Google

Setembro de 2018

Modelo para normas responsáveis de proteção de dados

Na nossa era digital, cada vez mais organizações usam dados pessoais para prestar cada vez mais serviços. O uso responsável dos dados pode beneficiar as pessoas, empresas e outras organizações no mundo inteiro. As normas protegem indivíduos e comunidades contra danos e o uso indevido dos dados, além de reforçarem a confiança que gera inovações e mudanças. A partir dos nossos esforços para a prestação de serviços inovadores que usam dados pessoais e da nossa experiência com a legislação internacional de privacidade em transformação contínua, sintetizamos o conjunto de princípios gerais a seguir. Esses princípios se baseiam nos regulamentos de privacidade estabelecidos e se destinam a organizações que tomam decisões sobre a coleta e o uso de informações pessoais. Este modelo ajuda o Google a avaliar as propostas legais e a defender normas de proteção de dados inteligentes, interoperáveis e adaptáveis.

REQUISITOS

Coletar e usar informações pessoais de forma responsável.
As organizações precisam respeitar os interesses individuais ao processar informações pessoais. Também precisam se responsabilizar pelo uso dos dados em prol das pessoas e da sociedade, reduzindo o risco de danos pelo uso de informações pessoais (dados que podem ser vinculados a uma pessoa ou um dispositivo pessoal).

Exigir transparência e manter as pessoas informadas.
As organizações precisam ser transparentes sobre os tipos de informações pessoais que coletam, por que coletam e como usam ou divulgam esses dados, principalmente para tomar decisões sobre uma pessoa. Os reguladores precisam incentivar as organizações a informar ativamente as pessoas sobre o uso dos dados no contexto dos próprios serviços, tornando as informações relevantes e úteis para os indivíduos.

Estabelecer limitações cabíveis às formas e aos meios de coletar, usar e divulgar informações pessoais.
A coleta, o uso e a divulgação de informações pessoais podem criar serviços úteis e inovadores, dentro dos limites apropriados para garantir que o processamento ocorra de forma compatível com interesses individuais e sociais.

Manter a qualidade das informações pessoais.
É necessário que as organizações tomem as medidas cabíveis para que as informações pessoais sejam sempre precisas, completas e atualizadas conforme a relevância aos fins a que se destinam. As ferramentas de correção e acesso aos dados, como mencionado abaixo, podem ajudar as organizações a cumprir essa obrigação.

Criar controles práticos para o uso de informações pessoais.

As organizações precisam disponibilizar mecanismos de controle individual apropriados, como a oportunidade de contestar o processamento de dados quando possível no contexto do serviço. Isso não exige um consentimento nem recurso específico a cada uso dos dados. Em muitos casos, o processamento das informações pessoais é necessário apenas para o funcionamento de um serviço. Da mesma forma, exigir que as pessoas controlem todos os aspectos do processamento de dados pode criar uma experiência complexa que desvie a atenção dos controles mais importantes sem os benefícios correspondentes.

Possibilitar o acesso, a correção, a exclusão e o download das informações pessoais pelo próprio indivíduo.
Cada indivíduo precisa ter acesso às informações pessoais que disponibiliza a uma organização e a opção de corrigir, excluir e exportar esses dados em formato legível por máquinas. Isso não só capacita as pessoas como também mantém o mercado inovador, competitivo e aberto a novos participantes.

Incluir requisitos para proteger as informações pessoais.
As organizações precisam adotar as precauções cabíveis para proteger as informações pessoais contra perda, uso indevido, acesso não autorizado, divulgação, modificação e destruição, além de notificar rapidamente as pessoas sobre violações de segurança com risco de dano significativo. Precauções básicas precisam ser adotadas em relação a qualquer coleta de informações pessoais, e outras medidas proporcionais relativas ao risco de danos precisam ser tomadas.

ESCOPO E RESPONSABILIDADE

Responsabilizar as organizações por compliance.
A responsabilidade pode e precisa ser estabelecida de muitas formas. Os legisladores e reguladores precisam definir requisitos básicos e cumpri-los com flexibilidade. Os programas de responsabilidade de mercado e safe harbor podem incentivar as práticas recomendadas, principalmente ao propor abordagens mais flexíveis para lidar com as tecnologias em transformação.

Focar no risco de danos para pessoas e comunidades.
Os reguladores precisam incentivar o design de produtos para evitar danos a pessoas e comunidades. A aplicação e as medidas judiciais precisam ser proporcionais aos possíveis danos envolvidos na violação. Não devem ser considerados ilegais os usos inovadores de dados só por serem inéditos, embora as organizações precisem se responsabilizar e evitar possíveis danos. Isso inclui um cuidado especial com informações confidenciais que possam representar um risco significativo. Para que as organizações desenvolvam mitigações eficazes, os reguladores precisam ter clareza sobre o que constitui um dano.

Distinguir entre serviços para o consumidor direto e serviços empresariais.
Como grande parte do processamento de informações pessoais é feita por uma empresa em nome de outra, quem processa muitas vezes não tem autoridade legal para tomar decisões independentes sobre como usar os dados nem atuar fora dos limites da orientação do cliente. Às vezes essa distinção é descrita como "processadores" versus "controladores", permitindo o uso eficaz de fornecedores autorizados e qualificados com custos extras mínimos de compliance, o que é importante principalmente para entidades pequenas. Os processadores podem consultar os controladores para atender a determinadas obrigações legais, inclusive de

transparência, controle e acesso, mas mesmo assim precisam se sujeitar às responsabilidades de segurança e programáticas básicas.

Definir a flexibilidade das informações pessoais para garantir incentivos e gerenciamento apropriados.
O escopo da legislação precisa ser amplo o bastante para abranger todas as informações que identificam um usuário específico ou um dispositivo pessoal ao longo do tempo, assim como os dados associados a esses identificadores, além de incentivar o uso de dados impessoais e menos arriscados quando adequado. A legislação precisa esclarecer se e como cada provisão é aplicada, inclusive no que diz respeito a informações agregadas, identificadas ou não e sob pseudônimos.

Aplicar as regras a todas as organizações que processam informações pessoais.
Cada vez mais os dados ganham importância em todos os setores da economia moderna. Exceto no contexto de relacionamentos específicos que já têm regras estabelecidas, como entre empregador/empregado ou advogado/cliente, a legislação precisa ser aplicada a todos os setores econômicos e a todos os tipos de organizações que processam informações pessoais. Embora alguns setores (por exemplo, o de saúde) possam ter mais regras, as normas precisam estabelecer referências para todas as organizações. A aplicação legal também precisa considerar as limitações de recursos de organizações diferentes, incentivando novos participantes e abordagens inovadoras e diversificadas às práticas de compliance.

Criar regras para melhorar o ecossistema e aceitar mudanças normativas e tecnológicas.
Assim como a tecnologia envolvida no processamento de dados, as normas sociais sobre privacidade e proteção de dados não são estáticas. Uma legislação básica pode esclarecer pontos básicos, enquanto revisões contínuas (como processos normativos, códigos de conduta, audiências administrativas) estabelecem orientações mais flexíveis, detalhadas e atualizáveis, sem uma reformulação substancial da estrutura legal. Os governos podem promover essas metas incentivando financeiramente pesquisas, práticas recomendadas e estruturas de código aberto. A criação de incentivos para as organizações criarem medidas avançadas de proteção à privacidade resulta na coleta e no uso responsável dos dados.

Aplicar o escopo geográfico conforme as normas internacionais.
A legislação de proteção de dados precisa seguir os princípios de territorialidade estabelecidos, regulamentando as empresas conforme elas façam negócios ativamente na jurisdição. A aplicação extraterritorial dificulta desnecessariamente o crescimento de novas empresas e cria conflitos de disposições legais entre jurisdições. Especificamente, não faz sentido que empresas pequenas se preocupem com conflitos com reguladores estrangeiros só porque algumas pessoas de outro país navegaram no site ou usaram o serviço delas.

Incentivar a interoperabilidade global.
Mecanismos que permitam um fluxo de dados transnacional são fundamentais para a economia moderna. As organizações se beneficiam de programas de compliance consistentes baseados nos princípios de proteção de dados amplamente compartilhados. Os países precisam adotar um modelo integrado de normas de privacidade, evitando sobreposições ou regras inconsistentes sempre que possível. Os reguladores precisam evitar requisitos conflitantes e imprevisíveis, o que gera a ineficiência e balcanização dos serviços, além de confundir as expectativas do consumidor. Especificamente, as restrições geográficas ao armazenamento de dados minam a segurança, a confiabilidade dos serviços e a eficiência empresarial. As normas de privacidade precisam ser compatíveis com os mecanismos de transferência de dados transnacional, os padrões industriais e outros mecanismos de cooperação entre organizações que garantam proteções associadas aos dados, não às fronteiras nacionais.