Boletim
fevereiro 2018

Prazo para adequação à legislação europeia de proteção de dados pessoais se aproxima

O Regulamento da União Europeia (UE) nº 2017/679, também chamado de Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation – GDPR*), tem o objetivo de estabelecer regras relativas à proteção de dados pessoais, em especial referentes ao seu tratamento e à sua livre circulação. Aprovado pelo Parlamento e Conselho da União Europeia em 2016, prevê obrigações e medidas que devem ser implementadas pelas empresas até 25 de maio de 2018, data de sua entrada em vigor, sob pena de severas sanções àquelas que não se adaptarem.

Os efeitos do GDPR não se limitam ao território da União Europeia e se estendem, inclusive, às empresas brasileiras que lá ofertam bens ou serviços, ainda que de forma gratuita e independentemente da existência de uma filial ou estabelecimento, desde que tais atividades envolvam o tratamento de dados pessoais de residentes europeus.

A seguir, destacamos alguns dos principais pontos a serem observados:

Licitude do tratamento de dados

O GPDR adota um conceito amplo para a atividade de tratamento, definindo-a como "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" (art. 4º, item "2").

De acordo com o regulamento, para que o tratamento de dados pessoais seja considerado lícito, uma das alternativas é a obtenção do consentimento expresso de seu titular, para uma ou mais finalidades específicas.

Caso esse consentimento se dê em declaração que diga respeito também a outros assuntos – como nos termos de uso de um provedor de aplicação de internet -, é fundamental que seja apresentado de forma que o distinga das demais disposições, de modo inteligível e de fácil acesso, e em linguagem clara e simples.

Nas hipóteses em que o tratamento é necessário para execução de um contrato no qual o titular dos dados pessoais seja parte, ou para o cumprimento de uma obrigação jurídica à qual o titular esteja sujeito, fica, entretanto, dispensado o consentimento.

Proibições ao tratamento

Salvo exceções, o GDPR veda "o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa" (art. 9º, item "1").

O tratamento de dados relacionados com condenações penais e infrações só pode ocorrer se sob o controle de uma autoridade pública, ou caso haja autorização em legislação específica do bloco econômico ou do Estado-membro da União Europeia em que se originou a condenação.

Responsabilidade pelo tratamento

O GDPR impõe que as empresas responsáveis pelo tratamento de dados pessoais adotem medidas técnicas de organização e de segurança que assegurem que o tratamento é feito em conformidade com o regulamento.

Só é possível aferir se as medidas são adequadas por uma análise que leve em conta as

São Paulo
Av. Brig. Faria Lima, 2601
12º andar - 01452-924
São Paulo, SP - Brasil
Tel: (11) 3555 5000

Brasília
SBN, Q 1, Bl B, 14, Ed. CNC
2º andar, sl. 201 - 70041-902
Brasília - DF - Brasil
Tel. (61) 2109 6070

Rio de Janeiro
Praia de Botafogo, 440
15º andar - 22250-908
Rio de Janeiro, RJ - Brasil
Tel: (21) 3503 2000

contato@levysalomao.com.br

OAB -SP 1405

especificidades do caso concreto, considerando natureza, âmbito, contexto e finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades de seus titulares.

Há padrões de códigos de conduta ou certificações que podem ser obtidas pelas empresas como meio de comprovação ao atendimento dessas obrigações.

Notificação sobre violação da segurança

O GDPR define a violação de dados pessoais como "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (art. 4º, item "12").

Ponto sensível a ser destacado é que o GDPR impõe a obrigação das empresas de comunicar às autoridades de controle dos membros da União Europeia sobre violação de dados pessoais no prazo de até 72 horas, salvo atraso justificado. Se a violação for capaz de causar elevado risco aos direitos e liberdades dos titulares dos dados, estes também deverão ser comunicados sobre a violação pela empresa responsável pelo tratamento. O GPDR não prevê um prazo para essa hipótese, porém impõe que a comunicação se dê sem demora injustificada.

Diretor de Proteção de Dados

O GDPR prevê hipóteses em que a designação de um Diretor de Proteção de Dados (*Data Protection Officer*) é obrigatória, notadamente caso (i) o tratamento seja efetuado por uma autoridade ou um organismo público; (ii) haja processamento de dados em grande escala; ou (iii) o tratamento envolva dados que só podem ser tratados em hipóteses excepcionais, nos termos do regulamento.

Em linhas gerais, o diretor terá a função de aconselhar a empresa nas atividades de tratamento de dados e ser o ponto de referência na comunicação com as autoridades de controle.

Sanções

De acordo com a natureza e a gravidade das infrações, a multa aplicável pode ser de € 10 milhões ou 2% do volume de negócios anual da empresa, a nível mundial, correspondente ao exercício financeiro anterior, o que for maior, ou de até € 20 milhões ou 4% do volume de negócios. Além disso, há a possibilidade de os Estados-membros preverem outras sanções, inclusive penais.

Considerações finais

Empresas que se relacionam com a comunidade europeia ou, de maneira geral, prestam serviços ou oferecem produtos *online* devem estar atentas às normas do GDPR e revisar suas práticas para que estejam compatíveis com o regulamento, evitando sujeição às sanções previstas no normativo europeu.

Allan Nascimento Turano
aturano@levysalomao.com.br