ESPECIAL

PROTEÇÃO DE DADOS

Como se prepara a revolução que traz o novo regulamento

Steve Marcus/Reuters

A implementação do novo Regulamento Geral sobre a Proteção de Dados (RGPD) em Portugal vai afetar a generalidade dos cidadãos e, especialmente, a generalidade das empresas, pela verdadeira revolução que traz ao nível dos direitos, dos deveres e do enquadramento em que vão ter de desenvolver a sua atividade. No entanto, podemos dizer que produzirá um maior impacto nos setores designados como "big handler data", isto é, naqueles que gerem e tramitam um maior volume de dados e informação. Este universo integra, principalmente, cinco setores: saúde, banca, educação, retalho e o setor público. "Considerando que os dados pessoais e a informação prosperam nestes setores, é evidente que o RGPD trará maiores desafios por virtude da complexidade dos seus sistemas e redes, volume de informação e dados pessoais, inúmeros subcontratados e cadeia de abastecimento e outras tantas complexidades", explica Andreia Teixeira, associate partner da AON Portugal, ao Jornal Económico.

Apesar de grande parte das organizações não ter uma política de proteção de dados e informação definida, evidencia-se um elevado nível de confiança por parte dos consumidores no que diz respeito à solidez da segurança informática do setor da banca e seguros. Enquanto a banca, por razões legais e regulatórias, sempre esteve sujeita a um escrutínio maior, os seguros, estão a atravessar a sua revolução tecnológica e têm de conciliar o impacto tecnológico com as exigências do RGPD.

Na análise que é feita neste Caderno Especial dedicado à protecção de dados, as consultoras contactadas pelo Jornal Económico consideram que já há caminho feito, mas que persistem desafios sérios a ser ultrapassados, a começar por uma alteração cultural. Aliás, Hugo Veríssimo Oliveira, advisory senior manager da PwC diz-nos que a transformação cultural poderá revelar-se, mesmo, como o principal obstáculo na adaptação e implementação do RGPD. E será um esforço generalizado a todas as organizações, a começar pela Comissão Nacional de Proteção de Dados, que será, no final, o regulador do mercado, mas que ainda carece do enquadramento necessário para operar na nova realidade e, também, dos recursos para ser eficaz e cumprir o papel que lhe está destinado.

Não se pense, porém que os desafios que se colocam em Portugal diferem, estruturalmente, do que se passa em outros dos Estados-membros. A adaptação envolve riscos e esforço em cada um dos países e, nos 28 da União Europeia, são reconhecidas outras tantas velocidades de adaptação, o que faz com que a importância da teia que tem de ser tecida em Portugal tenha a importância do todo europeu, porque se trata aqui, em última análisem, de criar um mercado único.

Como a informação é o novo ouro, como referem os especialistas da Universidade Católica que ouvimos, será preciso uma profissionalização consistente, com especialização de funções.

No Forum, ouvimos quase duas dezenas de protagonistas da mudança que está a ser operada. É avaliado o processo de implementação do RGPD e feito um ponto de situação sobre em que ponto os agentes se encontram no processo de adaptação à nova realidade.

PUB

ANÁLISE

Portugal está "a uma transformação cultural" de cumprir o RGPD

O Regulamento Geral sobre a Proteção de Dados permite o livre fluxo de dados em todo o Mercado Único Digital. A cada país cabe ultrapassar os seus entraves e chegar a 25 de maio a uma só voz europeia.

SÓNIA BEXIGA
sbexiga@jornaleconomico.pt

O Regulamento Geral sobre a Proteção de Dados (RGPD), com entrada em vigor agendada para 25 de maio deste ano, permite o livre fluxo de dados em todo o Mercado Único Digital.

Tendo como principal meta uma maior proteção da privacidade dos cidadãos europeus, pretende reforçar a confiança e a segurança dos consumidores, e abrir oportunidades para as empresas, sobretudo as de menor dimensão.

Este regulamento traduz-se num conjunto único de regras para todo o continente que garanta segurança jurídica às empresas e o mesmo nível de proteção dos dados dos cidadãos em toda a UE. Por outro lado, aplica as mesmas regras a todas as empresas que prestam serviços na UE, mesmo que tenham sede em países terceiros.

Para o consumidor, as grandes alterações passam pelo reforço do direito à informação, de acesso e "direito a ser esquecido". Também um novo direito à portabilidade permitirá transferir os seus dados de uma empresa para outra.

Contudo, proceder a todas alterações, a um só ritmo entre os 28 Estados-membros não foi possível. Já no início deste ano, a Comissão Europeia confirmou que os preparativos estão a avançar a ritmos diferentes e, nesta fase, apenas dois já adotaram legislação nacional relevante. Se por um lado a Comissão vem sublinhar que os Estados-membros devem acelerar a adoção de legislação nacional e garantir que as novas medidas estão em conformidade com o regulamento, por outro, reafirma que devem assegurar que as respetivas autoridades nacionais sejam dotadas dos recursos financeiros e humanos necessários para garantir a sua independência e eficiência.

Neste capítulo, a Comissão consagra 1,7 milhões de euros para financiar as autoridades de proteção de dados, mas também para garantir a formação de profissionais na área. Estão disponíveis 2 milhões de euros adicionais para apoiar as autoridades nacionais em campanhas de sensibilização junto das empresas, em especial das PME.

É agora ou... agora.
E há entraves por ultrapassar

Os desafios que se colocam a todos os Estados-membros podem agigantar-se em Portugal e para Carlos Basto, partner da EY, a principal explicação para esta situação prende-se com a maturidade do nosso tecido empresarial que "nunca se preparou verdadeiramente". Hoje, defende, "o nível de maturidade das nossas organizações seja extremamente baixo comparado com outros países da CE, tais como Alemanha ou Espanha, onde estes temas tiveram já a devida atenção". Em seu entender, este 'gap' faz com que o nível de transformação necessário para adequar as organizações ao RGPD implique "um forte investimento da organização", quer nos processos de negócio e nas tecnologias de informação, quer "no mais difícil, ou seja, a mudança de cultura que é preciso incutir nas pessoas relativamente à forma como tratam este tipo de informação", sublinha ainda Carlos Basto.

Outro dos fatores de peso nesta equação, é o preço. Ou seja, para o gestor, constitui igual entrave ter de decidir entre propostas díspares na abordagem de implementação e nos preços finais. Afirmando que, neste momento, "há de tudo na abordagem ao mercado", Vitória Pinhão, partner da Auren, explica que há

Fabrizio Bensch/Reuters

Regras severas e coimas dissuasoras: todas as autoridades de proteção de dados terão a possibilidade de aplicar multas até 20 milhões de euros ou, no caso de uma empresa, de 4 % do seu volume anual de negócios a nível mundial

empresas que oferecem apenas uma abordagem jurídica, outras, mais tecnológica, e ainda há empresas que se propõem a desenhar todos os procedimentos e processos ou só os relacionados com os clientes. "A Auren tem encontrado, até, empresas com um diferente entendimento do âmbito de aplicabilidade do RGPD. As diferentes abordagens refletidas na disparidade dos preços deixam quem decide pouco confortável para fazer uma escolha informada", reforça Vitória Pinhão. Em matéria de entraves, elege ainda a necessidade de envolver a recolha de informação de muitas áreas de operação, obrigando à constituição de grupos multidisciplinares (uma forma de organização, defende, ainda "pouco comum" nas PME portuguesas); bem como a ausência de metodologias de trabalho e de 'compliance'; incapacidade financeira para investir em tecnologia de segurança; e ainda, uma "insuficiente" sensibilização dos colaboradores para a relevância da proteção de dados.

Transformação cultural e RH também pesam

Às mudanças na arquitetura tecnológica e no 'modus operandi' dos sistemas de informação da organização, obrigando a um esforço financeiro e processual que poderá fazer estender o prazo de implementação, Hugo Veríssimo Oliveira, advisory senior manager da PwC, junta, e sublinha, a transformação cultural que poderá revelar-se como o principal obstáculo na adaptação e implementação do RGPD. Assim, a velocidade a que esta transformação ocorre é, em seu entender, "naturalmente mais lenta", dependendo do nível de resistência à mudança da organização. A este cenário acresce ainda o papel que o regulador irá desempenhar. Hugo Veríssimo Oliveira considera que ainda não foi definida a linha de atuação da CNPD, facto que entende poder vir a " limitar e/ou inibir a atuação das organizações no que diz respeito à conformidade".

Esta 'check list' não fica fechada sem referirmos a questão dos recursos humanos e das suas competências. Considerando que um dos principais desafios colocados pelo RGPD é o assegurar do nível de competência ideal e especialização, Paulo André, managing partner da Baker Tilly explica que 50% das empresas não reservaram orçamento para a formação dos seus recursos em RGPD, e 68% ainda não atualizou os seus processos. Por outro lado, apenas 40% das empresas nomearam um encarregado de proteção de dados para regular a conformidade com o RGPD e quase 50% dos encarregados ppor esta conformidade não têm uma qualificação formal ou relevante. Paulo André não deixa de salientar a questão do 'budget limitado' para este tema, sobretudo nas PME, mas nas quais os recursos são escassos e as limitações financeiras são os maiores problemas. Adiantando ainda quem, em média, o orçamento típico para a conformidade com o RPGD é inferior a 5800 euros.

Vencer barreiras? É por aqui

Para cumprir, e idealmente até 25 de maio próximo, a implementação do RGPD, cada empresa terá de encontrar a sua forma de ultrapassar os entraves. Para Carlos Basto, as empresas têm, desde já, iniciar um programa de sensibilização, comunicação e formação intenso, abrangente a toda a organização, que tenha como objetivo a transformação do modo como as pessoas agem perante este tema. Adicionalmente torna-se "imperioso" construir uma análise criteriosa de gestão de risco relativamente às áreas/ processos com maior impacto em dados privados sensíveis. Esta análise permitirá balancear o investimento nessas áreas, mostrará quais mais críticas e qual deverá ser o 'roadmap' de prioridades.

Vitória Pinhão, por seu turno, chama a atenção para a necessidade da oferta de serviços dever ser operacionalizada numa "lógica de customização", sendo obrigatório um diagnóstico multidisciplinar inicial da realidade da empresa, antes de apresentar quaisquer soluções. E, as soluções em si, devem ser construídas com metodologias de trabalho assentes em processos de gestão e 'compliance', que otimizem a empresa como um todo, e não sirvam, apenas, para cumprir o RGPD.

Para endereçar a já sublinhada "transformação cultural", Hugo Veríssimo Oliveira, afirma que é essencial a definição de um modelo de governação e relacionamento com níveis de participação, funções e responsabilidades "claramente atribuídos e que conjugue os princípios do RGPD, bem como a aderência à realidade da organização, resultando na produção de políticas sólidas para a gestão da proteção de dados". Este modelo deverá ser seguido da estruturação de um plano de comunicação, a difundir pela organização e que suporte a consciencialização do tema da privacidade e da gestão da mudança, assim como da definição de um plano de formação que garanta o envolvimento de todos os colaboradores.

Ainda em matéria de recursos humanos, Paulo André salienta a importância de o DPO ter de ser "um bom comunicador, diplomata e com muita independência", sendo que as empresas, por uma questão de eficiência interna, podem nomear pessoas existentes para ocupar o cargo. E apesar de os consultores externos serem a escolha da maioria das empresas, estas devem identificar um "embaixador" do RGPD dentro da organização (DPO ou não) que centralize o levamento dos dados e dos processos, sendo que as valências técnicas a exigir serão as de marketing, informática, segurança e jurídicas. ●

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

CNPD precisa de mais leis para se preparar

O regulador destaca que a Assembleia da República é que decidirá sobre os meios que vai disponibilizar para o seu funcionamento.

MARIANA BANDEIRA
mbandeira@jornaleconomico.pt

O novo petróleo são dados, e o regulamento europeu quer garantir que a matéria-prima não se torna um propulsor de guerras e fonte de rendimento de vários países, tal como o seu "antecessor". A Comissão Nacional de Protecção de Dados (CNPD), enquanto futuro regulador por excelência, já começou a discutir a sua adaptação interna ao documento, mas precisa de mais detalhes regulatórios.

"Não é possível concluir esse trabalho sem que o quadro legal esteja completo. Aguarda-se a legislação complementar que tem de ser feita para dar plena aplicação ao Regulamento, pelo que para já é prematuro falar sobre isso", disse fonte da CNPD ao Jornal Económico.

O legislador começou por renovar o mandato de cinco anos de Filipa Calvão enquanto presidente da CNPD no final de outubro de 2017, nos termos do artigo 166.º da Constituição, do 25º da Lei n.º 67/98,e do 3º da Lei n.º 43/2004. A publicação em Diário da República refere ainda que José Grazina Machado se mantém como vogal.

Atualmente composta por sete membros, a CNPD tem como principal função controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais. Terá recursos para as novas responsabilidades? O mesmo porta-voz frisou que será também a Assembleia da República a decidir que meios vai disponibilizar para o funcionamento da CNPD, "num cenário de obrigação do Estado-Membro em dotar a autoridade de proteção de dados dos recursos técnicos, humanos e financeiros necessários para cumprir as suas competências".

Enquanto autoridade nacional de controlo de dados pessoais, a entidade começou a alertar os portugueses desde cedo, dado que o RGPD se encontra em vigor desde abril de 2016. No início de janeiro, a CNPD publicou um conjunto de '10 medidas para preparar a aplicação do regulamento europeu da proteção de dados' e dedicou um "Espaço RGPD" a orientações específicas sobre o tema destinadas a todos.

"O RGPD aplica-se a todo o setor privado e setor público. Ninguém está excluído da sua aplicação, com exceção dos tribunais na sua função jurisdicional e das autoridades competentes para a prevenção e investigação criminal e repressão de infrações penais, as quais têm uma legislação própria de proteção de dados. Quem já tinha um bom nível de cumprimento da Lei de Proteção de Dados terá menos trabalho para fazer agora", explicou o regulador.

Sobre o todo-poderoso D*ata Protection Officer*, a profissão emergente da nova lei, a comissão refere que desempenhará "seguramente um papel muito importante dentro da organização, contribuindo para um alto nível de cumprimento das obrigações legais de proteção de dados". ●

"Não é possível concluir esse trabalho de adaptação interna sem que o quadro legal esteja completo", consideram os responsáveis pela CNPD

ESPECIAL PROTEÇÃO DE DADOS

ENTREVISTA JOÃO RIBEIRO DA COSTA E JORGE PEREIRA DA SILVA coordenadores do Programa RGPD da Universidade Católica

"Os dados pessoais são o novo ouro"

O valor da Privacidade tem que ser incutido na cultura da organização, defendem os docentes da Católica.

ALMERINDA ROMEIRA
aromeira@jornaleconomico.pt

Cristina Bernardo

João Ribeiro da Costa, Head of Digital Transformation Católica-Lisbon e Jorge Pereira da Silva, Dean Faculdade de Direito da Universidade Católica, coordenadores do Programa de Programa de Regulamentação Geral de Proteção de Dados (RGPD) da Católica, explicam ao Jornal Económico o que vai mudar com o novo Regulamento de Proteção de Dados, o que há que acautelar e as oportunidades que se prefiguram para cidadãos, empresas e administração pública.

O que significa o novo Regulamento da Proteção de Dados?
Acima de tudo o RGPD deve ser visto como uma oportunidade, uma enorme oportunidade! Como disse o *Economist* em Maio último, "The world's most valuable resource is no longer oil, but data", há um novo ativo que permitiu criar as maiores empresas globais da atualidade. A proliferação dos dados digitais mostrou a centralidade do valor dos dados pessoais e o valor da privacidade.
Esta consciência representa uma oportunidade para as organizações melhorarem o seu grau de conformidade com os princípios de tratamento de dados (a maioria dos quais hoje já constam da atual lei de proteção de dados). Uma oportunidade para questionar processos internos, categorias de dados tratados e formas de interagir com os titulares dos dados. Uma oportunidade para integrar a proteção de dados como parte dos valores da sua marca por forma a melhorar os seus resultados comerciais.

Quais são os principais desafios que as novas regras trazem aos empresários portugueses?
O primeiro desafio é a cultura da organização. O valor da Privacidade tem que ser incutido na cultura da organização, começando pela administração. O reconhecimento de que os dados pessoais são o "novo ouro" tem que ser estabelecido a partir da administração.
O segundo desafio tem a ver com a segurança da informação, a vasta maioria das organizações não tem estrutura (tecnologia, processos e competências) para assegurar os níveis de protecção da segurança necessários para cumprir com o Regulamento.
O terceiro desafio, que deriva dos dois anteriores, é a gestão da mudança, para que os novos processos sejam mais do que documentos escritos.

> A bem das relações económicas entre a Europa e os Estados Unidos, a existência de um mecanismo que facilite as transferências de dados entre empresas dos dois países é inevitável, diz Jorge Pereira da Silva

> Do lado dos cidadãos, o ponto fundamental é perceberem a 'pegada digital' que deixam no dia-a-dia, e perceberem os riscos que correm se as empresas e organizações que armazenam essa informação não forem confiáveis, diz João Ribeiro da Costa

Quais as principais questões que se colocam aos cidadãos?
Claramente que o RGPD vem reforçar os direitos dos titulares dos dados. As organizações irão passar a processar menos dados pessoais, os quais serão mantidos por menos tempo e com recurso a tecnologias mais seguras e com melhores controlos de acesso. Por outro lado, os direitos ARCO (Acesso, Retificação, Cancelamento e Oposição) do titular dos dados são significativamente reforçados. Por fim, a introdução do direito à portabilidade permitirá uma melhor escolha de mudança de operadores económicos.

Quais as implicações reais associadas ao quotidiano profissional?
Do lado dos cidadãos, o ponto fundamental é perceberem a "pegada digital" que deixam no dia-a-dia, e perceberem os riscos que correm se as empresas e organizações que armazenam essa informação não forem confiáveis. Se os meus posts de Facebook aparecerem em público isso preocupa-me? Se as fotografias e vídeos que guardei na Dropbox forem divulgados isso incomoda-me? Ou se a minha lista de compras dos últimos anos for revelada? Do lado dos profissionais das empresas o ponto crítico é perceber como lidar com o "novo ouro" no dia-a-dia.

Estamos a escassas semanas da entrada em vigor do Regulamento de Proteção de Dados. Qual é a vosso percepção relativamente à adaptabilidade das empresas portuguesas ao novo regime?
Trata-se de um caso de miopia. A dois anos da entrada em vigor do regulamento não conseguiram ver os respetivos impactos, agora quando finalmente o conseguem ver melhor, já o consideram difícil de executar em pouco tempo. O cumprimento do regulamento é uma jornada continua, por isso, nunca é tarde para começar pois qualquer passo dado nos coloca num nível de conformidade melhor que o anterior.

... e da administração pública?
Não difere muito da anterior.

A segurança da passagem de dados é muito provavelmente a questão mais sensível de todo o processo. Como avalia, por exemplo, a introdução do novo sistema de "escudo protetor"?
A bem das relações económicas entre a Europa e os Estados Unidos, a existência de um mecanismo que facilite as transferências de dados entre empresas dos dois países é inevitável, quer se chame *Privacy Shield* ou tenha outro nome qualquer. Obviamente que o grande problema está relacionado com o facto de as normas americanas estabelecerem obrigações de partilha de informação com os serviços de segurança (NSA, etc. e que foram reveladas ao publico por Edward Swoden), incluindo dos dados dos cidadãos europeus tratados por empresas nos Estados Unidos. Mas no final trata-se de uma questão cuja solução futura passará sempre pelas vias diplomáticas.

Além da criação da função especifica do *Data Protection Officer*, que oportunidades oferece o novo regime em termos de emprego?
Especialistas em *Privacy by Design*, especialistas na negociação de contractos com subcontratantes (outsourcing). ●

"Como abordar o RGPD a menos de quatro meses da data limite"

HUGO VERÍSSIMO OLIVEIRA
Advisory Senior Manager da PwC

Com o aproximar do dia 25 de maio, dia de entrada em vigor do Regulamento Geral sobre Proteção de Dados, as organizações que ainda não abordaram o tema da privacidade relativas à estratégia a adotar, devem optar por dar prioridade à transformação e capacitação em detrimento da avaliação e diagnóstico da maturidade relativamente à proteção de dados.

Algumas organizações começaram o processo com maior antecedência, permitindo-lhes maior flexibilidade na definição da estratégia a seguir para a conformidade com o Regulamento, realizando numa primeira fase a aferição do nível de maturidade da organização e partindo dessa base para o desenho de um Roadmap para a conformidade e consequente implementação e operacionalização do mesmo.

No entanto, considerando o tempo disponível até à entrada em vigor do regulamento, as estratégias atuais de implementação devem focar-se na operacionalização.

Nesse sentido, são essenciais três fases que permitam às organizações incorporar com brevidade os mecanismos necessários à mitigação do risco de não cumprimento do RGPD: Capacitação, Piloto e Plano de Rollout.

A fase de Capacitação (fase 1) consiste na definição do governo e modelo de operação da privacidade na organização, identificando e caraterizando os componentes chave. Nomeadamente, estrutura de governo para a privacidade, políticas, códigos de conduta, ativos tecnológicos, entre outros. De forma a garantir uma implementação efetiva e robusta do modelo e mitigação dos riscos de incumprimento, deverão ser igualmente definidos mecanismos e controlos que monitorizem a sua aplicação. O exercício de capacitação da organização constituirá, em si mesmo, uma aferição do nível de maturidade atual (identificando necessidades), bem como a definição da maturidade ambicionada à medida que são implementados novos processos.

Da capacitação avança-se para o Piloto (fase 2), que visa testar a aplicabilidade e eficácia do modelo, arquitetura, processos e procedimentos definidos na fase anterior.

Para tal, numa primeira fase, são identificados dentro da organização os departamentos/áreas com processos de tratamento de dados pessoais "chave" (mais críticos e/ou sensíveis) e onde as transformações tendam a ser a mais relevantes e profundas. Daqui parte-se para o Plano de Rollout (fase 3), isto é, alargar os processos Piloto aos restantes processos da organização. Para o efeito, devem ser priorizados os processos de acordo com a sua criticidade.

Certamente, existirão níveis de esforço muito distintos, dadas as maturidades em que cada organização se encontra. No entanto, a Estratégia de Implementação aqui delineada não deve ser vista como one fits all uma vez que garante flexibilidade suficiente e consideração pelas especificidades de cada organização.

Para garantir o sucesso de implementação desta Estratégia, é fulcral que as organizações despoletem desde já um processo de consciencialização para o tema da privacidade e proteção de dados, a difundir pela organização, que permita mitigar situações de resistência cultural que possam surgir e, ultimamente, garanta o entendimento da importância do cumprimento com o Regulamento Geral sobre Proteção de Dados.

pwc

LISBOA
Palácio Sottomayor
Rua Sousa Martins, 1 - 2º
1069-316 Lisboa, Portugal
Tel.: (+351) 213 599 000
Fax: (+351) 213 599 999

PORTO
o'Porto Bessa Leite Complex
Rua António Bessa Leite, 1430 - 5º
4150-074 Porto, Portugal
Tel.: (+351) 225 433 000
Fax. (+351) 225 433 499

CIDADE DA PRAIA
Edifício BAI Center, Piso 2 Direito
Avenida Cidade de Lisboa
C.P. 303 Cidade da Praia
República de Cabo Verde
Tel.: (+238) 261 5934
Fax: (+238) 261 6028

LUANDA
Edifício Presidente
Largo 17 de Setembro n.º 3
1º andar - Sala 137
Luanda - República de Angola
Tel.: (+244) 227 286 109
Fax: (+244) 222 311 213

Valeriano Di Domenico/WEF

ESTUDO

Maioria das empresas não sabe quanto vai gastar com novas regras de dados

Só 2,5% dos decisores acredita que a sua organização está preparada para o regulamento que entra em vigor já em maio.

MARIANA BANDEIRA
mbandeira@jornaleconomico.pt

Os investimentos e os custos que o Regulamento Geral da Proteção de Dados (RGPD) vai obrigar as empresas a fazer em 2018 ainda não são certos para 52% delas. O estudo "*Breaking GDPR: Become a Master*", desenvolvido pela consultora IDC para a Microsoft Portugal, conclui que, da minoria de empresas que tem consciência desses valores, 50% das 627 inquiridas refere que será superior a 50 mil euros.

Nas empresas com mais colaboradores, que representam 60% da amostra e as mais bem informadas, 25% admite que elaborar um programa para estar em conformidade com as novas regras poderá ascender os 300 mil euros. O facto de as empresas ainda terem fracas estimativas sobre o dinheiro que terão de gastar para responder às exigências estará relacionada com o facto de só 2,5% dos decisores acreditar que a sua organização está preparada para o regulamento que entra em vigor já em maio.

Se o orçamento é diferente consoante a dimensão da empresa, o mesmo não acontece em termos de preocupações. Mais de 300 decisores apontam como desafios do novo quadro legal "a definição de processos" e a "identificações, classificações e gestão dos dados" e como benefícios "a melhoria da segurança e privacidade da informação".

A CIP - Confederação Empresarial De Portugal revê-se nas posições da BusinessEurope, de que faz parte, sobre o novo regulamento de proteção de dados. A organização de Bruxelas, que representa a comunidade empresarial da União Europeia, considera que a indústria quer responder aos requisitos legais, mas o dinamismo do quadro regulatório torna a tarefa difícil.

Os patrões asseguram que "todos os setores de atividade estão preocupados com o facto de que a intenção original de estabelecer um único conjunto de regras de proteção de dados não será alcançada com o RGPD", uma vez que é notório que o diploma "deixa muita margem de manobra" aos Estados-Membros e suas autoridades de proteção de dados.

A CIP e a BusinessEurope apoiam a criação do elo de cooperação entre os reguladores, o chamado Gabinete Europeu de Proteção de Dados, desde que haja mais transparência sobre este órgão independente, nomeadamente detalhes de "alcance, orçamento e regulamentação".

Um dos aspetos que realçam no RGPD é a definição do conceito de processamento de alto risco. "É tão vaga que pode ser atribuída a qualquer tipo de processamento e impõe obrigações de notificação onerosas e incertezas que irão provocar atrasos na elaboração de relatórios consistentes sobre violações de dados", defendem.

As inseguranças financeiras sobre a lei e as suas reais implicações ainda assombram os negócios a nível mundial. Na 13ª edição do "*The Global Risks Report 2018*", o Fórum Económico Mundial destacou a fraude ou roubo de dados como um dos cinco principais riscos em termos de probabilidade. Entre 2008 e 2018, este risco só surgiu duas vezes na tabela do Top5: no ano passado e agora, na versão mais recente do estudo, tendo subido de 5ª posição nas preocupações para 4ª. "Por exemplo, em 2016, as empresas revelaram violações de mais de 4 mil milhões de registos de dados, mais do que o total combinado dos dois anos anteriores", justificou o grupo que se reúne em Davos.

OPINIÃO

RGPD: uma oportunidade cultural e processual

RUI RIBEIRO
Professor Universitário

A evolução do mercado digital nos últimos anos, em particular com a explosão de produção de dados, onde se destacam os oriundos de aplicações instaladas em dispositivos móveis, tem potenciado, cada vez mais, um conhecimento detalhado sobre o que são as pessoas, o que fazem, onde estão, as rotinas, os amigos, os inimigos, os humores, os tiques, as fobias, etc. Hoje, empresas como o Facebook ou a Google, provavelmente saberão mais de nós, do que nós mesmo. Foi neste âmbito, e depois de vários anos de discussão sobre até onde as empresas poderão usar a informação pessoal dos seus clientes, que a União Europeia (UE) em 2016, com um período de transição de 2 anos, adotou o Regulamento Geral de Proteção de Dados (RGPD), com vista a garantir o direito à privacidade dos dados pessoais, bem como definir as regras de circulação desses mesmos dados. Analisando o panorama de preparação em Portugal à temática, denota-se que a grande maioria do tecido empresarial português está ainda num estado de 'negação' por ter, durante estes dois anos, atuado como se fosse algo que os informáticos e os jurídicos resolveriam. E... chegamos a fevereiro de 2018, a 3 meses do fim da fase de transição do GDPR!E... depois do 'estado de choque' e do 'acordar', algumas das empresas já entenderam que estão perante um desafio organizacional envolvendo toda a empresa: marketing, RH, financeiro, vendas, operações. De forma resumida, há um projeto estrutural a realizar, capaz de garantir que os sistemas informáticos sofram uma reengenharia para facilmente identificar, detetar, registar e controlar quem, como e quando acedeu a informação com dados pessoais, tal como importa rever todos os processos de comunicação com os clientes, desde o simples formulário online até aos procedimentos de relação de informações nos atendimentos presenciais ou telefónicos. Mas há muito mais: preparar mecanismos de direito ao esquecimento e à portabilidade de dados, criar formas de provar quais são as fontes de informação de origem dos dados, reanálise e revisão contratual com prestadores de serviços, designar o Encarregado de Proteção de Dados, criar um plano de proteção de dados, etc.. São, de facto, muitas as tarefas cruciais para o cumprimento do RGPD, e o tempo urge. Há contudo uma que é fundamental não esquecer, pois é aquela que garantirá a continuidade constante do cumprimento do RGPD, que é: comunicar a toda a organização, a todos os colaboradores. E comunicar a mudança de hábitos que praticam e carecem de ser alterados. Os dados pessoais são cada vez mais sensíveis e críticos, não só para garantir a capacidade de tornar a empresa mais competitiva, mas também para se procurar não passar o limite do direito à privacidade. É um equilíbrio que será mais difícil de conseguir, mas que será essencial daqui para a frente.

Entre as muitas tarefas cruciais, uma se impõe: comunicar o RPGPD a toda a organização e a todos os colaboradores

Impactos e Oportunidades do novo Regulamento Europeu de Proteção de Dados

Dr.Fernando Antas da Cunha
Managing Partner Antas da Cunha Ecija & Associados

João Ferreira Pinto
jpinto@adcecija.pt

Advogado, Sócio responsável TMT/Privacy/Cibersegurança da Antas da Cunha Ecija & Associados; Mestre em Segurança da Informação e Direito do Ciberespaço (Instituto Superior Técnico – Univ. Lisboa)

Que alterações impõe o novo regulamento?
O novo Regulamento Geral (UE) sobre a Proteção de Dados (RGPD), impõe grandes alterações na forma como as empresas e a Administração Pública (Central, Local, etc.) têm de passar a tratar os dados pessoais dos seus clientes, trabalhadores, "administrados", etc. a partir de 25 de Maio de 2018.
Desde logo uma alteração "radical", na forma como têm de passar a registar e documentar todos os tratamentos dos dados pessoais e a manter "evidências" do cumprimento do RGPD. Segundo o novo Princípio da Responsabilidade Proactiva (Accountability), o responsável pelo tratamento deve cumprir e tem de poder comprovar (a todo o tempo) o cumprimento do Regulamento. O que significa manter um registo actualizado (incluindo em formato eletrónico) de todos os tratamentos de dados pessoais, bem como das medidas de segurança e das medidas técnicas e organizativas adequadas para cumprir o RGPD.
Outra alteração profunda, diz respeito ao reforço dos direitos dos titulares dos dados pessoais, quer através da ampliação dos atuais direitos ("ARCO") de Acesso, Retificação, Cancelamento e Oposição, quer através da criação de novos direitos de Portabilidade Digital ou do direito ao Apagamento/Esquecimento.
Outra novidade diz respeito à obrigatoriedade de realizar avaliações de impacto de risco no tratamento de dados pessoais, os PIA (Privacy Impact Asseeement), numa perspetiva de segurança da informação.
Uma outra alteração significativa diz respeito à obrigação de reportar determinados incidentes de segurança à autoridade de controlo e aos próprios titulares dos dados, nos casos de maior risco, o que deve suceder num prazo de 72 (setenta e duas) horas a contar do conhecimento da quebra de segurança.
Com uma forte preocupação de compliance, o RGPD introduz a obrigatoriedade de nomear um Encarregado de Proteção de Dados (um Data Protection Officer), em determinados casos, por ex. na Administração Pública, cuja função consiste em zelar pelo cumprimento das obrigações do RGPD, bem como servir de elo de comunicação junto da autoridade de controlo e dos próprios titulares dos dados.
Uma última alteração de vulto diz respeito às pesadas coimas até 20.000.000 Euros ou 4% do volume de negócios anual global (se for mais elevado) com que pode ser sancionado o incumprimento do RGPD.

As empresas e os cidadãos estão preparados para enfrentar as alterações?
Na sua larga maioria as empresas e o Estado ainda não estão bem conscientes dos profundos impactos das novas obrigações do RGPD, apesar do largo período de 2 anos que está a decorrer para proceder à adaptação, desde que foi publicado em 2016.
Por outro lado, os próprios cidadãos não estão ainda suficientemente informados de todos os seus direitos enquanto titulares dos dados, nem têm consciência ("awareness") do imenso poder que passam a deter sobre as empresas e o Estado enquanto responsáveis pelo tratamento de dados pessoais. Até 25 de Maio de 2018 data da aplicabilidade do RGPD muito ainda há por informar, formar e "evangelizar". Aqui o Estado tem um papel e uma responsabilidade principal de alerta dos cidadãos para os seus direitos.

Quais são os principais problemas?
Os problemas principais são a falta de conhecimento dos gestores de topo destas novas obrigações do RGPD (incluindo a sua própria responsabilização pelo incumprimento do RGPD), bem como a falta de formação dos Recursos Humanos que nas empresas e no Estado vão tratar dados pessoais sem terem a noção das novas obrigações e alterações do RGPD a partir de 25 de Maio de 2018.

O que é necessário para resolver os problemas?
É essencial uma forte campanha de informação e formação. As empresas que perceberam em 2016 que se tratava de uma "oportunidade" para se melhorarem e tornarem mais competitivas ao cumprir o RGPD, estão hoje na "linha da frente" da sua concorrência.

UNIÃO EUROPEIA

Direitos, deveres e multas. Uma só regra para os 28

Os principais benefícios do novo Regulamento Geral sobre a Proteção de Dados recaem sobre as pessoas, organizações e empresas, sendo que as PME foram contempladas com vanstagens específicas.

SÓNIA BEXIGA
sbexiga@jornaleconomico.pt

QUAIS SÃO OS BENEFÍCIOS PARA OS CIDADÃOS?

Com as novas regras, os cidadãos passam a ter o "direito a ser esquecido"; um acesso mais fácil aos seus dados com informações mais detalhadas obre como são processados (essa informação deve estar disponível de forma clara e compreensível). O direito à portabilidade de dados tornará mais fácil para transmitir dados pessoais entre fornecedores de serviços; o direito de saber quando os dados foram alvo dos hackers: as empresas e as organizações devem notificar a autoridade nacional de supervisão da proteção de dados e comunicar ao visado, o mais rapidamente possível, para que este possa tomar as medidas adequadas.

O QUE É O "DIREITO A SER ESQUECIDO"?

A diretiva atual já dá aos indivíduos a possibilidade de pedir para apagar os seus dados, particularmente quando se entende que já não são necessários para o fim para o qual foram solicitados. Por exemplo, se um cidadão tiver dado o seu consentimento ao processamento para um propósito específico (como exibir numa das redes sociais) e deixa de querer este serviço, não há motivo para manter os dados no sistema. Particularmente nas situações em que envolve crianças que tornaram os seus dados acessíveis, muitas vezes sem entender completamente as consequências, não devem ficar presas a esta situação para o resto de suas vidas. Isto não significa que, a cada pedido apresentando, todos os seus dados pessoais devam ser apagados para sempre. Se, por exemplo, a retenção dos dados for necessária para a execução de um contrato, ou para o cumprimento de uma obrigação legal, os dados podem ser mantidos o tempo que for necessário para esse fim. As disposições propostas sobre o "direito a ser esquecido" são muito claras: a liberdade de expressão, bem como a pesquisa histórica e científica são salvaguardadas. Por exemplo, nenhum político poderá ter declarações anteriores apagadas da internet. Isso permitirá, por exemplo, que os sites noticiosos continuem a operar com base nos mesmos princípios.

QUAIS SÃO OS BENEFÍCIOS PARA AS EMPRESAS?

O RGPD proporciona clareza e consistência das regras a aplicar e restaura a confiança do consumidor, permitindo assim que as empresas aproveitem em pleno as oportunidades no mercado único digital. As empresas só terão que lidar com uma única autoridade de supervisão, e não 28, tornando mais simples e mais barato para as empresas fazer negócios na UE. As mesmas regras para todas as empresas, independentemente de onde estão estabelecidas, sendo que também para s que têm sede fora da Europa passa a ser obrigatório aplicar estas mesmas regras quando oferecerem bens ou serviços no mercado da UE.

HÁ VANTAGENS ESPECÍFICAS PARA AS PME?

O RGPD destina-se a estimular o crescimento económico, reduzindo os custos e a burocracia para as empresas europeias, entre as quais constam as pequenas e médias empresas (PME). A partir do momento em que passa a existir uma só regra, e não 28, a reforma ajudará as PME a entrar em novos mercados. Na nova realidade, as PME não precisam de nomear um encarregado (responsável) de proteção de dados, a menos que a atividade principal exija a monitorização regular e sistemática de pessoas em grande escala ou se forem processadas categorias especiais de dados pessoais, nomeadamente raciais ou étnicas reveladoras ou crenças religiosas. Ainda assim, não precisarão de ter um colaborador a tempo inteiro, podendo recorrer a um consultor pontualmente. As PME não precisam de manter registos de atividades de processamento, a menos que este não seja ocasional ou suscetível de resultar em risco para os direitos e liberdades da pessoa em causa. As PME não terão a obrigação de denunciar todas as violações de dados, a menos que as violações representem um alto risco para os direitos e liberdades dos cidadãos envolvidos.

EMPRESAS EM FALTA PODEM SER MULTADAS?

O RGPD estabelece uma variedade de ferramentas para fazer cumprir as novas regras, incluindo penalidades e multas. Quando se trata de decidir uma multa adequada, cada caso será cuidadosamente avaliado e há uma série de fatores que serão tidos em consideração: gravidade/duração da violação; número de pessoas envolvidas e nível de danos sofridos; caráter intencional da infração; quaisquer ações tomadas para mitigar o dano; grau de cooperação com a autoridade de supervisão. O regulamento estabelece ainda dois limites máximos para as multas se as regras não forem respeitadas: o primeiro teto fixa multas até um máximo de 10 milhões de euros ou, no caso de uma empresa, até 2% do volume de negócios total anual. O teto mais alto tem como limite máximo 20 milhões de euros ou 4% do volume de negócios anual mundial. As multas serão sempre ajustadas às circunstâncias de cada caso. ●

Foto cedida

ENTREVISTA ALEXANDRE NILO DA FONSECA ACEPI

"O grande desafio está nas empresas mais pequenas"

Com as micro e PME em maioria em Portugal, apenas as grandes empresas estarão já prontas para cumprir o RGPD.

A nova esta legislação, para o presidente da direção da ACEPI – Associação da Economia Digital, assenta "claramente, num espírito de proteção do consumidor".

Que impacto terá o RGPD nas empresas portuguesas e particularmente no comércio eletrónico?

Julgo que este é um tema que, apesar de ser um desafio grande pela complexidade e pela mudança a que obriga, a grande parte das empresas teve oportunidade de acompanhar porque não é um tema que tenha surgido de um dia para o outro. Obviamente que é sempre um tempo curto seja para o que for que implique grandes mudanças, há desafios aqui que podem vir a ser complicados de implementar, ainda que as empresas portuguesas tenham sempre a capacidade de se reinventar. Mas acima de tudo, e para uma associação como a ACEPI, a preocupação deve ser o cumprimento pelas melhores práticas, a defesa, por um lado, de um comércio eletrónico que seja justo e equilibrado entre as empresas, mas também que os consumidores estejam defendidos nos seus interesses. É por isto que nos pautamos e a nossa preocupação é garantir sempre que as empresas estão em linha com a legislação e com as boas práticas. As empresas têm vindo a preparar-se e a fazer os seus melhores esforços neste sentido ao longo dos últimos meses, estamos obviamente expectantes em relação ao que vai acontecer no dia zero desta implementação e ver quantas empresas estão realmente preparadas e quantas não estão. E ver também se o próprio Estado, enquanto legislador mas também enquanto fiscalizador estará ele próprio preparado para esta mudança. Apesar do tempo parecer curto, porque é já em maio, penso que as grandes empresas ter-se-ão preparado e, como em tudo na vida, as mais pequenas têm mais dificuldade. Este não é um processo fácil para uma pequena empresa e o tecido empresarial português é constituído essencialmente por micro e pequenas empresas, e portanto, o principal desafio está precisamente nas pequenas, para as quais o processo é mais complexo.

E quais são esses problemas que o RGPD levanta às empresas portuguesas?

A implementação deste processo obriga a uma mudança substancial da forma como se procede e a implementação d determinado tipo de processos numa pequena empresa portuguesa em que muitas vezes a equipa não chega a ter cinco colaboradores, ainda que tenham muitos fornecedores e clientes, poderá não ser fácil, por exemplo no caso dos pequenos comerciantes, garantir o cumprimento da legislação num curto espaço de tempo contando para tal com estes recursos para preparar essa mudança e para operar no dia-a-dia. Não se discute aqui a bondade e mérito da legislação mas sim o facto de uma grande empresa ter meios para fazer estes processos de transformação, e estou certo de que as grandes estarão neste caminho, mas as restantes, tendo até em conta algum desconhecimento dos gestores nestas áreas, acho difícil que consigam investir tempo do seu dia-a-dia neste tipo de matérias. ● *SB*

Novo Regulamento Geral de Proteção de Dados: Uma oportunidade de acrescentar valor às organizações

O cumprimento do RGPD (Novo Regulamento Geral da Proteção de Dados), passa, fundamentalmente, pelas empresas implementarem um sistema de gestão de tratamento e protecção de dados pessoais numa perspetiva de autorregulação e melhoria contínua com pensamento baseado no risco.
O nível de complexidade e o impacto que a implementação terá no dia-a-dia das organizações, estarão, obviamente, relacionados com a natureza das empresas, a área de atividade, a dimensão e o tipo de tratamento de dados pessoais que realizem.
Mas, independentemente do seu tamanho ou setor de atividade, esta será uma oportunidade de otimizar os processos de gestão da empresa, aumentando a confiança no relacionamento com os diversos stakeholders (clientes, fornecedores, parceiros de negócio) e potenciando a fidelidade dos clientes. Na economia do conhecimento e da referenciação digital, esta melhoria da reputação da empresa, irá, com certeza, ter uma repercussão positiva no potencial de aumento das vendas no médio prazo.
Com o cumprimento do novo RGPD (Novo Regulamento Geral da Proteção de Dados) as empresas estarão ainda mais protegidas contra ataques cibernéticos que possam violar a privacidade dos dados pessoais e, consequentemente, pôr em causa a continuidade do negócio. O risco das ameaças cibernéticas emergentes tendo como alvo preferencial os dados pessoais aumentará uma vez que as empresas "deverão denunciar violações de dados aos reguladores dentro de 72 horas" enfrentando multas avultadas (até quatro por cento do volume de negócios anual) caso não cumpram; tendo também que notificar os titulares dos dados. Esta obrigatoriedade torna-se apetecível para pedido de resgates.
Este risco deve, por isso, ser seriamente tido em conta e a sua mitigação é outra boa oportunidade que o RGPD aporta às PME´s.
Paralelamente, se a empresa efetuar a correta implementação do Regulamento, estará, também, a garantir a ausência de multas.

25 de maio de 2018: O prazo aproxima-se

O Novo Regulamento Geral de Proteção dos Dados Pessoais foi publicado pela União Europeia em 4 de Maio de 2016 e tem que estar implementado já em 25 de Maio de 2018.
Com a aproximação da data limite para a implementação, a maioria das PME´s, apesar de conscientes da responsabilidade que têm, ainda não iniciou o processo, um atraso que tem que ser recuperado nestes quatro meses que faltam. O facto deve-se, em alguns casos, a uma perceção de que são necessários apenas pequenos ajustes, havendo ainda tempo suficiente. Noutros casos, em que há necessidade de apoio externo à implementação, o atraso deve-se à enorme "variedade" de propostas muito díspares entre si (quer ao nível da abordagem de implementação do regulamento, quer ao nível do preço do serviço), que deixam confuso quem decide sobre quem e, em que moldes deve adjudicar os serviços de apoio, adiando a decisão.
No entanto, as medidas práticas e organizativas a implementar no âmbito do RGPD, porque carecem duma abordagem pluridisciplinar entre as áreas de Gestão de Processos e Procedimentos, "Legal" e Tecnologias da Informação; e do envolvimento de todos os departamentos que manipulem dados pessoais, revestem o projeto de implementação de alguma complexidade e morosidade, impondo a necessidade de iniciar o diagnóstico com a maior brevidade possível.

VITÓRIA PINHÃO, ENGª
Responsável pelo Departamento de Consultoria da Auren Portugal
vitoria.pinhao@auren.pt

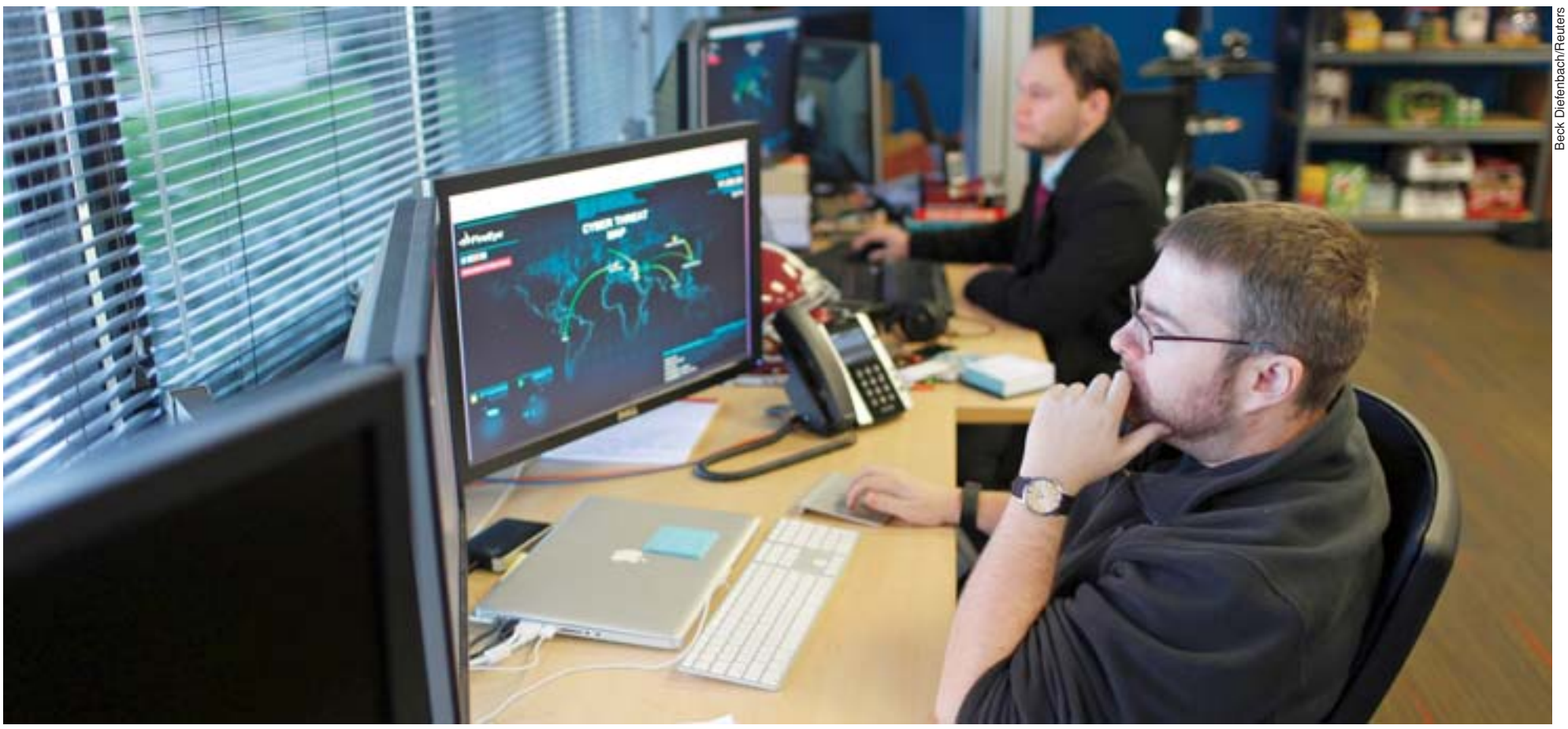
ABORDAGEM AUREN: DIAGNÓSTICO INICIAL E SOLUÇÕES MULTIDISCIPLINARES

"Quando a Auren começou a abordar o mercado, encontrou várias dúvidas sobre a aplicabilidade do Regulamento e visões ou demasiado complexas, ou demasiado simplistas da implementação. Após as nossas equipas realizarem o diagnóstico inicial e as primeiras sessões de esclarecimento, as dúvidas dissiparam-se e os nossos clientes passaram a olhar para o processo (de implementação do RGPD) como uma oportunidade de melhoria."
A Auren disponibiliza consultoria para a implementação deste regulamento numa abordagem pluridisciplinar e à medida de cada organização. A nossa abordagem inicia-se com um diagnóstico transversal às políticas, processos de gestão e sistemas informáticos em vigor na empresa; sendo a solução de implementação proposta em função dos recursos financeiros e dos recursos humanos de cada organização.

BOAS PRÁTICAS PARA A IMPLEMENTAÇÃO DO RGPD

- ✔ Adotar uma boa estratégia de privacidade e comunicá-la de forma eficaz, para potenciar vendas;
- ✔ Nomear um responsável pelo sistema de tratamento e protecção de dados pessoais;
- ✔ Diagnosticar procedimentos e implementar medidas de rastreabilidade;
- ✔ Fazer uma avaliação de riscos;
- ✔ Dar formação a colaboradores e aculturar a organização para um pensamento baseado no risco, fortemente vocacionada para o compliance;
- ✔ Rever as políticas de privacidade, bem como os contratos nas organizações com impacto crítico no tratamento e protecção dos dados pessoais;
- ✔ Preparar resposta rápida e adequada em caso de violação de dados pessoais incluindo a notificação de todas as partes interessadas;
- ✔ Preparar procedimentos que demonstrem que o regulamento está a ser cumprido;
- ✔ Elaborar registos das atividades;
- ✔ Verificar o estado/nível de segurança dos dados pessoais e da informação oferecido pelas tecnologias e outros;
- ✔ Reforçar mecanismos de segurança e protecção dos dados;
- ✔ Clarificar a informação prestada aos titulares dos dados sobre o tratamento dos seus dados e os seus direitos.

ESPECIAL PROTEÇÃO DE DADOS



Beck Diefenbach/Reuters

PROFISSÃO

DPO. Quem é o responsável pela proteção de dados?

O Encarregado de Proteção de Dados (DPO) vai integrar o 'job description' de muitas empresas e de muitas organizações.

ANTÓNIO SARMENTO
asarmento@jornaleconomico.pt

A partir de Maio, as empresas têm de nomear um responsável pela protecção de dados, criado pelo novo regulamento europeu, estimando-se que serão necessários 75 mil profissionais. "O cargo do Responsável da Proteção de Dados é particularmente exigente, constitui o ponto de contacto para a autoridade de controlo, tendo que ter conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como a capacidade para desempenhar as funções de informar e aconselhar, controlar a conformidade, sensibilizar e formar, auditar e cooperar com a autoridade de controlo, entre outras", resumem os organizadoras na página de Internet criada para a formação destes profissionais (as formações estão a cargo da Associação Empresarial de Portugal, em Leça da Palmeira, e decorrem entre fevereiro e março).

Só pelo facto de não designarem este encarregado de protecção de dados, que irá monitorizar o cumprimento do regulamento e ser o ponto de contacto com o regulador (a Comissão Nacional de Protecção de Dados), as empresas arriscam pagar uma multa. "O quadro sancionatório do regulamento. Ou seja, aquilo que hoje devia ser já uma preocupação generalizada das organizações, passou a sê-lo com a aplicação de coimas até 10 milhões ou 20 milhões de euros, consoante a gravidade da infração, ou 2% ou 4% do volume de faturação", explicou João Costa Quinta, sócio da DLA Piper numa entrevista ao Jornal Económico.

Criada no âmbito do novo Regulamento Geral de Proteção de Dados (RGPD), que vem revolucionar o enquadramento jurídico da proteção de dados pessoais, o DPO é uma das novidades deste novo quadro legal, que, por exemplo, impõe um prazo de 72 horas para comunicar incidentes com dados e limita a capacidade das empresas pedirem e usarem dados pessoais ao fim para que realmente se destinam e com uma janela temporal definida.

O DPO será o garante do cumprimento do RGPD na empresa e o interlocutor entre os vários stakeholders

"O DPO personifica a autorregulação dos dados pessoais nas organizações. Parte das funções que eram da Comissão Nacional de Proteção de Dados (CNPD) passam para a responsabilidade das organizações que devem designar um DPO sempre que estejam perante as situações previstas no RGPD", explicou ao Jornal Económico, Andreia Teixeira, Senior partner da AON.

Esta responsável acrescenta que as situações previstas no RGPD parecem incluir um vasto leque de organizações e empresas vinculadas a designar um DPO, pois são utilizados conceitos indeterminados e deixa-se também alguma margem para a lei nacional definir o que se enquadra no conceito de "autoridades ou organismo público".

Uma vez que o RGPD pretende salvaguardar a independência do DPO, este só responderá perante a administração/gerência e não deverá receber instruções sobre o exercício das suas funções, não podendo ser destituído por tal, esclarece a especialista.

"Na hora de nomear um DPO são vários os aspetos a ter em consideração, nomeadamente, verificar se não existe um eventual conflito de interesses com a função que o DPO já desempenhava previamente e continuará a desempenhar cumulativamente (ex.º: diretor de IT ou de recursos humanos)", acrescenta Andreia Teixeira.

A sua relação com as outras áreas da empresa deverá ser potenciada com vista a promover a conformidade com o RGPD. O recomendável é que o DPO seja coadjuvado por uma equipa multidisciplinar que o apoie e contribua para o cabal cumprimento das obrigações impostas pelo RGPD.

"Em suma, o DPO será o garante do cumprimento do RGPD na empresa e o interlocutor entre os vários stakeholders (titulares dos dados, autoridade de controlo, entre outros)", conclui a responsável. ●

Encarregado de Protecção de Dados – ter ou não ter?

JOANA ANDRADE CORREIA
Advogada
Raposo Bernardo & Associados - Sociedade de Advogados

O Encarregado de Protecção de Dados (EPD) será uma figura central em todo o processo de implementação e cumprimento das regras do Regulamento Geral sobre a Protecção de Dados (RGPD), cuja entrada em vigor está prevista para 25 de Maio de 2018.

A sua importância é inegável, o que facilmente se entente se atentarmos em algumas das suas principais funções, como o controlo da conformidade com as normas aplicáveis, a avaliação do impacto sobre a protecção de dados, a cooperação com a autoridade de controlo, desempenhando ainda um interessante papel de ponto de contacto com aquela, bem como com os titulares dos dados que abordem a empresa. A sua intervenção basear-se-á na avaliação do risco para as empresas, para além de as aconselhar sobre metodologias a seguir na recolha e tratamento de dados, definir que domínios devem ser objecto de auditoria, bem como zelar pela conservação do registo das actividades de tratamento.

E tem sido precisamente a propósito do EPD que têm surgido algumas das mais relevantes dúvidas, desde logo saber-se com clareza que empresas e entidades estão obrigadas a designar este responsável.

Se tivermos em conta o que resulta do Regulamento deve entender-se que a designação de um EPD é obrigatória quando se verifiquem as seguintes situações:

i. Se o tratamento de dados for efetuado por autoridade ou organismo público (independentemente dos dados objeto de tratamento);

ii. Se as atividades principais do responsável pelo tratamento de dados ou do subcontratante consistirem em operações de tratamento que exijam um controlo regular e sistemático dos titulares dos dados em grande escala;

iii. Se as atividades principais do responsável pelo tratamento de dados ou do subcontratante consistirem em operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações.

Por categorias especiais de dados devemos considerar os que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

Sem prejuízo de se verificar alguma destas situações, mesmo quando não é obrigatório designar um EPD, as empresas e demais organizações são inteiramente livres de designá-lo, a título voluntário, o que será sempre bem acolhido pelas entidades responsáveis pela fiscalização do cumprimento do RGPD.

Algumas empresas que já iniciaram o processo de adaptação ao regulamento dentro das suas estruturas, têm manifestado dificuldades na interpretação das situações em que é obrigatório designar um EPD, uma vez que o RGPD estabelece enquadramentos muito genéricos.

É disso exemplo, desde logo, o que entender como «atividades principais» no contexto de certa empresa. Naturalmente, pode entender-se como se tratando dos actos essenciais para a actividade da empresa, que não têm mero carácter acessório, e sem os quais os seus objectivos não podem ser concretizados, os quais incluem também todas as atividades em que o tratamento de dados constitui parte indissociável das atividades do responsável pelo tratamento ou do subcontratante.

Na verdade, a generalidade das organizações exerce determinadas atividades de suporte à gestão, como serão os casos do processamento de remunerações dos seus colaboradores ou atividades comuns de apoio informático à empresa. Trata-se de exemplos de funções de apoio necessárias para a atividade principal ou para a área de negócio central da organização. E embora sejam necessárias e importantes, por norma estas atividades são consideradas funções acessórias e não a atividade principal.

Do mesmo modo, o conceito de «grande escala» também inspira algumas dúvidas. Recomenda-se assim que sejam tomados em consideração os seguintes critérios para determinar se o tratamento é efectuado em grande escala:

i. O número de titulares de dados afetados – como número concreto ou em percentagem da população em causa;

ii. O volume de dados e/ou o alcance dos diferentes elementos de dados objeto de tratamento;

iii. A duração, ou permanência, da atividade de tratamento de dados;

iv. O âmbito geográfico da atividade de tratamento.

Ainda nesta sequência, para efeito de definição dos casos em que o EPD é obrigatório, o regulamento determina que tal também deverá acontecer quando as actividades principais consistam em operações de tratamento que exijam um controlo regular e sistemático dos titulares dos dados.

A noção de controlo regular e sistemático dos titulares dos dados não está, de igual modo, definida no RGPD, mas inclui claramente, entre outras, todas as formas de definição de perfis de pessoas, por exemplo para fins de promoções comerciais baseadas em dados, publicidade comportamental, programas de fidelização, controlo de dados respeitantes ao bem-estar, à condição física ou à saúde. Por «regular» devemos considerar que é contínuo ou que ocorre a intervalos específicos num determinado período, que é recorrente ou repetido em horários estipulados, bem como constante ou periódico. E finalmente, será «sistemático» quando ocorre de acordo com um sistema predefinido, organizado ou metódico, realizado no âmbito de um plano geral de recolha de dados ou efetuado no âmbito de uma determinada estratégia.

O EPD pode ser interno ou externo à empresa e, no caso de grupos empresariais, estes podem designar um único EPD, desde que esteja «facilmente acessível a partir de cada estabelecimento», dado ser o ponto de contacto em relação aos titulares dos dados, à autoridade de controlo e também, internamente, no seio da organização. Deve possuir conhecimentos especializados no domínio das normas e práticas de proteção de dados, de tecnologias da informação, segurança de dados, bem como capacidade para promover uma cultura de proteção de dados no seio da organização.

É importante que lhe sejam disponibilizados meios e recursos para o exercício das funções de EPD, tal como um importante grau de autonomia no seio da empresa, o que significa que não deve receber instruções quanto à forma de tratar uma questão, à forma de investigar uma queixa ou à necessidade de consultar a CNPD, como autoridade de fiscalização. No entanto, esta autonomia não implica que lhe sejam conferidos poderes decisórios que extravasem as suas funções. Até porque o responsável pelo tratamento ou subcontratante permanecem responsáveis pelo cumprimento das normas de protecção de dados. Será também importante, caso se trate de um EPD interno, precaver situações de conflitos de interesses, constituindo boa prática a aprovação interna de códigos de conduta ou regulamentos com vista a precaver estes conflitos e a resolver os que eventualmente surjam.

Com o apoio de Raposo Bernardo & Associados.

RAPOSO BERNARDO

ESPECIAL PROTEÇÃO DE DADOS

FORUM OS DESAFIOS DO NOVO

O Regulamento Geral de Proteção de Dados vai obrigar todas as organizações a encontarem a melhor maneira de adptarem a sua estrutura - humana e tecnológica - às novas necessidades, mas também a perceber como as novas regras vão impactar a forma como têm feito negócio até aqui e o que terá de ser alterado. Estes exercícios são para já, porque o novo mundo tem data marcada - 25 de maio - e obrigama uma resposta aos desafios. Foi isso que fomos perguntar a 15 protagonistas.

QUAIS SÃO OS PRINCIPAIS DESAFIOS QUE SE COLOCAM COM O NOVO REGULAMENTO?

DANIEL REIS
PLMJ Advogados
Sócio

SISTEMA DE *COMPLIANCE*

O sistema de autorregulação criado pelo Regulamento vai forçar as organizações que tratam dados pessoais (empresas e entidades do setor público) a fazer algum que nunca fizeram: analisar o impacto que a sua atividade tem para a privacidade das pessoais e decidir quais as medidas de segurança – técnicas e organizativas – a aplicar em função do impacto registado.
Além disso, o princípio da responsabilidade determina que, além de cumprir a lei, as organizações terão de ter a capacidade de demonstrar que cumprem a lei. Ora, esta demonstração do cumprimento só é possível através da criação e implementação de um sistema de *compliance*. Neste sentido, os principais desafios são:
• Como garantir que a organização consegue, de forma consistente e continuada, analisar todos os tratamentos de dados pessoais.
• Como assegurar que existe uma visão transversal dentro da organização dedicada ao tema dos dados pessoais.
• Como conjugar as diferentes valências necessárias: a função jurídica, a função tecnológica e a função operacional.
• Sobretudo para as PME, como suportar os custos relacionados com projetos de diagnóstico e implementação, contratação de novos trabalhadores e de consultores externos.

LEONOR CHASTRE
Cuatrecasas, Gonçalves Pereira
Sócia

"MOST WANTED: DPO"

O maior desafio com que deparam as entidades públicas e privadas e que decorre do Regulamento geral de proteção de dados é a designação pelos Responsáveis pelo tratamento e subcontratantes, nos casos expressamente previstos, de um Encarregado de Protecção de dados.
As regras do RGPD relativas ao DPO aplicam-se igualmente no caso de designação voluntária. Assim, e quando a organização não esteja obrigada em nomear um DPO e ainda assim opte por nomear ou disponha de uma pessoa responsável pelo cumprimento das regras e princípios aplicáveis em matéria de protecção de dados, deve ter cuidado para garantir que essa pessoa não seja considerada um DPO, uma vez que trará e implicará obrigações adicionais em conformidade com o RGPD.
Dentro da estrutura organizativa o DPO reportará ao nível de gestão mais alto da organização - ou seja, ao nível da Administração. O WP 29 refere, por motivos de transparência e clareza jurídica, que o contrato de prestação de serviços preveja uma clara repartição das tarefas no seio da equipa do DPO externo e a designação de uma única pessoa como contacto principal e pessoa «responsável» do cliente.
Levanta-se ainda a questão de quem será, de que departamento/área escolher o DPO, nomeadamente no caso em que a organização opta por recorrer a um trabalhador da sua organização, em vez de proceder a uma contratação externa. A resposta a esta pergunta não é linear. No sentido de assegurar que o EPD esteja acessível, o GT 29 recomenda ainda que o DPO esteja localizado na União Europeia.

CARLOS PINTO CORREIA
Linklaters
Partner

MAIOR ALTERAÇÃO EM 20 ANOS

O Regulamento Geral de Proteção de Dados ("RGPD") representa a maior alteração verificada nos últimos 20 anos no regime europeu de proteção dados pessoais e privacidade. As mudanças necessárias para assegurar o cumprimento com o RGPD são muitas e exigem uma grande capacidade de adaptação por parte das entidades envolvidas na recolha e tratamento de dados pessoais. A necessidade de adaptação é o maior desafio que se coloca com RGPD, devido às novas regras e obrigações que brotam deste no regime.
É particularmente de destacar o facto de o RGPD introduzir regras mais exigentes para a obtenção do consentimento para a recolha de dados pessoais, regras essas que são aplicáveis aos dados já recolhidos antes da implementação do RGPD mas que deverão continuar a ser tratados após 25 de maio de 2018. Estas novas regras poderão apanhar alguns responsáveis pelo tratamento de dados desprevenidos, uma vez que será necessário verificar em que circunstâncias foi obtido o consentimento para o tratamento desses dados recolhidos antes da implementação do RGPD, sendo que, se as circunstâncias em que o consentimento foi obtido não respeitarem as novas regras, terá de ser obtido um novo consentimento, sob pena de o tratamento de dados se tornar ilícito.

LETÍCIA ANTUNES DUARTE
ABC Legal
Sócia

SENSAÇÃO DE DESCONFORTO

A data está fixada: 25 de maio de 2018 – 78 dias úteis para o início da aplicação do Regulamento Geral sobre Proteção de Dados (RGPD). O grande desafio que se coloca às organizações, seja como responsáveis de tratamento (RT), seja como subcontratados, é a consciencialização.
O RGPD reforça os direitos dos titulares dos dados (TD) e centra a responsabilidade e controlo a sua aplicação nos RT, que devem implementar medidas adequadas e eficazes para assegurar e comprovar a observância das normas e dos princípios da proteção dos dados pessoais.
Este novo quadro legislativo cria uma sensação de desconforto no seio das organizações, que se veem constrangidas a ter que introduzir alterações, por vezes profundas, na sua estrutura organizativa e de negócio, no relacionamento com os seus clientes e colaboradores.
No entanto, o RGDP deverá ser encarado numa perspectiva de otimização, como um investimento no desenvolvimento de negócios, potenciando um estreitamento nas relações de confiança entre os RT e os seus clientes e potenciais clientes, assim como com os seus colaboradores, tanto mais que devemos ter como assente que os TD estão cada vez mais cientes dos seus direitos e dos meios ao seu dispor para os exercer e procuram cada vez mais relacionar-se com organizações transparentes e que lhes oferecem garantias de qualidade e legalidade.

PUB

REGULAMENTO

LUÍS NETO GALVÃO
SRS Advogados
Sócio

PRIORIDADE IMEDIATA DA CNPD

Um dos principais desafios colocados pelo Regulamento Geral de Proteção de Dados (RGPD) há quase dois anos, aquando da sua aprovação, foi o de dar-se a conhecer às empresas e organismos públicos. Esse desafio parece ter sido ganho em Portugal, pelo menos, no que toca às empresas, para o que a imprensa teve um papel determinante. Agora resta o desafio maior da sua implementação em 25 de maio deste ano, num contexto de crescente transformação digital.
Estamos a liderar um número significativo de projetos de implementação do RGPD, com desafios sectoriais próprios. É notória, a este nível, a necessidade de um maior envolvimento das estruturas representativas empresariais, nomeadamente para favorecer o surgimento de Códigos de Conduta, aliás previstos no RGPD. Esperam-se novidades ao longo do corrente ano, já que a própria Comissão Nacional de Proteção de Dados (CNPD) elegeu o tema como uma das suas prioridades mais imediatas.
De resto, iremos ter um novo quadro legislativo de adaptação ao direito nacional do RGPD, bem com uma renovada lei orgânica da CNPD. Como o processo legislativo (mais visível) ainda está no seu inicio, o desafio a este nível será o de ter este quadro normativo atempadamente pronto e implementado pelos seus destinatários.

INÊS ANTAS DE BARROS
Vieira de Almeida
Advogada Associada

MUDANÇA DE PARADIGMA

O Regulamento Geral sobre a Proteção de Dados (“RGPD”), que se tornará aplicável a 25 de maio, traz, para as organizações, grandes desafios e oportunidades.
O novo cenário legal acarreta uma mudança de paradigma, assentando numa lógica de autorregulação, impondo às organizações a recolha e manutenção de evidências de cumprimento das novas obrigações legais. A implementação exige uma abordagem holística aos vários *streams* - legal, tecnológico e processual -, que poderá implicar uma alteração mais ou menos substancial, dependendo da estrutura e estratégias atualmente prosseguidas. O universo de alterações necessárias dependerá do grau de maturidade de cada organização, da respetiva organização e estrutura e da complexidade do tratamento de dados levado a cabo. As obrigações específicas de cada setor a nível de segurança da informação, obrigações perante os titulares dos dados e terceiros, deveres de reporte e prazos de conservação são aplicáveis e deverão ser tidas em conta aquando do desenho e implementação do RGPD.
Existem ainda algumas incertezas que poderão ter impacto na forma como as organizações devem implementar o RGPD, desde logo, as exigências do quadro legal nacional, a interação com as autoridades de controlo, a articulação com futura legislação comunitária e o processo de harmonização entre os vários Estados-Membros. É essencial que, nesta data, as organizações tenham já identificado os requisitos para assegurar a Compliance, assim como definido um plano de ação.

JOÃO FERREIRA PINTO
Antas da Cunha & Associados
Sócio

“AWARENESS”

Os principais desafios que se colocam com o novo Regulamento Europeu sobre a Proteção de Dados (RGPD) dizem respeito a uma mudança de cultura nas empresas e na Administração Pública (AP) no que diz respeito à privacidade e à proteção de dados pessoais.
Em especial este desafio coloca-se em três grandes áreas. Em primeiro lugar, nas pessoas, isto é, nos Recursos Humanos que efetivamente lidam e tratam dados pessoais no dia-a-dia, os quais têm de ser informados e formados para uma cultura de *“awareness”* sobre proteção de dados pessoais. Em segundo lugar, um desafio no que diz respeito à organização de processos e procedimentos relativos ao tratamento de dados pessoais. Por exemplo, redefinir a exposição e acesso de dados pessoais só a determinados perfis de trabalhadores dentro da empresa e da AP, designadamente só permitir acesso aos colaboradores que necessitam tratar os dados e não a todos e quaisquer colaboradores. Em terceiro lugar, os Sistemas de Informação, que têm de dar resposta às novas exigências de segurança e confidencialidade, mas também aos novos requisitos legais do RGPD. Por exemplo, a resposta perante um pedido de apagamento/esquecimento ou um pedido de portabilidade digital dos dados pessoais para um concorrente por parte de um cliente.

BAKER TILLY
Growth through collaboration
Audit | Tax | Advisory

Winner 2016
Baker Tilly International
Network of the Year
Accounting
Accountant
International Accounting Bulletin and The Accountant Awards 2016

INTERNATIONAL TAX REVIEW
World's Leading Tax Firm 2016 (Portugal)
World's Transfer Pricing Firm 2016 (Portugal)
Transfer Pricing Firm of the Year 2014 (Portugal)
Indirect Tax Leader 2016 (Tiago Almeida Veloso)

ESPECIAL PROTEÇÃO DE DADOS

INÊS HENRIQUES DE MATOS
Azeredo Perdigão & Associados
Advogada Associada

ACRÉSCIMO DE BUROCRACIA

Propomo-nos analisar, pela sua relevância, os desafios em matéria de tratamento de (i) dados pessoais de menores e (ii) dados pessoais relativos à saúde. No caso do tratamento de dados pessoais dos menores, assunto de actualidade inquestionável, sobretudo com a crescente utilização pelos mesmos de meios tecnológicos e acesso às redes de internet, tendo o menor idade inferior a 16 anos, o tratamento só é lícito se o consentimento for prestado pelos titulares das responsabilidades parentais da criança. Ora, a forma e os exactos contornos segundo os quais se irá processar a prestação de consentimento, considerando as exigências do NRPD e compatibilizando-as com necessidades tecnológicas actuais, serão um inequívoco quebra--cabeças para os Estados-Membros que, inclusive, têm liberdade para definir a idade mínima para utilização destes meios, nunca inferior a 13 anos. Paralelamente, o RNPD define consentimento como manifestação de vontade livre e explícita, que deve consistir numa acção positiva. Significa isto que o consentimento tácito é tido por inválido. Neste sentido, as unidades de saúde devem, para fazer face a esta exigência, obter declaração de consentimento escrita assinada pelos utentes, para tratamento dos seus dados de saúde, fazendo antever um desafiante acréscimo de burocracia e do acervo documental arquivado nestas unidades, com custos administrativos e meios humanos adicionais.

JOÃO LUÍS TRAÇA
Miranda & Associados
Sócio

SANÇÕES PESADAS

O maior desafio do RGPD está relacionado com o facto de o seu incumprimento fazer incorrer as organizações em sanções pesadas e de poder originar danos reputacionais, como a obrigatoriedade de em certos casos informar os titulares que ocorreu uma violação de dados (ex: hacking). Embora o RGPD introduza alterações e inovações relevantes, muitos dos princípios nele previstos não são novos e já constam da atual lei de proteção de dados, mas não são cumpridos pela vasta maioria das organizações em Portugal. Para estas organizações, do sector público à PME, o desafio do RGPD consiste em alterar a cultura e processos para converter a proteção de dados em parte dos valores que devem promover. Esta alteração passa por assumir o seguinte princípio, fácil de verbalizar e difícil de aceitar no contexto organizacional: os dados pessoais tratados pelas organizações pertencem apenas aos respetivos titulares! Tratar dados pessoais é antes de mais uma responsabilidade para com a pessoa individual a quem esses dados pertencem.
Por onde iniciar então o processo de conformidade? Nada chegará a bom porto se não se convencer a liderança para importância do RGPD. Apoio vindo do topo é o tiro de partida.

CARMINA CARDOSO
DLA Piper ABBC
Associada Sénior

CONSCIENCIALIZAÇÃO

O principal desafio é a mudança de paradigma e procedimentos. A consciencialização das entidades que o tratamento de dados não é uma questão marginal, mas uma preocupação central na sua atividade. Só estando cientes que tratam diariamente dados pessoais e que esse tratamento impõe o cumprimento rigoroso de um acervo de obrigações, sob pena de consequências gravíssimas, é promovida a alteração de procedimentos. Só quando interiorizarem que os dados não são bens próprios, mas que pertencem aos seus titulares - que são quem deles pode dispor -, é que as entidades se pautarão pelo RGPD.
O segundo grande desafio será o da minimização. É difícil assimilar que só é permitido recolher e tratar os dados absolutamente necessários ao tratamento.
A concretização dos princípios *privacy by design* e *privacy by default* não é simples.
Outro desafio é resistir à tentação de manter e tratar dados que, encontrando-se nas bases de dados, não foram recolhidos nos termos da lei, para cujo tratamento não foi obtido consentimento ou que já deveriam ter sido eliminados.
Um dos principais desafios é o da responsabilidade. As entidades terão de assimilar e cumprir, de mote próprio, todas e cada uma das obrigações do RGPD, e responder pelas suas decisões, sem poder escudar-se no controle prévio da CNPD.
Neste momento o maior desafio é o tempo. A esmagadora maioria das entidades ainda não adotou procedimentos conformes com o RGPD e o tempo escasseia.

ARMANDO MARTINS FERREIRA
Abreu Advogados
Sócio

REVISÃO DE PLATAFORMAS

O Regulamento Geral da Proteção de Dados opera uma mudança de paradigma. A partir de 24 de maio de 2018, deixarão de existir as notificações prévias e as autorizações para efeitos de tratamento de dados e passará a existir um princípio geral de responsabilidade reforçada (accountability), nos termos do qual serão as empresas, através dos RT e eventuais SuB, responsáveis pelo cumprimento do regulamento e pela demonstração desse cumprimento. Será essencial para as empresas a gestão desta nova responsabilidade, ao mais alto nível, de modo esclarecido e consciente. Neste contexto, os principais desafios que, na minha opinião, se colocam são os seguintes:
• A determinação de um processo corporativo que defina os instrumentos, competências e metodologias necessários ao cumprimento das obrigações impostas pelo regulamento, incluindo em matéria de rastreabilidade dos dados;
• A revisão e adequação das plataformas e instrumentos de intercomunicação com os titulares dos dados (contratuais, operacionais, etc.) para assegurar o exercício efetivo e transparente dos direitos que estes dispõem, incluindo em matéria de informação, consentimento expresso e esclarecido, direito ao apagamento.
• A definição do quadro e estatuto do DPO e dos elementos de ligação, incluindo o RT e os SuB's (as suas atribuições, direitos e obrigações);
• E, por último, a implementação de sistemas de monitorização e controlo do sistema, dos processos e dos comportamentos.

JOÃO CRUZ RIBEIRO
JPAB Advogados
Sócio

RESPOSTA A INCIDENTES

O primeiro desafio que o RGPD colocou talvez já tenha sido ultrapassado: sensibilizar os operadores económicos para o problema e convencê-los de que será necessário adoptar modificações substanciais em diversos níveis das respectivas operações.
A matéria de protecção de dados está longe de ser nova e tem sido palco de discussão jurisprudencial a nível interno e também no TJUE (veja-se, a título de exemplo, o acórdão Worten, ECLI:EU:C:2013:355). Mas é inegável que o RGPD introduz mudanças muito significativas, desde logo ao nível dos conceitos e dos princípios, bem como ao nível dos direitos dos titulares dos dados.
Destacamos as alterações relacionadas com a avaliação de impacto na protecção de dados (DPIA), a protecção desde a concepção e por defeito, a figura do encarregado de protecção de dados e a resposta a incidentes e respectivas notificações.
Estas e outras alterações conduzem à necessidade de uma avaliação integrada dos aspectos legais, processuais e técnicos, que não se esgotam em si mesmos, pois devem ainda ser enquadrados com o restante quadro normativo, designadamente a Directiva NIS (*securityof network andinformationsystems*).

JOANA MOTA
Uría Menéndez-Proença de Carvalho
Advogada

CULTURA DE RESPONSABILIDADE

O RGPD representa uma alteração copernicana na forma como se encaram as questões da proteção de dados pessoais. Por um lado, porque vem dar aos cidadãos mais direitos e um maior controlo sobre os seus dados; por outro, porque as organizações transitam de um modelo de hetero-regulação para um sistema de autorregulação e, nesse contexto, passam a ter mais obrigações ao nível da informação que prestam aos titulares dos dados e, sobretudo, ao nível da responsabilidade, através da identificação e mitigação de riscos e de demonstração do cumprimento das regras. Esta alteração paradigmática terá reflexos, desde logo, no funcionamento interno das organizações, que ficam obrigadas a implementar medidas de governança exigentes, mas ao mesmo tempo ajustadas às suas necessidades (avaliações de impacto, privacidade desde a conceção e por defeito, notificações à autoridade de controlo).
A adaptação a estas novas regras não será fácil nem imediata, uma vez que implica uma alocação de recursos – financeiros e humanos – e uma familiarização de conceitos para os quais ainda não existe grande conhecimento ou sensibilização. Apesar disso, é absolutamente necessário que a cultura de responsabilidade não seja ignorada ou menosprezada pelas organizações. Esta atitude releva não só por causa das consequências que podem advir do incumprimento das regras (desde o enquadramento sancionatório, passando pelos danos reputacionais), mas também porque representa uma oportunidade ímpar para reforçar a confiança dos cidadãos na segurança do mundo digital, contribuindo para fomentar um crescimento sustentado da economia e do mercado único na União Europeia.

JOÃO LEITÃO FIGUEIREDO
CMS Rui Pena & Arnaut
Advogado Associado

NOVOS MODELOS DE AVALIAÇÃO DE RISCO

O RGPD revolucionou o quadro regulamentar no que concerne à proteção de dados, obrigando as entidades a um esforço de adaptação legal, organizacional e técnico significativo. O maior desafio das organizações será a criação de uma nova cultura no tratamento de dados, congregando, harmonizando e unificando esforços de departamentos internos que vão desde o jurídico, aos sistemas de informação, recursos humanos, marketing ou de risco.
As organizações enfrentam desafios significativos de integração das mudanças que o RGPD traz na sua atividade diária, designadamente a proteção de dados desde a conceção ou por defeito, cujo impacto real ainda não conseguem efetivamente mesurar, mas que deverão acautelar através da internalização de algumas tarefas atualmente na esfera da CNPD. As organizações são ainda desafiadas a desenvolver modelos de avaliação de risco robustos e adequados e incorporar os mesmos como um pressuposto essencial da sua atividade.
Os titulares dos dados estão, dia após dia, mais informados sobre os seus direitos e atentos à atividade das organizações, pelo que estas deverão definir e implementar os mecanismos adequados ao exercício dos direitos dos titulares previstos no RGPD.

NELSON RAPOSO BERNARDO
Raposo Bernardo & Associados
Sócio

EMPREENDIMENTO

A predisposição dos líderes e do *management* das empresas e outras organizações para aceitar a mudança de paradigma do modo como têm sido encarados os dados pessoais é claramente o desafio número um. Diria mesmo que sem uma consciencialização absoluta de que a privacidade e os dados das pessoas são valores jurídicos muito relevantes e que merecem uma tutela primacial, por parte do sistema jurídico, em relação à generalidade dos interesses empresariais ou corporativos, de pouco servirá a adopção de medidas e procedimentos técnicos avulsos para implementação do Regulamento.
O desafio número dois tem amplitude geracional e corresponde a um reconhecimento da maturidade das empresas: abandona-se o paradigma do controlo prévio, seguido de uma quase ausência de fiscalização a posteriori para um modelo de ausência de controlo prévio a que se seguirá, certa e desejavelmente, uma fiscalização permanente das boas práticas corporativas. As empresas deixam de estar sujeitas a autorizações e notificações prévias, que de alguma maneira dificultavam a actividade empresarial, muitas vezes pela demora da decisão, para passarem a um regime de ausência de controlo prévio, mas com uma relevante responsabilização pelos procedimentos definidos e pelas práticas implementadas. Perceber que esta mudança vai ser mesmo uma grande mudança, e saber estar à altura respondendo com maturidade e uma nova cultura empresarial faz parte importante do desafio dois.
Um terceiro desafio: aproveitar a oportunidade da mudança de paradigma. Este grande empreendimento que as empresas têm pela frente tem de correr bem. As empresas estarão a teste, têm de conseguir demonstrar que estão à altura de aceitar a responsabilidade de definirem e conformarem-se com regras exigentes, sem beneplácito ou entrave prévio de qualquer entidade. E com isso conquistar o legítimo direito a que este modelo de maturidade empresarial seja expandido para muitos outros domínios em que ainda se vive na desconfiança da capacidade das empresas, dificultando por isso a sua iniciativa à entrada, através de processos de autorização morosos, custosos e muitas vezes inúteis, para logo depois das autorizações serem concedidas se relaxar o controlo permanente, de tal maneira que as semelhanças entre o cenário autorizado e o cenário implementado por vezes não passam de uma pura coincidência.

PUB

Empresas terão mais obrigações no tratamento de dados pessoais

LETÍCIA ANTUNES DUARTE
SÓCIA DA ABC LEGAL - SOCIEDADE DE ADVOGADOS, SP, RL
Encarregada de Proteção de Dados certificada pelo European Centre on Privacy and Cybersecurity da Universidade de Maastricht

Existem Responsáveis de Tratamento que vão estar obrigados à nomeação de um Encarregado de Proteção de Dados (EPD), uma figura determinante no processo de adaptação da respetiva estrutura às exigências introduzidas pelo RGPD e ao qual caberá a responsabilidade de pilotar o programa de compliance a implementar. Concretamente, deverá ser designado um EPD sempre que o tratamento seja efetuado por uma autoridade ou um organismo público, quando as atividades principais consistam em operações de tratamento que exijam um controlo regular e monitorização sistemática dos titulares dos dados em grande escala e, ainda, quando as atividades principais consistam em operações de tratamento em grande escala de categorias especiais de dados, como seja dados sensíveis.

ABC Legal – Sociedade de Advogados, RL
Avenida Conselheiro Fernando de Sousa,
19 B-C 1070-072 Lisboa - Portugal
+351 213 584 480
abclegal@abclegal.com.pt

ABCLEGAL

PUB

EY
Building a better working world
No mundo digital será que fazemos melhor ou apenas mais?
Quanto melhor a pergunta. Melhor a resposta. Melhor trabalha o Mundo.
© 2017 Ernst & Young, Limitada. All Rights Reserved.