14 TÓPICOS SOBRE A LGPD QUE VOCÊ PRECISA SABER.

Este eBook consolida os principais tópicos associados a Lei Geral de Proteção de Dados Pessoais (LGPD) que profissionais técnicos e jurídicos devem conhecer antes de iniciar projetos em busca da conformidade.

ostec
Segurança digital de resultados

ÍNDICE

INTRODUÇÃO

No início de agosto de 2018, o governo brasileiro sancionou a Lei nº 13.709, chamada de Lei de Proteção de Dados Pessoais, uma normativa que regula como empresas do setor público e privado devem tratar os dados pessoais de cidadãos brasileiros.

A lei já vinha sendo debatida há 8 anos no Congresso brasileiro e serve para complementar o Marco Civil da Internet, em vigor desde 2014. Incentivados pelos últimos escândalos envolvendo venda de dados de usuários do Facebook por parte da Cambridge Analytica, que teria influenciado a eleição americana, governo e sociedade civil se viram obrigados a modernizar a legislação, garantindo aos cidadãos maior segurança para os dados, principalmente em ambientes online.

Neste cenário, tanto usuários como empresas, que mantenham dados pessoias, precisam agir de acordo com as orientações apresentadas na LGPD.

Este e-book consolida 14 dos principais tópicos associados a Lei Geral de Proteção de Dados, para que pessoas e profissionais possam dar os primeiros passos rumo ao entendimento da lei. Continue a leitura.

TÓPICO #1

O QUE É E PARA QUE SERVE A LEI DE PROTEÇÃO DE DADOS?

A nova lei visa estabelecer regras e limites para a coleta, guarda e transferência de dados de pessoas, principalmente em meios digitais. A partir de agora, casos como o da Cambridge Analytica poderão ser punidos com muito mais rigor e celeridade, se acorrerem no Brasil.

Com a lei, toda informação coletada, seja por empresas ou não, como dados cadastrais, nome, endereço, e-mail ou até mesmo textos, fotos e outros tipos de informações presentes em redes sociais, precisam ter o consentimento expresso do titular para serem armazenadas ou enquadrarem-se às exceções da lei.

Esta solicitação de uso deve ser feita de forma clara e objetiva e sempre respeitando a finalidade para qual foi especificada. Assim o cidadão tem a garantia de que toda informação a ser coletada será tratada de maneira responsável, evitando divulgações e comercialização não autorizadas.

Com a implantação da Lei de Proteção de Dados, o número de ligações de empresas que você nunca teve contato e que, mesmo assim, sabem tudo sobre você, deve diminuir. Agora, empresas que comercializam dados sigilosos de seus usuários podem ser severamente punidas.

TÓPICO #2

O QUE SÃO "DADOS PESSOAIS", AFINAL?

Uma das primeiras preocupações da lei é deixar claro o que significa "dado pessoal", para que não exista margem para interpretações evasivas e errôneas.

Portanto, dado pessoal é toda informação relacionada a uma pessoa que possa, isoladamente ou em conjunto com outros dados, permitir sua identificação, como por exemplo: nome, apelido, endereço residencial, endereço de e-mail, endereço IP, fotos próprias, formulários cadastrais, números de documentos, etc.

Inclusive dados como preferência sexual, política, dados de consumo, entre outros que podem ser usados de forma discriminatória ou que permitem formar perfis comportamentais ou para fins de propaganda, também são considerados como "sensíveis" e podem receber proteção dependendo do contexto.

TÓPICO #3

JÁ EXISTE LEI PARECIDA EM OUTROS LUGARES?

Em maio de 2018, a União Europeia também sancionou o Regulamento Geral de Proteção de Dados (RGPD ou GDPR), que substituiu a Diretiva de Proteção de Dados (criada em 1995) e também trouxe mais segurança aos cidadãos do bloco.

Além da UE, na América Latina temos países como o Chile, Colômbia, Costa Rica, Peru, Uruguai e Argentina que também possuem leis no mesmo nível da GDPR para a proteção dos dados de seus cidadãos.

TÓPICO #4

O QUE É E PARA QUE SERVE A LEI DE PROTEÇÃO DE DADOS?

As empresas, a partir de 18/09/2020, são obrigadas a coletar somente os dados realmente necessários e essenciais aos serviços prestados, além de deixar claro para quais fins está colhendo estas informações e dando a opção ao usuário de aceitar ou não de forma clara e objetiva.

Caso aceite, poderão ser coletados dados de cadastro como nome, endereço, CPF etc, além de preferências de consumo, hábitos, condições de saúde, orientação sexual, preferências políticas, informações acerca do patrimônio e situação creditícia, que poderão ser tratados para diversos usos, inclusive propaganda eleitoral.

Por isso é importante que os usuários estejam atentos aos serviços para os quais cedem suas informações e, ainda que pareça difícil, se atentem às clausulas que explicam quais os dados serão coletados e para quais fins serão utilizados.

OBS: Crianças não poderão ter seus dados utilizados por empresas, a não ser que tenham a autorização de um dos pais ou responsável legal.

TÓPICO #5

QUAIS TIPOS DE DADOS PESSOAIS NÃO SE APLICAM A ESSA LEI?

Dados sobre a saúde das pessoas estão livres para serem utilizados para fins de pesquisa, por intitutos credenciados. A lei também não se aplica aos dados que são usados para fins jornalísticos ou artísticos, para fins acadêmico, para investigações, repressão de crimes, ou em casos de segurança pública e defesa nacional.

TÓPICO #6

É POSSÍVEL ALTERAR, APAGAR OU TRANSFERIR DADOS COLETADOS?

Apartir de agora, com a Lei de Proteção de Dados, o usuário pode decidir o que será feito com as informações que cede a uma empresa. Ele pode pedir alteração e, inclusive, a exclusão de seus dados.

Por exemplo, com a nova lei, provedores de serviços de e-mail, devem possibilitar que os titulares transfiram mensagens de sua conta de e-mail para um outro provedor de serviço, sem maiores transtornos. Também será possível solicitar a revisão de decisões automatizadas, geradas por mecanismos de classificação, tal como os utilizados por empresas fornecedoras de crédito.

Dados pessoais também poderão ser transferidos para outros países, desde que eles também tenham medidas que assegurem a proteção destes dados para seus cidadãos e que o titular do mesmo esteja devidamente comunicado sobre o compartilhamento internacional do dado.

Além disso, após o encerramento da relação entre a empresa e o cliente, a lei ordena que as informações pessoais obtidas até então, também sejam excluídas, exceto se houver obrigação legal ou outra razão justificável para a sua preservação.

TÓPICO #7

QUAIS SÃO OS PRINCIPAIS "ATORES" ENVOLVIDOS NA LEI?

De acordo com o Artigo 5° da Lei, é possível identificar quatro atores, que possuem papéis distintos, como apresentado a seguir:

Titular: É toda e qualquer pessoa, cujos dados pessoais são objeto de tratamento.

Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador, os titulares e a autoridade nacional.

Agentes de tratamento: São representados pelo Controlador e Operador.

TÓPICO #8

O QUE É O RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS? DPIA – DATA PROTECTION IMPACT ASSESMENT

O DPIA é um documento que fica sob responsabilidade do Controlador do dado. Este deve conter a descrição dos processos de tratamento de dados pessoais que podem gerar riscos à liberdade e aos direitos fundamentais das pessoas, bem como medidas e mecanismos para mitigação de risco. Tal documento pode ser solicitado pela agência Nacional de Proteção de Dados sempre que julgado conveniente, com garantia de sigilo sobre segredos comerciais e industriais presentes no mesmo.

TÓPICO #9

PARA QUE SERVE O MODELO DE REPORT DE INCIDENTES

A Lei orienta que o Controlador deverá comunicar à autoridade nacional, e ao titular do dado, a ocorrência de incidentes de segurança que possam acarretar em risco ou danos relevantes para os titulares. O relatório deve conter informações relevantes sobre o incidente, tais como: natureza dos dados pessoais afetados, titulares envolvidos, medidas técnicas de segurança utilizadas para a proteção do dado e as medidas a serem adotadas para reverter ou mitigar os efeitos do prejuízo, além de outros itens contidos no Artigo 48 da presente Lei.

TÓPICO #10

HÁ PUNIÇÕES EM CASO DE VAZAMENTO OU MAU USO?

As empresas devem garantir a segurança de todas as informações de seus usuários, impedindo acessos não autorizados, destruição, alteração ou qualquer forma de tratamento inadequado ou ilícito.

E, caso isso aconteça, os proprietários destes dados deverão ser informados imediatamente sobre toda a extensão dos vazamentos e possíveis danos, além de medidas de segurança a serem tomadas.

Caso seja comprovada a infração da lei, a empresa pode receber desde advertências, até multas simples ou diária equivalente a 2% do seu faturamento, porém limitadas ao valor máximo de 50 milhões de reais.

TÓPICO #11

QUEM VAI FISCALIZAR? EXISTE ÓRGÃO REGULADOR?

No dia 27 de dezembro de 2018, Michel Temer aprovou a Medida Provisória 869, que regulamenta a criação da agência Nacional de Proteção de Dados (ANPD). A agência foi integrada ao Gabinete da Presidência da República, sendo responsável por regular a Lei Geral de Proteção de Dados no Brasil.

Juntamente com a ANPD, Ministério Público e Procon atuarão na fiscalização para cumprimento da LGPD.

TÓPICO #12

A LEI SE APLICA APENAS A EMPRESAS BRASILEIRAS?

A lei se aplica a qualquer empresa que colete dados de cidadãos brasileiros, mesmo que esteja fora do Brasil.

Por exemplo: se o Google coleta os dados de um usuário brasileiro, mas essa informação é processada e utilizada somente nos Estados Unidos, ainda assim a empresa precisará seguir a legislação brasileira.

TÓPICO #13

QUANDO A LEI COMEÇA A VALER?

Com a aprovação da MP pelo ex-presidente Temer, em dezembro de 2018, o prazo estabelecido para lei entrar em vigor foi de 24 meses. Depois de muitas idas e vindas a LGPD entrou em vigor no dia 18/09/2020. Contudo, vale ressaltar que as sanções e multas entram em vigor apartir de agosto de 2021.

TÓPICO #14

COMO AS EMPRESAS PRECISAM SE PREPARAR?

Não serão só as grandes corporações que deverão se preocupar com a nova lei. Pequenas empresas que armazenam dados de colaboradores, parceiros e prestadores de serviço também terão que estar em conformidade, tendo que criar mecanismos para

proteger estas informações, além de explicitar sempre para quais fins estas serão utilizadas.

A lei também exige que exista um encarregado para dialogar com a autoridade nacional, aceitar reclamações dos titulares, orientar funcionários, prestar esclarecimentos e tomar as devidas providências quando necessário.

É importante também que a empresa possua um bom aconselhamento jurídico que oriente na elaboração de contratos e termos de cessão de dados, levando sempre em consideração o cumprimento da lei e o bem-estar dos usuários.

Dessa forma, se torna extremamente relevante que toda organização que trabalhe armazenando informações de seus usuários, passe a adotar medidas especiais para a manutenção e segurança de suas redes.

CONSIDERAÇÕES FINAIS

O profissional de tecnologia se tornará uma peça chave neste processo, principalmente no que tange a elaboração de estratégias para minimizar os riscos associados ao vazamento de informações sensíveis dos clientes, de maneira geral. A exposição de dados, intencional, ou não, pode gerar prejuízos muito representativos para as empresas, independentemente do seu porte ou segmento. Já existem variações de Ransomware que ao invés de solicitar resgate para liberação dos dados sequestrados durante o ataque, pedem resgate para não tornar tais informações públicas, o que pode gerar um impacto muito maior do que a perda do dado em si.

Para finalizar este e-book, uma última dica. Avalie sempre a idoneidade dos aplicativos que você costuma utilizar, assim como as informações que são solicitadas por cada um deles, fazendo uma análise crítica sobre a real necessidade de exposição de dados sensíveis para uso dos mesmos. Na dúvida, não insira seus dados e lembre-se: Simples informações de nome, endereço, telefone etc, podem ser utilizadas em ações de engenharia social para aplicação de golpes.

Receber promoções, ou contatos indesejados de telemarketing certamente são os usos mais frequentes dos dados que os usuários inserem em formulários de sites e aplicativos, contudo o uso não é limitado a isso.

CONTINUE LENDO

SE VOCÊ GOSTOU DO ASSUNTO E GOSTARIA DE NOVAS LEITURAS, FIQUE A VONTADE PARA CONSULTAR ATRAVÉS DOS LINKS ABAIXO TEMAS RELACIONADOS EM NOSSO PORTAL.

VOCÊ SE INTERESSOU PELO CONTEÚDO?

ESCLAREÇA SUAS DÚVIDAS COM ESPECIALISTAS NO ASSUNTO

CONVERSE COM ESPECIALISTA

facebook.com/ostec

linkedin.com/company/ostec-business-security

contato@ostec.com.br

www.ostec.com.br

ostec.blog

ostec

Segurança digital de resultados