ENTENDA A GDPR

CYBER SECURITY NEWSLETTER MAIO 2018

A sua empresa está pronta?

Você certamente recebeu diversos e-mails no decorrer desta semana referentes à atualização dos termos e condições de privacidade de empresas em que você se inscreveu para receber notícias ou fez compras de serviços online no passado.

Com a entrada da nova legislação Europeia de Proteção de Dados – GDPR, em vigor hoje, dia 25/05, muitas empresas estão ainda despreparadas diante das necessidades que a regra demanda a empresas que oferecem seus serviços a cidadãos europeus. A diretriz determina como o as empresas e os indivíduos coletam, armazenam e compartilham dados sobre indivíduos na Europa, sendo aplicada em todos os estados da UE a partir de 25 de maio de 2018.

De acordo com a UE, o regulamento procura "harmonizar" leis de privacidade de dados anteriormente díspares em todos os estados membros da UE, ao mesmo tempo que confere maior proteção e direitos aos cidadãos.

Mesmo que uma empresa não tenha presença na Europa, mas possui relacionamento com clientes ou parceiros europeus, deverá respeitar o novo regulamento. Desde grandes instituições a pequenas plataformas de e-commerce, se há coleta ou tratamento de dados pessoais de um indivíduo que está no território da União Europeia, de forma relacionada à oferta de bens ou serviços, ainda que fornecidos gratuitamente, haverá sujeição às normas do GDPR.

A GDPR fornece diferentes obrigações para o controlador e o processador de dados:

Um controlador é a entidade que determina as finalidades, condições e meios do processamento de dados pessoais, enquanto o processador é uma entidade que processa dados pessoais em nome do controlador.

DESTAQUE

GDPR É APLICÁVEL EM:

■ Empresa brasileira sem subsidiárias na UE, oferecendo serviços de mídia social gratuita, através de um site hospedado no Brasil para indivíduos na União Europeia;

■ Se um brasileiro vive na UE, mas não é de fato um cidadão da UE (por exemplo, expatriado);

■ Uma pessoa acessa o site de um e-commerce no Brasil de sua casa na UE para efetuar uma compra. Eles fornecem dados pessoais, como detalhes do cartão de crédito e seu endereço residencial na UE, para a entrega do produto.

GDPR NÃO É APLICÁVEL EM:

■ Um turista da União Europeia acessa o site de uma pizzaria brasileira próxima do seu hotel no Brasil e fornece dados como nome para solicitar uma entrega de pizza para o seu hotel no Brasil.

Lista das principais medidas

■ A regulamentação estabelece os direitos dos indivíduos e visa a facilitar o acesso a informações pessoais detidas pelas empresas, bem como define as obrigações impostas às organizações.

•. Designar responsáveis pela proteção de dados (DPO - Data Protection Officer);

Qualquer empresa que processa mais de 5000 registros em um período de 12 meses precisa alocar um responsável pela gestão dos dados (DPO). Um DPO pode atender a uma empresa ou um grupo de empresas e será responsável por monitorar a conformidade com as regras do GPDR e realizar avaliações de proteção de dados, bem como treinar pessoal em políticas globais. DPOs não podem ocupar uma posição dentro da organização que os leve a determinar os propósitos e os meios de processamento de dados pessoais, como CEO, COO, CFO, diretores de marketing, RH ou TI (como outros com tais poderes determinantes). O artigo WP29 recomenda regras internas para evitar qualquer conflito.

• Estabelecer um programa de segurança cibernética;

•Seguir padrões de segurança de processamento de dados;

Organizações devem manter registros internos de todas as atividades de processamento de dados. As informações registradas precisarão incluir o nome e os detalhes da organização, os fins do processamento de dados, a descrição de categorias de indivíduos e dados pessoais, os destinatários, os detalhes das transferências de dados e os cronogramas de retenção de dados.

• Responsabilidade documentada;

As organizações devem manter registros internos de todas as atividades de processamento de dados. As informações registradas precisarão incluir o nome e os detalhes da organização, os fins do processamento de dados, a descrição de categorias de indivíduos e dados pessoais, os destinatários, os detalhes das transferências de dados e os cronogramas de retenção de dados. É importante notar que sob o GDPR as empresas serão proibidas de transferir dados para um país terceiro que não possua leis adequadas de proteção. A Comissão Europeia avaliou os países com leis de proteção de dados “satisfatórias” e mantém uma lista de “países aprovados”. No Brasil, como não há uma lei regente de proteção de dados, empresas que necessitam fazer a transferência de dados de um estado europeu devem ter tomar as devidas garantias para a proteção de dados pessoais em concordância ao que segue a GDPR.

•. Entender o consentimento e exclusão permanente de dados

As organizações que processam dados pessoais devem comprovar que têm autorização para usar os dados que retêm. Qualquer pessoa tem o direito de suspender o seu consentimento a qualquer momento. Por isso, a empresa deve facilitar o processo de cidadãos que solicitarem a exclusão de seus dados pessoais dos registros de uma determinada organização.

Exemplo dos efeitos regulatórios da GDPR e como a multa será aplicada

■ Como o GDPR pode ser aplicado contra organizações de países terceiros, uma vez que um órgão responsável não poderia multar uma empresa no Brasil?

Os controladores/processadores não pertencentes à Espaço Econômico Europeu(EEE) devem nomear um representante local na Europa que responderá pelas ações da empresa em território europeu.

■ O que aconteceria se uma organização fora da UE se recusasse a pagar a multa, acreditando que estava fora da jurisdição da UE?

Ação de imposição sob os tratados internacionais e possíveis sanções.

Lei de Proteção de Dados no Brasil

■ No Brasil, a legislação aplicável em matéria de proteção de dados é esparsa, encontrando fundamentos na Constituição Federal, no Código Civil, no Código de Defesa do Consumidor, Lei de Sigilo Bancário, Lei de Sigilo Médico e no Marco Civil da Internet, dentre outros diplomas legais.

O artigo 927 do Código Civil em seu parágrafo único aponta: “haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem”. Outros dispositivos legais acompanham o princípio da responsabilização objetiva devido ao risco do negócio, principalmente na legislação consumerista.

Recentemente, uma comissão no MPF foi formulada para promover a proteção dos dados pessoais, sugerir diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade e estimular a adoção de padrões para serviços e produtos que facilitem o controle dos titulares sobre seus dados pessoais. Em julho o Senado aprovou por unânimidade a PL53/2018 - Lei Geral de Proteção de Dados Brasileira (LGDP), refletindo a GDPR e aplicada a qualquer empresa que oferta ou fornece bens ou serviços envolvendo dados de indivíduos.

Assim como na GDPR, as empresas devem se adaptar à nova regra, adequando seus processos, assegurando o sigilo de dados e implementação de boas práticas as quais incluem definições técnicas e boa governança. Passa a ser obrigatório o consentimento do indivíduo e comunicar ao órgão competente e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. As sanções vão desde a suspensão de atividades, multas que variam entre 2% do faturamento da empresa a R$ 50 milhões.

Seguro Cyber_

Todas as empresas independentes de sua atuação possuem exposições Cyber. As exposições relacionadas à tecnologia são reais e cada vez mais presentes de natureza global, agindo sem levar em consideração geografia, setor ou tamanho da empresa. Para empresas que tratam com várias jurisdições e possuem exposições que estão sujeitas a leis de proteção de dados como o GDPR devem demonstrar às autoridades velocidade em mitigar os danos que um vazamento de dados pode causar. Veja o exemplo dos eventos ocorridos com empresas como Banco Inter, Netshoes, Movida, XP Investimentos, Vivo, Equifax, Facebook e outras que perderam valores capitais significantes após a divulgação de incidentes.

O seguro cibernético é projetado para apoiar e proteger empresas em relação a estes e-riscos em evolução. Ele fornece cobertura abrangente desde os custos de restauração, reconstrução de sistemas de computador e dados aos custos de gestão de crise como investigação forense, custos de defesa tanto para questões envolvendo órgãos reguladores – sejam eles diretamente envolvidos a leis de proteção de dados ou por ações de órgãos reguladores como MPF, CVM, Procon, etc. - e como custos de danos sofridos pelas partes que tiveram suas informações violadas, reparo de imagem, perda de receita entre outras coberturas.

O aumento global de ataques cibernéticos fez com que as empresas considerassem uma apólice de Seguro Cyber de cobertura ampla e bem planejada, não apenas para cobrir os riscos decorrentes de uma violação do GDPR, mas também para o imediato acesso a especialistas previstos nestas apólices.

Além disso, o GDPR cria uma exposição significativa não apenas para o seguro Cyber, mas também para o Seguro de D&O. Com a prestação de contas como um tema central no novo regulamento, a Responsabilidade Cibernética não é mais o único seguro relevante a ser considerado e a ênfase também deve ser colocada no seguro de Responsabilidade de Diretores.

A constante evolução das ameaças está claramente impondo responsabilidades adicionais aos diretores. O impacto financeiro de uma violação de dados pode ser enorme; como tal, os diretores devem se preocupar tanto com sua obrigação fiduciária perante a empresa quanto com seus acionistas, bem como com os ativos pessoais dos diretores, que estão em risco no caso de uma reivindicação por alegada gestão ilícita. Em uma situação em que um incidente cibernético tem um efeito material no valor do acionista da empresa, ou mesmo no valor da reputação, os litígios certamente ocorrerão, especialmente se houver um lapso por parte do conselho para garantir a exposição cibernética.

CONTATO

Marta Helena Schuh
Cyber Specialist
+55 (11) 3156-3975
marta_schuh@jltbrasil.com