elastic

Usando o Elastic para impulsionar a conformidade com leis globais de privacidade

Resumo executivo

Para operar com sucesso no mundo digital moderno, as organizações estão focando em dados, especialmente em seu papel na IA. Como resposta, uma explosão de leis e regulamentações de privacidade está remodelando o cenário global de negócios. Acompanhar essas evoluções regulatórias não se resume a reduzir e mitigar riscos; trata-se de um diferencial competitivo relevante, no qual a conformidade com o cenário jurídico e regulatório de privacidade em rápida transformação também pode aumentar a confiança dos clientes, impulsionar o crescimento financeiro e fortalecer a resiliência operacional.

Este artigo técnico apresenta conceitos essenciais de legislação de privacidade de dados e demonstra como as organizações podem implantar a plataforma robusta do Elastic não apenas para atender aos requisitos aplicáveis de dados pessoais, mas também para operacionalizá-los com rapidez, eficiência e confiança. Descreveremos os seis princípios fundamentais de privacidade que são amplamente aplicáveis às regulamentações de privacidade de dados em todo o mundo e os relacionaremos às soluções da plataforma Elastic, ajudando as organizações a transformar a privacidade de dados de uma obrigação regulatória em uma vantagem competitiva.

Observação: este artigo é fornecido apenas para fins informativos e não se destina a constituir aconselhamento jurídico. Consulte seu próprio assessor jurídico para obter orientação legal.

Contexto e introdução às leis globais de privacidade

As leis globais de privacidade criam desafios cada vez mais complexos para organizações que coletam dados pessoais. Como os dados pessoais são amplamente considerados uma das commodities mais valiosas do mundo, a conformidade com as leis de privacidade pode ser um importante impulsionador de negócios para empresas, enquanto o não cumprimento pode prejudicar significativamente o crescimento de uma companhia.

À medida que as organizações coletam mais dados pessoais, encontrar uma solução escalável para gerenciar e proteger esses dados torna-se cada vez mais essencial para demonstrar responsabilidade e construir uma reputação positiva como fornecedor confiável em um mundo cada vez mais consciente em relação à privacidade.

Embora existam diferenças entre as diversas leis de privacidade, muitas compartilham determinados princípios gerais.

As principais leis de privacidade incluem:

- O Regulamento Geral sobre a Proteção de Dados da União Europeia (“GDPR”) e seu equivalente no Reino Unido
- Leis estaduais de privacidade dos EUA, como a Lei de Privacidade do Consumidor da Califórnia (“CCPA”)
- A Lei Geral de Proteção de Dados brasileira (“LGPD”)
- A Lei de Proteção de Informações Pessoais e Documentos Eletrônicos do Canadá (“PIPEDA”)
- Lei sobre a Proteção de Informações Pessoais do Japão (“APPI”)

A flexibilidade e a escala da oferta da plataforma Elastic capacitam as organizações a navegar e gerenciar a conformidade com esses diversos e complexos requisitos legais.

Dados pessoais

Já se foram os dias em que o conceito de “dados pessoais” se limitava a identificadores óbvios, como nomes completos, endereços de e-mail, identificadores governamentais e números de telefone. Atualmente, as leis de privacidade ao redor do mundo definem dados pessoais de forma ampla, de modo a abranger qualquer informação que possa ser associada a um dispositivo ou indivíduo específico.

Uma boa regra prática é assumir que as leis de privacidade provavelmente se aplicam quando a informação puder ser vinculada a um identificador único de uma pessoa. Com smartphones, dispositivos de IoT e outros dispositivos computacionais onipresentes na vida cotidiana, a coleta de dados pessoais cresceu exponencialmente em organizações de todos os setores, criando uma necessidade urgente e inegável de produtos e serviços que permitam às organizações gerenciar com confiança o processamento desses dados.

Controladores e processadores

As leis de privacidade em todo o mundo normalmente impõem obrigações distintas, mas muitas vezes sobrepostas, às organizações, dependendo de atuarem como “controladoras” ou “operadoras” de dados pessoais.

- **Controladoras,** também chamadas de “businesses” sob a CCPA, determinam as finalidades e os meios de processamento de dados pessoais. São as entidades que tomam decisões independentes sobre quais dados pessoais coletar e como processá-los.
- **Operadoras,** também chamadas de “service providers” sob a CCPA, prestam serviços a uma controladora contratante, ou, em alguns casos, a outra operadora, e só podem processar dados pessoais estritamente de acordo com as instruções da controladora, com a finalidade de prestar serviços a ela.

Embora obrigações diferentes se apliquem a controladoras e operadoras, a conformidade em cada papel exige compreender os tipos de dados pessoais que estão sendo processados e ser capaz de localizar dados pessoais de forma direcionada, escalável e eficiente.

A maioria das leis de privacidade ao redor do mundo também concede aos indivíduos o direito de exercer determinados direitos sobre seus dados, como acesso, exclusão e correção. Com prazos relativamente curtos para resposta, o uso de uma plataforma como o Elastic para analisar de forma eficiente conjuntos de dados estruturados e não estruturados não apenas ajuda a otimizar a conformidade, como também reduz os riscos de investigações regulatórias e litígios cíveis.

Princípios fundamentais de privacidade

As leis globais de privacidade frequentemente se baseiam em princípios fundamentais de privacidade. De forma geral, são eles:

1

Aviso

As leis de privacidade exigem que as organizações forneçam informações precisas e atualizadas sobre suas práticas de privacidade.

2

Privacidade desde a concepção

As leis de privacidade exigem que as organizações avaliem como suas práticas podem impactar os direitos de privacidade e os interesses dos indivíduos e projetem seus produtos de forma a cumprir essas leis.

3

Direitos

As leis de privacidade conferem aos indivíduos determinados direitos sobre seus dados pessoais, que podem incluir direitos de acesso, exclusão e correção.

4

Minimização de dados

As leis de privacidade exigem que as organizações pratiquem a minimização de dados, ou seja, que coletem e processem apenas os dados pessoais necessários para as finalidades empresariais para as quais foram coletados, e imponham limites de retenção e políticas de exclusão para garantir que as organizações não mantenham dados além do necessário.

5

Segurança

As leis de privacidade exigem determinados padrões de segurança para proteger dados pessoais.

6

Notificação de incidente

As leis de privacidade e segurança impõem uma série de obrigações às organizações que enfrentam um incidente de segurança ou um ataque envolvendo dados pessoais.

O custo da não conformidade

A não conformidade com leis de privacidade pode resultar em penalidades elevadas, honorários advocatícios e danos à reputação. Penalidades regulatórias sob frameworks como o GDPR e a CCPA podem ser significativas o suficiente para impactar materialmente o resultado financeiro de uma empresa, enquanto litigantes também podem buscar indenizações por violações de privacidade, incluindo ações coletivas após ataques envolvendo dados.

De acordo com um relatório da IBM Security e do Ponemon Institute, o custo médio de um ataque envolvendo dados em 2024 foi de US$ 4,88 milhões, o que representou um aumento de 10% em relação ao ano anterior. O Cyber Risk Report da AON constatou que 56 eventos cibernéticos amplamente divulgados causaram, em média, perdas de 27% no valor das ações das organizações impactadas em 2024. Esse tipo de dano reputacional pode igualmente comprometer de forma irreversível a vantagem competitiva de uma organização. Nesse cenário, conformidade não é apenas um custo, mas um investimento estratégico.

Usando o Elastic para suas necessidades de conformidade em proteção de dados

O Elastic ajuda as organizações a encontrar respostas relevantes com velocidade sem precedentes por meio de soluções empresariais abertas e flexíveis. A conformidade com leis de privacidade ao redor do mundo exige compreensão de todo o seu ecossistema de dados: onde os dados pessoais estão armazenados, como circulam e de que forma são processados. É nesse ponto que a plataforma Elasticsearch se destaca, simplificando e automatizando esses processos para uma conformidade contínua e eficiente. A seguir, apresentamos o valor do Elastic mapeado aos seis princípios fundamentais de privacidade descritos acima.

Aviso

Os recursos de mapeamento de dados do Elastic permitem que as organizações compreendam o escopo e os tipos de dados pessoais distribuídos por servidores organizacionais e além.

Transparência é um princípio central das leis de privacidade. Os indivíduos têm o direito de entender quais tipos de dados pessoais uma organização coleta sobre eles, as finalidades da coleta e as circunstâncias em que seus dados são divulgados a terceiros. As leis de privacidade frequentemente exigem que as organizações disponibilizem políticas de privacidade abrangentes, como a própria Declaração de Privacidade da Elastic, explicando esses conceitos conforme apresentado na Central de Confiança da Elastic.

Para cumprir esse princípio de transparência, uma organização deve compreender o escopo dos dados pessoais que coleta. Isso exige um exercício robusto de mapeamento de dados, que consiste em um processo sistemático para identificar e documentar todos os fluxos de dados pessoais dentro de uma organização.

Sem uma solução escalável, as organizações frequentemente acabam dependendo de uma combinação desorganizada de planilhas ultrapassadas, respostas a questionários de inventário de dados e entrevistas pontuais com diferentes unidades de negócio para identificar quais dados pessoais são coletados e como circulam dentro e fora da organização.

Na melhor das hipóteses, os registros podem estar corretos em um determinado momento, apenas para depois se tornarem desatualizados diante das exigências de coleta e processamento de dados em uma economia impulsionada por dados.

O Elastic pode ajudar as organizações a obter insights essenciais para aprimorar seus processos de mapeamento de dados. Sem visibilidade sobre os tipos de dados pessoais coletados, onde esses dados estão armazenados e com quem são compartilhados, uma organização não consegue confirmar a conformidade com as leis de privacidade. Ao indexar informações sobre seus fluxos de dados no Elastic, seus poderosos recursos de pesquisa de texto completo permitem identificar rapidamente aplicações, tabelas, consultas ou relatórios que utilizam dados pessoais.

O uso do Elastic para otimizar o mapeamento de dados também ajuda as organizações a cumprir obrigações contratuais previstas nas leis de privacidade, pois os fluxos de dados identificados determinam as partes com as quais a organização deve celebrar adendos de proteção de dados, mecanismos de transferência de dados ou outros acordos específicos para a proteção de dados pessoais. Da mesma forma, as cadeias de fornecimento atuais podem abranger centenas ou milhares de fornecedores e subprocessadores. A capacidade de indexar e realizar pesquisas de texto completo instantaneamente em milhares de contratos também pode facilitar relatórios sobre a situação de fornecedores e, mais importante, viabilizar programas proativos de gestão de fornecedores.

Privacidade desde a concepção

As organizações podem usar o Elastic para reforçar a privacidade desde a concepção, inclusive incorporando princípios de minimização de dados.

Se uma organização estiver considerando usar o Elastic como repositório de dados pessoais, os recursos do Elastic Cloud Enterprise, ou ECE, o software central de orquestração do Elastic, podem colocá-la no caminho certo desde o início. O princípio da proteção de dados desde a concepção consiste em tratar dados pessoais como um ativo valioso, limitando o acesso, mantendo a precisão, implementando controles adequados de segurança de dados e restringindo os períodos de retenção.

Diferentemente de arquiteturas tradicionais com um único datastore massivo e camadas complexas e sobrepostas de controles de acesso, exigidas para permitir que diferentes projetos acessem apenas determinados dados, o Elastic permite que usuários instanciem novos clusters do Elasticsearch para cada projeto e incluam apenas os dados relevantes para esse projeto no respectivo cluster.

Essa arquitetura distribuída possibilita a minimização de dados pessoais, outro princípio fundamental de privacidade. Por exemplo, clientes podem usar o Elastic para categorizar dados em camadas de armazenamento, em que informações de logs de acesso alimentadas pelo Elastic ajudam empresas a identificar dados não utilizados e, assim, orientar políticas e práticas de retenção de dados.

O Elastic também permite que as organizações compreendam quando e como conduzir avaliações de impacto à proteção de dados, ou DPIAs. Nos termos do GDPR e de regulamentações semelhantes, uma DPIA é uma avaliação, em alguns casos obrigatória, utilizada para garantir que o processamento de dados pessoais seja realizado de forma responsável e com a minimização de qualquer potencial dano aos indivíduos. Saber onde os dados estão armazenados, como são processados e para onde fluem agiliza a realização de DPIAs, que tradicionalmente podem exigir apoio multifuncional entre diferentes unidades de negócio para compreender os usos de dados pessoais. As DPIAs, por sua vez, demonstram conformidade fundamental ao mesmo tempo que permitem às organizações limitar o processamento de dados pessoais ao que é autorizado pelas leis globais de privacidade.

Direitos do titular dos dados

As organizações podem usar o Elastic para identificar dados pessoais relevantes, avaliar a aplicabilidade dos direitos dos titulares e atender às solicitações desses titulares.

As leis globais de privacidade concedem aos indivíduos determinadas opções sobre como seus dados pessoais são processados. Essas opções normalmente incluem direitos de acesso, exclusão e correção de dados pessoais, além do direito de se opor a determinados tipos de processamento. Os recursos de mapeamento de dados do Elastic formam a base sobre a qual as organizações podem processar solicitações de titulares de dados.

- **Acesso:** o Elasticsearch permite que as organizações pesquisem em seus repositórios de dados para identificar dados pessoais em toda a organização, incluindo a identificação de tabelas, consultas, relatórios ou aplicações que utilizam dados pessoais. As organizações também podem usar o Elastic para viabilizar funções de pesquisa para usuários finais, permitindo que pesquisem seus próprios dados. Conceder aos usuários finais recursos robustos de pesquisa reduz a demanda por suporte, pois eles podem utilizar ferramentas de autoatendimento para localizar e exportar seus dados. Quando as ferramentas de autoatendimento não forem suficientes, o Elastic permite que as organizações pesquisem rapidamente seus próprios repositórios para atender a solicitações de acesso de titulares.

- **Exclusão:** após usar o Elastic para identificar os dados pessoais mantidos sobre um indivíduo, uma organização pode utilizá-lo para transformar esses dados, incluindo marcá-los para retenção sob uma exceção de exclusão, excluí-los permanentemente ou aplicar outras técnicas de exclusão permitidas pelas leis de privacidade, como anonimização e determinados tipos de pseudonimização. Utilizar o Elastic para transformar dados pessoais de forma rápida e sem a necessidade de desenvolvimento técnico complexo ajuda as organizações a permanecerem em conformidade, evitar escrutínio regulatório e manter a utilidade dos dados dentro dos limites das leis globais de privacidade.

- **Correção:** da mesma forma, as leis de privacidade frequentemente permitem que indivíduos solicitem a correção de seus dados pessoais. O Elastic pode isolar os dados pessoais mantidos sobre um indivíduo, permitindo que a organização concentre esforços no processamento da solicitação, e não na localização dos dados.

- **Restrições:** algumas leis de privacidade, como o GDPR e seu equivalente no Reino Unido, também preveem o direito de se opor ou o direito de solicitar a limitação do processamento de dados pessoais. As organizações podem usar os recursos de mapeamento e categorização de dados do Elastic para determinar rapidamente como responder a essas solicitações e restringir permissões de acesso e uso conforme necessário, economizando tempo valioso e permitindo que as equipes de conformidade respondam dentro dos prazos reduzidos estabelecidos por essas leis.

Minimização de dados

Conforme apresentado na seção *Privacidade desde a concepção*, o Elastic viabiliza recursos de minimização de dados para empresas. Os princípios de minimização de dados exigem que as organizações coletem, processem e limitem a retenção de dados pessoais ao que for necessário para alcançar as finalidades autorizadas de processamento.

Por exemplo, uma forma de minimizar o processamento de dados pessoais para cumprir essa obrigação é por meio da **pseudonimização**, isto é, a substituição de identificadores pessoais por valores substitutos, ou da **anonimização**, isto é, a remoção completa de identificadores pessoais para que o indivíduo não possa mais ser identificado. Descubra como uma importante companhia aérea europeia utiliza o pipeline de ingestão do Elastic para ofuscar dados sensíveis antes do armazenamento. Esses resultados podem ser alcançados com o uso do Logstash, uma integração disponível no Elastic que ingere dados de múltiplas fontes para viabilizar sua transformação, incluindo anonimização e pseudonimização, promovendo assim os objetivos de minimização de dados e reduzindo riscos de segurança..

O uso do Elastic para mapeamento e auditoria de dados também permite que as organizações analisem de forma mais aprofundada o uso real dos dados pessoais retidos, possibilitando ajustar de maneira mais eficaz os períodos e as políticas de retenção de dados.

Segurança e notificação de incidente

Para mais informações sobre como o Elastic pode ajudar as organizações a proteger dados pessoais e responder rapidamente em caso de incidente envolvendo dados, consulte nosso artigo técnico sobre segurança.

Conclusão

Privacidade de dados não é apenas um requisito regulatório, é uma exigência estratégica de negócios. Com multas elevadas, interrupções operacionais, danos reputacionais e a confiança dos clientes em jogo, as organizações precisam de uma maneira confiável e escalável de mapear, categorizar, gerenciar, transformar, analisar e excluir seus dados. O Elastic simplifica cada etapa desse processo, oferecendo a escalabilidade necessária para garantir conformidade e fortalecer a confiança dos clientes.

