Leis de Privacidade dos Dados: Reduzindo a Burocracia

Relatório da Ovum encomendado pela Intralinks

ovum

INTRA LINKS™

ovum

Índice

Resumo Executivo 1

Introdução 2

As empresas enfrentam os desafios da conformidade 4

A continuidade do uso da nuvem é inevitável 4

As empresas não estão tomando medidas básicas para a proteção dos dados confidenciais 5

Os regulamentos de privacidade dos dados não são uniformes, deixando as empresas globais vulneráveis e confusas 6

Regulamentos europeus em vias de aprovação definirão a norma para a privacidade de dados globais, mas colocarão em risco a economia da UE 7

O local de armazenamento dos dados é um ponto essencial de controle, mas de difícil definição 8

Os regulamentos impõem altíssimos custos 9

As organizações com sede nos EUA estão sob pressão 9

Recomendações 10

Apêndice 11

Metodologia 11

Autor 11

Ovum Consulting 11

Aviso de direitos autorais e de direitos legais 11

INTRA LINKS

Resumo Executivo

Um movimento global pelos direitos de privacidade apresenta riscos comerciais e econômicos significativos

Os governos nacionais estão aprovando leis de privacidade de dados novas e mais rígidas para a proteção de dados dos cidadãos, dos interesses de segurança nacional e para potencialmente estimular os setores locais.

Para analisar o impacto dos regulamentos de privacidade e soberania dos dados em constante evolução, a Intralinks encomendou à Ovum, no terceiro trimestre de 2015, um estudo internacional com a participação de 366 tomadores de decisões de TI.

Principais resultados incluem:

Os regulamentos de privacidade dos dados entram em conflito direto com as práticas de computação em nuvem, de software como serviço (SaaS) e de computação móvel das empresas

A computação em nuvem é uma parte estabelecida do cenário de TI empresarial, e a previsão é que a adoção continue a aumentar na próxima década. Processos de negócios que fazem intenso uso de informações baseiam-se em SaaS e, isso, juntamente com a mudança para plataformas de computação móvel, impõe um enorme desafio à tarefa de controlar a localização dos dados e acatar os regulamentos de privacidade. Ainda assim, nos próximos três anos, 78% dos participantes do estudo planejam usar aplicativos em nuvem e baseados em SaaS, até mesmo para o armazenamento e compartilhamento de dados confidenciais e regulamentados.

Líderes empresariais mostram-se profundamente pessimistas sobre as potenciais consequências dos novos regulamentos de privacidade dos dados

O novo estudo mostra que as organizações estão conscientes do problema representado pela privacidade dos dados, porém, estão se esforçando para encontrar uma resposta para ele. Quando perguntamos sobre a General Data Protection Regulation (GDPR), a lei única de proteção de dados e privacidade da União Europeia em vias de aprovação, 52% disseram que acham que esta resultará em multas para suas empresas, e dois terços acham que ela forçará alterações na estratégia comercial das empresas europeias.

O custo da conformidade regulamentar será substancial, contudo, o custo da não conformidade será maior

Mais de 70% dos participantes preveem um aumento dos gastos para atenderem aos requisitos da soberania de dados, e mais de 30% esperam aumento no orçamento superior a 10% nos próximos dois anos. Entre aqueles que planejam atualizar suas estratégias de privacidade de dados nos próximos três anos, 38% planejam contratar especialistas no assunto, e 27% contratarão um diretor de privacidade.

As organizações com sede nos EUA estão particularmente vulneráveis

O efeito Snowden é real. Entre 20 economias industrializadas, os EUA estão classificados como o país menos confiável e o mais propenso a obter acesso não autorizado a informações confidenciais, com a China em segundo lugar e a Rússia em terceiro, neste quesito. Os novos regulamentos também colocarão as empresas dos EUA em desvantagem ainda maior, pois 63% dos participantes acreditam que os regulamentos propostos de GDPT da UE dificultarão ainda mais a concorrência para as empresas dos EUA, e 70% acham que a nova legislação favorecerá empresas com sede na Europa.

A maioria das organizações não usa a tecnologia com a eficácia necessária para abordar as preocupações com a privacidade dos dados

Espantosamente, muitas organizações não tiram proveito das tecnologias disponíveis para a proteção dos dados confidenciais. Apenas 44% dos participantes do estudo supervisionam as atividades dos usuários e fornecem alertas para violações à política de dados, e apenas 53% classificam as informações para se alinharem aos controles de acesso. Quase metade (47%) não tem políticas ou controles para gerenciar o acesso a sistemas de armazenamento e compartilhamento de arquivos em nuvem criados para o mercado doméstico, como o Dropbox.

As empresas globais precisam de uma abordagem organizada à soberania de dados, abrangendo pessoas, processos e tecnologia.

Os líderes empresariais reconhecem a necessidade de assumirem uma abordagem equilibrada à soberania e a privacidade dos dados. Quando indagados sobre estratégias de investimento, 55% disseram que planejam novas atividades de treinamento para os funcionários, 51% reformularão e adaptarão políticas, e 53% se prepararão adotando novas tecnologias.

As empresas se deparam com regulamentos de privacidade globais contraditórios e conflitantes, e precisam ter opções de tecnologia que abrajam todas as eventualidades.

A revolução da soberania de dados ameaça criar um cenário tecnológico fragmentado, no qual diferentes jurisdições impõem exigências inconsistentes e, muitas vezes, incompatíveis para a forma como dados pessoalmente identificáveis são armazenados, processados e compartilhados. Isso já está criando confusão e incerteza, deixando questões fundamentais sem resposta, como a forma correta de interpretar as exigências associadas ao local de armazenamento dos dados. As empresas precisam ter opções de tecnologia que lhes permitam reagir a um ambiente regulamentar em rápida transformação.

Introdução

Mesmo antes de as revelações de Edward Snowden mostrarem a plena extensão da vigilância eletrônica da Agência de Segurança Nacional (NSA) dos EUA, a privacidade de dados já estava na pauta global. A espionagem pelo governo, combinada com vazamentos maciços de dados nos últimos anos forçaram os governos nacionais a reconhecerem que as leis de privacidade atuais originam-se da época em que documentos em papel predominavam e precisam atualizar-se de acordo com as realidades da economia digital. O resultado tem sido uma onda sem precedentes de novas leis que têm por objetivo reger a forma como certos dados confidenciais podem ser coletados, processados e compartilhados.

Países tão diversos quanto o Brasil, Singapura e Rússia estão endurecendo suas leis. A UE aproxima-se do fim de um extenso processo de revisão da legislação nessa área, que afetará qualquer organização que opere em seus países-membros. A imposição dessas restrições ocorre porque as empresas começam a dissolver as fronteiras tradicionais e os funcionários estão mais em dispositivos móveis, o que, juntamente com a migração para sistemas de TI baseados em nuvem, pode causar conflito com essas novas leis. As obrigações de conformidade advindas da legislação estão se tornando mais complexas, particularmente para as empresas que operam entre diferentes jurisdições e particularmente no contexto do modo como a legislação se aplica aos dados armazenados por serviços baseados em nuvem.

No terceiro trimestre de 2015, a Intralinks encomendou à Ovum, fornecedora líder em soluções empresariais de colaboração na nuvem, um estudo que visa entender as implicações dos regulamentos de privacidade de dados em empresas multinacionais.

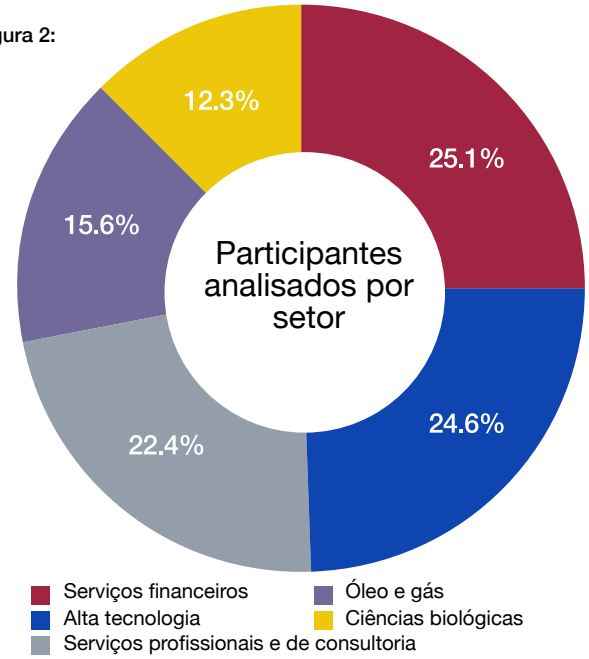
O estudo explorou as seguintes questões:

- Como as organizações estão se preparando para lidar com a soberania dos dados?
- Qual será o impacto dos novos regulamentos de privacidade de dados?

- Como as empresas adaptarão os seus negócios para cumprir as novas obrigações de privacidade?
- Quais são as diferenças de opinião em diferentes países e distintas jurisdições?
- Que decisões de tecnologia auxiliarão no cumprimento das obrigações de privacidade dos dados?
- Quais são as boas práticas para a adaptação aos novos regimes regulamentares?

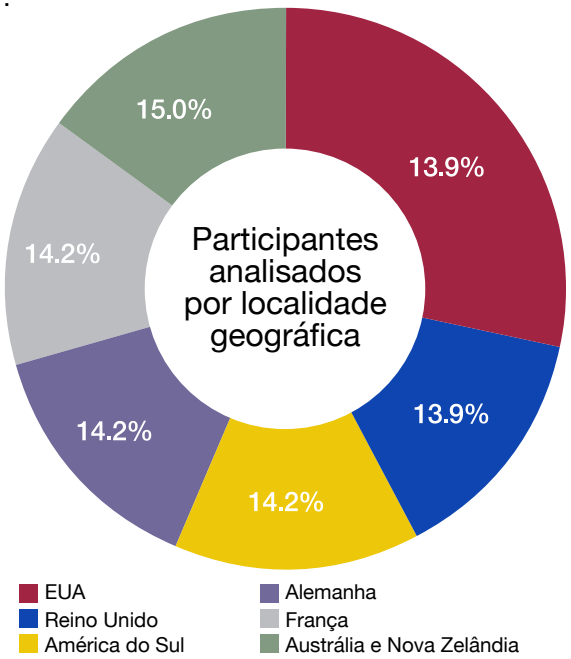
O estudo da Ovum incorpora informações obtidas de 366 participantes do mundo inteiro, em organizações de diferentes tamanhos, em diversos setores (consulte as Figuras 1, 2 e 3). A faixa demográfica foi escolhida deliberadamente para incluir vários tipos de organizações e países afetados pelos regulamentos de privacidade e obrigações de soberania dos dados.

Figura 2:



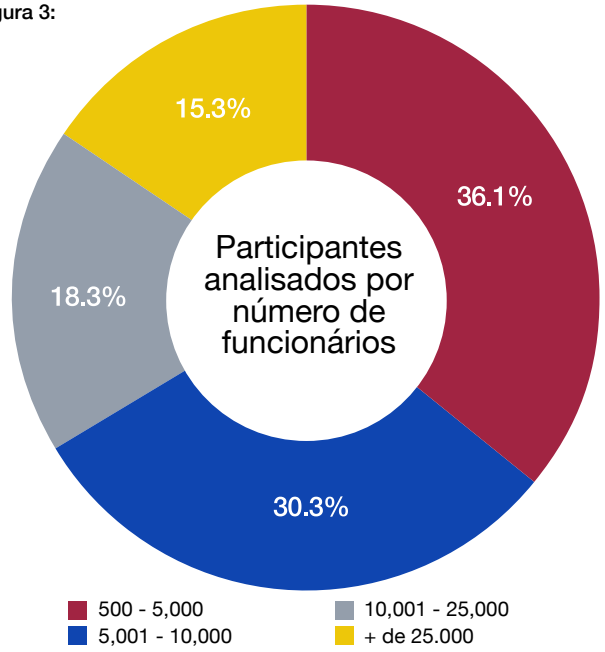
Source: Ovum

Figura 1:



Source: Ovum

Figura 3:



Source: Ovum

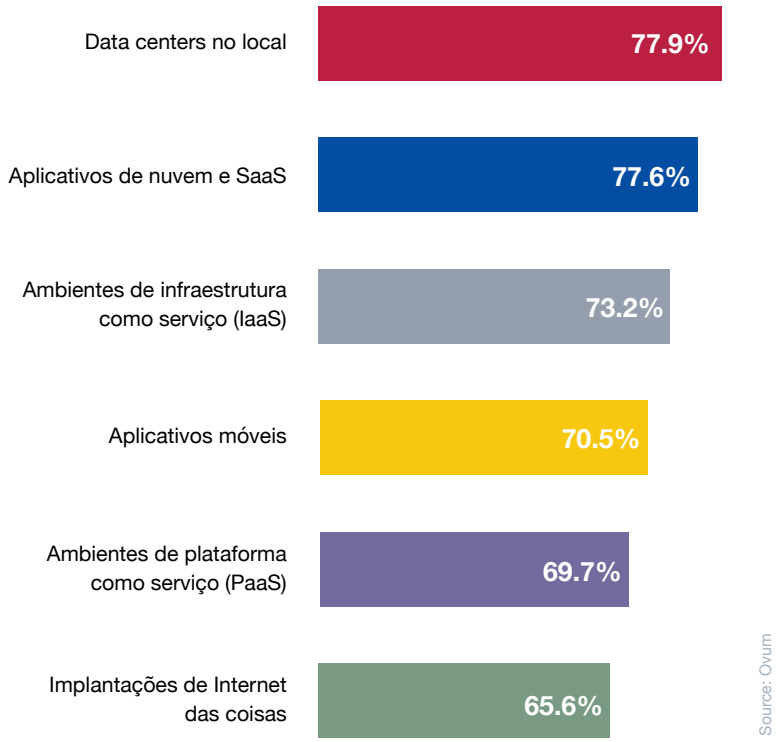
As empresas enfrentam importantes desafios de conformidade

A continuidade do uso da nuvem é inevitável

A computação em nuvem impulsiona a produtividade nas empresas modernas. Ela conecta toda a força de trabalho, consolida relacionamentos entre as organizações, parceiros de negócios e clientes, e conecta socialmente todas as pessoas. Ela transformou o modo como nos comunicamos e lidamos com as informações, mudando radicalmente as empresas mais sólidas do mundo e a forma como os orçamentos de TI são gerenciados. O recente estudo da Ovum revelou, por exemplo, que um sexto do orçamento geral das empresas já é gasto normalmente em SaaS, e que há previsão de aumento nos gastos em soluções baseadas em nuvem. Aproximadamente quatro quintos das empresas já utilizam ou planejam utilizar a computação em nuvem entre modelos de implantação (privada, pública e híbrida) e serviço (IaaS, PaaS e SaaS), representando um aumento em relação a dois terços das empresas no início de 2014. O mercado está se expandindo, à medida que a adoção por novas gerações assume a linha de frente. A segunda onda de adoção alcançou o seu momento máximo, e uma terceira onda de empresas recém-chegadas também começou a crescer em 2015.

O estudo sobre a soberania dos dados fornece novas evidências sobre o nível de confiança na nuvem para o armazenamento de dados regulamentados e confidenciais. Isso contrasta acentuadamente com o que ocorria há alguns anos, quando a discussão colocava em cheque a própria confiabilidade da nuvem. Agora, confiamos na nuvem para a proteção dos ativos mais confidenciais (consulte a Figura 4), o que demonstra uma mudança positiva na forma como vemos hoje seu papel nos negócios. O estudo revelou também que 58% dos participantes confiam na nuvem para todas as operações comerciais, apesar do potencial impacto dos regulamentos de privacidade dos dados em vias de aprovação, que pretendem alterar a forma como os dados são armazenados, transferidos e acessados no mundo inteiro.
Portanto, mesmo com mudanças nos regulamentos, a decisão pela computação em nuvem já foi tomada. Ainda assim, a regulamentação dos dados mantidos em nuvem está se tornando rapidamente o maior problema para advogados, políticos e empresas, enquanto tentam equilibrar a privacidade dos dados com acesso e produtividade.

Figura 4: Respostas a "Em quais desses ambientes tecnológicos os seus dados regulamentados e confidenciais estarão presentes nos próximos três anos (ou seja, em meados de 2018)?"



A Ovum acredita que parte do motivo para o favorecimento da computação em nuvem é a questão da disponibilidade de recursos. Não é segredo que as organizações muitas vezes têm recursos limitados para a implantação da proteção correta para os dados regulamentados e confidenciais, ou para comprovar a conformidade adequada quando os dados são mantidos no local. Portanto, a proteção dos dados em si está se tornando outro motivo para a adoção da nuvem, porque a opinião dos clientes é que seus provedores tendem a reunir as melhores soluções possíveis de segurança como parte do pacote de serviços oferecido.

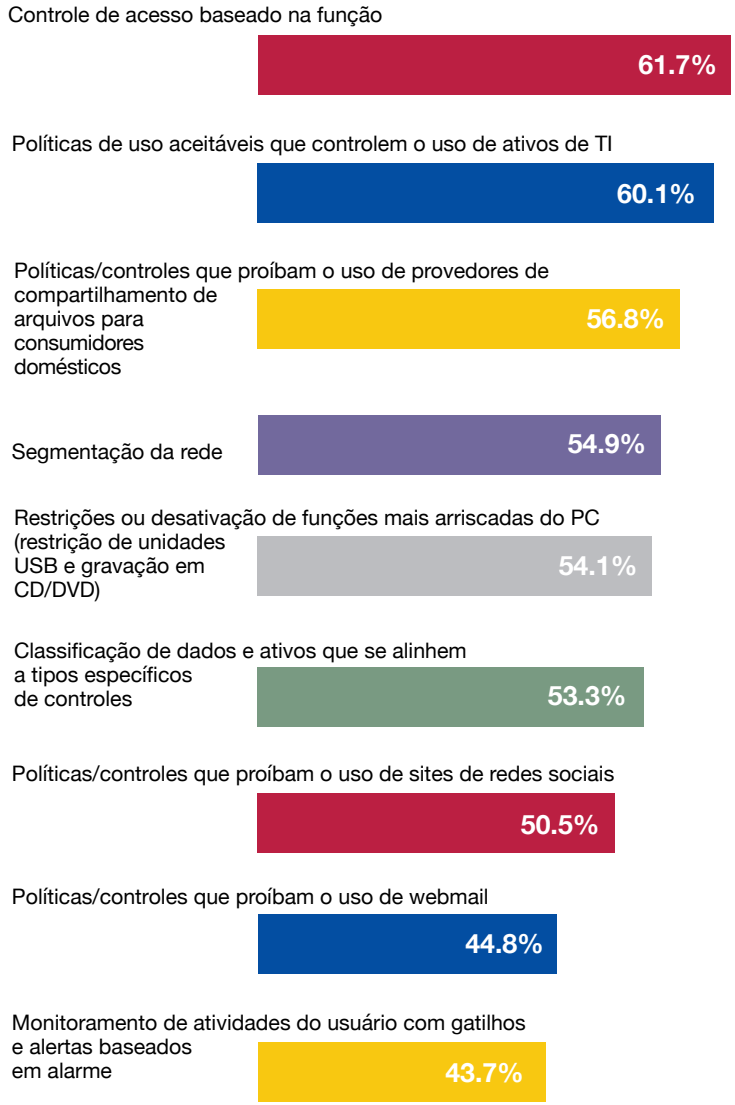
As empresas não estão tomando medidas básicas para a proteção dos dados confidenciais

Descobrimos que as empresas não estão assumindo sequer as medidas mais rudimentares, e que apenas 54% delas desativam recursos do PC, como o uso de unidades externas, e apenas 57% bloqueiam o acesso a aplicativos de armazenamento e compartilhamento de arquivos para o mercado doméstico sem controle empresarial, como o Dropbox.

É provável que as organizações com estas lacunas na proteção dos dados recorram aos provedores de nuvem para obterem ajuda, em vez de gastarem tempo e recursos tentando corrigir internamente os problemas com os dados. Uma análise adicional dos resultados do estudo revela que a deficiência geral em medidas para a proteção dos dados se aplica particularmente a pequenas e médias empresas. É provável que, para elas, a atualização dos recursos de proteção de dados exija um investimento desproporcionalmente superior, o que explicaria este resultado.

O foco no cliente por todos os tipos de organizações no escopo preciso desta proteção tende a aumentar, à medida que as empresas assumem maiores responsabilidades de conformidade no sentido de fornecer proteções adequadas para dados confidenciais, e as tecnologias relevantes para tal estão nas mãos de provedores de nuvem e de SaaS.

Figure 5: Respostas a "Que políticas, processos e controles a sua organização utiliza atualmente para auxiliar na proteção de dados e impedir o uso incorreto?"



Source: Ovum

Os regulamentos de privacidade de dados não são uniformes, deixando as empresas globais vulneráveis e confusas

Leis novas e mais rígidas de privacidade de dados causarão ainda mais problemas para as empresas que, atualmente, ainda não implementam medidas para a proteção dos dados. Atualmente, as leis de privacidade de dados são criadas de acordo com o local, sem qualquer estrutura geral que as controle e imponha ordem. Empresas multinacionais, que operam em várias jurisdições, enfrentam uma série de leis que exigem diferentes respostas (consulte a Tabela 1). Além disso, não está claro exatamente como as leis atuais poderão mudar. Por exemplo, a lei de Safe Harbor, um acordo de 15 anos sobre a transferência de dados entre a UE e os EUA, foi declarada inválida recentemente, afetando aproximadamente 4.000 empresas que não podem mais transferir legalmente os dados fora da UE para os EUA sem a cobertura de outros dispositivos legais como cláusulas-modelo, ou regras empresariais obrigatórias. Isso deixa as empresas globais, especialmente aquelas com presença na Europa, confusas sobre o curso de ação mais seguro e preocupadas com a possibilidade de violarem a lei com novas regras.

Tabela 1: Estado atual dos regulamentos de proteção de dados

País/região	Definição de dados pessoais	Formulários de consentimento necessários para o tratamento de dados pessoais	Regras para a transferência de dados pessoais para o exterior	Solicitações de dados por órgãos públicos	Penalidades
UE	Informações relacionadas a uma pessoa física identificada ou identificável. A versão preliminar do regulamento inclui endereços IP.	"Consentimento não ambíguo." A versão preliminar do regulamento tem o objetivo de introduzir o consentimento explícito.	A EC e os estados-membros decidem se um terceiro país fornece proteção adequada; se não, há a obrigatoriedade de salvaguardas.	Não está claro após a revogação da Diretiva de Retenção de Dados. Legislação nacional ainda formalmente em efeito.	As sanções são decididas em cada país. A versão preliminar do regulamento propõe multas de até 2% da movimentação anual de vendas da empresa.
EUA	Não está claro. Varia de acordo com diferentes leis/ setores.	"Consentimento prévio por escrito ou digital", sujeito ao Communications Act (Lei das Comunicações).	Sem regras específicas. A Federal Trade Commission (FTC, Comissão Federal de Comércio) dos EUA sustenta que a legislação dos EUA ainda é aplicável quando os dados são provenientes dos Estados Unidos.	Geralmente, é necessário emitir um mandado judicial. O FBI e outras agências têm exceções abrigadas pelo Patriot Act (Lei Patriótica dos EUA).	As sanções variam, de acordo com diferentes leis.
Austrália	"Informações ou um parecer, real ou não, registrados de forma material ou não, sobre um indivíduo identificado ou indivíduo razoavelmente identificável."	As organizações devem assumir "medidas razoáveis para as circunstâncias" para avisar as pessoas sobre a coleta de dados.	As organizações que transferem informações devem tomar medidas razoáveis para garantir que os princípios da lei não sejam violados, quando os dados forem enviados a outro país.	Um órgão governamental não deve coletar informações pessoais, a menos que tais informações sejam razoavelmente necessárias ou se relacionem diretamente a uma ou mais de suas funções ou atividades.	Multas cíveis de até US$ 1,57 milhões (AUD1,7 milhões) para violações da lei graves ou recorrentes.
Singapura	"Dados, verdadeiros ou não, sobre uma pessoa que possa ser identificada com base em tais dados ou juntamente com outros dados ou informações aos quais a organização provavelmente tenha acesso."	Deve-se obter o consentimento por escrito ou registrado, de modo que possam ser armazenados para consulta futura, embora possam ser obtidos verbalmente.	Transferências de dados são permitidas quando o mesmo nível de proteção aos dados é concedido no país que os recebe.	Organizações e órgãos públicos que ajam em nome de um órgão público estão isentos do abrigo da Lei de Proteção de Dados (PDPA).	Penalidades financeiras em valor não excedente a US$ 799.000 (1 milhão SGD).
Brasil	O "Enquadramento Civil da Internet" será finalizado com regulamentos mais detalhados.	"Consentimento livre, fundamentado e explícito." Regulamentos futuros poderão definir a questão em mais detalhes.	A transferência é permitida, mas as empresas precisarão acatar a legislação brasileira se qualquer coleta/processamento de dados ocorrer no Brasil.	O tempo de retenção é de um ano para registros de conexão de provedores de serviços de Internet (ISPs) e de seis meses para provedores de aplicativos. A polícia ou os tribunais poderão exigir extensão do prazo.	Até 10% do movimento das vendas da empresa no Brasil, excluindo-se impostos, e suspensão temporária ou completa das atividades de coleta e processamento de dados.

Source: Ovum, and quoted verbatim text from legislation

Regulamentos europeus em vias de aprovação definirão a norma para a privacidade global dos dados, mas colocarão em risco a economia da UE

Em termos de PIB, a UE como um todo é a maior economia global, de acordo com o Fundo Monetário Internacional (FMI) e o Banco Mundial. Desse modo, ela está em condições de definir o padrão regulamentar para outras regiões globais, e qualquer legislação europeia afetará inevitavelmente todas as empresas com operações internacionais. As primeiras disposições para a proteção da privacidade dos dados na UE ocorreram sob a Diretiva de Proteção de Dados de 1995. Entretanto, há alguns anos, houve um amplo reconhecimento entre as autoridades da UE de que a tecnologia havia evoluído e exigia um novo regime de regulamentos (a GDPR iminente) para abordar a adoção empresarial de smartphones, tablets, conectividade universal de banda larga e serviços em nuvem.

A Tabela 2 fornece um resumo das principais alterações na GDPR. O nosso estudo revelou que as empresas globais pretendem mudar suas operações comerciais em alguns países europeus após a finalização da GDPR. De acordo com a nossa amostra, 78% das empresas dos EUA, 62% daquelas do Reino Unido, 46% das empresas da América do Sul, 71% das alemãs, 58% das empresas francesas e 71% das empresas da Austrália e Nova Zelândia (ANZ) pretendem analisar suas abordagens. Isso pode representar um forte golpe econômico para a UE, cuja prosperidade baseia-se nos negócios internacionais. O custo vem em apoio a esta decisão, com 68% dos participantes globais acreditando que a GDPR aumentará imensamente os custos de fazer negócios com a UE. Além disso, 85% das empresas dos EUA acreditam que será mais difícil competir com empresas da UE, o que pode significar redução do número de empresas dos EUA que operam na UE. Esses resultados demonstram a gigantesca incerteza que envolve a GDPR, com algumas empresas prevendo um impacto negativo sobre os negócios globais, e provavelmente para a economia da UE como consequência.

Outra preocupação mencionada pelos participantes diz respeito a potenciais penalidades. A extensão das multas para as empresas no caso de violação da GDPR é potencialmente de 2% da receita global, o que significa bilhões de dólares para as maiores empresas do mundo. De acordo com o nosso estudo, mais de 50% das empresas globais acreditam que serão multadas como resultado da GDPR.

Tabela 2: Algumas das principais alterações na GDPR.

Publicação da GDPR	Mudança	Impacto
Tudo em um só lugar	As empresas acordarão sua posição em termos de conformidade com um único regulador para toda a UE, e não com um para cada estado-membro	Simplificação da conformidade Obs.: ainda não há 100% de garantia de que este plano entrará em vigor
Processadores de dados	A legislação de privacidade de dados estende-se além dos controladores de dados e está sujeita a uma nova classe de ator, o processador de dados	Os provedores de serviços em nuvem, provedores de SaaS e outros precisam acatar a Lei de Privacidade de Dados da UE
Extraterritorialidade	As empresas com sede fora da UE estão sob a influência da lei quando lidam com dados de residentes na UE	Provedores de serviços fora da UE podem precisar investir em data centers locais, como uma das formas de abordar a questão
Residência dos dados	Os dados sobre titulares dos dados da UE não podem ser transferidos para fora da EEA sem cobertura legal. (consulte as informações fora desta tabela sobre o fim da cobertura sob a certificação de Safe Harbor)	Idem anterior
Criação de perfil	Um titular precisará fornecer consentimento para o repasse dos seus dados a outros controladores de dados que não seja aquele a quem forneceu seus dados para fins de criação de perfil	Isso afetará potencialmente os processadores de dados, se estiverem usando ou encaminhando informações para outros controladores de dados, ou se eles próprios estiverem usando os dados para fins de criação de perfil. Obs.: ainda há debates sobre a necessidade de o consentimento ser explícito ou implícito

Source: Ovum

No geral, a maioria das multinacionais (57%) acredita que a GDPR é uma reação exagerada às práticas de vigilância reveladas pelo material trazido a público por Edward Snowden. Vale notar que os participantes europeus também concordam com esta impressão, com 57% dos participantes alemães, 51% daqueles no Reino Unido e 46% dos participantes franceses dizendo que a GDPR é uma reação exagerada para o problema de direitos de proteção de dados. Novamente, a motivação por trás dessas respostas tende a ser as implicações de custo, da perspectiva de multas e estratégia de negócios.

A localização dos dados é o ponto de controle crítico, mas de difícil definição

Sob a perspectiva legislativa, a questão de "onde estão os dados" é fundamental. No debate sobre a soberania dos dados, preocupações fundamentais incluem a localização dos dados e a clara definição do ponto de controle sobre os dados com identificação pessoal. Em nosso estudo, vimos incerteza e confusão sobre esses conceitos aparentemente óbvios. A capacidade de exercer a soberania sobre os dados corporativos (controlar o acesso a eles) e a conquista da conformidade dependem muito da localização dos dados, porque o seu local de armazenamento é um fator para determinar a legislação que os rege e o nível de acesso que deve estar disponível. Exercer controle sobre a localização dos dados é uma dificuldade considerável para muitas organizações, pois a maior parte dos sistemas não dá suporte ao conceito da localização dos dados como uma decisão relacionada aos negócios e, especialmente, não os sistemas baseados em nuvem. A complexidade que envolve esta questão se torna maior ainda, porque a definição exata da localização dos dados para fins de conformidade varia para diferentes artigos da legislação e pode estar aberta à interpretação jurídica em alguns locais. As empresas que tentam conquistar a conformidade podem precisar ter opções que ofereçam controle sobre a localização física, lógica, legal e política dos dados. Na verdade, já ocorrem discussões legais em tribunais do mundo inteiro, com base no conceito fundamental de localização e controle dos dados e em quem tem jurisdição sobre tais dados (um exemplo é o caso da Microsoft envolvendo dados armazenados em Dublin, Irlanda, que está sendo solicitado por um juiz dos EUA).

O nosso estudo (consulte a Tabela 3) mostra que não há consenso sobre essas questões de localização dos dados. Também descobrimos que 50% das empresas participantes planejavam mudar a abordagem primária para este controle nos próximos três anos. Assim, poderá haver incerteza sobre a capacidade da abordagem atual dos nossos participantes para atender aos novos requisitos e também sobre a abordagem que deveriam escolher. Isso também pode sugerir que as empresas estão aguardando por normas definitivas. É imperativa a necessidade de uma abordagem que forneça diversas opções técnicas, como a capacidade de oferecer controles para a localização física e lógica.

Tabela 3: Abordagens atuais/possíveis dos participantes ao problema da privacidade dos dados

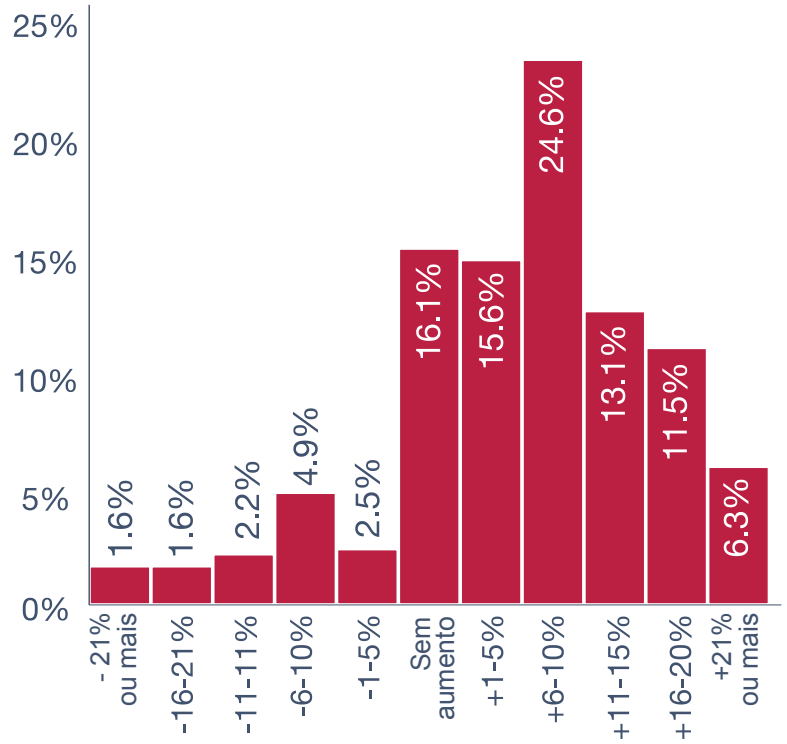
Resposta	Abordagem principal atual	Consideração desta abordagem
Tomamos nossas decisões sobre a privacidade dos dados usando a localidade jurídica dos dados (que se refere aos países que tendem a ter jurisdição sobre os dados – e à jurisdição cujas leis devem ser violadas para que alguém tenha acesso aos dados contra a sua vontade.) – ex. um país responsável por suas próprias leis que regem essas matérias	26%	27%
Tomamos as nossas decisões sobre privacidade de dados usando a localização lógica dos dados: (a localidade geográfica a partir do qual é exercido o controle sobre determinada função de computação, isto é, onde reside o ponto de criptografia).	27%	33%
Tomamos nossas decisões sobre a privacidade dos dados usando a localização física dos dados: (tradicionalmente, as localidades geográficas em que as informações são realmente gravadas para armazenamento).	33%	24%
Tomamos nossas decisões de privacidade de dados usando a localização política dos dados (este é o ponto provável de aplicação de pressão governamental para a divulgação do conteúdo).	14%	15%

Source: Ovum

Os regulamentos impõem custos imensos

À medida que muda o clima regulamentar, como em Hong Kong, Singapura e Rússia, por exemplo, os orçamentos também são afetados. A regulamentação da privacidade dos dados é, tradicionalmente, um problema legal; porém como agora ela afetará as funções de tecnologia e compliance, nosso estudo mostra que muitas empresas estão esperando contratar funcionários nesses departamentos para gerenciarem as implicações dos iminentes regulamentos de privacidade de dados. Em termos de segmentação dos resultados, 19% preveem contratações no departamento jurídico, 31% preveem contratações no departamento de tecnologia, e 34% preveem contratações no departamento de compliance. Por sua vez, isso levanta outras questões sobre alterações nas funções e competências dos departamentos jurídico, tecnológico e de compliance, que serão extremamente úteis quando os novos regulamentos entrarem plenamente em vigor. De acordo com nossos resultados, os participantes acreditam que os profissionais de tecnologia e compliance são as contratações mais apropriadas em apoio ao que geralmente é definido como um problema legal, e é provável que eles vejam mais especialistas de tecnologia e compliance aprendendo mais sobre a lei de privacidade dos dados nos próximos anos.

Figura 6: Respostas a "Que alterações no orçamento você prevê nos próximos dois anos como resultado da reforma regulamentar global em relação à proteção de dados/soberania de dados?"



Source: Ovum

Claramente, com este amplo escopo de impacto, os custos se acumularão. O nosso estudo indica o efeito esperado sobre o orçamento geral (consulte a Figura 6). Vale notar que mais de 30% dos participantes esperam aumentos no orçamento de no mínimo 10% e que quase um quarto deles prevê algo entre 6% e 10%. No geral, mais de 70% dos participantes esperam aumentos no orçamento, devido ao regulamento de privacidade de dados prestes a ser aprovado.

As organizações com sede nos EUA estão sob pressão

Como consequência das revelações de Edward Snowden sobre as atividades de vigilância da Agência de Segurança Nacional (NSA) dos EUA, o país enfrenta muita desconfiança. Solicitamos que os participantes classificassem os principais países industrializados com base em sua crença de que acessariam seus dados sem permissão, e os EUA foram considerados os menos confiáveis, com China e Rússia vindo em segundo e terceiro lugares, respectivamente. Na verdade, o devido processo legal (due process) nos EUA fornece ampla proteção à privacidade, possivelmente melhor até mesmo que a dos países europeus. Contudo, as opiniões têm sido imensamente influenciadas por matérias incessantes nos meios de comunicações, cujo fluxo aumentou mais ainda após as revelações. Novos regulamentos na Europa também colocarão as empresas dos EUA em posição de desvantagem. No nosso estudo, 63% dos participantes acreditam que os regulamentos propostos de GDPT da UE dificultará ainda mais a concorrência para as empresas dos EUA, e 70% acham que a nova legislação favorecerá empresas com sede na Europa.

Recomendações

Os problemas relacionados à soberania dos dados advindos da legislação terão grande impacto sobre um grande número de organizações que operam em âmbito internacional. As empresas precisam equilibrar as demandas comerciais, jurídicas e de consumo ao lidarem com informações com identificação pessoal. Atualmente, as ações necessárias são:

Estabelecer a estratégia de soberania dos dados

Empresas que operam em mercados internacionais e coletam informações com identificação pessoal (IPI) estão sujeitas aos regulamentos de privacidade de dados em todos os países em que fazem negócios. As organizações não estão isentas de responsabilidade por utilizarem um provedor externo para o gerenciamento dos dados. O primeiro passo é reconhecer esta responsabilidade e criar uma estratégia para reagir. Essa estratégia deve ser gerenciada por uma equipe executiva central, responsável pelo estabelecimento de controles, políticas e procedimentos para manter a conformidade. A sua equipe de GRC já pode ter iniciado este processo, mas a equipe executiva precisa apoiá-la.

Conduzir uma avaliação de risco de privacidade

A boa governança deve incorporar a identificação de riscos significativos para a organização. O contexto é extremamente importante ao avaliar-se a exposição da privacidade, e certos setores, como o farmacêutico e de seguros, enfrentam supervisão e exames regulamentares significativos. A avaliação de risco de privacidade deve começar com a classificação das informações em amplas categorias (IPI e informações confidenciais da empresa, por exemplo), e seu mapeamento em relação aos processos comerciais atuais e localidades relacionadas. Identificar e analisar regulamentos pertinentes de privacidade em cada jurisdição na qual a empresa opera. Preparar-se para mudar os processos de negócios para atender às demandas regulamentares. Talvez você já tenha tecnologias que possam auxiliar na avaliação do seu conteúdo (por exemplo, ferramentas de classificação de dados como o Atlas) e, inversamente, talvez você tenha tecnologias em uso que aumentem o seu risco (por exemplo, ferramentas de compartilhamento doméstico de arquivos, como o como o Dropbox).

Incluir pessoas

Questões legais e tecnológicas dentro do escopo da avaliação dos efeitos dos problemas de soberania dos dados: reconhecimento de que a privacidade e soberania dos dados são desafios complexos que afetam toda a sua empresa. Treinar a sua equipe é tão fundamental quanto implantar soluções tecnológicas para o gerenciamento dos fluxos de trabalho. Não é financeiramente viável ou legalmente sensato manter o foco apenas na tecnologia, no processo ou na atividade dos funcionários individualmente, porque todos os três são importantes.

Inicie as discussões agora

Com provedores de tecnologia e de serviços sobre seus planos de atender às novas exigências legislativas: fornecedores experientes já estão preparados para abordar as preocupações com a privacidade dos dados.Ter opções é fundamental, porque as leis serão inconsistentes de um país para outro, e mudam rapidamente. Os fornecedores devem ser capazes de responder a perguntas sobre a localização física e lógica dos dados e ter contratos de serviços que também ofereçam flexibilidade legal.

Appendix

Metodologia

O estudo da Ovum, conduzido no terceiro trimestre de 2015, incorpora 366 respostas de organizações de diferentes tamanhos, em diferentes áreas do mundo e em vários setores. A análise dos resultados do estudo foi realizada no contexto de consultorias contínuas com clientes da Ovum, discussões com fornecedores do setor e pesquisas secundárias.

Autor

Alan Rodger, Analista Sênior de Gestão de TIC (Tecnologia de Informação e Computação) Empresarial
alan.rodger@ovum.com

Ovum Consulting

Esperamos que esta análise ajude os nossos clientes a tomar decisões comerciais embasadas e criativas.A equipe de consultoria da Ovum poderá ajudar você a esclarecer possíveis dúvidas.

Para obter mais informações sobre os recursos de consultoria da Ovum, entre em contato conosco diretamente em consulting@ovum.com.

Copyright notice and disclaimer

O conteúdo deste produto está protegido pelas leis internacionais de direitos autorais, direitos de banco de dados e outros direitos de propriedade intelectual. O detentor desses direitos é a Informa Telecoms and Media Limited, nossas afiliadas ou outros licenciados. Nomes de empresas e logotipos de produtos contidos ou mencionados neste produto são nomes comerciais, marcas de serviço ou nomes de fantasia de seus respectivos proprietários, incluindo Informa Telecoms e Media Limited. A cópia, reprodução, distribuição ou transmissão deste produto por qualquer forma ou meio sem a permissão prévia por escrito da Informa Telecoms e Media Limited são expressamente proibidas. Embora tenhamos feito esforços razoáveis para garantir que as informações e o conteúdo deste produto estejam corretos na data de sua primeira publicação, nem a Informa Telecoms, nem a Media Limited ou qualquer pessoa envolvida ou empregada pela Informa Telecoms e pela Media Limited se responsabilizará por quaisquer erros, omissões ou outras imprecisões. Os leitores devem verificar de modo independente quaisquer fatos e números, já que nenhuma responsabilidade pode ser aceita a esse respeito; os leitores assumem total responsabilidade e risco, em conformidade, pelo uso de tais informações e conteúdo.

Todas as opiniões expressas neste produto por autores ou colaboradores individuais são de sua total responsabilidade e não refletem necessariamente as opiniões da Informa Telecoms e Media Limited.

ovum

FALE CONOSCO

www.ovum.com
askananalyst@ovum.com

FILIAIS INTERNACIONAIS

Pequim
Dubai
Hong Kong
Hyderabad
Johannesburg
Londres
Melbourne
Nova York
San Francisco
Sao Paulo
Tóquio

INTRA LINKS™