1.Privacy

Nossas organizações coletam uma enorme quantidade de dados, e há leis de privacidade que provavelmente se aplicam a uma grande parte dessas informações. Neste vídeo, discutiremos algumas dessas preocupações com a privacidade e como as organizações são obrigadas a proteger seus dados.

Em muitas regiões, a privacidade começa nos níveis local e estadual. Existe uma grande quantidade de dados coletados pelos governos locais, especialmente informações sobre nossas casas, veículos e licenças médicas. No nível nacional, há leis que protegem a privacidade de todos no país. Um exemplo são as leis HIPAA, que regulamentam o setor de saúde e afetam todos os cidadãos de um país.

Muitos países também estão trabalhando juntos para garantir a privacidade de seus cidadãos, independentemente de onde vivam. **Um exemplo de lei de privacidade que afeta vários países é o GDPR** (Regulamento Geral de Proteção de Dados), uma regulamentação da União Europeia que protege a privacidade de todos que vivem na região. Entre os dados protegidos pelo GDPR estão nome, endereço, fotos, e-mails, informações bancárias, postagens em redes sociais e muito mais.

O GDPR devolve o controle desses dados para os usuários, permitindo que eles decidam o que acontece com suas informações pessoais. Se alguém deseja remover seus dados de um site, basta solicitar a exclusão, e o site é obrigado a cumprir essa solicitação. Esse princípio é conhecido como "direito ao esquecimento". O GDPR define um "titular de dados" como qualquer pessoa identificável por meio dessas informações, o que significa que, na prática, todos nós somos titulares de dados.

Além do GDPR, muitas outras leis de privacidade adotam essa abordagem, colocando a proteção dos dados sob a perspectiva do usuário, ao contrário das leis anteriores que atribuíam essa responsabilidade principalmente às empresas.

Dentro das organizações, a gestão de dados envolve diferentes papéis. O "dono dos dados" é o responsável principal pelos dados em uma determinada área, como o vice-presidente de vendas que gerencia dados de clientes ou o tesoureiro que supervisiona as informações financeiras. Além disso, há os "controladores de dados", que decidem como os dados são usados, e os "processadores de dados", que realizam o processamento dessas informações. O processador pode ser interno ou um terceiro contratado para gerenciar os dados.

Um exemplo comum dessa relação ocorre entre o departamento de folha de pagamento de uma empresa e um prestador de serviços de pagamento. O departamento de folha de pagamento atua como o controlador de dados, decidindo salários e datas de pagamento, enquanto a empresa terceirizada processa efetivamente os pagamentos.

Quando dados sensíveis são compartilhados com terceiros, como prestadores de serviço, muitas empresas utilizam acordos de confidencialidade

(NDAs) **para garantir a privacidade dessas informações**. Assim como uma empresa que fabrica produtos mantém um inventário de seus bens físicos, organizações que armazenam dados mantêm um "inventário de dados", que registra quais informações são coletadas, quem é responsável por elas, a frequência de atualização e o formato dos dados.

Para garantir a conformidade com as regulamentações de privacidade, as empresas precisam compreender como os dados são utilizados, tanto internamente para colaboração e segurança de TI, quanto externamente ao compartilhar informações com terceiros. Antes de compartilhar qualquer dado, é essencial garantir que sua divulgação esteja de acordo com as leis e regulamentações aplicáveis.