CISION

O Jornal Económico

ID: 73407148

02-02-2018 | Segurança

Meio: Imprensa
País: Portugal
Period.: Ocasional
Âmbito: Economia, Negócios e.

Pág: 12
Cores: Cor
Área: 26,00 x 32,20 cm²
Corte: 1 de 4

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. Aém 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.

CISION

ID: 73407148

O Jornal Económico

02-02-2018 | Segurança

Meio: Imprensa
País: Portugal
Period.: Ocasional
Âmbito: Economia, Negócios e.

Pág: 13
Cores: Cor
Área: 16,26 x 30,26 cm²
Corte: 2 de 4

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 início, 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.

CISION

O Jornal Económico

ID: 73407148

02-02-2018 | Segurança

Meio: Imprensa
País: Portugal
Period.: Ocasional
Âmbito: Economia, Negócios e.

Pág: 14
Cores: Cor
Área: 26,00 x 26,34 cm²
Corte: 3 de 4

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*).

CISION

O Jornal Económico

ID: 73407148

02-02-2018 | Segurança

Meio: Imprensa
País: Portugal
Period.: Ocasional
Âmbito: Economia, Negócios e.

Pág: 15
Cores: Cor
Área: 26,00 x 28,91 cm²
Corte: 4 de 4

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.