PÍLULAS DE CONHECIMENTO

4

Protegendo os dados pessoais de acordo com os requisitos legais da LGPD – Lei Geral de Proteção de Dados

Nela abordaremos as questões técnicas envolvidas com a LGPD, tais como:

- Quais os tipos de dados e informações que deverão ser protegidos pelas corporações;
- Medidas técnicas a serem tomadas pelas corporações na proteção dos seus dados e informações;
- Medidas administrativas a serem implementadas visando a prevenção da perda de dados e informações pelas corporações;

Uma iniciativa

SINDIMOV – CONFORMIDADOS – GRUPO ASSOCIA+

SINDIMOV
SINDICATO DA INDÚSTRIA DO MOBILIÁRIO DE SÃO PAULO

ASSOCIA+

CONFORMIDADOS®
TREINAMENTO - EDUCAÇÃO - CONSULTORIA

Entendendo a necessidade da proteção de dados

Estamos vivendo na era da economia digital, na qual os dados, quando tratados, possuem um alto valor.

Assim, uma pergunta é recorrente no mercado:

Quais são os dados que devem ser protegidos?

Com o surgimento da Lei Geral de Proteção de Dados Pessoais, muitos ainda podem se perguntar quais são os dados que são protegidos pela Lei. Como já adiantamos, todos as informações relacionadas aos indivíduos (titulares de dados pessoais) que os identifiquem ou tornem-nos identificáveis são classificadas como dados pessoais, devendo elas serem protegidas de acordo com os requisitos legais.

Dados pessoais não são apenas dados que identifiquem diretamente um indivíduo, tais como o número do RG, CNH ou Título de eleitor, mas também outras como o seu perfil psicológico e características hereditárias que também servem de exemplo para ilustrar o conceito.

Existem dezenas de dados pessoais que devem ser protegidos segundo a égide da LGPD, porém estes não são os únicos tipos de dados pessoais que são tratados pelas empresas e que merecem atenção, preocupação e proteção especial.

É muito comum que empresas lidem com dados estratégicos, bem como com dados que são confidenciais e que por isso merecem também atenção especial. Isso somado aos dados que não podem ser divulgados por força legal. Para tais categorias de dados, é muito difícil de se identificar quais são os mais importantes, quais são os mais estratégicos, quantos são confidenciais bem como quais deles não podem ser divulgados por questões legais. Independentemente das dificuldades, estes dados devem ser classificados segundo os modelos de negócio e necessidades internas das corporações, além de serem devidamente rotulados a fim de que sejam facilmente identificadas as suas criticidades e especialidades.

PÍLULAS DE CONHECIMENTO

4

Classificação das informações

Os padrões internacionais não entram no detalhe dos níveis de classificação da informação a serem adotados em uma organização, devendo esta ser uma tarefa que lhes cabe, a qual deve respeitar os seus modelos de negócios e necessidades internas.

É fato que quanto mais complexa for uma organização, é possível que tenha mais níveis de classificação do que outras menos complexas. É fato também que quanto maior for o valor das informações, bem como quanto maior forem as consequências trazidas por acessos indevidos às mesmas, maior deverá ser o nível de classificação delas.

Visando facilitar o entendimento, citamos abaixo exemplos de níveis de classificação que podem ser adotados pelas corporações:

CONFIDENCIAL	Nível mais alto de confidencialidade. As informações classificadas neste nível poderão causar impacto e consequências severos, caso acessos não autorizados sejam realizados nas informações assim classificadas;
RESTRITA	Representa um nível intermediário de confidencialidade. As informações classificadas nesse nível poderão causar um menor impacto caso acessos não autorizados sejam realizados, mas ainda com consequências importantes;
INTERNA	Representa o menor nível de confidencialidade a ser medido. As informações classificadas nesse nível não poderão causar impactos e consequências significativos caso acessos não autorizados sejam realizados;
PÚBLICA	Não existem impactos ou consequências

Rotulagem das informações

Para que as informações já classificadas possam ser utilizadas de forma correta e conveniente, elas devem ser também devidamente rotuladas, segundo as regras definidas internamente, de acordo com os modelos de negócio e necessidades internas das corporações, respeitadas as mídias utilizadas para os seus tratamentos (mídias eletrônicas ou mídias físicas – papel).

A definição de que os ativos de informação físicos recebam no seu canto superior direito a indicação dos seus níveis de confidencialidade, bem como que as mesmas informações sejam repetidas em diferentes partes dos documentos utilizados ou envelopes que os transportam não é complexo e inclusive fácil de ser entendido. A maior questão neste sentido se resume ao fato de os dados eletrônicos terem também que serem rotulados visando as suas proteções de acessos indevidos e de serem enviados para fora das organizações de forma desautorizada.

Tecnologias modernas e inclusive viáveis economicamente existem para o tratamento destes tipos de rotulagem, necessitando de suporte especialista para que sejam implementadas nas empresas.

Princípios legais associados à segurança da informação

Os princípios da LGPD apresentam questões ligadas com a área de segurança da informação. Esse é um fato, muitas vezes não notado por parte das corporações, o que pode comprometer as suas adequações de acordo com os requisitos legais da LGPD.

O princípio legal da SEGURANÇA apresenta a seguinte redação:

Art. 6º - VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

A Lei deixa clara que MEDIDAS TÉCNICAS e MEDIDAS ADMINISTRATIVAS devem ser adotadas pelas corporações aptas a proteger os dados pessoais que tratam. Mas, o que significa isso?

Por **MEDIDAS TÉCNICAS** entenda-se todas as ferramentas de TI, aplicativos e dispositivos de segurança utilizados visando garantir a segurança dos dados tratados pelas corporações, dentre os quais se encontram os dados pessoais por elas tratados. É claro que cada corporação, baseada no seu modelo de negócios e nas suas necessidades internas, definirá as soluções mais adequadas e mais apropriadas de serem utilizadas.

Assim, torna-se imperativo que cada empresa conheça muito bem os ativos de informação que trata, conhecendo as suas importâncias internas e riscos de serem tratados de forma desautorizada, a fim de que possam definir os recursos mais adequados para protegê-los.

Por **MEDIDAS ADMINISTRATIVAS**, entenda-se todas as políticas de segurança da informação, bem como normas e procedimentos internos definidos pela corporação visando manter a proteção dos seus ativos de informação.

Tais políticas de segurança da informação deverão ser definidas de acordo com o modelo de negócios e necessidades internas de cada corporação, baseadas em padrões internacionais definidos e internacionalmente reconhecidos sobre o tema, os quais foram criados a fim de organizar os padrões de Segurança da Informação no mundo.

As normas da família ISO/IEC 27000 são exemplo, convergindo para o Sistema de Gestão de Segurança da Informação (SGSI), tendo como as normas mais conhecidas as ISO 27001 e ISO 27002.

Questão: Quais são as áreas internas da empresa responsáveis pelas necessárias adequações aos requisitos legais da LGPD?

Esta é uma excelente questão, que será respondida NA PRÓXIMA EDIÇÃO das pílulas de conhecimento!

PÍLULAS DE CONHECIMENTO

NÃO PERCA A PÍLULA Nº 5!

DÚVIDAS E PERGUNTAS

Ficou com alguma dúvida, ou quer fazer uma pergunta sobre algum dos temas abordados nesta PÍLULA?

Mande e-mail para: PROJETOS@SINDIMOV.ORG.BR
ou para: WhatsApp: 11- 97445-6060
Coloque no Título: DÚVIDA PÍLULA 4
Identifique: Seu nome e a empresa que representa.

Realização

Apoio

Empresa Parceira
Associados do SINDIMOV, têm condições de atendimento e de negociação especiais.
Fone: 11 3280-4030
E-mail: contato@conformidados.com.br