GUIA

Operações de M&A e LGPD

NÚMERO 6/10

A Year in Privacy

powered by b/luz

Autores

Mariana Pires Monteiro

Odélio Porto Júnior

Dandara Ramos Silvestre da Silva

Rafaella Resck Braoios

Matheus Botsman Kasputis

Coordenador e Revisor

Fernando Bousso

Projeto Gráfico

Fernanda Muchon

Laura Klink

Lucas Bittencourt

índice clicável

índice

‹voltar para o índice

Introdução

O objetivo deste Guia é analisar os principais impactos da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – "LGPD") nas operações de compra e venda de empresas – podendo estas envolver a compra de participação societária (quotas ou ações) ou ativos. Neste Guia, tais operações estão referidas como operações de M&A (ou simplesmente "M&A" – *mergers and acquisitions*).

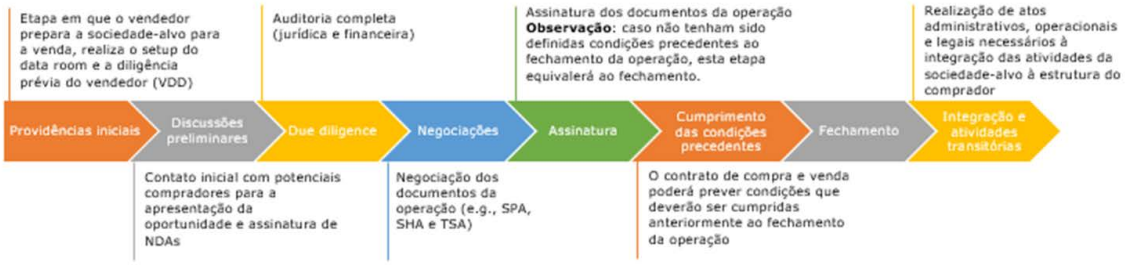
Nos últimos anos, questões relacionadas à privacidade, proteção de dados e segurança da informação deixaram de ser preocupações atreladas a indústrias e modelos de negócio específicos, e passaram a ser consideradas preocupações a serem confrontadas antecipadamente em todas as operações de M&A.

Sendo assim, este Guia, elaborado pelo B/Luz, explica de forma objetiva e prática quais são as principais preocupações a serem consideradas pelos agentes do mercado nas diferentes etapas das operações de M&A, sobretudo durante a realização de auditorias legais (*due diligences*), na negociação de contratos e nas atividades de integração do negócio adquirido à estrutura do comprador.

‹voltar para o índice

01 Cronograma das operações de M&A

É comum que as operações de M&A observem um cronograma estruturado, previamente acordado entre as partes. Pensando nisso, apresentamos a seguir um cronograma[1] com a indicação das etapas típicas de um M&A, seus agentes e as principais atividades realizadas em cada etapa.



Ressaltamos que as etapas de um M&A podem variar a depender da estrutura definida entre as partes da operação. As operações de M&A costumam adotar três diferentes estruturas, que podem impactar na natureza do trabalho a ser desenvolvido nas etapas prévias e posteriores à conclusão do M&A. São elas:

- **transferência de ações (ou quotas):** operações deste tipo consistem na transferência de ações detidas pelo vendedor na sociedade-alvo para o comprador. A sociedade-alvo carrega consigo um legado de responsabilidades por suas práticas de privacidade e proteção de dados, podendo incluir responsabilidades por incidentes de segurança. A princípio, não é necessário notificar ou obter o consentimento dos titulares de dados para a transferência de ações. Contudo, a notificação dos titulares ou a obtenção do consentimento destes, podem ser necessárias para o compartilhamento das bases de dados de consumidores e colaboradores da sociedade-alvo com as empresas do grupo do comprador, nos casos em que, por exemplo, o comprador deseje utilizar tais bases de dados para a promoção dos seus negócios[2].

- **transferência de ativos:** as operações de M&A podem envolver a transferência de ativos específicos ou da totalidade de uma unidade de negócios de uma empresa para outra. Em determinadas jurisdições, a transferência de parte de um negócio (p.ex., uma unidade de negócios) pode ensejar a sucessão do comprador em responsabilidades referentes ao negócio ad-

[1] CZARNECKI, Marcin; WEISS, Justin B. Privacy in M&A transactions: the playbook. Dezembro, 2021, p. 10. Disponível em <https://iapp.org/media/pdf/resource_center/prosus_privacy_in_ma_transcations_playbook.pdf>. Acesso em 20 de junho de 2022.

[2] CZARNECKI, Marcin; WEISS, Justin B. Op. cit., p. 11.

quirido. Além disso, a transferência de bases de dados pode requerer o cumprimento de determinadas condições – tais como a notificação e/ou a obtenção do consentimento dos titulares de dados. Em algumas jurisdições, podem ser necessárias notificações adicionais às autoridades de proteção de dados[3].

- **fusão e/ou incorporação:** a fusão é a operação pela qual se unem duas ou mais sociedades para formar uma sociedade nova, que lhes sucederá em todos os direitos e obrigações[4]. A incorporação, por sua vez, é a operação pela qual uma ou mais sociedades são absorvidas por outra, que lhes sucede em todos os direitos e obrigações[5]. Apesar das sociedades (fusionadas ou incorporadas) tornarem-se uma única entidade, pode ser necessária a adoção de determinadas medidas sob a perspectiva de privacidade e proteção de dados posteriormente à conclusão da operação – sobretudo para a integração dos negócios.

A aquisição de uma sociedade ou porções de um negócio, pode ser justificada, por exemplo, pelo potencial de uma determinada tecnologia desenvolvida pela sociedade-alvo aumentar a capacidade de coleta, análise ou outras modalidades de tratamento de dados pessoais pelo comprador e/ou pela relevância das bases de dados pessoais mantidas pela sociedade-alvo para o enriquecimento dos negócios do comprador[6]. Dessa forma, é importante avaliar desde as etapas prévias e posteriores à operação de M&A, **(i)** os riscos relacionados aos usos de dados pessoais pretendidos pelo comprador após a conclusão da operação; **(ii)** os custos relacionados à adequação da sociedade-alvo às leis de proteção de dados aplicáveis sob as perspectivas operacional, contratual e de governança (sobretudo para a adequada integração da sociedade-alvo à estrutura do comprador); e **(iii)** os riscos e custos financeiros associados à não adequação da sociedade-alvo às normas de proteção de dados em etapa prévia à consumação do M&A.

[3] Ibid.

[4] Lei nº 6.404/1976, art. 228.

[5] Lei nº 6.404/1976, art. 227.

[6] SOLER, Rogério. PRIMEIRAS REFLEXÕES SOBRE OS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) EM OPERAÇÕES DE FUSÃO E AQUISIÇÃO (M&A) NO BRASIL. 2020. p.4. Disponível em https://itsrio.org/wp-content/uploads/2021/03/Rogerio-Soler-Junior_Primeiras-Reflexoes-sobre-os-Impactos-da-Lei-Geral-de-Protecao-de-Dados-LGPD-em-Operacoes-de-Fusao-e-Aquisicao-MeA-no-Brasil-.pdf

‹voltar para o índice

02 Auditoria (*due diligence*)

2.1. O que é uma *due diligence*?

A *due diligence* consiste em um método de auditoria de negócios, realizado com o intuito de conhecer e minimizar eventuais riscos do processo de M&A. Durante a *due diligence,* a sociedade-alvo divulga aos potenciais compradores informações sobre os seus negócios e contingências associadas. Por meio da auditoria, é possível definir questões centrais, como **(i)** a quantificação de ativos e passivos da sociedade-alvo para adequação do preço da oferta (*valuation*); **(ii)** a identificação de contingências futuras, permitindo a correta alocação de riscos conhecidos ou potenciais pelo comprador; e **(iii)** a definição da estrutura da operação, bem como do conteúdo dos documentos do M&A.

Sob a perspectiva de privacidade e proteção de dados, a *due diligence* é a primeira etapa em que um profissional de *privacy* costuma ser envolvido. O profissional de *privacy* buscará, sobretudo, **(i)** avaliar o nível de adequação da sociedade-alvo e a maturidade das suas rotinas em relação às leis e regulamentações de privacidade e proteção de dados; **(ii)** identificar obstáculos que possam estar relacionados à etapa posterior à aquisição da sociedade-alvo (isto é, a integração da sociedade-alvo ou do ativo adquirido à estrutura do comprador); e/ou **(iii)** verificar situações que possam limitar (ou até inviabilizar) os usos dos dados pessoais pretendidos pelo comprador após a aquisição da sociedade-alvo. No último caso, o comprador que deseje, por exemplo, expandir o escopo do tratamento de dados realizado pela sociedade-alvo e/ou utilizar os dados coletados por ela para a promoção de suas atividades, deverá atentar às restrições impostas pela LGPD e demais regulamentações aplicáveis, que podem resultar em custos adicionais à operação ou exigir a adoção de cuidados adicionais no tratamento dos dados pessoais.

Conclui-se, portanto, que uma das principais funções da *due diligence* nas operações de M&A é a obtenção de informações que permitam conhecer o real status da sociedade-alvo, identificando os riscos do negócio adquirido ou eventuais obstáculos posteriores à conclusão da operação. Para tanto, são observados indicadores financeiros, tributários, trabalhistas, comerciais e operacionais da sociedade-alvo. Sendo que, com a vigência da LGPD, a avaliação das práticas de proteção de dados também passou a ser um importante fator a ser avaliado durante a auditoria, a fim de identificar eventuais riscos associados aos tratamentos de dados realizados pela sociedade-alvo.

2.2. Recomendações para realização da *due diligence*

Para além das apurações superficiais sobre incidentes de segurança, processos judiciais ou administrativos e fiscalizações relacionadas à proteção de dados, o processo de *due diligence* deve envolver aspectos mais profundos. A auditoria que objetive avaliar a conformidade da sociedade-alvo com as legislações de proteção de dados, bem como identificar eventuais riscos relacionados às atividades de tratamento de dados pessoais realizadas pela sociedade-alvo, deve endereçar, sobretudo, os seguintes aspectos: **(i)** aspectos procedimentais, relacionados à condução do processo de auditoria; e **(ii)** aspectos substantivos, relacionados ao grau de adequação da sociedade-alvo.[7]

Primeiramente, destaca-se que, durante o processo de *due diligence*, uma grande quantidade de informações transita entre a estrutura do comprador e da sociedade-alvo. Caso dentre as informações circuladas estejam bases de dados que identifiquem ou tornem identificáveis pessoas naturais (como colaboradores, clientes ou parceiros de negócios), tal fluxo de informações será classificado como um tratamento de dados pessoais, aplicando-se, portanto, as diretrizes da LGPD. Nesse sentido, é necessária a adoção de medidas procedimentais que garantam a proteção adequada às informações compartilhadas entre as partes durante o processo de auditoria.

Devido à sensibilidade das informações tratadas, além do caráter sigiloso da operação, é prática comum às operações de M&A o estabelecimento de documentos preliminares que disponham sobre a confidencialidade das informações tratadas durante o processo de *due diligence*. Entretanto, as exigências da LGPD vão além das medidas de confidencialidade frequentemente previstas nos documentos preliminares. É necessária, também, a inclusão de cláusulas que estabeleçam as regras de proteção de dados que deverão ser observadas pelas partes envolvidas no processo de auditoria, além da regulamentação dos seguintes temas:

- **responsabilidades:** delimitação das responsabilidades das partes pelo tratamento dos dados compartilhados, bem como a definição das partes como agentes no tratamento de dados.

[7] SOLER, Rogério. Op. cit., p. 8.

• **limitação das finalidades de tratamento:** inclusão de disposições contratuais que limitem as finalidades para quais os dados compartilhados podem ser tratados pelo comprador; e

• **medidas técnicas** que devem ser adotadas pelas partes para o endereçamento de questões relativas à segurança dos dados compartilhados, preservação dos direitos de titulares e medidas de transparência relativas aos referidos compartilhamentos.

Por sua vez, os aspectos substantivos a serem observados durante a auditoria, dizem respeito à avaliação de elementos que indiquem o grau de adequação da sociedade-alvo às diretrizes da LGPD e de outras legislações aplicáveis à privacidade e proteção de dados. Como primeiro passo para a realização dessa análise, deve ser considerado, de forma ampla, o contexto da operação de M&A, as especificidades do negócio da sociedade-alvo, incluindo a análise dos seguintes aspectos[8]:

• **o modelo de negócio da sociedade-alvo**, identificando as situações em que a sociedade-alvo trata dados pessoais e as respectivas finalidades a fim de avaliar se o tratamento de dados realizado pela sociedade-alvo para a viabilização do seu negócio cria algum obstáculo ou risco adicional ao negócio do comprador. Essa análise é importante nos casos em que, por exemplo, (i) as operações da sociedade-alvo estão sujeitas às regras de um setor específico no qual o comprador não opera (p.ex., a sociedade-alvo atua no setor farmacêutico e o comprador não) e/ou (ii) a sociedade-alvo trata dados pessoais sensíveis no contexto das suas atividades (e o comprador não realiza esse tipo de tratamento).

• **as leis de proteção de dados aplicáveis,** avaliando as leis aplicáveis às atividades da sociedade-alvo, bem como as especificidades de tais legislações frente à legislação aplicada aos negócios do comprador (sobretudo nos casos em que se apliquem aos negócios da sociedade-alvo leis de privacidade e proteção de dados de outras jurisdições).

• **o uso dos dados após a conclusão da operação,** verificando se haverá alguma modificação no modelo de negócio e na estrutura das operações da sociedade-alvo após a conclusão da operação e integração aos negócios do comprador (por exemplo, nos casos em que o comprador deseja utilizar as bases de dados de consumidores da sociedade-alvo para promoção de suas atividades).

[8] CZARNECKI, Marcin; WEISS, Justin B. Op. cit., p. 14.

• **a estrutura da operação,** considerando quais serão os impactos da estrutura da operação às atividades de tratamento de dados pessoais anteriormente realizadas pela sociedade-alvo. Em alguns casos, sobretudo em operações envolvendo empresas de tecnologia, a estrutura da operação pode ser pensada para permitir que as atividades de tratamento da sociedade-alvo não sejam afetadas de modo relevante (por exemplo, para permitir que consentimentos coletados de usuários anteriormente à operação permaneçam válidos).

• **as políticas do comprador:** avaliar como o programa de privacidade e proteção de dados da sociedade-alvo se alinha ao programa do comprador e considerar as atividades que deverão ser realizadas (e o investimento necessário) para adequar os processos internos da sociedade-alvo ao programa do comprador.

A análise dos aspectos listados acima pode ser realizada a partir da auditoria dos seguintes elementos, entre outros:

• **registro das operações de tratamento de dados pessoais:** as organizações que realizam o tratamento de dados pessoais devem manter um registro das operações realizadas. A análise de tais registros durante o processo de *due diligence* pode fornecer importantes informações sobre os principais usos de dados pessoais realizados pela sociedade-alvo, sendo possível identificar a conformidade dessas atividades com a LGPD, bem como identificar eventuais riscos associados a tais tratamentos. No mesmo sentido, a inexistência de registros de tratamento oferece indícios de pouca maturidade em relação ao tema de proteção de dados.

• **histórico de incidentes:** deve ser observado o histórico de incidentes de segurança nos quais a sociedade-alvo já esteve envolvida, com a análise (i) dos elementos causadores dos incidentes (por exemplo, ataque de terceiros mal-intencionados ou falhas de segurança); (ii) a postura adotada pela sociedade-alvo na resolução do incidente; e (iii) as medidas adotadas após os incidentes, sobretudo em relação às medidas corretivas implementadas para evitar novos incidentes.

• **parceiros e contratos:** avaliação de contratos e acordos que envolvam o compartilhamento de dados com terceiros e análise das medidas adotadas pela sociedade-alvo para endereçar aspectos de privacidade e proteção de dados (por exemplo, inclusão de disposições contratuais específicas referentes à privacidade e proteção de dados).

Por fim, é recomendável que a auditoria não se restrinja unicamente aos aspectos jurídicos, sendo necessário também a avaliação por auditorias especializadas dos aspectos técnicos de segurança da informação para que os riscos associados ao descumprimento de rotinas de segurança possam ser endereçados de forma precisa e adequada.

2.3. Como endereçar os riscos verificados durante a *due diligence*

É natural que, por vezes, algumas limitações inviabilizem a pronta adoção de todas as medidas necessárias para prevenir os riscos identificados durante a *due diligence*. A título exemplificativo, a falta de conscientização de colaboradores da vendedora sobre privacidade e proteção de dados é um risco que deve ser endereçado paulatinamente por requerer mudanças de cunho cultural e educacional, incorporadas com o tempo. Por outro lado, medidas como a revisão de contratos sensíveis ou de políticas de governança de dados costumam ser adotadas com mais prontidão, por exigirem das partes diligências tão somente jurídicas e comerciais.

Os riscos verificados durante a *due diligence* devem, por isso, ser ordenados conforme uma prioridade – considerando, por exemplo, **(i)** o cronograma da operação de M&A; **(ii)** o tempo, esforço ou custos associados às medidas para adequação; e **(iii)** os possíveis danos e prejuízos em matéria de privacidade e proteção de dados. Essa é uma particularidade pertinente às operações de M&A e à maioria das legislações de privacidade e proteção de dados, incluindo a LGPD, que adotam um uma abordagem regulatória baseada em riscos (*risk-based approach*)[9].

Apesar da priorização das atividades variar conforme as particularidades de cada ativo ou segmento de negócios, a categorização dos riscos pode seguir alguns critérios comuns baseados no cronograma da operação de M&A. Czarnecki e Weiss,[10] por exemplo, sugerem os seguintes critérios para o endereçamento dos riscos:

[9] V. WP29. Statement on the role of a risk-based approach in data protection legal frameworks. Maio, 2014. Disponível em <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>. Acesso em 20 de junho de 2022.

[10] CZARNECKI, Marcin; WEISS, Justin B. Op. cit., p. 16.

Critérios para o endereçamento de riscos em operações de M&A	
Riscos que podem ser endereçados pré-fechamento	Incluem-se os riscos mais prioritários em matéria de privacidade e proteção de dados pessoais e/ou que podem ser resolvidos sem esforço, tempo ou custo expressivos.
Riscos que podem ser endereçados pós-fechamento	Incluem-se os riscos menos prioritários em matéria de privacidade e proteção de dados pessoais e/ou que somente podem ser resolvidos com esforço, tempo ou custo expressivos. Devem ser negociadas adequadamente com o vendedor.
Riscos que podem ser endereçados em declarações e garantias	Incluem-se os riscos que, se concretizados, podem ser completamente reparados (e.g. vulnerabilidades em sistemas de segurança não declaradas, danos materiais etc.).
Riscos que impactam a precificação do negócio	Incluem-se os riscos que impactam ou podem impactar na auditoria do preço ou no preço efetivo de mercado da sociedade-alvo (e.g. incidentes de segurança da informação não declarados).
Outros riscos que devem ser considerados pelo comprador	Incluem-se os riscos que não podem ser endereçados no momento, mas que são relevantes para o comprador (e.g. futuras regulamentações editadas pela Autoridade Nacional de Proteção de Dados).

Em linhas gerais, sinalizamos que a impossibilidade de endereçar todos os riscos de privacidade e proteção de dados no pré-fechamento da operação não deve inviabilizar a sua conclusão. Nesse sentido, é importante, sobretudo, que o comprador prepare um **plano de ação identificando e categorizando os riscos verificados na *due diligence,*** bem como a data ou o momento previsto para a adoção das medidas de salvaguarda consideradas, de tal sorte que essa documentação possa ser eventualmente apresentada a autoridades reguladoras em linha com o princípio da prestação de contas *(accountability)* previsto na LGPD.

A depender do volume da operação, também faz bem mencionar a importância de o comprador desenvolver uma estratégia de comunicação aberta com os órgãos fiscalizadores e, principalmente, com a Autoridade Nacional de Proteção de Dados, aproveitando-se do caráter preventivo de fiscalização da agência,[11] a fim de demonstrar boa-fé, buscando reduzir o risco regulatório.

[11] LGPD: "Art. 55-J. Compete à ANPD: [...] XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; (Incluído pela Lei nº 13.853, de 2019)".

2.3.1. Precedentes envolvendo o endereçamento de riscos de privacidade e proteção de dados

A seguir, apresentamos dois casos emblemáticos de operações de M&A que receberam expressiva repercussão nos meios de comunicação devido a, sobretudo, o endereçamento de riscos de privacidade e proteção de dados.

a) Marriott International Inc. & Starwood Hotels and Resorts Worldwide Inc.

Em 30 de outubro de 2020, a autoridade de proteção de dados do Reino Unido *(Information Commissioner's Office – ICO)* comunicou[12] o sancionamento de uma multa no valor de 18,4 milhões de euros à Marriott impactando a aquisição da rede de hotéis Starwood pela empresa.

A penalidade refere-se a um incidente de segurança da informação ocorrido em 2014, consistindo em uma invasão aos sistemas da Starwood que afetou a segurança de 339 milhões de registros de hóspedes, contendo informações de cadastro e de contato e dados referentes a passagens aéreas e programas de fidelidade. O incidente, que garantiu privilégios ilimitados ao invasor e o acesso e a edição irrestrita dos dados pessoais, teria sido detectado apenas em setembro de 2018, dois anos após aquisição da rede Starwood pela Marriott.

Diante disso, apesar de a Marriott haver adquirido a Starwood apenas em 2016, o ICO entendeu que a empresa não adotou medidas técnicas e administrativas suficientes na proteção dos dados pessoais armazenados nos respectivos sistemas, de tal maneira que o incidente foi apenas detectado e combatido tardiamente.

b) Verizon Communications Inc. & Yahoo! Inc.

A *Securities and Exchange Comission (SEC)* dos Estados Unidos aplicou, em 24 de abril de 2018, a multa de 35 milhões de dólares a Yahoo! Inc.[13] em incidente de segurança no qual invasores russos violaram a segurança dos sistemas de informação da empresa e tiveram acesso a dados cadastrais, a dados de contato e às credenciais de acesso às contas Yahoo, incluindo usuário e senha, de mais de 500 milhões de usuários.

[12] Information Commissioner's Office. Penalty Notice – Case ref: COM0804337. Outubro, 2020. Disponível em <https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf>. Acesso em 20 de junho de 2022.

[13] Securities and Exchange Comission. Administrative Proceeding – File No. 3-18449. Abril, 2018. Disponível em <https://www.sec.gov/litigation/admin/2018/33-10485.pdf>. Acesso em 20 de junho de 2022.

Segundo a Comissão, além de a Yahoo! não ter adotado os controles de segurança adequados para prevenção e combate ao incidente, a empresa manteve-se também inerte por dois anos quanto ao dever de notificar publicamente o ocorrido. Dessa forma, embora tenha tido conhecimento sobre o incidente desde 2014, a divulgação ocorreu apenas em 2016.

Ocorre que a publicização da multa à Yahoo! deu-se em meio às negociações de venda da empresa junto à Verizon, e esta, após tomar conhecimento do incidente, exigiu a renegociação do contrato de compra e venda das ações da companhia (SPA) – ora avaliadas em 4,825 bilhões de dólares –, com o desconto de 350 milhões de dólares, equivalente a 7,25% do preço inicial.

‹voltar para o índice

03 Contratos

3.1. Considerações sobre contratos de compra e venda

Os riscos mencionados na Seção 2 acima, terão impacto direto nos contratos que estruturam as operações de M&A – sobretudo, nos contratos de compra e venda de participação societária (ações ou quotas) ou de ativos. É comum que tais instrumentos sirvam como mecanismo para a alocação dos riscos identificados durante a auditoria e endereçamento de outras questões relacionadas à privacidade e proteção de dados obrigando as partes ao que for pactuado.

Listamos a seguir as principais cláusulas utilizadas em contratos de compra e venda para a repartição contratual de responsabilidades. São elas:

• **Declarações e garantias:** as declarações e garantias servem para que a sociedade-alvo e/ou o vendedor atestem a veracidade de determinados fatos e circunstâncias apresentados ao comprador durante o processo de *due diligence*. Esta cláusula deve compreender, entre outras, declarações e garantias relacionadas **(i)** à inexistência de incidentes de segurança da informação; **(ii)** à inexistência de restrições legais à cessão e transferência das bases de dados objeto da aquisição; **(iii)** à inexistência de investigações, notificações e/ou procedimentos administrativos ajuizados por autoridades relacionados à privacidade, proteção de dados e segurança da informação (p.ex., pela ANPD, Ministério Público, órgãos de defesa do consumidor e/ou autoridades setoriais etc.); **(iv)** à inexistência de reclamações e/ou ações judiciais ajuizadas por titulares de dados; e **(v)** à garantia de que os negócios da sociedade-alvo estão em conformidade com todas as leis e regulamentações aplicáveis à privacidade, proteção de dados e segurança da informação[14].

• **Indenização:** as cláusulas de indenização referem-se à obrigação do vendedor de reembolsar o comprador por contingências conhecidas pelo vendedor em etapa prévia ou no momento da consumação da operação de M&A. Normalmente, as cláusulas de indenização não preveem a indenização do comprador por eventos futuros, posteriores à conclusão da operação. É possível, entretanto, que as partes negociem um período transitório (p.ex., 6 meses) dentro do qual o vendedor deverá indenizar o comprador. Esse tipo de negociação é comum nos casos em que os efeitos de uma violação às leis e/ou regulamentações precisam de tempo para se materializar (como ocorre em situações envolvendo questões ambientais e/ou, no caso de proteção de dados, incidentes de segurança). Considerando o momento pelo qual estamos

[14] SOLER, Rogério. Op. cit., p. 13.

passando (em que a LGPD ainda é recente e as empresas ainda apresentam baixo grau de adequação), a negociação de períodos transitórios pode servir como um bom mecanismo para mitigação de riscos futuros e desconhecidos pelo comprador – sobretudo se considerarmos que a implementação das medidas de adequação da sociedade-alvo às exigências da LGPD provavelmente ficará a cargo do comprador[15].

• **Condições para o fechamento:** as condições para o fechamento podem abranger diversas obrigações, tais como **(i)** a obrigação de executar ações específicas relacionadas à implementação de um programa de governança de dados (p.ex., atualização de avisos de privacidade, implementação de política de cookies e adequação da jornada dos usuários em plataformas digitais da sociedade-alvo); **(ii)** obtenção de autorizações regulatórias específicas (p.ex., nos casos em que a autorização é necessária para a transferência de bases de dados); **(iii)** obrigação da sociedade-alvo conduzir os seus negócios de acordo com regras específicas (p.ex., informar o comprador da ocorrência de incidentes de segurança da informação); e/ou **(iv)** a obrigação do vendedor de realizar determinadas ações para facilitar a integração após o fechamento[16].

• **Obrigações pós-fechamento:** as obrigações pós-fechamento correspondem a uma categoria mais ampla. Por um lado, elas podem estar relacionadas a ações específicas exigidas do vendedor para permitir que o comprador assuma adequadamente os negócios da sociedade-alvo. Por outro lado, essas obrigações podem requerer que o time de privacidade da sociedade-alvo implemente determinadas medidas de privacidade e proteção de dados[17].

3.2. Serviços transitórios

Em razão da dependência entre os negócios da sociedade-alvo e da vendedora, a vendedora poderá prestar serviços à sociedade-alvo durante um período acordado entre o comprador, o vendedor e a sociedade-alvo até que sejam cumpridas as condições para a cessação desse serviço. Tais serviços – os chamados serviços transitórios *(transitional services*) – compreendem atividades que normalmente envolvem o compartilhamento ostensivo de dados pessoais como, por exemplo, acesso à infraestrutura de tecnologia da informação, atendimento ao cliente e processos de recursos humanos.

---

[15] SOLER, Rogério. Op. cit., p. 14.
[16] CZARNECKI, Marcin; WEISS, Justin B. Op. cit., p. 17.
[17] Ibid.

O tratamento de dados pessoais nos serviços transitórios deve também ser objeto de regulação contratual entre a sociedade-alvo e o vendedor, seja por meio de acordo de tratamento de dados específico ou cláusulas de proteção de dados ou adendos ao contrato de prestação de serviços transitórios (*transitional services agreement* - TSA). Os termos e as condições para esses serviços poderão considerar, entre outros, os seguintes aspectos de privacidade e proteção de dados pessoais:[18]

- o enquadramento e a responsabilidade das partes como agentes de tratamento e a categoria dos dados pessoais objeto do tratamento;

- a obrigação de o vendedor atuar de exclusivamente de acordo com as instruções da sociedade-alvo;

- a obrigação de o vendedor implementar medidas de segurança adequadas ao compartilhamento dos dados pessoais;

- a obrigação de cooperação entre as partes no atendimento às requisições dos direitos de titulares de dados;

- a obrigação de o vendedor notificar imediatamente a sociedade-alvo a respeito de vazamento de dados atual ou potencial e mitigar os efeitos do vazamento;

- a obrigação de o vendedor eliminar os dados da sociedade-alvo tão logo encerrado o período de transição; e

- a confirmação do vendedor de que ele pode realizar o compartilhamento dos dados sem qualquer efeito adverso à estrutura e conteúdo das informações.

No que diz respeito aos mecanismos de segurança adotados, é importante a garantia não apenas da segurança organizacional, por meio de acordos de confidencialidade, mas também da segurança técnica, por meio da implementação de criptografia, controles de acesso aos arquivos compartilhados e segregação lógica da base de dados utilizada pela sociedade-alvo. Sempre que possível, o compartilhamento não deve envolver informações excessivas, em conformidade com o princípio da necessidade dos dados previsto na LGPD.

[18] Ibid.

‹voltar para o índice

04 Pós- fechamento

Conforme mencionado anteriormente, após a conclusão da operação de M&A, o comprador passa a suportar os riscos relacionados à condução das atividades de tratamento de dados pela sociedade-alvo. Logo, é importante que o comprador esteja ciente das medidas de segurança da informação, privacidade e proteção de dados a serem implementadas às rotinas da sociedade-alvo anteriormente à conclusão da operação e/ou a partir da data do fechamento.

Sinalizamos abaixo alguns exemplos de medidas que devem a serem tomadas pelo vendedor, pela sociedade-alvo e pelo comprador após a data de fechamento:

I. Transferência da base de dados

As transferências de bases de dados costumam ocorrer em operações de vendas de ativos. Nestes casos, recomenda-se que a transferência da base de dados (ou das credenciais para acesso à base de dados) seja realizada de forma segura, seguindo restrições relacionadas à transferência internacional de dados pessoais. Os envolvidos na operação devem se certificar de que seu acesso aos dados pessoais é realizado em conformidade com a lei, visto que eles também podem ser considerados controladores de dados e estarão sujeitos às responsabilidades decorrentes de violações à legislação de proteção de dados[19].

Além disso, para a transferência de dados pessoais em uma operação de M&A, é necessário ter uma base legal que justifique esse tratamento na legislação brasileira. A depender da jurisdição, podem ser aplicáveis restrições legais à transferência internacional dos dados entre a sociedade-alvo e o comprador. Recomenda-se, portanto, que o comprador se certifique de que tais restrições sejam cumpridas antes de realizar a transferência.

Não menos importante, é definir um meio seguro para o compartilhamento das informações, que atenda aos padrões de segurança da informação, de governança de proteção de dados e aos princípios gerais das leis e demais normas regulamentares.

II. Aviso aos titulares de dados

Recomendamos que seja avaliada a necessidade de notificação dos titulares dos dados pessoais ou a atualização dos avisos de privacidade existentes (p.ex., em plataformas digitais) para refletir as mudanças resultantes da operação de M&A. Tais atualizações podem ser necessárias para permitir que os

[19] Ibid.

titulares exerçam seus direitos elencados no caput do artigo 18 da LGPD, e para atender ao princípio da transparência.

III. Notificação a autoridades de proteção de dados e atualização de registros

Em algumas jurisdições, pode ser necessário notificar ou atualizar determinados registros junto às autoridades de proteção de dados dentro de prazos específicos para a conclusão da operação de M&A. Em relação à legislação brasileira, a LGPD não estabelece obrigação de notificar a Autoridade Nacional de Proteção de Dados – ANPD a respeito da conclusão do M&A (e não existe, até esta data, regulamentação a esse respeito pela ANPD).

IV. Atualizações dos mapeamentos

Por fim, recomenda-se que os mapeamentos da sociedade-alvo sejam atualizados para refletir as mudanças resultantes da operação de M&A. O mapeamento funciona como um registro fotográfico do momento em que a empresa se encontra, e mantê-lo atualizado é essencial para permitir que a empresa tenha registrado todo o fluxo de tratamento de dados pessoais. Sugere-se, portanto, que sejam alterados, conforme aplicável, os agentes envolvidos no tratamento de dados pessoais, eventuais mudanças de encarregado pelo tratamento de dados pessoais, bem como os terceiros com os quais os dados são compartilhados etc.[20]

[20] CZARNECKI, Marcin; WEISS, Justin B. Op. cit, p. 19.

b/luz

deixa com a gente

Para saber mais, acesse nosso site ou
nos acompanhe nas redes sociais.

baptistaluz.com.br