Um jornal popular relatou: Um porta-voz do procurador-geral da província disse que as novas ordens não dão à polícia o poder de entrar nas casas para verificar a conformidade, nem os oficiais podem parar os motoristas ou perguntar aos pedestres para onde estão indo. "Por si só, estar fora não é evidência suficiente de um descumprimento da ordem de permanência em casa", disse Stephen Warner.

Especialista internacional em privacidade, presta consultoria (incluindo treinamento de funcionários) para organizações que desejam modernizar sua abordagem de privacidade ou de governança de informações. É instrutora do curso de Gestão de Privacidade e Roubo de Identidade do Seneca College (Toronto, Canadá), que faz parte do programa de Fintech da faculdade. Também é co-instrutora, com a Dra. Ann Cavoukian, no curso online "Privacy by Design: the global privacy framework", oferecido pela Chang School na Ryerson University, Toronto, Canadá. Foi nomeada editora de projetos do Comitê ISO (PC317) para o recém-estabelecido padrão internacional de Privacy by Design para bens de consumo e serviços, a norma ISO 31700. Foi Diretora do Departamento de Política e Projetos Especiais no Escritório do Comissário de Informação e Privacidade de Ontário, Canadá (IPC), enquanto a Dra. Ann Cavoukian foi a Comissária. Seu departamento conduziu educação pública e conscientização, e conectou com uma ampla gama de partes interessadas para apoiar o papel de liderança da Dra. Cavoukian em endereçar, proativamente, questões de privacidade e tecnologia que afetam o público, também conhecidas como Privacy by Design.

“Os trabalhadores também não são obrigados a ter provas de seu empregador de que estão viajando para ou de seu local de trabalho.” Este mesmo relato da mídia inclui uma declaração dos Chefes de Polícia de Ontário: A Associação de Chefes de Polícia de Ontário confirmou que os oficiais não vão parar as pessoas apenas para perguntar sobre as ordens de permanência em casa. “Os indivíduos não podem ser obrigados a explicar por que estão fora de sua residência”, disse o porta-voz Joe Couto. “Quando as pessoas entenderem que nossos oficiais não vão procurar pessoas que por acaso estejam fora como eu, passeando com meu cachorro, acho que vão se sentir muito melhor. Simplesmente entrar no carro e ir ao supermercado imaginando se verão as luzes [da polícia] nos retrovisores, isso não vai acontecer.” Que alívio! Mas posso assegurar que, durante esses vários dias antes deste esclarecimento, senti medo e ansiedade ao questionar minha liberdade e perda de privacidade. Culpe os efeitos de um semi-isolamento de 11 meses seguindo regras rigorosas de saúde pública para conter o vírus ou passar muito tempo ouvindo relatórios pandêmicos para garantir que eu permaneça atualizada e informada – tudo o que posso dizer é que o significado da privacidade e, da mesma forma, do Dia Internacional da Privacidade, assumiu um novo sentido para mim este ano – a importância da privacidade para a liberdade agora faz parte da minha narrativa.

03

Dr. Ann Cavoukian, Ph.D.

"A proteção de dados pessoais é essencial: lidere o caminho com Privacy by Design"

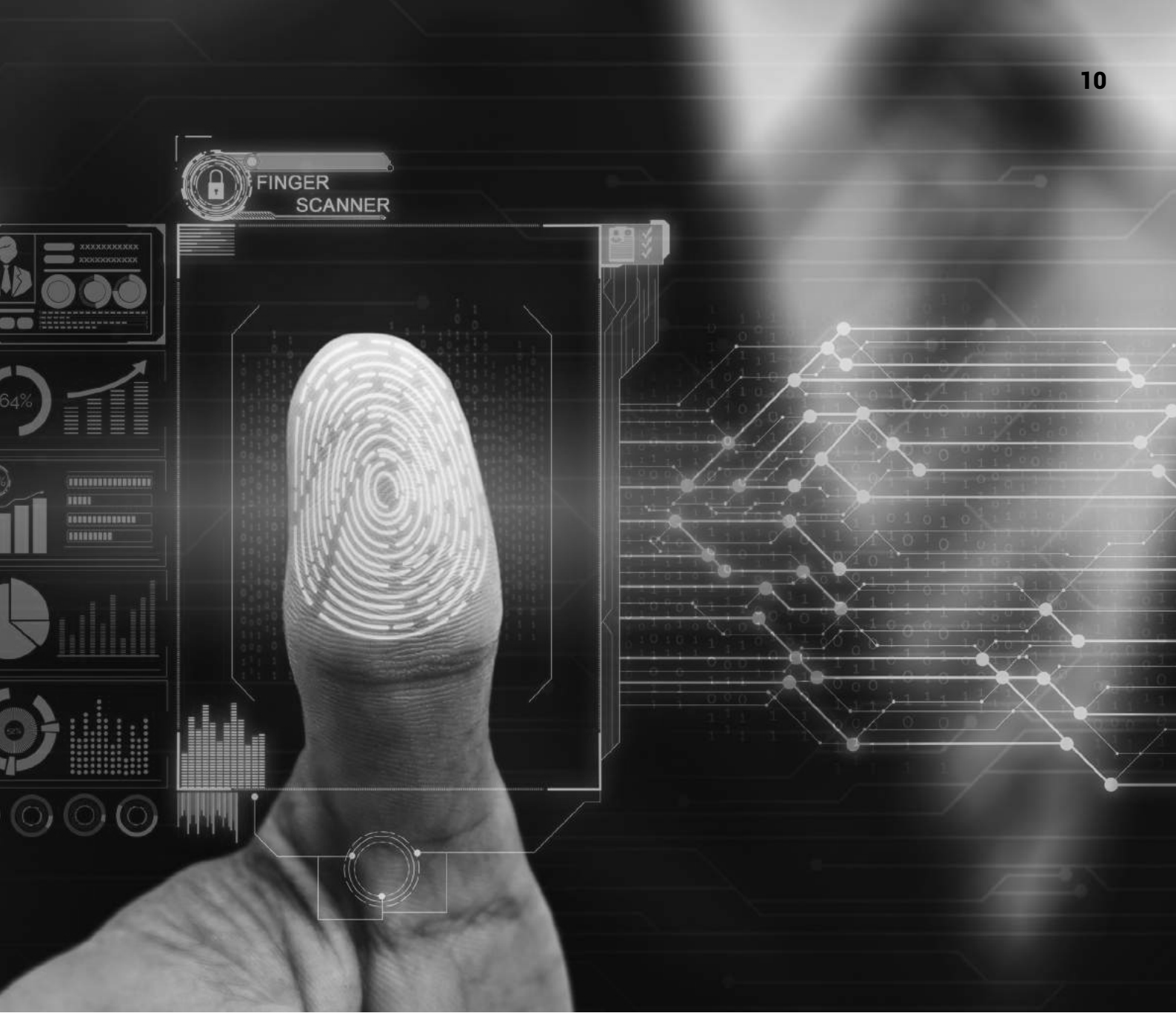
Vamos dissipar os mitos: privacidade não significa "ter algo a esconder". Privacidade é diferente de sigilo, é ter controle pessoal. É garantir a liberdade de escolha, a autodeterminação informativa, e o contexto, nesses casos, é fundamental.

A privacidade é essencial para a liberdade, uma vez que ela é a condição necessária para a prosperidade e bem-estar social. A inovação, a criatividade e a prosperidade resultantes de uma sociedade requerem liberdade, e a privacidade é a essência da liberdade.

Afinal, sem privacidade, os direitos humanos e individuais, os direitos de propriedade e as liberdades civis (os motores conceituais de inovação e criatividade) não poderiam existir de uma maneira significativa.
Além disso, a vigilância é a antítese da privacidade, e uma de suas consequências negativas é justamente limitar a capacidade cognitiva de uma pessoa para a inovação e a criatividade. É por esse motivo que a Privacidade por Design (Privacy by Design) é tão importante e tem sido adotada como um padrão internacional. Precisamos dissipar o mito que privacidade não coexiste com inovação, pois a verdade é que esta depende da primeira para existir.

Sendo assim, em 2010, uma resolução internacional reconheceu o conceito de "Privacy by Design" como um componente essencial à proteção da privacidade. Isso é muito importante porque a maioria das violações de privacidade permanece não detectada, e os reguladores só têm conhecimento da ponta do iceberg. Dessa forma, o compliance regulatório, por si só, é insustentável como modelo único para garantir o futuro da privacidade. Além disso, os custos de uma abordagem reativa para violações de privacidade em empresas é alto, com ações judiciais coletivas, danos à marca e perda de confiança do consumidor.

Reconhecida como uma das maiores especialistas em privacidade do mundo. Atualmente, é diretora executiva do Privacy and Big Data Institute da Ryerson University. Foi nomeada como Information and Privacy Commissioner de Ontario, Canada, em 1997, servindo por três mandatos e elevando o órgão regulador recém-criado para uma agência de primeira classe, conhecida em todo o mundo por sua liderança e inovação de ponta. Criadora do Privacy by Design, um framework que busca incorporar a privacidade de forma proativa às especificações de design de tecnologias de informação, infraestrutura de rede e práticas de negócios, de modo a atingir a proteção mais forte possível.



Para tanto, o principal artigo sobre os princípios fundamentais do Privacy by Design já está disponível em 40 idiomas. Basicamente, podemos resumir os princípios em dois fundamentos:

1. Evite o surgimento de danos: Seja proativo!

2. Elimine os modelos de soma zero! Livre-se dos modelos de ganha-perde e soma zero. Passe a usar o modelo de soma positiva e descubra o poder do "E"! Crie um cenário onde todos ganham, em detrimento de uma abordagem de "ou/ou" ("vs.") envolvendo compensações desnecessárias e falsas dicotomias. Ou seja, substitua o "vs." por "e".

Os 7 princípios fundamentais que compõem o framework de Privacy by Design são:

1. **Proativo não reativo: preventivo, não corretivo;**
2. **Privacidade como configuração padrão;**
3. **Privacidade incorporada ao design;**
4. **Funcionalidade total: soma positiva, não soma zero;**
5. **Segurança de ponta-a-ponta: proteção total do ciclo de vida;**
6. **Visibilidade e transparência: mantenha aberto;**
7. **Respeito pela privacidade do usuário: mantenha centrado no usuário.**

A aplicação desses princípios se tornam ainda mais importante em 11 áreas, quais sejam:

a) Câmeras CFTV / Vigilância em sistemas de trânsito de massa;

b) Biometria usada em cassinos e instalações de jogos;

c) Medidores inteligentes e a rede inteligente;

d) Comunicações Móveis;

e) Near Field Communications;

f) RFIDs (identificação por radiofrequência) e tecnologias de sensores;

g) Redesenhando a geolocalização por IP;

h) Assistência Médica Domiciliar Remota;

i) Big Data e análise de dados;

j) Vigilância de proteção à privacidade;

k) SmartData.

Desde a sua criação, o Privacy by Design conquistou muito espaço ao redor do globo. Na carta do Japan Institute for Promotion of Digital Economy and Community (JIPDEC), de 28 de maio de 2014, o Privacy by Design foi considerado um dos conceitos mais importantes pelos membros do Instituto Japonês. As empresas do setor privado do Japão disseram que

era necessário insistir no princípio de Soma Positiva, não Soma Zero, e aplicar o Privacy by Design.

Em 2018, o General Data Protection Regulation (GDPR) entrou em vigor, não apenas fortalecendo e unificando a forma como a proteção de dados pessoais é regulamentada, mas também concedendo aos indivíduos maior controle sobre seus próprios dados. A linguagem de "Privacidade / Proteção de Dados por Design" e "Privacidade como o Padrão" apareceu pela primeira vez em um estatuto de privacidade, que foi aprovado recentemente na UE.

Existem várias semelhanças entre o Privacy by Design e o GDPR.

O próprio Regulamento faz diversas referências ao framework no artigo 25 e em outros. O Information Age (24/09/2015) destaca que o Privacy by Design teve uma grande influência em especialistas em segurança e reguladores e que "não é exagero dizer que, se você implementar o PbD, terá dominado o GDPR."

O Comissário de Privacidade do Canadá também destaca no 2016-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act:

"As organizações também devem ser mais transparentes e responsáveis por suas práticas de privacidade. Porque elas conhecem melhor o seu negócio, é justo que esperemos que elas encontrem formas eficazes, dentro do seu próprio contexto específico, para proteger a privacidade dos seus clientes, nomeadamente através da integração de abordagens como o Privacy by Design."

Existe também uma Certificação de Privacy by Design para empresas, relançada em parceria com consultoria global, que consiste na realização de uma auditoria de todas as práticas para ver se estão atendendo os 7 princípios. Isso faz com que as pessoas confiem nos relacionamentos de negócios, mantém a fidelidade dos clientes e gera vantagem competitiva porque as pessoas valorizam a privacidade.

Certamente, o GDPR foi muito importante para a consolidação do PbD e escalou os seus princípios a um nível global, conforme destaquei no artigo Privacy By Design - Ready For Takeoff (2016):

"A aprovação do GDPR da UE (...) está trazendo o PbD à mente conforme as operações pessoais são ajustadas para cumprir as novas regras do GDPR (...) Resumindo, o GDPR já deu ao PbD nova visibilidade e vigor. A mudança de soma positiva está a caminho - não apenas para a Europa, mas em todo o mundo."

No caminho dessa soma positiva, criei, juntamente com outros profissionais, o Global Privacy and Security by Design, entidade que trabalha junto aos setores privado e público para promover inovação com privacidade, segurança e interesses da organização. Em outras palavras, a nova organização foi criada para educar governos e empresas sobre como desenvolver políticas e tecnologias em que privacidade, segurança pública e Big Data trabalhem juntos para resultados de soma positiva (ganha-ganha).

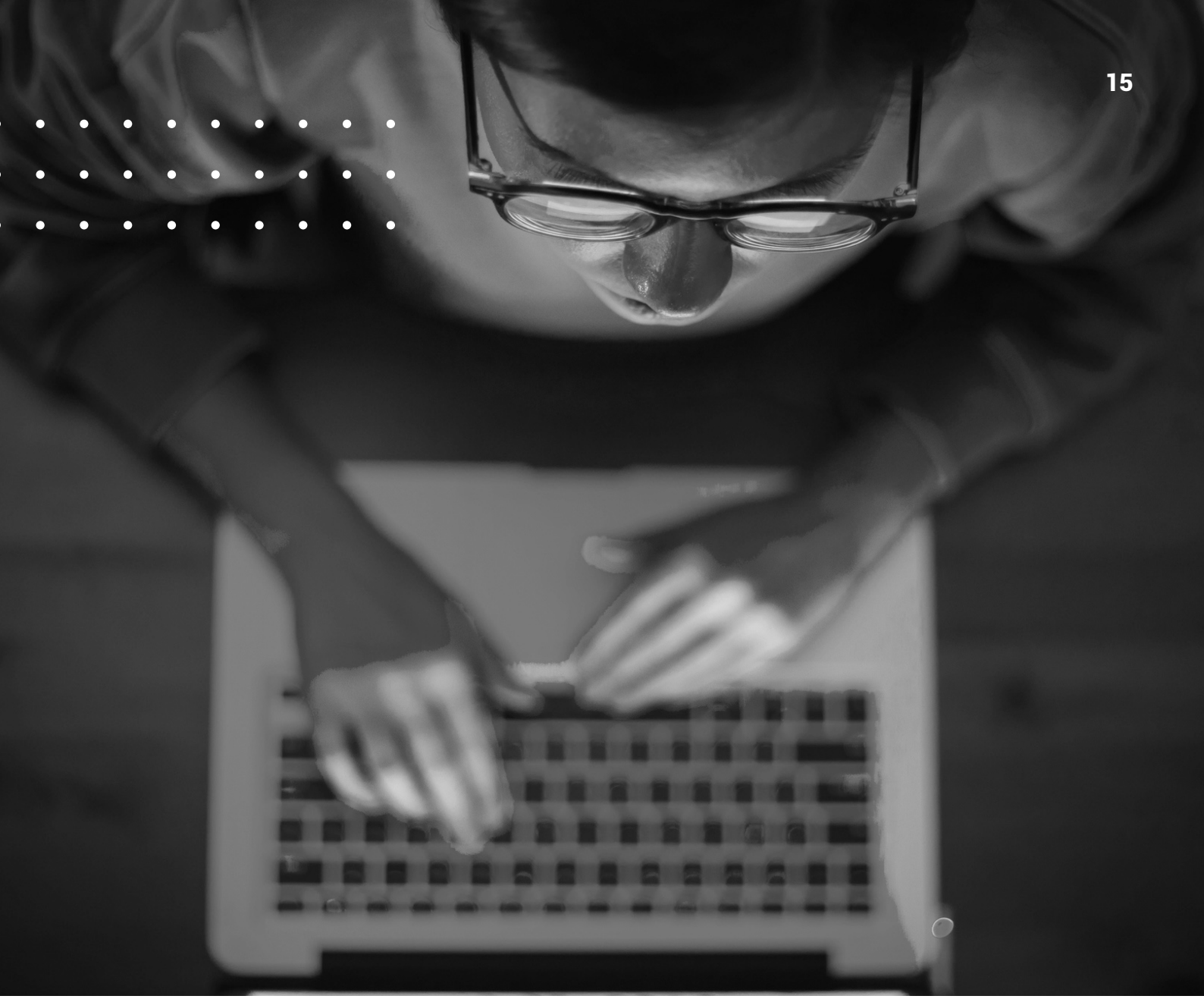
Os membros fundadores incluem:

- Darren Entwistle, CEO da TELUS Inc.;
- Michael Chertoff, 2º Secretário de Segurança Interna dos EUA;
- Gilles de Kerchove, Coordenador da UE de luta Antiterrorista;
- Greg Wolfond, CEO da SecureKey;
- Joseph Simitian, Supervisor do Condado de Santa Clara, CA e ex-presidente do Comitê de Privacidade do Senado Estadual da Califórnia.

A organização desenvolve pesquisas e possui uma extensão recém-criada de Privacy by Design, com foco em privacidade e segurança!

Também temos um curso online de Privacy by Design: The Global Privacy Framework, promovido por meio da Ryerson University, que tem por objetivo aprofundar o estudo do Privacy by Design e suas aplicações, bem como criar um espaço de diálogo entre profissionais de diversos países que aplicam o framework.

Existe uma necessidade premente de abandonar a "soma zero" e as proposições "ou/ou" ou que envolvam um interesse "versus" outro, como "privacidade vs. segurança pública". Precisamos alterar essa mentalidade para uma abordagem de "soma positiva", duplamente habilitadora, com a privacidade e a segurança pública juntas, por exemplo.



Em resumo:

• Os riscos de privacidade e segurança são melhor gerenciados incorporando, de forma proativa, os princípios de Privacy by Design, evitando incidentes com dados pessoais e danos aos titulares.

• Foco na prevenção: É muito mais fácil e mais econômico criar privacidade e segurança desde o início, em vez de depois do ocorrido, refletindo o tratamento mais ético dos dados pessoais.

• Abandone o pensamento de soma zero: Adote sistemas duplamente habilitadores: privacidade e segurança; privacidade e utilidade de dados.

• Seja esperto: Lidere com privacidade desde a concepção (Privacy by Design), não privacidade por acaso (privacy by chance) ou, pior, privacidade por desastre (privacy by disaster)!

04

Dr. Anna Zeiter, LL.M.

"Como gerir um time global de privacidade durante uma pandemia"

Eu lidero o time de privacidade do Ebay e tenho por volta de trinta pessoas trabalhando comigo, o que já era desafiador antes da pandemia. Antes da pandemia, eu estava viajando bastante para garantir que o time estivesse reunido, engajado. Também despendia muito tempo participando de conferências, encontrando com colegas, como também fazendo reuniões com autoridades e órgãos reguladores, buscando entender os novos desafios do mercado de marketing. Como vocês sabem, privacidade é um assunto global: o GDPR entrou em vigor dois anos atrás, e temos agora também a LGPD no Brasil, CCPA e o CPRA chegando na Califórnia, várias leis de privacidade surgindo ao redor do mundo.

Como você pode assegurar, como líder de uma equipe global, que você está fazendo uma boa gestão num ambiente que muda tanto e durante uma pandemia, onde todo mundo tem que trabalhar de casa? Para abordar esse tema, eu vou trazer 4 (quatro) itens de como fazer a gestão de uma equipe internamente. Provavelmente, todos vocês passam pelos mesmos desafios com o trabalho na modalidade home office, utilizando ferramentas como o Zoom. No meu caso, tenho uma equipe com seis fusos horários diferentes, de diferentes cidades. Então, como assegurar que as pessoas estão trabalhando bem, juntas, principalmente agora que já faz quase um ano do início da pandemia? Você deve conhecer todos os mecanismos para assegurar que se conectem ao Zoom, deve ter reuniões e cafés através do Zoom, isso é padrão. Mas, como profissional de privacidade, também é importante estar bem conectado à empresa e com importantes stakeholders (interessados) de outras equipes.

Chief Privacy Officer da eBay Inc. e membro da Diretoria da International Association of Privacy Professionals (IAPP). Membro do Comitê da Global Tech DPO Network na Irlanda e membro do Grupo de Trabalho de Transformações Digitais do Fórum Econômico Mundial, especialmente co-liderando o fluxo de trabalho Business of Data & Data Valuation. Graduada com distinção pelo Programa LL.M em Direito, Ciência e Tecnologia da Stanford Law School. De 2009 a 2013, trabalhou como advogada em dois escritórios de advocacia internacionais em Hamburgo, especializada em proteção de dados, TI e direito do comércio eletrônico. Ph.D. sobre liberdade de expressão e direito da mídia pela Universidade de Hamburgo. Anna Zeiter regularmente dá palestras em conferências internacionais de proteção de dados, leciona em universidades (por exemplo, na Universidade de Berna e na Universidade de Göttingen) e publica artigos sobre questões atuais de proteção de dados, por exemplo, no Stanford Transatlantic Technology Law Forum, na European Data Protection Law Review e em outras revistas internacionais.

A privacidade geralmente é a aranha que está na teia, porque a privacidade toca muitas outras áreas. Tem relação com dados, e estes, na maior parte das empresas, estão em toda a parte. Antes da pandemia, a maior parte do meu tempo internamente era gasto no escritório, encontrando pessoas, realizando reuniões, conversando com pessoas na lanchonete, ouvindo as pessoas falarem sobre projetos novos. Então, o que eu posso fazer como uma profissional de privacidade, é realizar uma boa conexão com outras pessoas. É muito importante você saber tudo que está acontecendo.

Na equipe de marketing, por exemplo, você precisa entender como está a publicidade, enquanto que, no RH, você precisa saber o que estão planejando - porque todas essas equipes lidam com dados pessoais e, como uma profissional de privacidade, é muito importante estar bem conectada com diferentes equipes da empresa e assegurar que você sabe o que está acontecendo. Se você não sabe o que está acontecendo, é muito difícil assegurar que a empresa esteja em conformidade com todas essas leis novas ao redor do globo. Isso foi realmente um desafio para a minha equipe, por isso eu sei o quanto é importante ser proativa com os diversos stakeholders.

Antes da pandemia eu podia encontrar na cafeteria o diretor responsável pela área Tributária, o diretor de Recursos Humanos - tomávamos café juntos, batíamos um papo rápido para entender o que estava acontecendo na empresa. Agora, eu tive que mudar a minha mentalidade e começar a ser muito proativa.

Passei a realizar calls com essas pessoas da empresa e falei para minha equipe que aquilo que fazíamos tomando um café agora precisamos fazer de uma forma mais estruturada, pois, se ficarmos acomodados, não vamos saber o que está acontecendo na empresa em termos de privacidade. Então, essa foi a parte da mudança interna.

Em relação à atuação externa, consistente no relacionamento com os parceiros, antes da pandemia as pessoas aproveitavam uma conferência para, durante o intervalo, tomar um cafezinho com seus pares, ouvir as notícias, saber que outras empresas enfrentavam os mesmos problemas e como lidavam com determinadas situações. Ao encontrar essas pessoas, você sentia aonde o mercado estava indo e isso é muito importante para uma organização - entender para que lado as empresas estão indo -, porque a maior parte das leis, como a LGPD, é nova e, às vezes, você não sabe como interpretar determinados assuntos.

É comum nos perguntarmos se estamos fazendo demais ou de menos. Por isso, é necessário entender como o mercado está se direcionando. Então, no passado era assim, e agora continua sendo muito importante entender como as outras empresas estão atuando. Mas, não está sendo fácil, porque, como vocês sabem, essas conversas não são online. Portanto, agora eu também entendo que eu preciso ser muito mais proativa e, às vezes, mandar um recado para alguém que eu encontrei, aleatoriamente. Assim, eu mando um e-mail ou mensagem no LinkedIn perguntando se podemos bater um papo de dez minutos e, na minha experiência, a maioria sente a mesma coisa. Ficam super felizes com a abordagem, querem se conectar online e querem também ter certeza de que estão entendendo o que os outros estão fazendo.

Como último ponto, gostaria de abordar a relação externa com os reguladores. Como todas essas leis são mais ou menos novas (o GDPR tem aproximadamente três anos, a LGPD é nova, o CCPA ainda tem um ano apenas e o CPRA também está vindo), é muito importante continuar conectado aos reguladores. Antes da pandemia, quando eu ia para conferências, se eu via um regulador ou autoridade, eu pensava que talvez pudesse ter a oportunidade de fazer uma pergunta depois da apresentação, ou poderia tomar um cafezinho e fazer uma pergunta como, por exemplo:

“Não entendi tal regra ou essa demanda jurídica. Será que você pode me ajudar a entender como posso implementar isso? Esta abordagem é correta?”

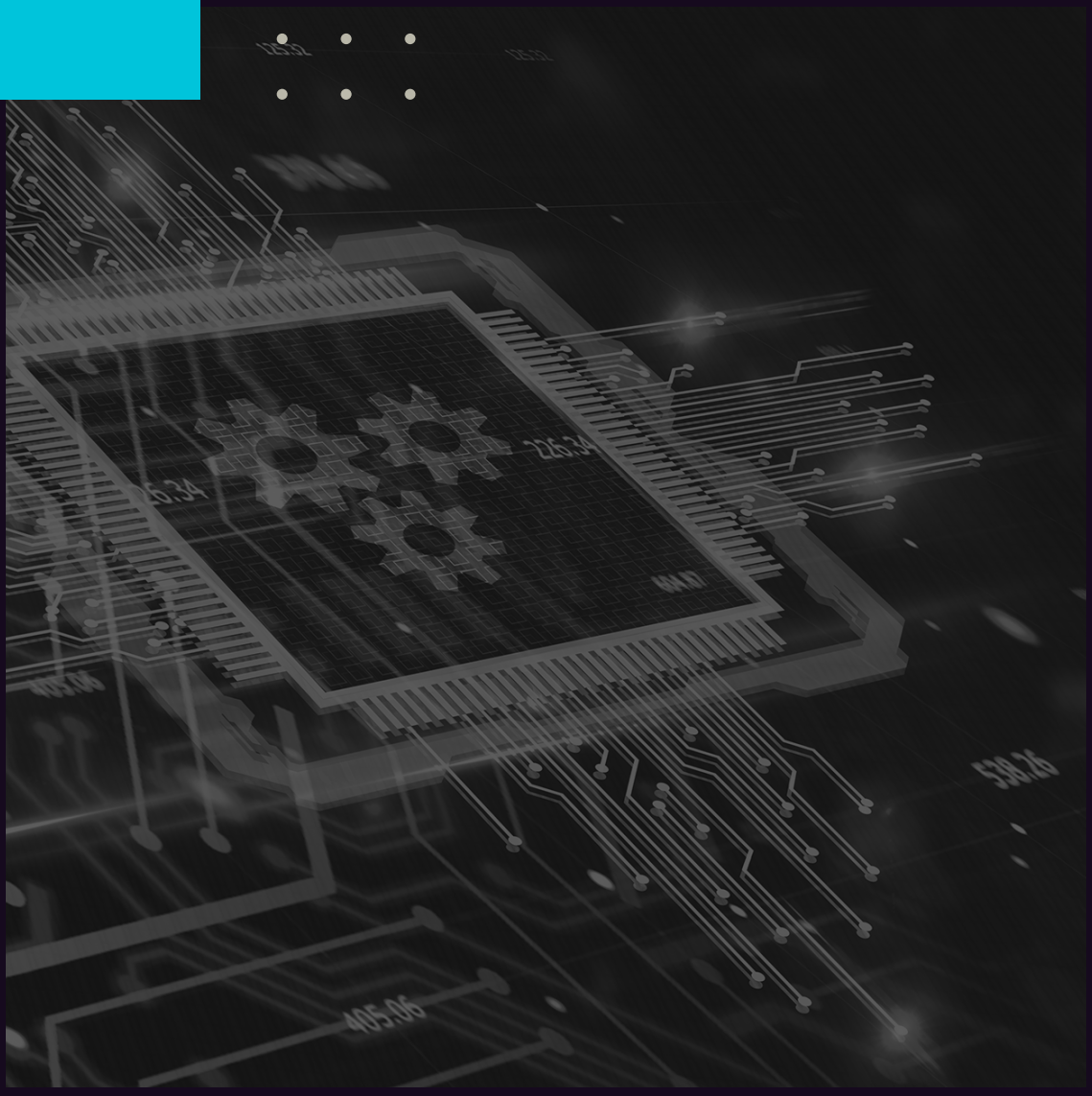
Precisamos ser mais proativos. Eu sei que a situação no Brasil é nova, mas o que eu recomendo, não apenas para aquelas pessoas que estão no Brasil, mas também em outros países, é que tente assegurar de que, quando você vê um evento online com os reguladores, se você quiser sentir ou saber o que está acontecendo no mercado, tente ser mais proativo.

Recentemente, eu falei com um dos reguladores europeus, adicionei ele no linkedin e falei que a palestra dele tinha sido ótima e que tinha algumas perguntas. Eles também estão interessados em estar conectados com a indústria e com advogados para entender quais são os problemas que as empresas enfrentam.

É necessário mudar a mentalidade e, principalmente, como profissional de privacidade, entendo que precisamos ser mais proativos durante a pandemia. **Dados são o centro, dados movem tudo. Como uma pessoa que trabalha com privacidade, você precisa saber onde estão esses dados na empresa, como esses dados estão sendo processados e, muitas vezes, a informação não vem até você.**

Você precisa ser muito proativo para entender, alcançar, ir até as pessoas e, mesmo durante a pandemia, entender o que está acontecendo. Dessa forma, você estará em uma melhor posição para assegurar que as novas exigências estejam sendo implementadas de uma forma adequada na sua empresa.

05



Daniela Cabella

"Como gerenciar com eficiência as atividades relacionadas à privacidade em uma organização usando o Scrum adaptado para privacidade"

Estamos vivendo um novo cenário, de maior enforcement da legislação em proteção de dados pessoais, com destaque para a LGPD brasileira que entrou em vigor em setembro de 2020. Há muito a ser feito, e os profissionais encarregados pela implementação de programas de governança em privacidade muitas vezes se questionam: "Por onde começo?"

Nós, que atuamos em startups de tecnologia, ainda temos dificuldades adicionais com a limitação de recursos humanos e financeiros disponíveis para a implementação, e ainda enfrentamos o desafio de mudanças constantes - tanto no cenário interno (devido à inovação, com criação e roll-outs frequentes de novos produtos e funcionalidades) como externo (com a regulamentação dos assuntos ainda abertos em proteção de dados, especialmente no Brasil).

Nesse contexto, entendemos que há uma necessidade de se adotar uma abordagem Ágil para a implementação, revisão e gestão eficaz de medidas de privacidade e proteção de dados. A priorização do que precisa e é possível ser feito precisa acompanhar, em tempo real, as mudanças internas e externas à organização, bem como estar adequada aos recursos humanos e financeiros disponíveis. Assim, desenvolvi, em conjunto com o Marcelo Martins, Scrum Master certificado, um trabalho de adequação do Scrum para Privacidade.

Antes de prosseguirmos, vamos lembrar aqui que as metodologias ágeis para desenvolvimento de software têm por base o Manifesto Ágil a seguir.

Daniela Cabella é Head of Privacy & Data Compliance e Data Protection Officer da Zoox Smart Data. Co-Founder e Instrutora na Complete Privacy, Professora no Global Institute of Law & Innovation, Advogada, CIPM, membro da IAPP e primeira pessoa a ser certificada como Data Protection Officer (DPO) pela Exin nas Américas. Subject Matter Expert em proteção de dados (GDPR e LGPD) para Exin. Trabalhou na equipe de Data Privacy em startup de tecnologia (no pilar de Segurança), como Advogada Especialista em Proteção de Dados em empresa de Big Data e em renomado Escritório de Advocacia de Direito Digital. Concluiu com sucesso o Bootcamp de Cybersecurity promovido pelo IGTI. Pós-graduada em Gestão da Inovação e Direito Digital pela FIA, e Bacharel em Direito pela USP.

Manifesto para Desenvolvimento Ágil de Software

Estamos descobrindo maneiras melhores de desenvolver software, fazendo-o nós mesmos e ajudando outros a fazerem o mesmo.

Através deste trabalho, passamos a valorizar:

• Indivíduos e interações mais que processos e ferramentas;

• Software em funcionamento mais que documentação abrangente;

• Colaboração com o cliente mais que negociação de contratos;

• Responder a mudanças mais que seguir um plano.

Ou seja, mesmo havendo valor nos itens à direita, valorizamos mais os itens à esquerda.

O Scrum é uma das abordagens ágeis para o desenvolvimento de software e tem sua origem em 1986. Naquele ano, Hirotaka Takeuchi e Ikujiro Nonaka publicaram um artigo na Harvard Business Review intitulado "The New New Product Development Game" com análise sobre a abordagem da Fuji-Xerox, Canon, Honda e NEC para a inovação no desenvolvimento de produtos.

Os autores perceberam que essas empresas eram mais flexíveis do que outras e podiam responder mais rapidamente aos problemas e resolvê-los de forma mais rápida e criativa, uma vez que organizavam equipes multifuncionais e com forte comunicação entre seus membros. Essa estrutura permitiu que eles tivessem uma forte interação e atividades sobrepostas durante o ciclo de desenvolvimento do produto, ao invés da abordagem "sequencial tradicional". Essa nova abordagem foi chamada de "abordagem do rugby".

No rugby, quando a bola sai do campo ou quando há qualquer outra necessidade de reiniciar o jogo (após uma falta, por exemplo), ambas as equipes se armam com oito jogadores de cada lado, segurando cada um com os braços "sobrepostos" aos companheiros e voltados para o adversário. Cada equipe tem o mesmo objetivo, que é disputar a posse da bola, e a expressão "Scrum" vem de "scrimmage", que significa "uma luta curta e não muito séria", segundo o Cambridge Dictionary.

Hoje, Scrum é uma abordagem Ágil para o desenvolvimento de software e, portanto, aplica os princípios declarados no Manifesto Ágil, criado e documentado em 2001.

A metodologia Scrum foi atualizada desde sua criação no início de 1990, e a última versão disponível foi publicada em novembro de 2020.

Este material traz a teoria sobre o Scrum e seus valores (Compromisso, Foco, Abertura, Respeito e Coragem), bem como orientações sobre como organizar a equipe e como implementar eventos Scrum (Sprint, Sprint Planning, Daily Scrum, Sprint Review e Sprint Retrospective) e artefatos (Product Backlog, Sprint Backlog e Incremento).

Para incorporar os benefícios da Agilidade e, mais especificamente, do Scrum, nosso primeiro passo foi adaptar o Manifesto Ágil para a Privacidade, mantendo o mesmo racional[1] de valorizar os dois itens em uma mesma frase, o da esquerda mais do que o da direita:

Manifesto para Gestão Ágil de Privacidade

Estamos descobrindo maneiras melhores de gerenciar atividades relacionadas à privacidade, fazendo-o nós mesmos e ajudando outros a fazerem o mesmo. Através deste trabalho, passamos a valorizar:

- **Titulares de dados e interações mais que processos e ferramentas;**
- **Privacy by design mais que compliance;**
- **Direitos dos titulares mais que obrigações internas dos agentes de tratamento;**
- **Responder a mudanças mais que seguir um plano;**

Ou seja, mesmo havendo valor nos itens à direita, valorizamos mais os itens à esquerda.

1 – Outros profissionais adaptaram o Manifesto, mas mudaram seu racional de valorizar dois fatores positivos, um acima do outro, para valorizar um fator positivo em vez de um negativo. Driel, RV (2016). Agile Scrum e o GDPR. LinkedIn. Obtido em https://www.linkedin.com/pulse/agile-scrum-gdpr-ruud-van-driel-cissp/.

O **primeiro princípio** significa, por exemplo, que se um titular dos dados exercer o seu direito, a organização deverá se mobilizar internamente para atendê-lo, ainda que não haja procedimentos internos suficientes ou que seja necessário não seguir tais procedimentos. E, nas interações, a comunicação em si e seu conteúdo são mais valorizados do que a forma como é feita. Isso dependerá, é claro, do cenário da empresa: quanto menor e menos complexa a operação, mais fácil será mobilizar equipes internas independentemente de processos e ferramentas.

"Privacy by design mais que compliance" significa que a empresa valoriza a conformidade legal, mas deseja obter mais do que um reconhecimento formal de que age legalmente - ela de fato valoriza a privacidade e busca torná-la totalmente integrada ao seu produto e ao negócio. Por exemplo, não é suficiente adicionar avisos de privacidade que simplesmente atendam aos requisitos legais em relação ao conteúdo (como descrever a finalidade de uso dos dados) - deve-se buscar ir além e tornar a mensagem do aviso de privacidade acessível, clara, adaptada ao modelo mental[2] do titular e que seja revelada no momento adequado na sua jornada, respeitando sua experiência como usuário do serviço ou produto oferecido pela empresa. Além disso, a empresa tem, de fato, uma preocupação em integrar medidas técnicas de privacidade e segurança da informação desde o início (by design) e por padrão (by default), e procura unir privacidade e os interesses do negócio em uma soma positiva (atendendo ao princípio de funcionalidade total do framework de Privacy by Design). Isso contribui para a maior proteção dos indivíduos e agrega valor ao produto/serviço e à empresa.

2 – Ferreira, R.M. e Cabella, D.M.M.S. Escrevendo e implantando os avisos de privacidade ("avisos de privacidade") na coleta do consentimento válido. Thomson Reuters Brasil (Ed.), Data Protection Officer (Encarregado) (pp.135-150). São Paulo: Revista dos Tribunais, 2020.

O **terceiro princípio** significa que, quando há necessidade de agir para atender aos direitos dos titulares, isso deverá ser priorizado em relação ao cumprimento de obrigações internas. Ambas as questões devem ser resolvidas, sendo que a primeira será atendida de forma prioritária. Segundo Michelle Chibba[3], essa priorização atende ao princípio de "respeito pela privacidade do usuário"[4] do framework de Privacy by Design, de manter todo o sistema centrado no titular de dados.

Finalmente, **"responder a mudanças mais que seguir um plano"** é o que dá flexibilidade a um DPO e permite a constante repriorização de atividades no meio da Sprint e reavaliação do backlog. Não fica "preso" a um plano de ação já traçado: consegue acompanhar e responder mais rapidamente a novos projetos e lançamentos da equipe de produto, bem como revisar o plano de ação face a uma nova regulamentação de privacidade e proteção de dados que acabou de entrar em vigor, por exemplo.

3 – Pesquisadora Associada do Privacy and Big Data Institute da Ryerson University (Canadá). Foi Diretora, Departamento de Políticas e Projetos Especiais do Escritório da autoridade de proteção de dados (Information and Privacy Commissioner - IPC) de Ontário, Canadá (IPC). Durante sua gestão de dez anos, seu departamento foi responsável pela realização de pesquisas e análises, bem como pela ligação com uma ampla gama de partes interessadas para apoiar o papel de liderança da Dra. Ann Cavoukian, Ph.D., na abordagem proativa de questões de privacidade e tecnologia, com destaque para o framework de Privacy by Design. Fonte: https://www.itu.int/en/ITU-T/academia/kaleidoscope/2015/Pages/Michelle-Chibba.aspx.

4 – Observação feita em leitura desta metodologia.

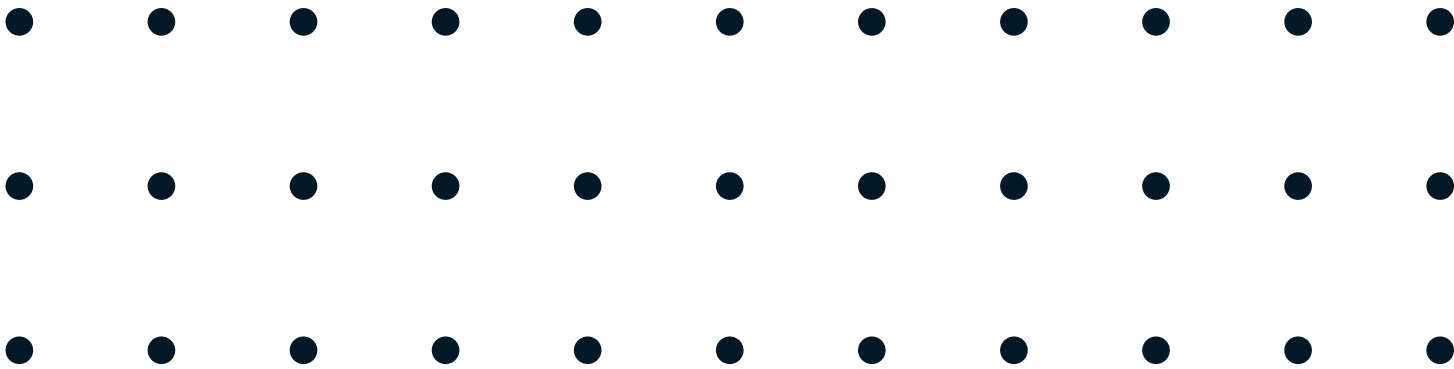
Com essa base sólida, seguimos para adaptar os principais pontos do Scrum para Privacidade:

Pilares

Transparência: É importante garantir que haja documentação do que está sendo feito, por quem, de que forma, o motivo, por quanto tempo, dentre outras informações que possam ser de interesse tanto de quem executa as atividades como de quem as coordena ou possui qualquer interesse nelas. O registro dos processos, requisitos de entrega e status, por exemplo, contribuem para auditorias, para o compliance em privacidade e proteção de dados e para a prestação de contas (accountability) de forma geral.

Inspeção: O acompanhamento constante interno de tudo o que está sendo feito pelos interessados (como o CEO, a Diretoria, os times que demandaram a área de Privacy, dentre outros) depende da existência de transparência. O preparo para a inspeção também pode contribuir para o sucesso em uma auditoria externa ou Due Diligence em Privacidade, por exemplo.

Adaptação: As medidas já implementadas de um programa de governança em privacidade devem ser revistas sempre que houver necessidade (por exemplo, para responder a mudanças trazidas por novas funcionalidades do produto ou por novas regulamentações). Além disso, os próprios processos internos da organização e da área de Privacy podem e devem ser constantemente revistos para fins de otimização.



Valores

A adaptação dos valores do Scrum para Privacidade incorpora os 7 princípios de Privacy by Design e o uso ético e sustentável dos dados pessoais.

Compromisso: O time de Privacidade tem compromisso com o uso sustentável de dados pessoais e com a privacidade proativa e preventiva, incorporada ao design, como configuração padrão e com segurança de ponta-a-ponta (em atendimento aos princípios nº 1, 2, 3 e 5 do framework de Privacy by Design).

Foco: O foco do time é a implementação do programa de governança em privacidade, buscando sempre uma abordagem de "soma positiva" (princípio nº 4 do framework de Privacy by Design).

Abertura: O time atua de forma transparente em relação a seus stakeholders e age em prol da transparência de sua organização em relação aos titulares de dados, ao mercado e às autoridades, em atendimento ao princípio nº 6 do framework de Privacy by Design ("visibilidade e transparência").

Respeito: Todas as ações devem ser pautadas pelo respeito em relação aos titulares de dados, em atendimento ao princípio nº 7 do framework de Privacy by Design ("respeito pelo usuário").

Coragem: O time de Privacidade, assim como o time de Scrum, tem a coragem de "fazer a coisa certa e trabalhar em problemas difíceis"[5], com o diferencial de fomentar a tomada de decisões pautadas pela ética sustentável em relação ao tratamento de dados pessoais e à privacidade dos titulares.

Time

Equipe multifuncional: Quando o número de funcionários e o orçamento são limitados para criar uma equipe multifuncional de Privacidade, recomenda-se envolver pessoas de outras equipes nas atividades de implementação do programa de governança em privacidade e alinhar, de antemão, a Sprint de Privacidade com a dos demais envolvidos. Não chega a ser um time formalmente constituído, mas material e temporariamente para determinadas atividades. Michelle Chibba observa[6] que, além de ser uma forma de superar a limitação de recursos, essa abordagem também agrega valor ao trazer diferentes perspectivas para uma mesma questão.

Fases e atividades sobrepostas: Na maioria das vezes, não há necessidade de terminar uma atividade para iniciar outra que seja igualmente importante e urgente para o programa de governança em privacidade. Em outras palavras, é possível realizar atividades em paralelo, como uma análise de risco e atendimento a direitos do titular. Neste ponto, Michelle Chibba destaca[7] que realizar multitarefas é bom desde que o framework esteja de fato implementado, para evitar que atalhos ruins sejam tomados.

5 – Conforme descrição dos valores do Scrum disponíveis em: https://www.scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-PortugueseBR.pdf pág. 5. Acesso em 25.01.2021.

6 – Observação feita em leitura desta metodologia.

7 – Idem.

Eventos

Sprints de privacidade: São eventos de duração fixa, e recomendamos que tenham duração de uma semana para manter a ênfase em metas de curto prazo e avanços constantes, com implementações graduais e incrementais. Há atividades que precisarão ser desenvolvidas em mais de uma Sprint, pois são mais complexas e demoradas - os "epics", como um relatório de DPIA ou PIA. Nesse caso, é importante dividir as atividades em "stories" a serem trabalhadas a cada semana.

Planning: É o evento de abertura da Sprint. Para as Sprints de 1 semana, recomendamos que a Planning tenha duração de 2 horas. Nessa etapa, define-se:

- **Por que esta Sprint é valiosa?** – Ou seja, qual valor agrega em relação ao programa de governança em privacidade e em termos de Privacy by Design. Por exemplo: Esta Sprint é valiosa pois irá acomodar, de forma "ganha-ganha" ou "soma positiva", os interesses da empresa em lançar a nova funcionalidade do produto que coleta e trata novos dados pessoais, o compliance em privacidade na validação do tratamento dos novos dados junto ao titular, e a experiência do usuário, com a criação de avisos de privacidade que sejam mostrados nos momentos mais adequados da jornada do usuário, sejam acessíveis e respeitem o modelo mental do usuário.

- **O que pode ser feito nesta Sprint?** – Definição das atividades/"stories" que serão trabalhadas na Sprint para implementação ou melhorias de aspectos do programa de governança em privacidade. Por exemplo, o que pode ser feito para fortalecer a implementação do framework de Privacy by Design, com a criação de "stories" na visão do titular dos dados ou do DPO[8], a depender do caso, para apoiar as atividades.

- **Como o trabalho escolhido será realizado?** – Definir se as atividades serão fracionadas ou não, se usarão determinada metodologia ou ferramenta, se o trabalho será desenvolvido 100% de modo interno pela empresa ou com o apoio de consultoria, dentre outros detalhes.

8 – Por exemplo: "Eu, como DPO, gostaria de criar um FAQ Interno de Privacidade para que quando algum cliente entrar em contato com nosso time de Customer Success (CS) e quiser saber se a nossa empresa é Controladora ou Operadora, nosso time de CS pode facilmente verificar esta informação e responder à pergunta do cliente de imediato, sem ter que esperar que eu esteja disponível para responder a consulta por email ou por outra ferramenta de comunicação interna.

A definição e registro dessas informações contribuem para o cumprimento dos pilares de Transparência, Inspeção e Adaptação.

Daily: A comunicação é a chave para o alinhamento. É recomendável manter uma reunião/call diária de 15 minutos com os stakeholders da Sprint. Esse compromisso ajuda a equipe a acompanhar o progresso, bem como identificar quaisquer problemas rapidamente e também resolvê-los de forma ágil. Esta, no entanto, não é o único momento de comunicação no dia, mas ajuda a tornar os demais mais focados e eficientes. Questões urgentes de privacidade e proteção de dados, por exemplo, devem ser comunicadas em tempo real aos tomadores de decisão. Conforme observa[9] Michelle Chibba, a Daily é uma boa forma de "institucionalizar" a comunicação, e isso, com o passar do tempo, acaba se tornando automático e até mesmo esperado. Além disso, com o passar do tempo, o processo e seus resultados melhoram para tornar esses 15 minutos mais específicos, focados e, portanto, mais eficientes e eficazes.

Sprint Review: Este evento semanal tem por objetivo apresentar os avanços e resultados da Sprint para os principais interessados, evidência do compromisso do time de Privacidade com a prestação de contas ("accountability"). A Review reforça o quanto a equipe de Privacidade, o DPO e a empresa avançaram na implementação e melhoria do programa de governança em privacidade. O ideal é que tenha duração de 30 minutos a 1 hora.

Sprint Retrospective: Este evento é interno do time de Privacidade. O DPO e o time de Privacidade devem verificar juntos as oportunidades de melhoria para aumento da qualidade e eficácia das atividades e entregas. O próprio time deve procurar encontrar seus problemas e criar um plano de ação para resolvê-los. É recomendável que haja apoio de um Scrum Master para essa tarefa. Há várias maneiras de se fazer a retrospectiva, e uma delas pode ser responder a **3 perguntas:**

"O que devemos COMEÇAR a fazer?" Por exemplo: Ser mais detalhistas na documentação. Isso gera maior eficiência e tomadas de decisão mais assertivas.

"O que devemos CONTINUAR a fazer?" Por exemplo: Trabalho em equipe, não acumular atividades além da capacidade de execução na Sprint, melhoria contínua nos processos, seguir a periodicidade nas cerimônias do Scrum para a Privacidade.

"O que devemos PARAR de fazer?" Por exemplo: Trabalhar em demandas incompletas, iniciar tarefas sem descrição clara e objetiva, não registrar o valor de cada Sprint.

Como bem observa[10] Michelle Chibba, essa abordagem tem conexão com o ciclo PDCA ("Plan, Do, Check, Act") e o registro desse processo também pode contribuir para maior visibilidade e transparência (e, portanto, "accountability") em relação a stakeholders.

9 – Observação feita em leitura desta metodologia.
10 – Idem.

Artefatos

Conforme definição na página 11 de "O Guia do Scrum", "os artefatos do Scrum representam trabalho ou valor. Eles são projetados para maximizar a transparência das principais informações."

- **Backlog de Privacidade:** Lista de tudo o que precisa ser feito para implementar e melhorar o programa de governança em privacidade da empresa. Recomendamos que o backlog seja priorizado com o uso das matrizes RUT e RICE, conforme adaptação para Privacidade que apresentamos no Anexo I do Programa de Governança em Privacidade da Zoox.

  Compromisso - Meta de Privacidade: É o objetivo de longo prazo do time de Privacidade que se materializa no Backlog de Privacidade - um estado futuro do programa de governança em privacidade que serve como alvo para o time realizar o planejamento. O programa de governança em privacidade é um veículo para entregar valor tanto para os titulares de dados quanto para a própria organização.

- **Backlog da Sprint:** É a lista de itens selecionados do Backlog de Privacidade para a Sprint ("o que" fazer), junto com a Meta da Sprint ("por que" fazer) e um plano de ação para entregar o Incremento ("como" fazer). É uma fotografia do progresso da Sprint que deve ser atualizada em tempo real para apoiar a Daily.

OBSERVAÇÕES

Tanto o Backlog de Privacidade e da Sprint podem ser gerenciados de forma efetiva com o uso de software de gerenciamento de projetos, que permitem um acompanhamento visual do desenvolvimento das atividades (ex: Monday, Notion). Outra opção é usar ou integrar o software de gerenciamento de projeto que a equipe de produto e tecnologia utiliza (como o Jira). A utilização de softwares como esses auxilia no desenvolvimento de métricas (KPIs[11]) de Privacidade.

Outra dica para melhor gerir as atividades é utilizar temas[12] (tags como "jurídico", "segurança da informação", "governança", "produto" etc.), iniciativas (identificando o pilar específico do programa de governança em privacidade e respectivo OKR[13] de Privacidade que serão atendidos), epics (atividades mais complexas) e stories (atividades mais simples) para manter o controle sobre as atividades.

Além disso, é fundamental incorporar privacidade e proteção de dados pessoais à estratégia e aos valores centrais da empresa, que orientam todas as equipes, para que haja maior compromisso de todos com a implementação do programa de governança em privacidade.

11 – Maiores informações sobre o que são indicadores-chaves de performance e sua utilidade disponíveis em: https://pt.wikipedia.org/wiki/Indicador-chave_de_desempenho.

12 – Rehkopf, M. (2020) Epics, histórias, temas e iniciativas. Atlassian Agile Coach. Obtido em https://www.atlassian.com/br/agile/project-management/epics-stories-themes.

13 – Maiores informações sobre o que são os "Objectives and Key Results" disponíveis em: https://pt.wikipedia.org/wiki/OKR.

Compromisso - Meta da Sprint: Segundo o Guia do Scrum, é o objetivo da Sprint, criado durante a Planning e adicionado ao Backlog da Sprint, que cria coerência e foco e, ao mesmo tempo, permite flexibilidade em termos do trabalho exato necessário para alcançá-la. Admite que o trabalho a ser desenvolvido possa, em certa medida, ser diferente do planejado, desde que ainda atinja a meta.

Cancelamento - Vale ressaltar que, se a Meta da Sprint se tornar obsoleta, o DPO (que faz o papel equivalente ao Sprint Product Owner) tem autoridade para cancelar a Sprint.

• **Incremento:** Pode-se dizer que é o avanço concreto em direção à Meta de Privacidade. É a soma dos trabalhos realizados e valores entregues, que são gerados a partir do momento em que se atenda a Definition of Done (DoD). Pode ser, por exemplo, um relatório pronto, um treinamento realizado - itens do programa de governança em privacidade que sejam atendidos.

DoR e DoD - A Definition of Ready - DoR (em outras palavras, a definição de "pronto para começar") e a Definition of Done - DoD (definição de "quando está finalizado"): são cruciais para manter o controle sobre qual trabalho está realmente pronto para ser começado (por exemplo: tem todas as informações necessárias) e para identificar claramente quando a atividade foi atendida em um nível satisfatório. Sempre há a possibilidade de ir além e criar, como o Spotify[14] fez, uma "Definition of Awesome", com parâmetros que ajudem a identificar o que precisa ser feito para que o programa de governança em privacidade seja implementado em um nível de "uau".

E aqui se encerra a adaptação do Scrum para Privacidade. Esperamos que esse trabalho também seja útil para outras organizações, de modo a facilitar e tornar mais eficiente a gestão e implementação do programa de governança em privacidade.

14 – Conforme mencionado no vídeo disponível em: https://www.youtube.com/watch?v=vOt4BbWLWQw, a partir do minuto 9:43.

06

Gustavo Babo

"Como incorporar a privacidade nas empresas para construir projetos eficientes e sustentáveis utilizando estratégias de privacy-centered design"

1 - Privacidade em Torres de Marfim

Os programas de privacidade nas empresas ganharam forma, competência e responsabilidade na medida que amadureceram as legislações de proteção de dados ao redor do mundo. Assim, os projetos de conformidade foram abastecidos com um enorme input de requisitos legais para serem analisados e implementados. Contudo, a estruturação dos programas, com demandas e interfaces completamente novas para muitas governanças corporativas, levantam preocupações sobre eficiência, incorporação, sustentabilidade e penetrabilidade das frentes de trabalho de proteção de dados nas empresas.

É possível observar dois principais motivos para os levantamentos. O primeiro é a incapacidade das demandas de privacidade se conectarem com as rotinas de trabalho dos colaboradores de forma eficiente. O segundo é a formatação de projetos que não refletem sobre a necessidade de serem incorporados de forma sustentável na governança das corporações e que não priorizam o desenvolvimento de uma cultura de proteção de dados de alta performance. Com isso, a área de privacidade torna-se pouco acessível e pouco integrada, além de possuir demandas com baixa penetrabilidade. Essa situação deve-se em diversos casos à aplicação de um oceano de políticas, procedimentos e diretrizes ineficientes, ou seja, regras sem aderência entre os colaboradores e nenhuma personalização para a dinâmica das áreas.

Além disso, as soluções de privacidade implementadas para os usuários também geram preocupações sobre experiência, usabilidade, transparência, satisfação e eficiência.

Data Protection Officer na Sympla. Pesquisador CNPQ nos temas Privacidade, Inteligência Artificial e Discriminação Algorítmica. Pesquisador DTec. Direito - UFMG. Bolsista do programa Youth@IGF da Internet Society (2018) e do CGI.br (2019). Global Shaper do Fórum Econômico Mundial. Co-fundador, palestrante, mentor e jurado de diversas iniciativas de aceleração de Lawtechs, multicampeão em Hackathons e autor de publicações em Privacidade e Proteção de Dados.

O desafio é intensificado com a priorização dos projetos em cumprir com as obrigações legais e não em construir interações de privacidade que sejam utilizáveis e úteis, ou seja, que as informações e controles de proteção de dados sejam fáceis de encontrar, compreensíveis e alinhados com as necessidades dos usuários[1]. As interfaces de privacidade normalmente cumprem com as regras estabelecidas pelas legislações, mas dificilmente consideram os critérios da análise heurística para avaliar a experiência das soluções.

Dessa forma, programas de privacidade podem estar sendo construídos em "torres de marfim", desconectadas da governança corporativa, desintegradas das rotinas de trabalho dos colaboradores e distantes das expectativas dos usuários. Para tanto, é imprescindível refletir sobre os objetivos dos próprios projetos, que ao concentrarem-se quase exclusivamente em cumprir com os requisitos legais aplicáveis, menosprezam a construção de conexões sólidas. Afinal, as consequências dessa problemática aumentam exponencialmente os riscos de violações aos direitos e liberdades dos usuários.

1 – An Introduction to Privacy for Technology Professional, 2020, Trevor Breaux, editor, International Association of Privacy Professionals IAPP, ISBN: 978-1-948771-91-7.

2 - Privacy-Centered Design

A solução para essa situação não é necessariamente empregar mais energia e mais recursos nos projetos ou torná-los mais rígidos. Pelo contrário, é possível ser ainda mais eficiente utilizando estratégias que vão trabalhar a construção dos programas além dos requisitos legais aplicáveis e ainda assim agregar certa personalização. Uma dessas alternativas para executar os programas é a implementação dos princípios do Privacy by Design, criados pela Dr. Ann Cavoukian.

Certamente, o framework é muito positivo para garantir eficiência, sustentabilidade, prevenção e penetrabilidade das demandas de privacidade, assim como auxilia na resolução de parte das preocupações abordadas anteriormente. A eficiência é o coração do conceito de data protection by design.

Para tanto, uma estratégia interessante para aplicar esses princípios pode ser chamada de Privacy-Centered Design. A ideia da estratégia consiste principalmente em orientar o projeto de privacidade para focar ao máximo na formatação das rotinas de trabalho de todas as áreas da empresa para que elas incorporem os interesses de privacidade de forma orgânica em suas operações.

Em outras palavras, a estratégia significa garantir que todas as áreas e as rotinas de trabalho da empresa sejam Privacy-Centered através do desenvolvimento de produtos de privacidade com experiências positivas e da elaboração de ferramentas para que os times considerem privacidade em suas tarefas e sejam capazes de identificar e resolver problemáticas do tema com autonomia.

Dessa forma, para aplicar a estratégia de Privacy-Centered Design é fundamental analisar como funciona a rotina de trabalho de cada área da empresa, a fim de entender como é o cotidiano operacional e construir instrumentos mais eficientes que as políticas internas.

Para realizar essa análise é recomendado que o profissional de privacidade passe por uma verdadeira imersão na área, através de onboarding, estudos, reuniões, conversas ou até utilizando as estratégias de job rotation, um mecanismo utilizado para aprender sobre a produtividade de diferentes cargos ou atividades, em que o profissional dedica determinado período para ser um colaborador temporário do time em que se deseja analisar, exercendo funções e responsabilidades.

Durante essa imersão, é possível ficar atento às interseções das rotinas com dados pessoais, com as interações com o programa de privacidade e com potenciais riscos nas atividades de tratamento. Ademais, é necessário analisar informações qualitativas de comportamento e identificar padrões utilizando Small Data[2].

Para tanto, o profissional de privacidade deve estudar com profundidade o cotidiano de trabalho de cada área, identificar quais ferramentas são utilizadas, como funciona a gestão, como é feita a priorização de demandas, o que é importante para o time, quais são as funções e responsabilidades de cada cargo, quais são os processos que funcionam bem e os que nem tanto. Afinal, "o termo Big Data é sobre máquinas e Small Data é sobre pessoas"[3].

É Importante destacar que a estratégia de Privacy-Centered Design pode ter resultados ainda mais significativos em empresas de tecnologia e inovação ou em áreas relacionadas ao desenvolvimento de produtos, serviços e estratégias. Isso acontece porque a governança dessas estruturas possui como característica principal a agilidade na ideação, validação, desenvolvimento e implementação de produtos e esses times normalmente operam com o mínimo de burocracias, regras e validações possíveis.

Dessa forma, a estratégia pode ser uma ótima alternativa, uma vez que aplicar todo aquele oceano de políticas no cotidiano de trabalho desses times não é só ineficiente, como também é incoerente e exemplifica perfeitamente a preocupação com os programas de privacidade construídos em "torres de marfim".

2 - Segundo o Small Data Group, "Small Data conecta pessoas com insights oportunos e significativos (derivados de big data e / ou fontes "locais"), organizados e empacotados - geralmente visualmente - para serem acessíveis, compreensíveis e acionáveis para as tarefas diárias".

3 - A frase foi dita por Allen Bonde em uma entrevista por telefone da eWeek.

3 - Conexão com os usuários

Primeiramente, precisamos problematizar as soluções de produto normalmente utilizadas nas demandas de privacidade. Como dito, os desenvolvedores estão acostumados em implementar interfaces apenas para cumprir com os requisitos legais, mas raramente envolvem especialistas em experiência do usuário para projetar uma interface de privacidade ou avaliar a sua viabilidade[4].

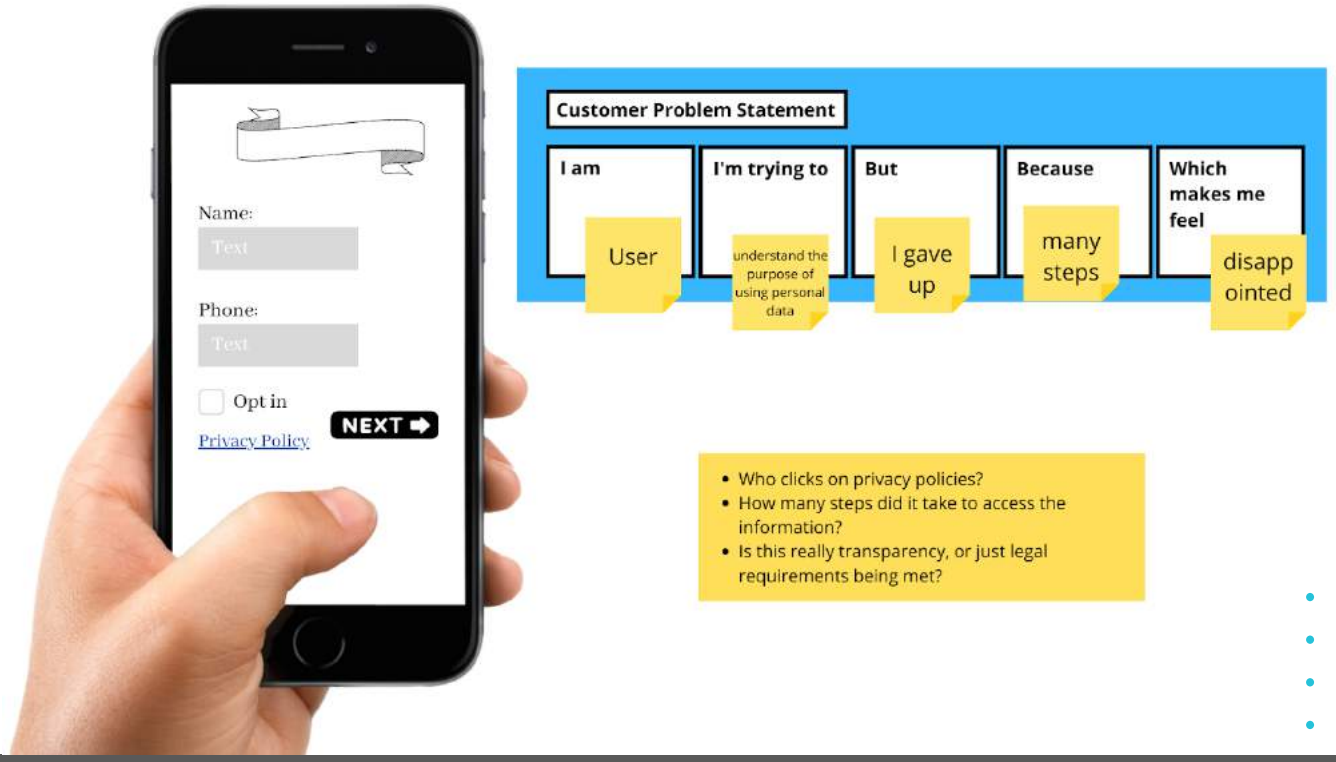
Assim sendo, as soluções implementadas se conectam pouco com as verdadeiras expectativas dos usuários e precisamos repensar essa situação através do conceito de Privacy-Centered Design. Como exemplo, vamos utilizar uma situação prática muito comum: o time de tecnologia implementou na plataforma, sem alinhar com o time de privacidade, um formulário com campos de preenchimento de dados para usuários interessados em receber uma proposta comercial.

As soluções adotadas nessa situação normalmente se limitam em inserir o link para a Política de Privacidade da corporação com um opt in ao final do formulário. Contudo, se o usuário deseja conhecer detalhes da atividade de tratamento e das finalidades de uso dos dados, será preciso enfrentar múltiplas etapas até acessar as informações e responder os questionamentos, o que normalmente resulta em desistência.

Até porque, segundo uma pesquisa realizada pela Universidade de Stanford, 97% dos usuários concordam com os termos e políticas grandes e difíceis sem acessá-las. Dessa forma, as empresas, ao se preocuparem apenas em cumprir com os requisitos legais, consideram que se um usuário não realizou a leitura da política de privacidade, então ele não se preocupa com a privacidade. Entretanto, é possível verificar que muitas vezes são as próprias soluções de privacidade que desencorajam o usuário a engajar com os seus direitos.

4 – An Introduction to Privacy for Technology Professional, 2020, Trevor Breaux, editor, International Association of Privacy Professionals IAPP, ISBN: 978-1-948771-91-7.

Para tanto, a fim de conectar melhor os usuários com as soluções e aumentar a satisfação e a usabilidade das interfaces de privacidade, basta que o time reflita com mais cuidado sobre quais os prováveis questionamentos de privacidade dos usuários. Uma ferramenta simples para essa análise é a Declaração do Problema do Titular, que consiste em entender quais as percepções do usuário com o produto durante sua jornada.

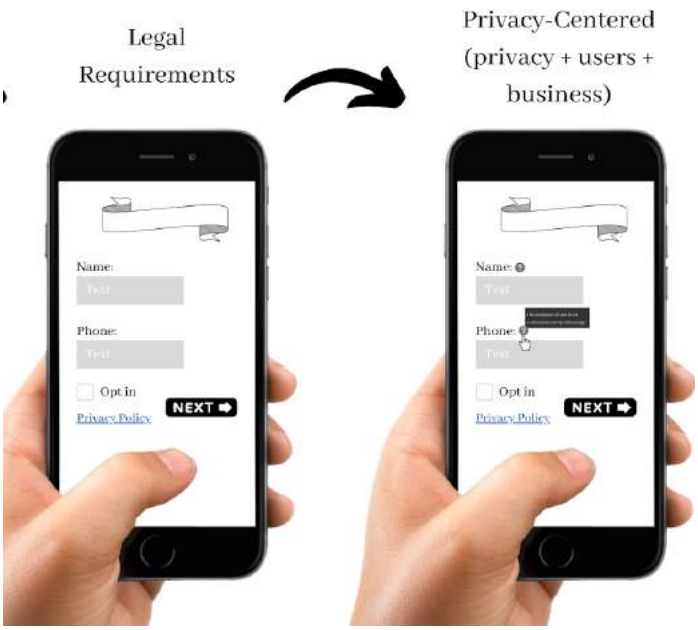


Portanto, ao analisar a situação, seria mais coerente inserir um privacy icon em cada campo de preenchimento de dados do formulário, com informações sobre a atividade de tratamento. A solução é uma boa prática ainda mais transparente, focada em antecipar possíveis questionamentos dos usuários, atender às suas legítimas expectativas e construir confiança através de uma interface digital.

Inclusive, **a privacidade é uma ótima oportunidade para construir uma interação positiva entre a empresa e os usuários**, uma vez que eles confiam mais quando acreditam que a corporação é justa, transparente e oferece opções e controles significativos[5]. Uma pesquisa realizada pela **Security Magazine** identificou que 52% dos usuários pagariam mais por um mesmo produto ou serviço de uma empresa com melhor segurança de dados, assim como 52% dos usuários afirmam que segurança é importante ou é o principal critério ao escolher um produto ou serviço.

Sendo assim, a dinâmica do Privacy-Centered Design resultou em soluções além do cumprimento das obrigações legais e melhorou a experiência e a confiabilidade ao inserir o privacy icon no formulário, conforme apresentado na imagem abaixo.

5 - An Introduction to Privacy for Technology Professional, 2020, Trevor Breaux, editor, International Association of Privacy Professionals IAPP, ISBN: 978-1-948771-91-7.



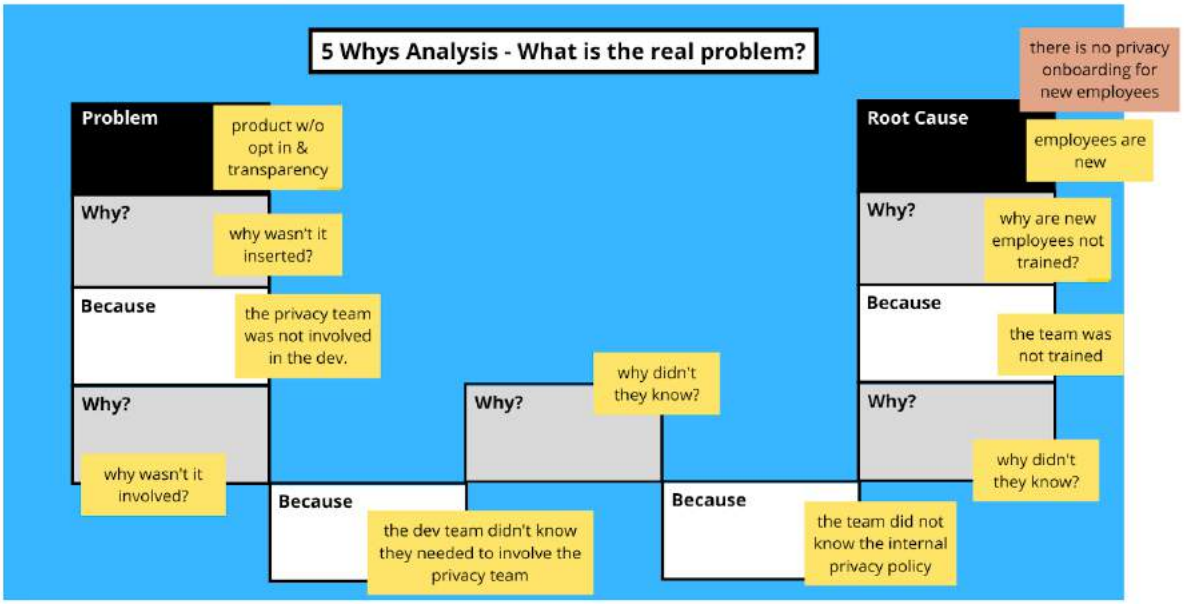
4 - Conexão com o business

Contudo, ainda tratando do caso apresentado, um outro problema foi abordado: o formulário foi implementado pelo time de produto sem nenhuma validação com o time de privacidade.

A primeira etapa de uma ação estratégica de Privacy-Centered Design para aprimorar a conexão com o business normalmente consiste em melhorar os mecanismos de interação e comunicação com os colaboradores para, posteriormente, criar ferramentas para que as próprias áreas saibam identificar e mitigar riscos em seu cotidiano.

É importante descobrir os motivos da inexistência de uma conexão entre o time de privacidade e o time de desenvolvimento, uma vez que, por mais que o risco tenha sido mitigado na situação, outros podem surgir com o tempo, pois é bem provável que outros produtos também sejam implementados sem incorporar privacidade.

Para entender a causa geradora do risco existe uma outra ferramenta conhecida como 5 Whys Analysis, que consiste em questionar sucessivamente o motivo de uma situação até chegar em sua causa raiz.



Assim sendo, em uma análise hipotética, foi possível identificar um problema estrutural relacionado à conexão da área de privacidade com a governança corporativa.

No exemplo, o time de desenvolvimento não realizou a interface pois não sabia da necessidade, embora já tenha sido realizado um treinamento explicando a política de privacidade interna. Ao questionar mais uma vez as razões, identifica-se a causa raiz da situação: os colaboradores deste time são novos e ainda não receberam o treinamento adequado.

Portanto, como resultado da análise, além da implementação da boa prática de privacy icon, também é conveniente reformular o onboarding para novos colaboradores, pois as comunicações com o time de privacidade não estavam sendo utilizadas como deveriam pelos novos colaboradores e isso pode motivar diversos riscos com o tempo.

Para essa primeira etapa, além do onboarding, é fundamental comunicar com a empresa sobre as interações das áreas com o time de privacidade, alertar sobre os canais de comunicação ou até disponibilizar um resumo para validação com práticas de gamificação.

5 - Conexão com os colaboradores

Por fim, para seguir com a segunda etapa da estratégia, é preciso consolidar e estruturar as informações das análises realizadas para desenvolver novos processos, fluxos e ferramentas eficientes e personalizadas para a operação dos times.

Muitas organizações estão confortáveis com processos de validações e reuniões com os colaboradores da área em determinado momento do projeto. Todavia, em outras, implementar um self-assessment para os times preencherem ou disponibilizar um checklist com orientações de privacidade podem ser uma alternativa mais eficaz. Ainda, em outras empresas, construir ferramentas robustas para cumprir com as validações de privacidade podem ser melhores opções, por exemplo, ao inserir um formulário convertido em código com práticas de versionamento através de comandos de commit.

Ademais, ferramentas orgânicas implementadas nas fases iniciais de ideação e desenvolvimento também se apresentam como ótimas soluções para incorporar privacidade em times ágeis de desenvolvimento. Independentemente da alternativa adotada, a conscientização e o treinamento das equipes é indispensável.

Para o exemplo analisado, é interessante construir ferramentas que fazem parte do cotidiano de trabalho ágil do time de desenvolvimento para que a privacidade seja considerada organicamente. Isso significa implementar um card em alguma das fases da metodologia de Software Development Life Cycle (SDLC) ou de Plan-Do-Check-Act (PDCA) ou quaisquer outras variantes utilizadas nesses times. Ademais, também é necessário considerar o funcionamento de outras dinâmicas de agilidade e interação contínua para avaliar as melhores soluções, tais como Scrum, Sprint e Kanban.

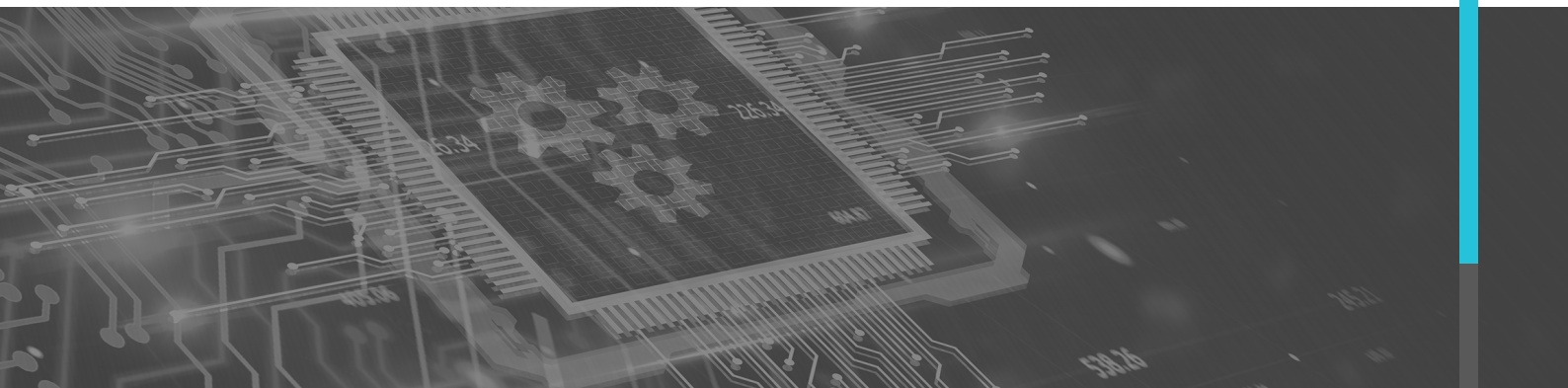
Já existem vários exemplos de ferramentas disponíveis publicamente para viabilizar estratégia de Privacy-Centered Design em times de produtos ou agilidade. Além do desenvolvimento de uma cultura de privacidade, a aplicação dessas ferramentas permite que privacidade seja considerada desde a ideação de produtos, serviços ou estratégias que utilizem dados pessoais, sem a necessidade de gerar interações burocráticas ou seguir regras que não compõem as rotinas de trabalho dos times.

Além disso, são ótimos procedimentos para accountability e para suportar a escalabilidade das demandas de privacidade de forma sustentável. Algumas dessas ferramentas são:

a) Privacy Personas: A ferramenta "Privacy Personas" provoca o time de desenvolvimento a questionar sobre privacidade ainda na fase de ideação do produto. Com ela, é possível avaliar quem é o titular, como ele compreende privacidade e quais são as suas preocupações de proteção de dados que o afastaria do produto, assim como iniciar o trabalho de mapeamento das atividades de tratamento. A ferramenta permite identificar diferentes soluções dependendo do público, como por exemplo, se o produto for voltado para a população idosa, será oportuno construir mecanismos ainda mais claros e visuais, mas se a persona for uma criança, a atenção é redobrada, pois trata-se de um usuário que muito possivelmente desconhece o que é privacidade e é preciso uma interação com os pais ou responsáveis.

b) Mapa da Empatia e Expectativa: A ferramenta "Mapa da Empatia e Expectativa" reflete sobre as preocupações e soluções da percepção do usuário sobre a atividade de tratamento, questionando sobre mecanismos de transparência, finalidades de uso dos dados pessoais, expectativas, reputação, elementos de confiabilidade, entre outros fatores.

c) Jornada do Usuário com Privacidade: A ferramenta "Jornada do Usuário com Privacidade" provoca o desenvolvimento de toda as etapas da experiência do usuário para incorporar os princípios do privacy by design, podendo ser utilizada com autonomia do próprio time de produto, com o auxílio do time de privacidade ou mesmo com um privacy champion.



Todavia, é recomendado que os profissionais de privacidade adaptem ou construam ferramentas novas, personalizadas para cada business e adaptadas para as rotinas de cada time da corporação, aplicando os princípios do privacy by design necessários para cada situação. Vale lembrar que o principal ponto da estratégia de Privacy-Centered Design é formatar rotinas de trabalho, logo a estratégia também deve considerar construir ferramentas para times como RH, Marketing, Suporte, Legal, entre outras.

Conclusão

É importante lembrar que "não existem balas de prata". Assim sendo, essas soluções não são únicas e absolutas, como também não substituem os trabalhos consolidados dentro da área de proteção de dados, mas o **Privacy-Centered Design** pode ser muito positivo para agregar diversos benefícios para os programas de privacidade, tais como eficiência, sustentabilidade operacional, escalabilidade, prevenção, responsabilidade, penetrabilidade, maturidade, autonomia, conexão, agilidade e prestação de contas.

Sendo assim, buscar formatar rotinas de trabalho de forma orgânica para incorporar privacidade apresenta-se como uma solução interessante para alcançar uma melhor performance nos projetos, implementar soluções de privacidade com boas experiências, evitar "torres de marfim", agregar esses vários benefícios nas frentes de trabalho da área e, principalmente, respeitar os dados pessoais dos usuários.

07

Raissa Moura

"Como implementar medidas de privacy by design utilizando uma adaptação da ferramenta ágil denominada Health Check"

As empresas que tratam dados pessoais devem implementar um programa de governança em privacidade que demonstre o seu compromisso em adotar processos e políticas internas que assegurem o cumprimento de normas e boas práticas relativas à proteção de dados.

A governança em privacidade, além de promover o compliance com as normas de proteção de dados vigentes, também (e principalmente) gera impactos positivos na operação da empresa e a valoriza na medida em que preserva e otimiza o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum.

No entanto, um dos maiores desafios da implementação do programa de governança em privacidade é aplicá-lo a todo o conjunto de dados pessoais que estejam sob o controle da empresa e, ao mesmo tempo, realizar processos de avaliação sistemática de impacto e risco à privacidade. Sendo assim, cabe ao profissional responsável pela área de proteção de dados a difícil missão de conhecer todos os novos produtos, serviços, incrementos, processos e procedimentos que acarretem o tratamento de novos dados pessoais para implementar as melhores práticas de proteção à privacidade por padrão antes mesmo do lançamento das novas funcionalidades.

A incumbência de ser onisciente e onipresente se torna ainda mais hercúlea quando se trata de empresas que adotam metodologias ágeis de gestão e mudanças constantes decorrentes dos processos de inovação, notadamente empresas de tecnologia e startups. Portanto, o DPO, ou profissional responsável pela proteção de dados e privacidade, não pode se limitar apenas a adaptar o programa de governança à estrutura, à escala e ao volume de suas operações. Mas, deve, sobretudo, ser criativo o suficiente para adaptá-lo também ao método ágil, implementando ferramentas eficientes que fomentem a cultura da privacidade e empoderem os colaboradores com o conhecimento necessário para a aplicação, de forma abrangente, do framework de Privacy by Design.

Head of Data Privacy e Data Protection Officer (DPO) na Incognia, com experiência na liderança de programa de governança em privacidade e implementação do framework de Privacy by Design como parte da equipe de Core Engineering da companhia. Legal Law Master em Direito Corporativo pelo IBMEC, é co-fundadora do Capítulo de Recife do movimento internacional de direito e tecnologia Legal Hackers. Também é co-fundadora e instrutora na Complete Privacy, além de professora em relevantes instituições e autora de publicações dentro da temática de Proteção de Dados e Privacidade.

Pensando em tudo isso, e buscando atingir os supracitados objetivos na condução do Programa de Governança em Privacidade da Incognia (empresa que desenvolve tecnologia privacy by design de biometria comportamental por localização), eu criei o Privacy Health Check. O Privacy Health Check é uma adaptação da ferramenta ágil Health Check Model desenvolvida pelo time de engenharia e agile coaches do Spotify sob licença Creative Commons. Através da realização de workshops e técnicas de visualização, o Health Check permite que gestores tenham noção de onde devem implementar seus esforços de melhoria, consigam identificar problemas sistêmicos e possam ajudar as equipes a se tornarem mais autoconscientes para que também se concentrem em seus próprios esforços de melhoria.

Portanto, a ideia de criar o Privacy Health Check nasceu do desejo de adaptar ferramentas ágeis que já existem para aproximar o DPO dos times ágeis e possibilitar a prática do Privacy by Design; ou, até mesmo, implementar metodologias ágeis em equipes que não são ágeis, mas que precisam e podem muito bem se beneficiar da ferramenta, uma vez que ela gera uma interação muito forte entre os integrantes do time e proporciona maior visibilidade do que está acontecendo nas diversas áreas da organização. A metodologia tem o potencial de auxiliar o líder de privacidade a direcionar melhor suas iniciativas e os seus esforços, tornando mais fácil o trabalho de gerenciamento de riscos dentro do programa de governança em privacidade.

O Privacy Health Check como aliado do Privacy by Design

A implementação do Privacy by Design demanda que o responsável pela a área de proteção de dados e privacidade esteja presente de alguma forma no momento de desenvolvimento de novos produtos, serviços e funcionalidades que envolvem a coleta de novos dados pessoais. Mas já sabemos que essa missão é muitas vezes inglória, pois é impossível fiscalizar tudo que acontece na empresa ao mesmo tempo. Então, o ideal é difundir o conceito e a consciência do que é o Privacy by Design para que os colaboradores se comprometam a desenvolver novos sistemas colocando a privacidade do usuário no centro de qualquer decisão.
Portanto, o Privacy Health Check tem por objetivo construir um diálogo mais assertivo entre a área de privacidade e as demais áreas da organização, superando dificuldades de comunicação, como, por exemplo, situações em que o DPO descobre um novo tratamento de dados depois do lançamento de uma nova funcionalidade, serviço ou produto, desafio que todos os profissionais que trabalham com proteção de dados e privacidade enfrentam.

Se quisermos uma atuação mais proativa dos times ágeis em relação à privacidade, é mandatório evitar programas de governança rígidos, burocráticos, com políticas de difícil interpretação e aplicação.

Um time ágil dificilmente vai conseguir esperar que o líder de privacidade faça uma análise profunda e dê um extenso parecer antes do desenvolvimento de uma nova ferramenta. Então, quanto mais os colaboradores internalizarem os conceitos necessários para prevenir os riscos à privacidade, quanto mais autonomia as equipes tiverem para implementar o **framework privacy by design**, maior segurança a empresa alcançará e, consequentemente, será capaz de oferecer mais benefícios aos titulares dos dados, pois os próprios colaboradores serão capazes de impedir que os riscos à privacidade se materializem.

Claro que ainda vão existir situações em que o profissional responsável pela proteção de dados e privacidade precisará ser envolvido. Por isso, é imprescindível criar mecanismos para que essa avaliação seja realizada sem entraves para o desenvolvimento do produto e sem atrasar as sprints e lançamentos do time ágil, com vistas a garantir uma análise de risco eficiente e medidas de mitigação eficazes. **Não adianta recorrermos apenas a modelos tradicionais, como formulários com várias perguntas, pois as respostas nem sempre serão verdadeiras, ou não darão a clareza suficiente do que está realmente acontecendo por trás das justificativas dadas.**

É muito importante contarmos com modelos inteligentes de avaliação de times ágeis como o Health Check. Sua adaptação nada mais é do que a solução encontrada para facilitar a avaliação das equipes ágeis e o seu comprometimento com a implementação dos 7 (sete) princípios do Privacy by Design. Originalmente, o Privacy Health Check foi criado para atender as necessidades dos times de produto, mas é possível adaptar o workshop para qualquer área, como Recursos Humanos, Marketing e Jurídico, por exemplo.

Como funciona o Health Check?

O Spotify recomenda os seguintes passos:

1. Organize workshops onde os membros de uma equipe discutem e avaliam sua situação atual com base em uma série de perspectivas diferentes (qualidade do trabalho, diversão, valor etc.);

2. Crie um resumo gráfico do resultado;

3. Use os dados para ajudar os times a melhorar.

Ao discutir os diferentes indicadores de saúde, o time constrói uma autoconsciência sobre o que está funcionando e o que não está. A ampla seleção de perguntas ajuda a expandir sua perspectiva. O Health Check também fornece uma perspectiva equilibrada, mostrando as coisas boas, bem como os pontos fracos.

Gestores que estão fora (ou parcialmente fora) do time obtêm um resumo de alto nível do que está funcionando e do que não está. Eles também podem ver padrões em várias equipes diferentes. Se você tem dezenas de equipes e não pode falar com todos sobre tudo, um resumo visual como este ajuda a descobrir como gastar seu tempo e com quem falar sobre o quê. O primeiro passo para resolver um problema é estar ciente dele. E esse tipo de visualização torna mais difícil para todos ignorar o problema.

O Spotify concluiu que as pesquisas online são péssimas, principalmente porque cortam a conversa, e essa é muito valiosa. Através da conversa franca, membros da equipe obtêm insights durante a discussão e o facilitador obtém insights sobre como ajudar efetivamente as equipes.

Portanto, os workshops com os times facilitam uma conversa face a face sobre os diferentes indicadores de saúde do time. Normalmente, uma ou duas horas é o suficiente.

Para facilitar essa dinâmica, o Spotify criou um baralho de “Cartas Incríveis”, cada carta é um indicador de saúde com um exemplo de “incrível” e um exemplo de “péssimo”, conforme pode ser visto abaixo:

Fonte: https://engineering.atspotify.com/2014/09/16/squad-health-check-model/

A ideia é que as pessoas consigam sinalizar sua opção, indicando o sinal verde ou o sinal vermelho. Então, tomando a carta “Fun” como exemplo, se a pessoa acha que o trabalho é super divertido, ela vai levantar o sinal verde e expor suas ideias. O facilitador deve criar um clima para que as pessoas se sintam seguras para expor suas percepções, principalmente as negativas.

Para cada pergunta, a equipe é convidada a discutir se eles estão mais perto de “incrível” ou mais perto de “péssimo”, empregando técnicas básicas de workshop, como a votação por maioria, por exemplo, para ajudá-los a chegar a um consenso sobre qual cor escolher para aquele indicador e qual é a tendência (estável, melhorando ou piorando).

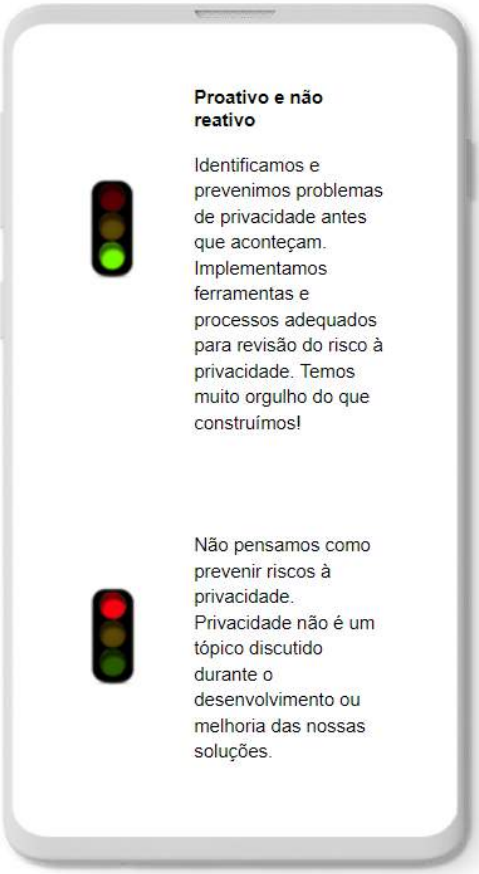
As perguntas foram elaboradas para cobrir uma ampla gama de perspectivas diferentes. Essas perguntas são apenas um ponto de partida, uma seleção padrão. As empresas são livres para remover, adicionar ou alterar as perguntas para o que acharem relevante. O importante é tentar limitar a 10 (dez) perguntas. Se tivermos mais perguntas do que isso, algumas provavelmente serão sobre o mesmo assunto e podem ser dispensadas.

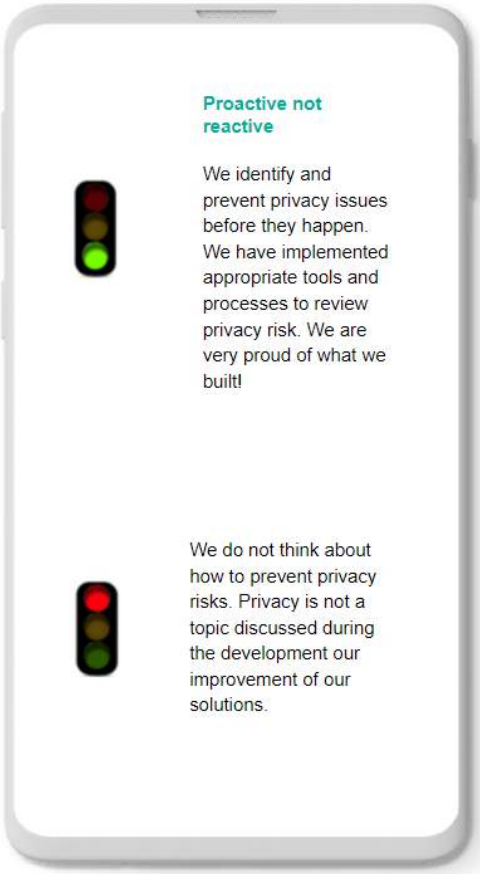
Essa metodologia é aplicada em empresas ágeis como Incognia, Netflix, Facebook, entre outras, e possibilita uma visualização muito rica do status de cada equipe. É bom ter em em mente que uma carta verde não significa que seja o melhor dos mundos, mas que pelo menos a pessoa considera que aquela situação está mais para positiva; se você tem uma carta com sinal amarelo não significa que está muito ruim, mas que na verdade a pessoa considera que existem melhorias importantes para serem implementadas, contudo a situação não é um desastre; o sinal vermelho, por sua vez, é utilizado quando a situação realmente está péssima e há melhorias significativas que precisam ser implementadas.

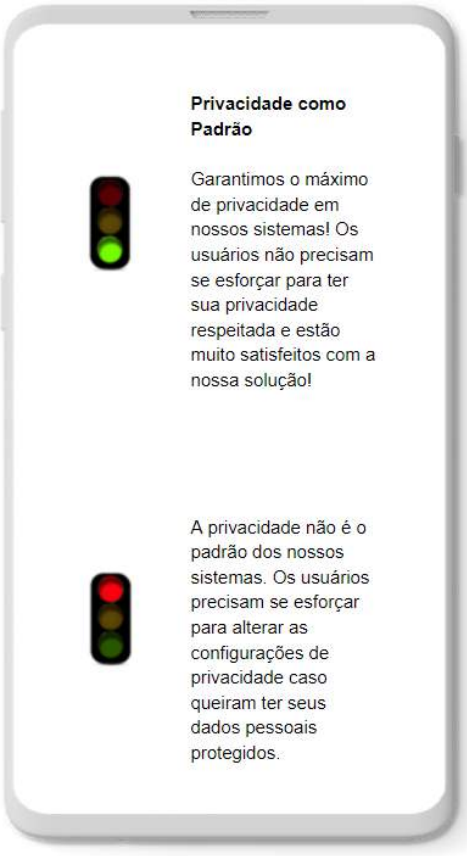
Como funciona o Privacy Health Check?

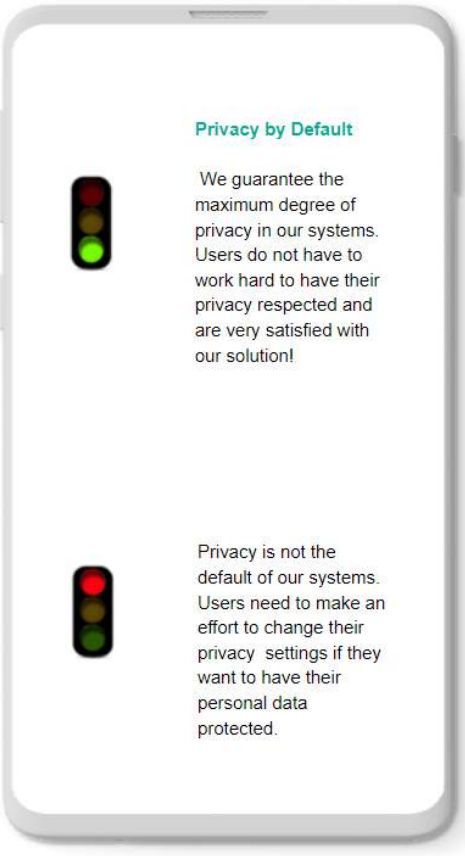
O workshop é gamificado através da confecção de cartas com afirmações positivas e negativas que deverão ser distribuídas entre os membros da equipe para que, em uma conversa descontraída, facilitada pelo profissional responsável pela proteção de dados e privacidade, possam externar sua opinião sobre a aplicação do Privacy by Design.
O objetivo é identificar os problemas sistêmicos relacionados à proteção de dados e privacidade, portanto as cartas foram criadas com base nos 7 (sete) princípios do Privacy by Design. Ao apresentar as cartas, muitas pessoas vão dizer que está horrível a aplicação de um determinado princípio, e você pode buscar entender o porquê; você vai conseguir identificar onde os times devem focar os esforços de melhoria; e você também vai ajudar esses times a ter consciência dos princípios do Privacy by Design. Ou seja, você avalia ensinando e isso é muito valioso.

Abaixo, você pode conferir as cartas do Privacy Health Check, disponibilizadas sob a atribuição Creative Commons-BY[1]:









1 - Credits: Privacy Health Check - Raíssa Moura Ferreira. .

Privacidade Incorporada ao Design

A privacidade é parte essencial da arquitetura dos nossos sistemas de TI e práticas de negócio. Amamos incorporar privacidade no design da nossa solução de forma segura e criativa!

Nós nunca pensamos na privacidade como uma funcionalidade essencial. Não está claro como incorporar privacidade no design do nosso produto e nas nossas práticas de negócio.

Privacy Embedded into Design

Privacy is an essential part of the architecture of our IT systems and business practices. We love to embed privacy into the design of our solution in a safe and creative way!

We never think about privacy as an essential feature. It is unclear how to incorporate privacy into our product design and business practices.

Funcionalidade total

Conseguimos acomodar os interesses legítimos do negócio e o respeito à privacidade ao mesmo tempo! Todos ganham: o negócio, os nossos clientes, os indivíduos e a sociedade.

Não implementamos as melhores práticas de proteção de dados e privacidade quando temos outras prioridades. Não conseguimos acomodar todos os interesses legítimos.

Full Functionality

We accommodate all legitimate business interests and respect for privacy at the same time! Everyone wins: the business, our customers, data subjects and the society.

We do not implement the best practices of privacy and data protection when we have other priorities. We are unable to accommodate all legitimate interests.

Funcionalidade total 2

Conseguimos acomodar os interesses legítimos do negócio e o respeito à privacidade ao mesmo tempo! Todos ganham: o negócio, os nossos clientes, os indivíduos e a sociedade.

Não conseguimos acomodar todos os interesses legítimos em uma soma positiva. Sempre que uma funcionalidade ameaça a privacidade desistimos dela sem procurar soluções alternativas.

Full Functionality 2

We accommodate all legitimate business interests and respect for privacy at the same time! Everyone wins: the business, our customers, data subjects and the society.

We do not know hot to accommodate all legitimate interests in a positive sum. Whenever a feature threatens privacy, we give it up without looking for alternative solutions.

Segurança de ponta-a-ponta

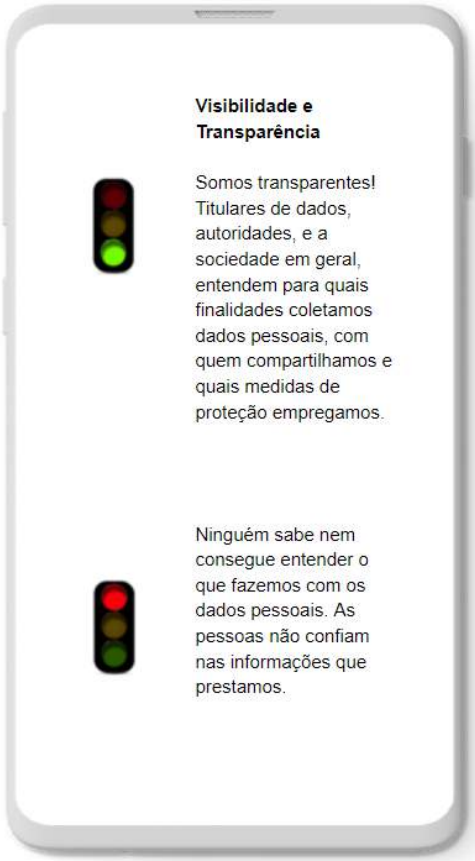
Protegemos as informações pessoais durante todo o ciclo de vida dos dados. Implementamos medidas de segurança robustas!

Não implementamos medidas de segurança robustas. Não garantimos o gerenciamento seguro do ciclo de vida dos dados de ponta-a-ponta.

End-to-End Security

We protect personal information throughout the entire life cycle of the data involved. We implement strong security measures!

We do not implement strong security measures. We do not ensure the secure lifecycle management of the information, end-to-end.



Exemplo 1:

Vamos tomar como exemplo a primeira carta com o princípio “Proativo e não reativo” que tem a seguinte afirmação positiva: “Identificamos e prevenimos problemas de privacidade antes que aconteçam. Implementamos ferramentas e processos adequados para a revisão do risco à privacidade. Temos muito orgulho do que construímos!”; e a seguinte afirmação negativa: “Não pensamos como prevenir riscos à privacidade. Privacidade não é um tópico discutido durante o desenvolvimento ou melhoria das nossas soluções”.

Quando o facilitador apresentar uma carta como essa, pessoas super sinceras poderão dizer “olha, realmente, a gente nunca pensa em privacidade, estamos pensando em atender os objetivos de negócio, e o time não está parando para pensar sob a perspectiva da privacidade”.

Cabe ao facilitador buscar o máximo de razões possíveis e já sair do workshop com um plano de ação, além de criar a consciência de que os desenvolvedores já deveriam estar pensando em privacidade e deveriam ter mecanismos para avaliar os riscos à privacidade de forma preventiva.

Exemplo 2:

Na Carta “Privacidade Incorporada ao Design", a afirmação positiva é “A privacidade é parte essencial da arquitetura de nossos sistemas de TI e práticas de negócio. Amamos incorporar privacidade ao design de nossa solução de forma segura e criativa!", enquanto que a negativa é: “Nós nunca pensamos em privacidade como uma funcionalidade essencial. Não está claro como incorporar privacidade no design do nosso produto e nas nossas práticas de negócio". A opção negativa é quase um pedido de socorro para o profissional de proteção de dados e privacidade interno ou consultor externo criar todos os mecanismos necessários para que a equipe aprenda como incorporar privacidade de fato no design dos novos produtos, agindo de forma proativa.

Exemplo 3:

A carta “Funcionalidade Total", por sua vez, é uma carta muito importante, pois quando implementamos o princípio da Funcionalidade Total, um dos meus preferidos, evitamos falsas dicotomias como interesse do negócio x privacidade, segurança x privacidade. Devemos sempre complementar o objetivo almejado com o respeito à privacidade para encontrar uma soma positiva. Então é muito importante saber se o time de fato faz isso e, assim, todos ganham - o negócio, os indivíduos e a sociedade, ou se há uma dificuldade para acomodar todos os interesses. É possível que diante de uma situação onde existe privacidade x interesse do negócio, por exemplo, as melhores práticas de proteção de dados e privacidade estejam sendo deixadas de lado. Portanto, é muito importante identificar o problema o quanto antes.

A carta “Funcionalidade Total 2” contempla a situação inversa. Muitos profissionais estão tão preocupados com o risco à privacidade e com as normas de proteção de dados, que não lidam bem com a avaliação de risco ou não sabem como implementar as medidas de mitigação adequadas. Terminam impondo uma visão mais conservadora e fazendo com que, na prática, muitos objetivos de negócio sejam deixados de lado e funcionalidades que seriam extremamente relevantes sejam abandonadas.

Esses profissionais geralmente têm muita aversão ao risco e impedem que as equipes criem soluções criativas ou não dão oportunidade para que pensem em outras soluções. Simplesmente estão descartando projetos e isso é muito grave para uma organização. Os especialistas em proteção de dados e privacidade, sejam profissionais do direito ou tecnologia, devem buscar sempre a funcionalidade total.

Como representar graficamente o resultado do Privacy Health Check?

A tabela abaixo demonstra como o Privacy Health Check deve medir e construir um quadro visual do que seria o status de cada time em relação à aplicação dos princípios do **Privacy by Design:**

Principles	Team 1	Team 2	Team 3
Proactive not reactive			
Privacy as a Default Setting			
Privacy Embedded into Design			
Full Functionality			
End-to-End Security			
Visibility and Transparency			
Respect for User Privacy			

Na primeira coluna da esquerda temos os princípios do Privacy by Design, enquanto que, na segunda coluna, temos a sinalização da decisão do time sobre cada carta. Então, se a maioria levantou a carta com o sinal verde, o facilitador deve perguntar a razão, bem como se todos estão de acordo para que a equipe chegue num consenso. Essa discussão é muito importante, porque gera informações ricas para a avaliação e plano de ação.

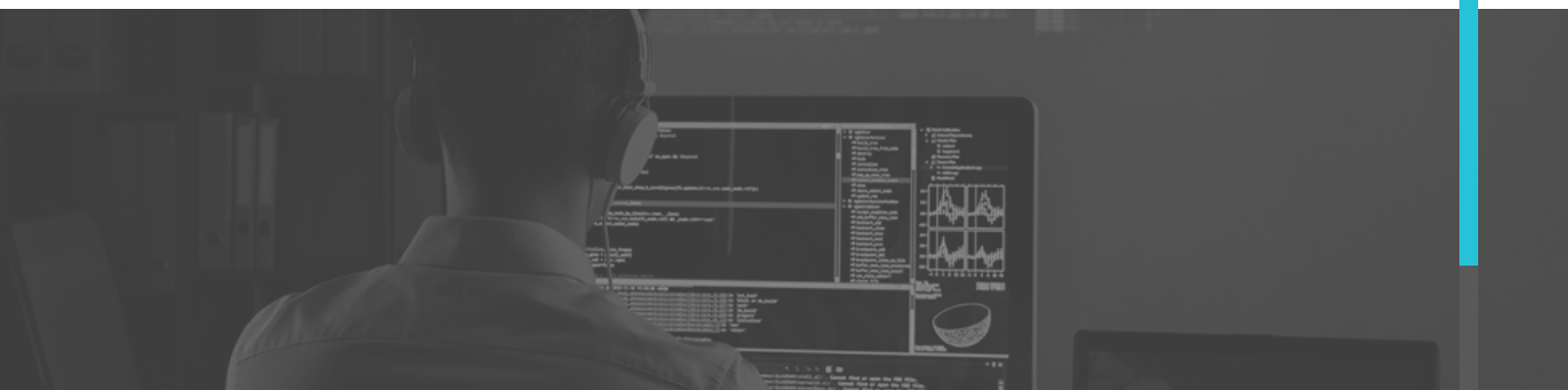
Também é imprescindível fomentar o debate entre os participantes que levantaram cartas com sinal vermelho, ainda que sejam a minoria, pois eles podem levantar pontos cruciais que os outros possivelmente não têm visibilidade, não perceberam ou não tiveram coragem de externalizar.

Esse debate pode, inclusive, fazer com que outros participantes mudem sua opinião e o facilitador deve dar oportunidade para que mudem também sua sinalização. Ao final da discussão, o facilitador deve colocar a representação da resposta final do time, através da maioria dos votos, e perguntar se aquela situação está estável, piorando cada vez mais ou se está melhorando.

As setas ao lado da sinalização mostram essa tendência - seta para o lado indica estabilidade, seta para cima indica melhoria, e seta para baixo indica piora, traduzindo a situação real da implementação do princípio. Existem situações, por exemplo, onde o time pode concluir que não há transparência suficiente para o titular do dado, portanto a situação está bem ruim e o sinal utilizado será o vermelho. Mas reconhecem que há um projeto em andamento para melhoria da transparência. Nesse caso, a seta apontando para cima ao lado do sinal vermelho deve indicar a tendência de melhoria.

É importante destacar que, durante o workshop, conseguimos compreender melhor qual a percepção do time sobre a implementação de cada um dos princípios do Privacy by Design, observando suas expressões, interações, visões e casos práticos trazidos para discussão. Esse resultado é dificilmente alcançado através de um questionário ou planilha de Excel com perguntas sobre o tratamento de dados pessoais. A riqueza de detalhes que o Privacy Health Check pode trazer é muito significativa.

Existem várias ferramentas de Health Check Model disponíveis online. Na Incognia, utilizamos o Team Retro. A ferramenta possibilita a edição das cartas e a adaptação do Privacy Health Check para o modelo de workshop remoto, além de contar com funcionalidades que permitem a visualização gráfica das respostas.



Os benefícios do Privacy Health Check são incontáveis e extremamente relevantes. Através dessa metodologia é possível, por exemplo:

a. Fomentar a cultura de privacidade;

b. Fazer com que as pessoas se importem mais com o assunto e entendam a relevância do tema de uma maneira leve e divertida;

c. Incorporar privacidade aos sistemas, tecnologias e práticas de negócio através dos planos de ação gerados nos workshops (é importante anotar tudo e pensar com o time quais as soluções que podem ser criadas em conjunto);

d. Agir de forma proativa e prevenir riscos, pois, através da organização periódica do workshop, a área de privacidade fica mais próxima de outras equipes;

e. Ajudar as equipes a enxergar suas próprias dificuldades;

f. Tomar conhecimento de situações que deveriam ter sido reportadas para o time de privacidade e não foram;

g. Gerar uma melhor visibilidade de como a organização está respeitando a privacidade através da implementação e monitoramento dos 7 (sete) princípios do Privacy by Design;

h. Gerar soluções de alto valor para o negócio, os indivíduos e a sociedade;

i. Demonstrar a efetividade do seu programa de governança em privacidade.

Quando implementamos privacidade na cultura organizacional, criamos uma estrutura que protege a privacidade por padrão, permitindo que os dados sejam utilizados em seu máximo potencial. Por outro lado, os programas de privacidade que focam apenas em mecanismos tradicionais de conformidade encontram muita dificuldade para se envolver com as diversas áreas da organização que podem ter objetivos estratégicos que parecem estar em conflito com a proteção de dados pessoais[2].

Sem dúvidas, o Privacy Health Check pode ser um excelente aliado ao programa de governança em privacidade, pois fomenta a cultura de privacidade ao mesmo tempo em que facilita o envolvimento com os diversos stakeholders da organização, além de permitir a atualização constante do programa com base nas informações obtidas com o monitoramento contínuo e avaliações periódicas realizadas por meio dos workshops de privacidade.

2 - Weller, Aaron; Leach, Emily. "How to build a culture of privacy".
Disponível em: https://iapp.org/news/a/how-to-build-a-culture-of-privacy/. Acesso em 21.01.2021.


ZOOX
SMART DATA
INCOGNIA™
Symplä