

negócios iniciativas

Este suplemento faz parte integrante do Jornal de Negócios n.º 3522, de 19 de Junho de 2017, e não pode ser vendido separadamente.

O novo Regulamento da Protecção de Dados

- Tudo o que muda com o regulamento
- Empresas precisam de soluções globais
- Perguntas e respostas das novas regras

Provedor da Protecção de Dados

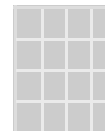
O perfil e a importância da nova figura

Implementação

Em que ponto estão os vários sectores

Inês Gomes Lourenço





Uma nova abordagem à protecção de dados

O Regulamento Geral de Protecção de Dados é uma mudança de abordagem na questão da segurança e da privacidade dos dados pessoais. Acrescenta à economia digital a dimensão da segurança e da credibilidade das organizações.

FILIPE S. FERNANDES

“É um regulamento complexo para o tecido empresarial dominado por PME e não é possível comprar uma solução chave na mão”, refere Pedro Faustino, executivo director da Axians. “Nesta questão não há uma bala de prata, que faça com que a empresa tenha um compliance perfeito”, diz Ignacio Berrozpe, sales engineer da Thales. Estes dois especialistas participaram no painel “O GPS da Implementação do Novo Regulamento da Protecção de Dados” na conferência “O Novo Regulamento da Protecção de Dados” organizada pelo Jornal de Negócios, em parceria com a Axians, a CMS e a Thales.

“As empresas recolhem muitos dados de que têm de extrair valor e os transformam numa vantagem competitiva. Não é um desafio apenas jurídico, processual, de organização, ou tecnológico. Se excluirmos uma destas dimensões estamos a ver o problema de uma forma muito redutora”, refere o responsável da Axians, Pedro Faustino, que afasta o cenário de drama e da

apologia do medo que o quadro sancionatório provoca: “Grande parte das organizações já tem parte deste trabalho feito. O tema da segurança dos dados pessoais e digitais não é um tema novo, por isso há organizações que já fizeram parte deste percurso.” Faltam o resto.

Auditoria de dados

“As empresas têm de se questionar como é que fazem a protecção de dados, que tecnologias têm, como vão cumprir os aspectos legais e de compliance”, refere Ignacio Berrozpe. “Esta regulação toca em vários aspectos pois tem a ver com a protecção de dados, mas também de uma forma mais geral com segurança dos dados e envolve vários objec-

tivos e funções da empresa.”

A abordagem começa por entender a cadeia de valor da organização de acordo com a missão a que se propõe, refere Pedro Faustino. Depois tem de se perceber os processos que suportam essa cadeia de valor e só depois ver que dados é que estão por trás desses processos. “À medida que vamos percorrendo esta cadeia e estas fases vamos afinando o problema e ver se há dados ou processos a que se aplique este regulamento”, explica Pedro Faustino. No final faz-se a cartografia da informação, o que é que se tem do ponto de vista de dados, o que são, como é que entram e saem, o que é que acontece dentro da empresa. “Depois vemos quais são os riscos associados à perda daquela informação, e que impacto é que têm, o que depende do grau de profundidade dos dados pessoais detidos e conforme o tipo de impactos assim se aplicam medidas diferentes”, conclui o especialista da Axians.

No final surge a recomendação sobre a aplicação a este universo de dados de um conjunto de processos e regras de tratamento e um conjunto de medidas de natureza tecnológica que se podem revelar necessárias para garantir que existe protecção de dados.

Segurança e credibilidade

“O regulamento é mais do que

uma moldura legal, é uma mudança de abordagem à questão da segurança e da privacidade dos dados pessoais. Este regulamento é uma coisa boa porque também acrescenta à economia digital a dimensão da segurança e, portanto, da credibilidade das organizações”, acentua Pedro Faustino.

Foram incluídas entidades que não estavam abrangidas pela diretiva, como por exemplo os subcontratantes, os business processers. Por outro lado, as entidades que não estão estabelecidas no Espaço Económico Europeu (que inclui a União Europeia e países como a Noruega, a Islândia e o Liechtenstein) podem, em certas situações, ser sujeitos à aplicação deste regulamento. “Para isso é necessário que essas entidades tratem de dados pessoais de residentes na União Europeia em conexão com bens ou serviços que são oferecidos aos mesmos ou quando exista um controlo dos comportamentos dos cidadãos situados no Espaço Económico Europeu”, refere João Leitão Figueiredo, advogado da CMS Rui Pena & Arnaut.

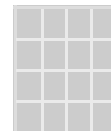
Mantém-se um conjunto de excepções e continuam a ser actividades que não estão abrangidas pelo regulamento como tratamentos de dados para fins criminais, controlo de actividades de segurança pública, tratamentos para fins exclusivamente domésticos ou pessoais. ■



Não é um desafio apenas jurídico, processual, de organização ou tecnológico.

PEDRO FAUSTINO
Executive director
da Axians





Tiago Freire, subdirector do Jornal de Negócios, com João Figueiredo, Ignacio Berrozpe e Pedro Faustino.

O consenso que muda

"O consentimento do titular dos dados deverá ser dado mediante um acto positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato electrónico, ou uma declaração oral" é o que está escrito no Regulamento Geral de Protecção de Dados. Houve pois um acréscimo dos requisitos para o consentimento.

O regulamento tentou eliminar alguns dos erros que foram detectados na vigência de duas décadas da directiva. "A figura do consentimento tem uma relação muito directa com a transparência, que surge reforçada ao longo do articulado", diz João Leitão Figueiredo.

Para tratar dados pessoais, as empresas têm de prestar muito mais informações ao titular dos dados. Têm de explicar o tipo de dados a recolher, tempo de armazenamento, os fins a que se destinam, se há tratamento automatizado, se são transferidos para outras entidades ou para fora do espaço económico europeu. Há um acréscimo de responsabilidade em que as empresas têm de considerar mecanismos alternativos para a recolha e tratamento de dados como por exemplo o contrato, que tem de ser feito em linguagem mais comum pois, caso contrário, leva à nulidade do mesmo. ■

O provedor da protecção de dados

Esta figura do encarregado da protecção de dados não tem uma definição jurídica específica, mas tem uma importância fulcral para um conjunto significativo de empresas.

"Aparentemente o DPO (Data Protection Officer ou Encarregado de Protecção de Dados) não é uma figura obrigatória para 90% das empresas", diz João Leitão Figueiredo. Um dos grupos de trabalho emitiu uma série de "guidelines" sobre as funções do DPO e quais as empresas que deveriam ter; não chegou a uma conclusão definitiva, por isso "nos 'guidelines' aconselha-se as empresas, em caso de dúvida, a nomearem um DPO". Até porque "tradicionalmente a protecção de dados estava longe de ser uma prioridade e o que este regulamento faz é pegar numa questão

não prioritária e transporta-a para o topo das preocupações da empresa, porque o DPO passa a reportar ao nível mais elevado de uma empresa", conclui o advogado da CMS Rui Pena & Arnaut.

Apesar de haver pouca rigidez jurídica sobre esta figura, ela é absolutamente essencial, até pelas suas funções, havendo alguma margem para as empresas criarem o posto. O artigo 37 do regulamento enuncia apenas três situações em que o encarregado da protecção de dados é obrigatório. As entidades públicas - excepto os tribunais no exercício das suas funções jurisdicionais -, quando a actividade principal da empresa, mesmo que seja por subcontratação, seja o tratamento de dados em grande escala ou quando tenham

como actividade principal o tratamento em grande escala de categorias especiais de dados e de dados pessoais relacionados com condenações penais e infracções. "Em alguns países inclinam-se para tornar esta obrigatoriedade genérica, como a Alemanha" diz João Leitão Figueiredo.

O DPO serve de intermediário entre as várias entidades com as quais as empresas se vão relacionar, como as autoridades de controlo, os trabalhadores, os clientes, os parceiros, e a estrutura de gestão. "O DPO terá poderes reforçados, e é obrigação das empresas apreenderem algo que é fundamental. O DPO pode ser ou não um trabalhador da empresa, conforme a opção da empresa, mas tem de ser garantido ao mesmo um grau de inde-

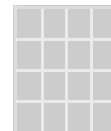
pendência na execução das suas funções" alerta João Leitão Figueiredo. Não existe em termos legais uma proibição em relação à acumulação de cargos na empresa. Mas existem pistas do modo como deve ser interpretado o DPO e o espírito não é o da acumulação de cargos que gerem conflito de interesses.

Esta é uma figura que "tem funções técnicas, legais e de gestão" refere Ignacio Berrozpe, sales engineer da Thales. Tem de fazer o mapeamento dos dados, definir as políticas de protecção de dados, implementar e monitorizar a protecção, fazer "assessment" sobre a utilização e o funcionamento do sistema, auditoria sobre o mesmo, e implementar soluções para as falhas detectadas pela auditoria e comunicar com as autoridades. ■



A figura do consentimento tem uma relação muito directa com a transparência, que surge reforçada.

JOÃO LEITÃO FIGUEIREDO
Advogado da CMS Rui Pena & Arnaut



80% das empresas “ignoram” novo regulamento

Estudo da CIP refere que as empresas ainda não estão sensibilizadas nem se estão a preparar para a entrada em vigor do regulamento de protecção de dados em 25 de Maio de 2018. E as sanções são pesadas.

“Um estudo feito pela CIP refere que mais de 80% das empresas ainda não desenvolveram qualquer actividade para se adaptarem a este novo regulamento, a um ano da sua entrada em vigor. Não é só o facto de deixar para a última hora, de facto não estão sensibilizadas para a necessidade de o fazer”, disse Armindo Monteiro, vice-presidente da CIP, durante o painel “Os dados sectoriais do novo regulamento” na conferência “O Novo Regulamento da Protecção de Dados”, organizada pelo Jornal de Negócios, em parceria com a Axians, a CMS e a Thales.

“A própria associação acordou um pouco tarde para o tema”, reconheceu Cristina Siza Vieira, presidente executiva da Associação de Hotelaria de Portugal. “Nem houve qualquer movimento por parte dos quase 700 associados nem das consultoras.” Além disso, o quanto custa ainda não chegou para assustar um pouco mais. Panorama diferente é o da distribuição. “Este sector gere muitos dados e as empresas já estão a tomar um conjunto de medidas para quando o regulamento entrar em vigor não serem apanhadas de surpresa”, referiu Ana Isabel Trigo Morais, directora-geral da APED.

Modelo de regulação muda

Ana Isabel Trigo Morais considera que é necessário um novo quadro regulatório, mas que não se deveria cair na sobre-regulação “que depois não permita às empresas serem competitivas e sobretudo com os grandes blocos económicos de competitividade como o americano e asiático, que no comércio electrónico está bastante mais à frente da Europa”.

Armindo Monteiro, que também é empresário na área das tecnologias, sublinhou a relação entre a protecção de dados e a segurança. “Fazer a transformação de dados em informação levou muitos anos, tinha inicial-

mente objectivos fiscais. Não havia uma cultura nas empresas de valorização da informação. Com a sofisticação dos negócios em Portugal, a informação passou a ser um activo e surgiram os problemas como o uso indevido da informação. E se tem valor pode ser roubado.” Acrescentou que “este é o problema: as empresas não protegem ainda a informação e

não têm nenhum sistema de protecção dos sistemas de informação”.

“A alteração do modelo de hetero-regulação para auto-regulação é uma das maiores preocupações das empresas de retalho”, afirmou Ana Isabel Trigo Morais. Uma empresa para licenciar, por exemplo, uma base de dados com informações sobre os cidadãos e consumidores, fazia o pedido à CNPD e aguardava pela validação. Agora não há uma validação prévia e as empresas vão passar a ter uma obrigação de “compliance” acrescida. “Mas levanta outra preocupação porque es-

tamos muito habituados a que muitas vezes os reguladores que nos fiscalizam tenham diferentes entendimentos e critérios de adequação quando realizam as suas fiscalizações.”

O direito ao esquecimento

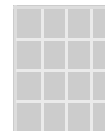
Armindo Monteiro referiu ainda o receio de como vai ser aplicado o quadro sancionatório. “Os empresários esperam que haja um sentido pedagógico em vez de um meramente sancionatório.”

Foram ainda enunciados proble-

mas como a falta de recursos especializados nas empresas, a necessidade de desenvolver mecanismos de dar resposta aos cidadãos e aos consumidores, nomeadamente quando têm de aplicar o direito ao esquecimento e quando têm de explicar na sua relação com os clientes como é que estão a utilizar os dados. Para Ana Isabel Trigo Morais, as empresas vão fazer grandes investimentos pois terá de haver, em muitos casos, “call centers”, funcionários formados para informar e responder aos clientes e um controlo maior sobre dados pessoais obtidos indirectamente. ■



Raul Vaz, director do Negócios, debateu “Os dados sectoriais do novo regulamento” com Ana Isabel Trigo Morais, Armindo Monteiro, Bartolomeu Noronha e Cristina Siza Vieira.



O caso prático da hotelaria

90%

PME

A esmagadora maioria das empresas do sector turístico são PME e não estão despertas para estas questões da protecção de dados.

Inês Gomes Lourenço

“

A alteração do modelo de hetero-regulação para auto-regulação é uma das maiores preocupações.

ANA ISABEL TRIGO
MORAIS

Directora-geral da APED

Os empresários esperam que haja um sentido pedagógico em vez de um meramente sancionatório.

ARMINDO MONTEIRO
Vice-presidente da CIP

A própria associação acordou um pouco tarde para o tema.

CRISTINA SIZA VIEIRA
Presidente executiva da Associação de Hotelaria de Portugal

”

Não há soluções “one size fits all”, pois a hotelaria é multifacetada. Por isso, a Associação de Hotelaria de Portugal desafiou dois parceiros com competências jurídicas, técnicas e tecnológicas para fazer uma matriz para ser usada por todos.

Inês Gomes Lourenço



A hotelaria tem de acelerar para estar pronta a tempo para as novas regras.

Há 75 anos, António Ferro, criador do conceito de Pousadas, dizia que quando estas deixassem de conhecer o cliente pelo nome, mas pelo número do quarto perdiam a sua essência. Hoje a hotelaria quer saber tudo sobre ele para lhe poder prestar o serviço e diferenciá-lo. “Todas as indústrias e todos os produtores de bens e serviços querem conhecer o cliente, mas a hotelaria e o turismo querem conhecê-lo em 360 graus e até um grande grau de intimidade, porque ajuda à diferenciação e isto significa cruzar muita informação”, referiu Cristina Siza Vieira, presidente executiva da Associação de Hotelaria de Portugal.

Este regulamento tem impacto no turismo em termos internos e internacionais, porque as empresas turísticas estão vocacionadas para o exterior. “Mas há forças de tração opostas”, como explicou Cristina Siza Vieira. Há um grande peso de PME, cerca de 90%, a quem este novo regulamento pouco diz. O seu core business não são os dados e vivem sobretudo das “online travellers agency”, como a Booking. Depois existem os grupos nacionais e internacionais que estão preparados para implementar e absorver estas regras.

Hóteis recolhem dados oficiais

Os hotéis estão obrigados a recolher dados e a facultar dados a autoridades públicas (SEF, INE e Banco de Portugal) que vão da nacionalidade dos seus hóspedes, idade, se viajam em família, quantos é que são. Há dados pessoais e outros até sensíveis, como a questão das alergias, etc.

A questão agora é a adaptação do novo regulamento. “Sente-se que não há soluções ‘one size fits all’, e estamos agora a dar os primeiros passos para partir este elefante às fatias e fazer um mapeamento”, diz Cristina Siza Vieira. Por isso, a Associação de Hotelaria de Portugal desafiou duas entidades com competências jurídicas, técnicas e tecnológicas, que co-

nhecem o sector, para encontrar uma matriz mais adaptável para que cada hotel possa fazer primeiro o levantamento da recolha de dados. Neste incluem-se os momentos em que recolhe dados, quais os suportes, o tipo de dados, onde os guarda, para que efeito é que recolhe. Depois poder propor aos associados um orçamento para acompanhar este processo, o “road compliance” até ao final. Tudo para que, como é timbre do sector, esteja pronto na data certa. “O turismo é caracterizado pelo ‘last minute’”, admite Cristina Siza Vieira.

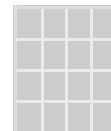
A cultura da organização tem de mudar e isso é muito perturbador porque a cultura da organização tem sido conhecer melhor o cliente e cruzar toda a informação. “A cultura tem de ser mudada, mas sem perder o conhecimento do cliente que é a alma da hotelaria”, remata Cristina Siza Vieira. ■

O atraso dos municípios

“Os municípios estão mais atrasados na aplicação do Novo Regulamento de Protecção de Dados do que as empresas porque vão ter outras grandes alterações este ano”, disse Bartolomeu Noronha, presidente do Observatório dos Municípios com base num inquérito feito junto dos 308 municípios e em que 90% revelavam não estar preparados para esta mudança. Em 1 de Julho entra em vigor o novo Código da Contratação Pública, que entre outras inovações cria o gestor de contrato e está prometida a descentralização de competências do Estado central, que se deve incluir o cadastro do território, para as autarquias ainda este ano. Estas duas alterações vão ter impacto na implementação do regulamento. Bartolomeu Noronha sublinhou o problema de quanto é que vai custar esta adaptação e que recursos são aportados às entidades públicas. Salientou ainda que os autarcas têm uma responsabilidade acrescida à das empresas que é a política. “Se as coisas correrem mal, a responsabilidade política é elevada e podem perder-se eleições por má protecção dos dados dos cidadãos de uma autarquia.”

Bartolomeu Noronha admite o atraso dos municípios nesta matéria.





Um regulamento para todas as empresas

Estado tem de ser exemplo

O princípio basilar do novo regulamento, que entra em vigor a 25 de Maio de 2018, é que o nível de protecção dos direitos e liberdades das pessoas singulares na recolha, tratamento e protecção de dados deve ser e terá de ser equivalente em todos os Estados-membros.

“O Novo Regulamento Geral de Protecção de Dados destina-se a todas as empresas sem qualquer exclusão”, disse José Luís Arnaut, managing partner da CMS Rui Pena & Arnaut, na sessão de abertura da conferência “O Novo Regulamento da Protecção de Dados”, organizada pelo Jornal de Negócios, em parceria com a Axioms, a CMS e a Thales.

“Hoje apenas uma reduzida percentagem de cidadãos europeus não se encontra conectado à rede global, dono de uma pegada digital. A presença no ‘social media’, a forma como a empresa trata os dados dos seus colaboradores, comunica com os clientes ou compra, torna a partilha de dados pessoais algo incontornável numa sociedade moderna”, referiu José Luís Arnaut.

Este predomínio actual de

componentes técnicas e tecnológicas justificou este novo regulamento geral sobre a protecção de dados. “Mais do que uma lei é uma necessidade e um direito”, sublinhou Pedro Afonso, CEO da Axioms, porque “a protecção de dados afecta todas as pessoas e a segurança é um pilar na nossa vida e em tudo o que fazemos”.

Armin Kruse, marketing director da CIC e expert no GDPR e Vormetric da Thales, defende que a protecção dos dados não é cibersegurança. “A protecção de dados é sobre informação e dados de indivíduos, a cibersegurança é a protecção dos sistemas de segurança em relação a ataques, têm stakeholders e objectivos diferentes, embora as soluções sejam semelhantes”.

A Thales é líder europeia em cibersegurança e em segurança de sistemas e, portanto, a “questão da

protecção dos dados é uma das questões-chave”, referiu Armin Kruse, que aliás referiu que o seu grupo, como multinacional e pela sua dimensão, está a experienciar o processo de adaptação de homogeneização dos dados pessoais dos seus colaboradores.

Pedro Afonso chamou a atenção para a simbiose e a interacção entre o mundo digital e o humano. Usou a analogia dos servidores de sílica para a tecnologia e os servidores de carbono para o humano. “Uns guardam, transportam dados que depois são transformados em informação, as pessoas tomam todos os dias decisões, às vezes são os algoritmos, com essas máquinas”. Por isso, a adaptação a este novo regulamento vai exigir às empresas um trabalho em rede e colaborativo com escritórios de advogados, consultores e empresas tecnológicas.

O princípio basilar do regulamento

O princípio basilar do novo regulamento é que o nível de protecção dos direitos e liberdades das pessoas singulares na recolha, tratamento e protecção de dados deve

ser e terá de ser equivalente em todos os Estados-membros, salientou José Luís Arnaut.

O Novo Regulamento Geral de Protecção de Dados entrou em discussão em 2012 para substituir a Directiva 95/46/CE. O regulamento constitui uma das mais amplas peças legislativas aprovadas na União Europeia. É um documento com mais de 100 páginas de articulados, tem um conjunto de conceitos inovadores como o direito a ser esquecido, a portabilidade dos dados e a prestação de contas.

“Há mão pesada para os que dirigem as empresas quando não executarem nem responderem a estas novas exigências”, alertou Arnaut. Nas violações de natureza formal, as coimas vão até dez milhões de euros ou, no caso de empresas, até 2% do seu volume de negócios anual a nível mundial correspondente ao exercício anterior. Nas violações de disposições de natureza material, a coima vai até 20 milhões de euros ou, no caso de uma empresa, até 4% do seu volume de negócios anual a nível mundial no exercício anterior. ■

Jaime Quesado, presidente da ESPAP, sublinhou que “na ‘data economy’ actual a importância dos dados é fulcral” e que na aplicação da legislação comunitária e nacional “há um benchmark internacional que temos de ter em atenção”.

“Administração pública e o Estado têm de dar o exemplo de cumprimento da lei, mas também de referencial de utilização do novo regulamento”, afirmou o presidente da ESPAP.

Jaime Quesado referiu-se às questões relacionadas com a organização interna e responsabilidade da governação, referindo que “independentemente das sanções a que os administradores e gestores vão ficar sujeitos a partir do próximo ano, há necessidade de melhoria dos circuitos internos que são absolutamente centrais”.

Destacou a importância de interfaces como associações empresariais, escritórios de advogados, e consultoras, para as PME, que têm mais dificuldades na adaptação ao novo contexto.

Falou dos desafios muito importantes do ponto de vista de defesa dos direitos dos cidadãos, do relacionamento com os stakeholders e do crescimento das próprias organizações. Destacou o desafio das equipas técnicas e de os administradores usarem a informação de forma estratégica, num contexto de uso mais regulado e mais cuidado. ■

Inês Gomes Lourenço



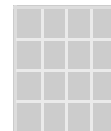
José Luís Arnaut abriu a conferência, juntamente com Pedro Afonso, da Axioms, e Armin Kruse, da Thales.



Há necessidade de melhoria dos circuitos internos, que são absolutamente centrais.



JAIME QUESADO
Presidente da Entidade de Serviços Partilhados da Administração Pública



OPINIÃO



PAULO MIRANDA
Business Development Manager
da Axiens Portugal

Regulamento Geral de Proteção de Dados - GDPRReady em 4 etapas!

A digitalização do negócio tem vindo a potenciar o aumento significativo do "valor" e "sensibilidade" da informação que é recolhida, armazenada, utilizada e processada pelos sistemas de informação que suportam o negócio das empresas em todo o mundo. É esse valor que sustentou uma cultura de "informação é poder", para o potencial de novos serviços e negócios através da evolução do negócio digital como, por exemplo: Internet Of Things (IoT), big data, machine learning, etc. Embora concorde com o potencial do "poder" da informação, a posse dessa informação é também um risco. Devido ao valor crescente dos dados, as ameaças e o impacto da sua perda ou roubo acompanharam esse crescimento.

As organizações têm agora menos de um ano para estarem prontas para a conformidade com o regulamento, e os seus responsáveis em vez de encararem o novo regulamento como um problema a resolver, devem encarar como uma oportunidade para garantir a aplicação das melhores práticas para a proteção de um dos ativos mais críticos para o sucesso do negócio da sua organização, que é a informação, incluindo os dados privados.

Os principais desafios da privacidade de dados são:

1. Como identificar e gerir os atuais problemas de privacidade?

Identificar e abordar todas as questões de privacidade que afetam a qualidade intrínseca e contextual, acessibilidade, segurança e conformidade legal de informações pessoais coletadas, usadas, armazenadas e processadas pela organização.

2. Como responder e minimizar o impacto no negócio de uma iminente brecha de dados?

Garantir que o risco de privacidade é mitigado de maneira consistente e efetiva. Proteger adequadamente os dados pessoais e informações associadas que possam revelar informação sobre titulares de dados através de controles para mitigar os riscos de privacidade a



Chris Ratcliffe/Alamy

níveis aceitáveis.

3. Como garantir a conformidade com a regulação europeia de proteção de dados?

Garantir o cumprimento dos requisitos legais de proteção de dados pessoais e que as obrigações de privacidade são atendidas, as expectativas das partes interessadas são geridas e que as penalidades por violação do regulamento são evitadas.

4. Como manter a confiança dos clientes e o valor da marca?

Garantir que a privacidade de dados entrega valor e suporta a confiança e o valor da marca, respondendo também aos requisitos do negócio.

As organizações não devem considerar que este desafio seja resolvido isoladamente apenas com serviços jurídicos, ou apenas através de políticas e processos, ou apenas através da aquisição de tecnologia. A abordagem mais eficaz e eficiente é a adoção de uma visão holística e integrada dos três pilares fundamentais para o sucesso de um projeto desta natureza, que são: (1) jurídico; (2) processos e (3) tecnologia.

Devem ser utilizados modelos maduros e já testados, como exem-

plo, as "frameworks", boas práticas e normas internacionais, como por exemplo a família de normas ISO 27001 (Gestão de Segurança da Informação), ISO 29001 (Princípios de Privacidade), COBIT®, Privacy By Design (Ann Cavoukian, Ph.D.), entre outras, considerando também uma visão de futuro, por exemplo, a integração com a diretiva europeia NIS (Security of Network and Information Systems - Segurança de Redes e Sistemas de Informação) que se tornará em breve lei nacional e obrigatória para as organizações que fornecem serviços essenciais.

Como estar GDPRReady em quatro etapas:

1. AVALIAÇÃO - Avaliar o estado atual da gestão da privacidade de dados:

Nesta etapa devem ser avaliadas as práticas atuais de privacidade de dados, descobrir os dados, os seus donos, os fluxos de recolha, uso e atividades de processamento. Avaliar o impacto no negócio e os riscos de privacidade.

2. DESENHO - Desenhar o modelo operacional de gestão da privacidade de dados:

Após a compreensão do contex-

to e realidade da organização, devem ser estabelecidas as funções, autoridades e responsabilidades para assegurar a gestão eficaz da privacidade de dados, bem como desenhar as Políticas Gerais e Operacionais de Privacidade de Dados, processos, procedimentos e os controles necessários para tratar os riscos identificados.

3. IMPLEMENTAÇÃO - Implementar o modelo operacional e os controles de privacidade:

Após a conceção do modelo operacional e dos controles necessários, deverá ser planeada e executada a implementação da estrutura de gestão de privacidade de dados juntamente com os controles de privacidade. Preparar, formar e sensibilizar as equipas e a organização para a operação do modelo de gestão da privacidade de dados.

4. GERIR - Operar, monitorizar, auditar, rever e melhorar continuamente:

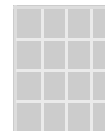
Após o início da operacionalização do modelo de gestão de privacidade de dados, este deverá ser mantido e melhorado continuamente. Monitorizar e medir os indicadores da política e dos processos. Testar a eficácia dos controles de privacidade e auditar a estrutura implementada. Através destes resultados, fazer revisão da gestão e tomar decisões efetivas para suportar a melhoria contínua do modelo de gestão de privacidade de dados.

Como resultados e benefícios é esperado através desta abordagem que:

1. Os dados pessoais estejam efetivamente protegidos;
2. Estar em conformidade com o Regulamento Geral de Proteção de Dados (RGPD/GDPR);
3. Seja mantida a confiança dos clientes e o valor da marca. ■

Artigo está em conformidade com o novo Acordo Ortográfico

Após o modelo estar implementado, é preciso mantê-lo e melhorá-lo continuamente.



OPINIÃO



JOÃO FIGUEIREDO
Advogado, CMS Rui Pena
& Arnaut

Prepare-se para a nova era da proteção de dados

Com a aproximação do dia 25 de maio de 2018, data da entrada em vigor do novo Regulamento Geral sobre a Proteção de Dados, diversas organizações já começaram a considerar as etapas necessárias para a respetiva adaptação e implementação.

Pese embora o modelo de implementação de um programa deva ser preferencialmente adaptado à realidade de cada organização, existem princípios enformadores e ações comuns que todas as organizações deverão considerar, sendo aconselhável a criação de um modelo exequível, prático e não disruptivo, baseado numa segmentação de atividades a desenvolver e não apenas na fase de análise e projeção, mas também na fase de concreta implementação.

Perante a complexidade e abrangência das tarefas previstas no regulamento, o primeiro passo para as organizações deverá ser uma séria priorização das ações com base em fatores específicos da sua atividade. Mas independentemente da natureza da sua atividade, as organizações devem promover um conjunto de atos significativos ao cumprimento do regulamento, entre os quais destacamos alguns:

Contratos comerciais – As organizações que estiverem a negociar contratos com subcontratantes (“processors”) deverão assegurar-se de que o novo contrato reflete as obrigações diretas dos subcontratantes nos termos do regulamento, compreendem as disposições obrigatórias revistas para contratos a celebrar com subcontratantes e os novos requisitos de notificação de violação de dados pessoais. Todos os contratos existentes com subcontratantes deverão, com a brevidade possível, ser revistos.

Anonimização – Verifique se os dados anonimizados atendem aos requisitos mais rigorosos para a anonimização introduzidos pelo regulamento. Caso não cumpram, determine se esses requisitos podem ser atendidos e analise as implica-



Kasper Pempel/Reuters

ções da aplicação do regulamento.

Autoridade de controlo – Determine a localização do seu estabelecimento principal e, nessa medida, quem é sua principal autoridade de controlo. Desenvolva e implemente procedimentos adequados à realização de auditorias ou ações de fiscalização por parte das autoridades de controlo.

Demonstração de conformidade – Considere o melhor mecanismo de demonstração de conformidade. Embora as políticas e processos escritos sejam cruciais, a exclusiva dependência de documentos, por norma extensos e que raramente são lidos ou seguidos na prática, poderá revelar-se insuficiente.

Registo central de processamento de dados – Promova a criação de um registo central de todo o processamento de dados pessoais que contenha as informações obrigatórias do regulamento – a auditoria e o modelo de implementação

devem auxiliar no preenchimento das informações necessárias.

Avaliações de Impacto de Privacidade de Dados (DPIA) – Implemente processos para garantir que as DPIA são efetuadas nos termos do regulamento e implemente políticas para um uso mais amplo das DPIA, porquanto ajudarão a cumprir os requisitos gerais de responsabilidade do regulamento.

Violação de dados – Desenvolva um procedimento detalhado de relatório de violação de dados e teste que funciona operacionalmente para permitir a conformidade com os requisitos de notificação do regulamento.

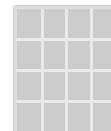
Seguro – Verifique os termos de qualquer apólice de seguro relevante para determinar se são necessárias alterações.

Formação – Certifique-se de que todos os que tenham acesso a dados pessoais recebem formação apropriada sobre o regulamento.

O dia 25 de maio de 2018 aproxima-se inexoravelmente, pelo que as organizações deverão iniciar de imediato o seu processo de adaptação cultural ao novo paradigma, pois somente assim as alterações jurídicas, organizacionais e técnicas poderão ser efetuadas de forma não disruptiva e adequada e poupar as empresas à mão pesada que a Comissão Europeia terá no caso das empresas incumpridoras. Porque a tarefa é árdua e complexa, não é despendendo a correta identificação de um modelo de implementação personalizado e profissional. ■

As organizações devem iniciar de imediato o seu processo de adaptação cultural ao novo paradigma.

Artigo está em conformidade com o novo Acordo Ortográfico



OPINIÃO

LUÍS AZEVEDO MAFRA
Sales Manager da Thales

Dados pessoais exigem cada vez mais segurança

A solução de protecção de dados da Vormetric já protege 17 das 30 maiores empresas a nível mundial com um volume de dados protegidos superior a 155 petabytes e encontra-se instalada em mais de 500.000 servidores.

Um dos desafios fundamentais da segurança cibernética é lidar com a velocidade da mudança. Com cada nova mudança de paradigma de computação – cloud, big data, IoT etc. – surgem novos recursos, desafios e possibilidades, mas surgem também novas vulnerabilidades de segurança.

Paradoxalmente, no entanto, as nossas atitudes e estratégias de segurança não estão em conformidade com este ritmo de mudança técnica. Para ilustrar, em média 63% dos entrevistados num recente "survey" sobre este tema responderam que as organizações implementam novas tecnologias antes de terem em vigor os níveis adequados de segurança para essas implementações.

A este cenário, acresce que as ameaças globais estão constantemente a evoluir, tornando para as organizações a protecção de dados em repouso, processamento de dados e dados em trânsito, um dos maiores desafios tecnológicos da actualidade.

Neste contexto, é natural que a publicação ou uso de dados pessoais indevidamente, por exemplo, a apropriação indevida da identidade, da carta de condução ou dos dados do cartão de crédito, se torne um acto apetecível. A estes actos indevidos acresce, por exemplo, a potencial utilização de dados pessoais para usos não autorizados, como para "cross-selling" com recurso a partilha de bases de dados pessoais de elevadíssimas dimensões. É neste contexto que a protecção de dados se torna tão premente, mesmo antes de ser obrigatória. Sendo que esta protecção não se limita apenas ao universo das ameaças espoliadas pelos "insiders" (colaboradores, parceiros, subcontratados, fornece-

dores, etc.) envolvidos na cadeia de valor das organizações, mas também engloba as ameaças externas, muitos das quais são bem financiadas, organizadas e muitas vezes, embora nem sempre, altamente sofisticadas.

Novo regulamento

Com a chegada do "novo" Regulamento Geral de Protecção de Dados introduzem-se novos conceitos que asseguram que os direitos dos particulares são significativamente reforçados. Neste contexto, as organizações são obrigadas a preparar-se para a introdução deste novo e desafiante quadro normativo. Após a célere identificação de quaisquer lacunas no cumprimento das regras relativas a protecção de dados, as organizações deverão proceder à implementação de um plano de "compliance", o qual passará muito provavelmente pela implementação tecnológica da protecção de dados em repouso e mecanismos de segurança aplicacionais.

A Vormetric é uma empresa do Grupo Thales dedicada à implementação de soluções de elevado desempenho para a securização de plataformas, aplicações e bases de dados, permitindo às empresas, instituições e organismos adaptarem-se rapidamente, com segurança e rapidez às necessidades de protecção e securização dos dados. A solução de protecção de dados da Vormetric já protege 17 das 30 maiores empresas a nível mundial com um volume de dados protegidos superior a 155 petabytes e encontra-se instalada em mais de 500.000 servidores. Adicionalmente a solução já assegura a protecção de dados de mais de 1.500 empresas localizadas em mais de 22 países.

A plataforma da Vormetric permite realizar de forma efectiva, escalável e agnóstica a protecção, encriptação e securização dos dados em repouso onde quer que estes residam, isto é, ficheiros, base de dados, aplicações ou servidores, e disponibiliza as funcionalidades que

permitem o desenvolvimento de protecção de dados a nível aplicacional, com a possibilidade de implementar políticas de "multitenant" e de domínio, sem degradar o desempenho dos sistemas existentes, e sem a necessidade de proceder à adaptação dos ambientes tecnológicos empresariais.

A solução da Vormetric

A solução é baseada num modelo de segregação de funções, nomeadamente das funções de gestão da segurança da informação (políticas de acesso), gestão dos sistemas de TI e os diversos e distintos perfis de utilizadores ("end users"). A plata-

forma da Vormetric regista todas as tentativas de intrusão/violação dos dados ou roubo dos mesmos, permitindo efectuar relatórios sobre a integridade dos dados e dos sistemas, bem como sobre o tipo e origem dessas acções criminosas, dando às empresas as ferramentas necessárias para efectuar o correcto "reporting" e controlo.

Assim, com esta solução as organizações podem compilar, analisar, tratar e reportar às autoridades todos os eventos e acontecimentos passíveis de serem, de forma rápida e expedita, facilitando todo o processo do ponto de vista tecnológico às empresas. Acresce que esses mesmos registos de eventos ("logs"), tentativas de acessos ou ataques internos e/ou externos (ex. ciberaques) podem ser exportados para um centro operacional de cibersegurança, por exemplo, um Centro de Cibersegurança da Thales, para tratamento e correlação de eventos e desenvolvimento de acções correctivas e preventivas sobre as infra-estruturas da organização em questão.

Fazendo uso de encriptação transparente, de um controlo de acessos robusto suportado pelas políticas de segurança da organização e de uma gestão centralizada das chaves, a solução de Encriptação Transparente da Vormetric permite securizar qualquer dado de forma eficiente sem disrupção, independentemente de ser uma estrutura física, virtual ou alojada em "cloud".

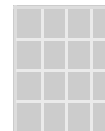
Finalmente será de referir que a solução Vormetric pode ser instalada através de licenças, appliances de SW em máquinas virtuais, com certificação FIPS 140-2 Nível 2, ou através da instalação de HW dedicado para FIPS 140-2 Nível 3. Paralelamente, a solução Vormetric pode também ser fornecida em regime de prestação de serviço anual, sob a forma, de avença mensal remotizada ou sob a forma de fornecimento em modo CAPEX (perpétuo). ■

O Grupo Thales

O Grupo Thales é uma multinacional de origem francesa, dedicada ao sector militar e de missão crítica civil. Com cerca de 70 mil colaboradores e presença em 50 países, o Grupo Thales tem um volume de facturação de 14'8 €. A Thales Portugal, SA é uma empresa 100% detida pelo Grupo Thales, que actua no mercado português e em diversas geografias internacionais, enquanto centro de competência para as soluções de comunicações de missão crítica para o sector dos transportes e segurança.

As fragilidades podem ser internas, de colaboradores das empresas, ou resultarem de ataques exteriores.

É neste contexto que a protecção de dados se torna tão premente, mesmo antes de ser obrigatória.



O novo Regulamento Geral da Protecção de Dados

A menos de um ano da entrada em vigor do novo regulamento, as dúvidas são mais do que muitas. Aos participantes na conferência do Jornal de Negócios foi dada a possibilidade de colocar questões, aqui respondidas pelos especialistas nas várias áreas: a CMS Rui Pena & Arnaut, a Axians e a Thales.

1

O que é um Encarregado de Protecção de Dados e quais as empresas que são obrigadas a terem esta figura?

A figura do Encarregado de Protecção de Dados (DPO) é uma das mais relevantes inovações do novo regulamento. Um significativo número de organizações será obrigado a nomear um DPO e assegurar que este tem condições para o exercício das suas funções, como sejam: o apoio activo da administração; tempo suficiente para o cumprimento das suas tarefas; recursos financeiros, infra-estruturas (instalações, equipamentos) e pessoal, quando apropriado; comunicação oficial da designação a todos os funcionários e autoridade de controlo; acesso a outros serviços dentro da organização para que possam receber suporte, opiniões ou informações essenciais desses outros serviços, bem como formação contínua.

Do ponto de vista das competências, o DPO deverá ter um profundo conhecimento da legislação e práticas nacionais e europeias de protecção de dados, incluindo uma compreensão aprofundada do regulamento, conhecimento das operações de processamento realizadas, conhecimento das tecnologias de informação e de segurança dos dados, conhecimento do sector empresarial e da organização e capacidade de promover uma cultura de

protecção de dados dentro da organização.

Note-se que, apesar dos DPO não se substituírem às empresas no que concerne à responsabilidade civil ou contra-ordenacional, serão um pilar essencial no cumprimento do regulamento e na criação de garantias para as organizações. (CMS Rui Pena & Arnaut)

2

O conceito de portabilidade dos dados, por exemplo o das preferências, dos clientes estão realmente prontos no início de aplicação do regulamento para serem partilhados?

Do que temos observado no nosso contexto nacional, diríamos que a maior parte das organizações ainda não estará pronta em Maio de 2018 neste tema. A questão da portabilidade de dados tem um factor muito importante para a sua boa operacionalização, o formato comum para a portabilidade dos dados. Essa é uma preocupação que cremos que deverá passar obrigatoriamente por uma concertação sectorial para acordarem um modelo e formato comum para a portabilidade desses dados. Percebemos que esse será um dos principais desafios deste regulamento para os sectores dos serviços essenciais (Utilities e Telcos), serviços financeiros e saúde. (Axians)

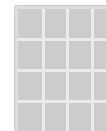
3

No caso de uma base de dados com informação do domínio público, por exemplo nomes de profissionais de saúde/n.º ordem profissional/especialização/local de trabalho, é necessário obter consentimento do titular dos dados/informá-lo de que temos esta informação?

Do ponto de vista estritamente tecnológico e no que toca à componente da protecção de dados/criptação dos dados pessoais em repouso nas bases de dados, será de destacar que a solução Vormetric da Thales permite a segregação de acesso em função do perfil de acesso concedido aquando da atribuição das políticas de acesso. O caso referido na pergunta é paradigmático, pois no caso de dados de saúde os mesmos possuem um cariz relevante e sensível, sendo portanto recomendável, senão necessário, assegurar o acesso "atomizado" aos dados em específico que a cada função cabe aceder para o exercício das suas funções, não obstante no global o dado pessoal ser o mesmo e provavelmente armazenado de forma única no mesmo registo, no caso dos pacientes. Assim, a cada profissional de saúde caberá aceder apenas aos dados pessoais do paciente que são relevantes para a sua função no exercício do seu contributo para o acto médico daquele paciente. (Thales)



O regulamento europeu é aplicável directamente aos Estados-membros, sem



necessidade de transposição local.

4

O que é a Avaliação de Impacto sobre Protecção de Dados (DPIA)? Que questões são tratadas no âmbito do DPIA? Que tipos de tratamento estão sujeitos a um DPIA? Como se deverá executar um DPIA?

De acordo com a definição da Comissão Europeia, o DPIA (Data Privacy Impact Assessment – Avaliação de Impacto da Privacidade de Dados) é um processo destinado a descrever o processamento de dados privados, avaliar a necessidade e a proporcionalidade de um processamento dos dados e ajudar a gerir os riscos aos direitos e liberdades das pessoas resultantes do processamento de dados pessoais (avaliando-os e determinando as medidas para os abordar).

O DPIA é uma avaliação de risco, que avalia o impacto da concretização de ameaças de privacidade de dados com a sua probabilidade de ocorrência, com o objectivo de serem identificadas estratégias de tratamento desses riscos num nível aceitável através de um racional de custo-benefício. (Axians)

5

O que é que muda no que diz respeito ao consentimento dado pelos indivíduos e pelas empresas?

O recurso ao consentimento para a recolha e tratamento de dados pessoais tem constituído uma prática recorrente em Portugal. As organizações têm privilegiado o consentimento como solução prática para assegurar a licitude do tratamento de dados pessoais de terceiros. O regulamento, contudo, veio criar barreiras adicionais às actuais práticas, e introduz regras muito mais rígidas às empresas quando se trata de obter o consentimento para recolha e tratamento de dados pessoais. As organizações são, assim, obrigadas a considerar mecanismos alternativos, como sejam o contrato com o titular dos dados, o cumprimento de uma obrigação jurídica, a defesa de interesses vitais do titular dos dados, o exercício de

funções de interesse público ou os interesses legítimos do responsável pelo tratamento.

Concretamente, a utilização de caixas pré-marcadas, o silêncio, a inactividade, o consentimento genérico ou obtenção do consentimento através de termos e condições genéricas deixarão de ser permitidos, na medida em que qualquer dos referidos mecanismos deixará de configurar como um meio de demonstração do cumprimento dos requisitos de consentimento do regulamento. Caso, ainda assim, as organizações pretendam privilegiar o consentimento como fundamento para o tratamento de dados pessoais, as regras mudam e são mais exigentes: o consentimento deverá ser concedido de forma desagregada dos demais termos e condições; deverão ser utilizados mecanismos que indiquem práticas activas dos titulares dos dados; o consentimento deverá ser óbvio, granular e facilmente identificável; a linguagem adoptada, simples e concisa; o titular deverá estar identificado, bem como as organizações que terão acesso aos dados; o consentimento deverá estar documentado em permanência e ser, com a periodicidade possível, renovado; deverá ser concedido em situações de equilíbrio entre as partes; e, por fim, deverá ser facilmente revogável. (CMS Rui Pena & Arnaut)

6

As empresas vão ser obrigadas a mudar os seus sistemas e a fazer uma nova recolha de dados?

Do ponto de vista estritamente tecnológico e no que toca à componente da protecção de dados/en-

criptação dos dados pessoais em repositórios nas bases de dados, a solução Vormetric da Thales assegura que tal não será necessário, garantindo uma continuidade nos processos sem quaisquer impactos para as empresas. É um sistema não intrusivo, “agnóstico” e não degradante da performance das infra-estruturas existentes (desde que estas estejam a operar abaixo dos 80% da sua capacidade). Assim, o processo de migração de um ambiente não protegido para um ambiente encriptado e protegido processa-se de forma suave, não disruptiva e sem perda de quaisquer dados ou contexto. Acresce que não serão necessárias adaptações nas bases de dados existentes e a encriptação e supervisão dos acessos às bases de dados, assim como, a sua protecção e monitorização são efectuadas pela solução Vormetric da Thales independentemente dos modelos, versões e fabricantes das bases de dados. (Thales)

7

Como é que as PME podem adequar-se ao novo regulamento?

O maior desafio para a conformidade com o novo regulamento será o nível de organização, gestão, controlo e estruturação dos seus dados, onde as organizações, independentemente da sua dimensão, que tiverem menores níveis de maturidade sobre a governação dos seus dados (físicos ou digitais), terão um maior esforço para conseguir atingir este nível de controlo e monitorização dos riscos de privacidade, bem como na operacionalização dos imperativos do regulamento ao nível processual sobre os direitos dos cidadãos europeus.

A abordagem de estar em conformidade deverá ser a mesma seja qual for a dimensão da organização. Com algumas diferenças particulares em função da natureza do seu negócio (por exemplo, se necessita ou não de um DPO – Data Privacy Officer), o modelo funcional da organização, e o estado actual da gestão e controlo dos seus dados, que pode implicar técnicas distintas de inventariação e desenho dos fluxos de dados pessoais, bem como no desenho e implementação dos controlos de privacidade. (Axians) ■

Todas as empresas devem dar atenção ao tema, mesmo que as exigências sejam diferentes.