PROTEÇÃO INTERNACIONAL DE DADOS

no Brasil, Alemanha e Polônia

Brasil

Proteção de Dados Pessoais no Brasil

Atualmente, inexiste legislação específica de proteção de dados no Brasil, estando o respectivo projeto de lei em trâmite. Entretanto, os princípios para a proteção de dados pessoais são garantidos pelos direitos constitucionais fundamentais à privacidade e intimidade e ao sigilo da correspondência.

A Lei n° 12.965/2014 ("Marco Civil da Internet"), que entrou em vigor no dia 23 de junho de 2014, disciplina especificamente a coleta, manutenção, tratamento e uso de dados na Internet. O Marco Civil da Internet aplica-se aos (i) usuários de Internet, (ii) provedores de conexão à Internet, ou seja, aqueles que promovem o envio e recebimento de pacotes de dados pela Internet mediante a atribuição ou autenticação de um endereço IP, e (iii) provedores de aplicações de Internet, ou seja, aqueles que fornecem um conjunto de funcionalidades que podem ser acessadas por meio de um computador ou qualquer dispositivo que se conecte à Internet.

Requisitos de Privacidade

Provedores de conexão e de aplicações de Internet apenas estão autorizados a processar dados pessoais mediante o consentimento expresso do usuário. Termos e condições ou qualquer acordo entre provedores e usuários devem conter informação clara e completa a respeito da coleta, uso, guarda, proteção e tratamento de dados pessoais.

Caros leitores,

Nos últimos anos, o Brasil vivenciou uma expansão do acesso à Internet e do uso de smartphones. Em consequência, o país se tornou não apenas um dos maiores mercados para sites de redes sociais e jogos, mas também para crescentes oportunidades no setor de e-commerce. A proteção de dados na Internet é um dos maiores desafios na era da economia digital. Empresas online, tanto brasileiras como estrangeiras, devem se familiarizar com as obrigações de proteção à privacidade e outras disposições relativas ao tratamento de dados dispostas no Marco Civil da Internet.

A Alemanha e a Polônia possuem leis de proteção de dados harmonizadas com o direito europeu e que impactam virtualmente qualquer coleta, processamento e transferência de dados pessoais. Tal inclui não apenas atividades de marketing e e-commerce, mas também transferência de dados entre empresas do mesmo grupo e questões de integração pós-aquisição. De fato, a terceirização e integração de determinadas operações, tais como administração de recursos humanos e operação de aplicações de software, frequentemente pressupõem a transferência de dados pessoais de empregados e clientes para um centro de processamento de dados compartilhado. Consequentemente, as empresas envolvidas devem realizar uma análise abrangente de questões relativas à proteção de dados, de maneira a assegurar o estrito cumprimento das regras aplicáveis.

Tendo em vista esse cenário, preparamos uma síntese dos principais aspectos relativos à proteção internacional de dados na Internet no Brasil, bem como sobre a privacidade e transferência internacional de dados na Alemanha e na Polônia. Esperamos que façam uma boa leitura.

Atenciosamente,

Holger Alfes, Alexander Liegl & Luiza Saito Sampaio

Dados pessoais, registros de conexão ou acesso ou comunicações privadas não podem ser divulgadas para terceiros salvo se houver consentimento expresso ou se requerido mediante ordem judicial.

Obrigações de Guarda de Registros

Provedores de conexão à Internet devem manter os registros de conexão (vale dizer, conjunto de informações referentes à data e hora de início e término da conexão e os endereços IP utilizados), sob sigilo, pelo prazo de um ano. De maneira similar, provedores de aplicações de Internet devem manter armazenados, sob sigilo, os registros de acesso a aplicações de Internet pelo prazo de seis meses.

Provedores de conexão à Internet são proibidos de manter armazenadas informações relativas ao acesso a aplicações de Internet. Por sua vez, provedores de aplicações de Internet, tais como sites de redes sociais e de buscas, não poderão guardar registros de acesso a outras aplicações de Internet sem que o titular dos dados tenha consentido previamente.

Aplicação do Marco Civil da Internet a Provedores Estrangeiros

De acordo com o artigo 11 do Marco Civil da Internet, caso a operação de coleta, armazenamento, guarda ou tratamento de registros de conexão ou acesso, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet ocorra no Brasil, a legislação brasileira deverá obrigatoriamente ser respeitada.

Dessa maneira, aplica-se a lei brasileira a empresas estrangeiras que ofereçam serviços para usuários brasileiros ou que, direta ou indiretamente por meio de uma integrante do mesmo grupo econômico, possua estabelecimento no Brasil.

Caso uma empresa estrangeira seja multada em decorrência da infração a obrigações legais relativas à manutenção de registros de conexão ou acesso ou a requisitos de privacidade, sua filial, sucursal, escritório ou estabelecimento respondem solidariamente.

Sanções para Violação da Proteção de Dados

Sem prejuízo das demais sanções cíveis, criminais e administrativas aplicáveis nos casos de violação da proteção de dados, as seguintes sanções dispostas no artigo 12 do Marco Civil da Internet podem ser aplicadas:

(i) Advertência, com indicação de prazo para adoção de medidas corretivas;

(ii) Multa de até 10% do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos;

(iii) Suspensão temporárias das atividades do provedor; e/ou

(iv) Proibição do exercício das atividades do provedor.

Isenção de Responsabilidade por Conteúdo Gerado por Terceiros

Provedores de conexão à Internet não respondem por dados decorrentes de conteúdo gerado por terceiros. A responsabilidade de provedores de aplicações de Internet em relação ao gerado por terceiros é restrita a conteúdo não tornado indisponível após ordem judicial dentro do prazo assinalado ou, nos casos específicos de conteúdo não autorizado de natureza sexual ou com nudez, após notificação extrajudicial pelo participante ou seu representante legal.

Alemanha

Proteção de Dados Pessoais na Alemanha

A Lei Federal Alemã de Proteção de Dados (*Bundesdatenschutzgesetz*, "BDSG") transferiu os termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995

Noerr Brazil Desk

Inserido em um escritório europeu de primeira linha, o Brazil Desk do Noerr oferece assessoria a empresas brasileiras que pretendam investir ou já realizem negócios na Alemanha e nos países da Europa Central e Oriental ("ECO"), bem como a empresas europeias que estejam presentes no mercado brasileiro ou que cogitem a entrada neste mercado.

O Brazil Desk do Noerr funciona como uma porta de entrada para uma ampla variedade de soluções jurídicas e fiscais oferecidas pelos nossos escritórios na Alemanha e ECO. No Brasil, trabalhamos em cooperação com uma rede de escritórios de advocacia "best friends".

A equipe do Brazil Desk do Noerr é formada por advogados qualificados no Brasil e na Alemanha e oferece os seguintes diferenciais a seus clientes:

- Consciência cultural
- Comunicação eficiente em português, alemão, inglês e russo
- Excelente conhecimento das respectivas jurisdições na Alemanha, ECO e Brasil
- Profundo conhecimento dos mercados brasileiro, alemão e da ECO
- Soluções interdisciplinares e know-how setorial compreendendo desde a indústria automobilística, os setores bancário e financeiro e de energia até os setores de construção de maquinário e imobiliário

("Diretiva Europeia de Proteção de Dados") para o direito alemão. Trata-se de uma longa tradição de legislação de proteção de dados na Alemanha, que se iniciou já em 1970, quando da promulgação da lei de proteção de dados do Estado de Hessen – a primeira lei geral de proteção de dados do mundo.

O objetivo da BDSG não se refere à proteção de dados enquanto tais, mas sim à proteção de indivíduos contra prejuízos a sua privacidade por meio do tratamento de seus dados pessoais. Portanto, a BDSG vai além da imposição de medidas de segurança e visa previamente limitar a coleta, processamento e uso de dados pessoais mediante a imposição de requisitos estritos.

Requisitos Legais

De acordo com a BDSG, qualquer coleta, processamento e uso de dados pessoais é proibida, exceto se passar um teste de duas fases.

Na primeira fase, há que se verificar se é superada a "proibição sob reserva de permissão" ("*Verbot mit Erlaubisvorbehalt*") disposta no artigo 4, par. 1° da BDSG. De acordo com esse dispositivo, a coleta, processamento e uso de dados pessoais apenas são lícitos quando permitidos ou prescritos pela BDSG ou outra lei, ou ainda caso haja consentimento pelo sujeito dos dados (ou seja, pessoa à qual os dados se referem).

A BDSG contém uma série de permissões aplicáveis a depender do tipo específico de dados e dos objetivos e escopo da coleta, processamento e uso pretendidos.

Dentre as transferências de dados permitidas pela BDSG, estão incluídas aquelas efetuadas como meio para a realização dos propósitos comerciais da empresa transferente, se e na extensão necessária para resguardar os interesses legítimos desta e desde que não haja razão para se assumir que o sujeito dos dados tenha um interesse legítimo prioritário em evitar tal transferência de dados (artigo 28, par. 1° (2) n° 2, BDSG).

Numa fase subsequente, há que se verificar se os dados são transferidos para um destinatário (centro de processamento de dados compartilhado) localizado em um país que não seja Estado membro da União Europeia ("UE") nem do Acordo sobre o Espaço Econômico Europeu ("EEE") e, em sendo este o caso, se tal país oferece um nível adequado para a proteção de dados de acordo com a perspectiva europeia (artigo 4b, par. 2° (2), BDSG).

Garantias de Proteção à Privacidade

A Comissão Europeia ("CE") elaborou uma lista de países, nos quais o nível de proteção de dados é considerado adequando em decorrência das leis aplicáveis nesses países. Atualmente, o Brasil não está incluído nessa categoria, sendo a Argentina e o Uruguai os únicos países sul americanos listados.

Se o destinatário está localizado no Brasil, as autoridades competentes para a supervisão da proteção de dados podem ainda assim autorizar a transferência de dados pessoais, desde que o controlador de dados adote garantias adequadas à proteção da privacidade e ao exercício dos respectivos direitos. Tais garantias podem resultar de cláusulas contratuais típicas ou de regras vinculativas para as empresas.

As cláusulas contratuais típicas se referem a cláusulas-modelo da CE, que se utilizadas *ipsis litteris*, tornam supérflua a autorização da transferência de dados pelas autoridades competentes no caso concreto.

Existem dois tipos de cláusulas contratuais típicas. O primeiro é utilizado na relação controlador-processador, em que os dados pessoais são processados por um centro de processamentos de dados compartilhado apenas para o propósito e de acordo com as instruções emitidas pela respectiva empresa transferente.

O outro tipo de cláusula é empregada na relação controlador-controlador, em que o destinatário possua uma certa discrição em relação ao escopo e propósito do uso dos dados recebidos da transferente.

Muitas vezes, as cláusulas-modelo da CE a serem utilizadas na Alemanha devem – de maneira diversa ao que ocorre em outros países da UE – ser complementadas por cláusulas adicionais que assegurem que também a primeira fase do teste mencionado acima seja superada.

Riscos do Descumprimento da BDSG

O descumprimento das regras da BDSG pode acarretar em multas de até € 300.000,00 por caso e até mesmo em sanções criminais.

As autoridades competentes para a supervisão da proteção de dados podem ainda proibir atividades de processamento de dados que estejam em desacordo com as regras aplicáveis, o que pode requerer a imediata alteração de processos já implementados, por sua vez, implicando em custos significativos.

Polônia

Proteção de Dados Pessoais na Polônia

Na Polônia, a Lei de Proteção de Dados Pessoais de 1997 (Jornal Oficial de 2014, item 1182, "LPD Polonesa") implementou a Diretiva Europeia de Proteção de Dados. A LPD Polonesa é aplicável ao processamento de dados pessoais, seja por meio físico ou eletrônico, e deve ser observada por quaisquer entidades públicas ou privadas que processem (coletem, alterem, usem, descartem etc.) dados pessoais.

Tais entidades são consideradas controladoras de dados, determinando o escopo e o propósito do processamento de dados. Além disso, no que se refere a serviços eletrônicos, há que se observar a Lei sobre Serviços Eletrônicos de 2002 (Jornal Oficial de 2013, item 1422, conforme alterada) que dispõe regras específicas e detalhadas.

Empresas brasileiras que processem dados pessoais por meios técnicos localizados na Polônia devem observar as regras polonesas relativas a proteção de dados da mesma maneira que empresas polonesas. Subsidiárias polonesas de empresas brasileiras estão sujeitas à lei polonesa.

Restrições à Transferência de Dados para o Brasil

Via de regra, quando dados pessoais de sujeitos poloneses são transferidos para fora do EEE, determinadas formalidades devem ser observadas pelo controlador de dados. O tipo de formalidade dependerá das garantias de proteção de dados em que se baseiam tais transferências.

Em princípio, o fluxo de dados para fora do EEE é permitido caso o país de destino garanta um nível adequado de proteção. Conforme mencionado acima, dado que o Brasil não consta da lista de países em que o nível de proteção de dados é considerado adequado, qualquer transferência de dados pessoais da Polônia para o Brasil dependerá do consentimento prévio da autoridade polonesa competente para a inspeção geral de proteção de dados (*Generalny Inspektor Ochrony Danych Osobowych*, "GIODO"), bem como da adoção de garantias para a proteção de dados pelo controlador.

Alterações à LPD Polonesa

Da mesma maneira que na Alemanha, na prática, a adoção de garantias à proteção de dados pessoais pode se dar por meio da (i) inclusão de cláusulas-modelo da CE nos contratos entre um controlador e outro controlador ou um controlador e um processador de dados, e (ii) da adoção de regras vinculativas para as empresas.

Atualmente, ainda que a transferência de dados esteja baseada em cláusulas-modelo da CE ou nas chamadas regras vinculativas para as empresas, faz-se necessário o consentimento prévio da GIODO. Entretanto, a partir de 2015, em razão das recentes alterações à LPD Polonesa, as empresas que adotem cláusulas-modelo da CE ou as referidas regras vinculativas estarão isentas da necessidade de obtenção deste consentimento prévio. Para a adoção de regras vinculativas, será necessária a aprovação prévia pela GIODO antes de que o processamento de dados com base nestas regras possa ser iniciado.

Em todos os demais casos, o consentimento formal da GIODO será necessário. Na prática, é importante ter esse requisito em mente, visto que se trata de um processo que pode durar diversos meses e que o consentimento é emitido a critério exclusivo da GIODO.

Alternativas

Alternativamente, a transferência de dados pessoais para o Brasil pode ocorrer mediante o consentimento por escrito do respectivo sujeito dos dados (por exemplo, clientes de uma loja online brasileira). Tal consentimento deve se referir específica e claramente à transferência de dados para fora do EEE. Além disso, o consentimento deve ser emitido livremente.

Outra alternativa se refere à transferência de dados necessária para a conclusão de um contrato entre o controlador de dados e o sujeito dos dados. Se uma transferência internacional de dados ocorrer desta forma ou com base no consentimento do sujeito dos dados, a notificação e o consentimento da GIODO não serão necessários.

Sanções da LPD Polonesa

O descumprimento da LPD Polonesa resulta em responsabilidade criminal, incluindo pena de reclusão de até três anos. Na prática, a ação penal é pouco provável.

Entretanto, a GIODO pode impor sanções ainda mais severas por meio de decisões administrativas. A autoridade pode requerer que a situação seja revertida a um estado de observância da legislação polonesa de proteção de dados. Em casos extremos, a empresa sancionada pode ter que deletar a base de dados contendo dados pessoais.

Para maiores informações, por gentileza, contatar:

Noerr Brazil Desk

Dr. Holger Alfes, LL.M.
Rechtsanwalt (Alemanha)
Attorney-at-law (Nova York)
T +49 69 971477-231
holger.alfes@noerr.com

Prof. Dr. Alexander Liegl
Rechtsanwalt (Alemanha)
T +49 8928628-266
alexander.liegl@noerr.com

Luiza Saito Sampaio, LL.M.
Advogada (Brasil e Portugal)
T +49 69 971477-414
luiza.saitosampaio@noerr.com

Tobias Kugler
Rechtsanwalt (Alemanha)
T +49 69 971477241
tobias.kugler@ noerr.com

Katarzyna Ziółkowska
Radca prawny (Polônia)
T +48 22 579 30 60
katarzyna.ziolkowska@noerr.com

www.noerr.com

A informação veiculada neste boletim informativo não substitui a assessoria jurídica em casos específicos.

© Noerr LLP 2014
www.noerr.com