



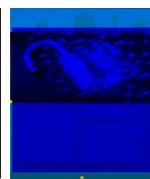
IT

Tema de Capa

RGPD: EMPRESAS AINDA NÃO ESTÃO EM CONFORMIDADE TOTAL

O RGPD entrou em vigor na sua plenitude há um ano, mas as empresas nacionais ainda estão a adaptar-se conforme explicaram, à **businessIT**, a CNPD e algumas entidades que acompanham a implementação do regulamento em Portugal.





Por: Mafalda Freire

Os dados são o novo petróleo: isto é o que todas as empresas apregoam e é inegável. É exactamente por isso e pelo facto de cada vez serem gerados mais dados que houve a necessidade de uma regulação que acompanhasse esta evolução. O RGPD trouxe para a agenda das empresas os conceitos de responsabilidade, protecção de dados by design e by default e uniformizou as situações referentes à privacidade e à protecção de dados entre os Estados-Membros da União Europeia (UE). No ano passado, a IDC e a Microsoft Portugal partilharam um estudo em que concluíram que mais de 50% dos decisores das maiores organizações nacionais não conheciam bem o RGPD e que apenas 2,5% dos decisores achava que sua organização estava preparada para lidar com o RGPD. Um ano após a implementação deste regulamento, as empresas mantêm-se preocupadas e querem estar conformidade, talvez porque as coimas não são brincadeira; mas o facto é que isto não é fácil. A Axians Portugal avaliou de que forma as organizações nacionais e multinacionais a operar em Portugal estão a cumprir os requisitos e as práticas actuais de gestão

da protecção dados pessoais: o nível médio de adesão aos requisitos do RGPD encontrado foi de cerca de 30%. A governança dos dados é a área em que existe maior conformidade com quase 46% das organizações a terem estes processos implementados ou em marcha.

ESTADO DE IMPLEMENTAÇÃO

A maturidade das empresas em relação à implementação do RGPD e ao nível da gestão de dados continua «muito baixa», segundo a IDC. Gabriel Coimbra, group vice president e director-geral da consultora em Portugal, diz que as empresas portuguesas têm, de forma genérica, «uma média de 1,7 numa escala de 1 a 5» e, no que toca especificamente à gestão de dados pessoais, a maturidade «não é muito maior». Miguel Gonçalves, business development manager da Axians Portugal, fala na experiência da empresa, que tem cooperado com nos últimos três anos com algumas das áreas de negócio mais representativas do tecido empresarial nacional: «Temos verificado melhorias significativas na adaptação das organizações. Estamos a falar de um gap considerável que encontramos um pouco por todas as organizações». O responsável acredita que,

O RGPD é «um processo contínuo» que deve ser encarado como «um elemento de crescimento do negócio e afirmação da reputação perante os clientes», diz Elsa Veloso.



actualmente, as organizações já estão «sensibilizadas» para o tema da privacidade e da segurança da informação e que «grande parte delas já iniciou acções no sentido de poderem cumprir com o regulamento». Contudo, segundo Miguel Gonçalves, isso não significa que esse cumprimento «esteja a ser feito na totalidade». A conformidade é, assim, um processo «on going» que requer um «grau de maturidade acima daquele muitas vezes encontrado».

ANO DE APRENDIZAGEM COM PROCESSOS EM FASE INICIAL

A Associação dos Profissionais de Protecção e Segurança de Dados (APDPO) é crítica em relação a este ano de implementação do RGPD e a sua presidente Margarida Ferreira refere que «lamentavelmente, a maioria das empresas portuguesas nem sequer sabe que o RGPD se lhes aplica». A responsável deu o exemplo de um organismo público que, através das associações empresariais, enviou um questionário sobre a aplicação do regulamento a quatrocentas mil empresas portuguesas e recebeu apenas duzentas respostas. Em concordância com esta opinião está Ricardo Henriques, sócio da Abreu Advogados, que considera que aquilo que foi feito até à data, «na maioria dos casos», terá apenas sido uma «primeira etapa de adequação, nos aspectos com maior visibilidade externa (avisos e políticas de privacidade e contratos com subcontratantes)», ficando ainda por percorrer «várias etapas de alterações que consciencializem todos os envolvidos no tratamento de dados pessoais da mudança de mentalidade e investimento necessário para uma verdadeira adequação ao RGPD». Já Clara Guerra, consultora coordenadora do serviço de informação e relações internacionais da Comissão Nacional de Protecção de Dados (CNPd) que é a entidade portuguesa que fiscaliza a aplicação do RGPD, é, apesar de tudo, um pouco mais optimista: «Foi essencialmente um ano de aprendizagem para todos - para as empresas, as entidades públicas, os cidadãos e, por último, também para a CNPD, que teve de lidar com algumas questões novas».

MEDIATISMO: AMIGO OU INIMIGO

A responsável do organismo de supervisão esclarece que a extrema mediatização do RGPD teve «efeitos benéficos, de consciencialização para um novo regime legal europeu, de investimento, esforço e empenho por parte de muitas organizações em criar uma cultura de protecção de dados». Ainda assim, Clara Guerra lembra que também houve «efeitos negativos, de grande confusão sobre o significado e alcance de algumas normas, uma avalanche de informação e contactos com os titulares». Além disso, a consultora diz que houve também «algum oportunismo para vender banha da cobra, tirando partido do cenário de elevada moldura contraordenacional» tendo existido organizações que «gastaram muito dinheiro em consultoria ou soluções informáticas que não são adequadas nem permitem cumprir devidamente as obrigações legais».

PME vs. GRANDES EMPRESAS

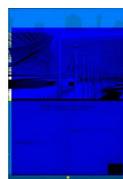
As grandes empresas são as que estão mais avançadas em relação ao RGPD, o que não é de estranhar, como explica Elsa Veloso, CEO e fundadora da DPO Consulting: «A nossa experiência diz-nos que as empresas com maior dimensão, fruto também da sua maior capacidade financeira, estão manifestamente num processo mais avançado de adaptação e de implementação do RGPD». Mas importa salientar que mais de 90% das empresas em Portugal são de dimensão micro ou PME e a especialista alerta para o facto de nestas organizações «existir um maior atraso» e que «urge modificar a curtíssimo prazo». Em sintonia com a DPO em relação a este cenário não muito animador para as pequenas e médias empresas está também o advogado Ricardo Henriques: «A discussão sobre a nova lei nacional tem contribuído para (...) dar um novo fôlego para a maratona que é o esforço de implementação de mudanças estruturais nos procedimentos das empresas para adequação ao RGPD». O executivo refere que «a verdade é que a parte substancial de adaptação está ainda por concluir na maioria das empresas do sector privado, onde as grandes empresas ou sucursais de multinacionais serão a excepção».

ADMINISTRAÇÃO PÚBLICA ATRASADA

O sócio da Abreu Advogados revela que, além disso, a «maioria do sector público» também está em falta na implementação do RGPD. Já Elsa Veloso é da opinião que administração pública está «numa fase muito inicial»

DATA PROTECTION OFFICERS

A figura do data protection officer (DPO) ou encarregados de protecção de dados foi criada pelo RGPD e é obrigatória para algumas organizações, nomeadamente entidades públicas e empresas que na sua actividade tenham acesso a dados pessoais em grande escala ou relacionados com dados criminais, entre outras situações. Mas esta é uma função em que persistem ainda muitos equívocos nas nomeações internas, sendo escolhidas pessoas sem o perfil exigido e, muitas vezes, com perfil incompatível com o exercício da profissão», explica Elsa Raposo, CEO da DPO Consulting. «Os DPO, em Portugal e em face do grau de maturidade das organizações, têm, obviamente desafios exigentes, sob o ponto de vista técnico, legal e de segurança, o que está amplamente relacionado com o seu rol de funções, previsto no RGPD». Certo é que as organizações «não estão cientes da importância de ter um DPO» diz a presidente da APDPO, Margarida Ferreira. «Só as grandes e as médias grandes e, eventualmente, as que têm clientes estrangeiros».



O RGPD é composto por 99 artigos e veio substituir a Directiva n.º 95/46/CE, aprovada em 1995.

em virtude da experiência que a sua empresa teve da implementação do regulamento em câmaras municipais. O sector público «tem ainda um largo caminho a percorrer, no que concerne à implementação de medidas técnicas e organizativas, exigidas pelo RGPD», revela. A CEO da DPO Consulting destaca ainda que a isto «não será alheia a intenção do sector público em ficar isento de coimas, o que a nova lei (nacional) só permitiu que venha a suceder mediante pedido justificado, a decidir pela Comissão Nacional de Protecção de Dados».

IMPACTO NEGATIVOS

O RGPD é um regulamento complexo, extenso e, por isso, acarreta muitos impactos à sua implementação, nem todos bons. O European Payment Report, relatório anual da Intrum que analisa o comportamento de pagamentos das empresas e do Estado, demonstra que com o novo regulamento a funcionar, apenas 8% das empresas europeias vêem um efeito positivo na sua implementação. Já em Portugal o número fixa-se em 7%. Além disso, no País, 48% dos inquiridos não sabe qual o impacto que o RGPD tem nas empresas e 62% afirma não saber qual o custo total da implementação das novas normas do RGPD na sua organização.

Em relação aos desafios, 26% aponta que o desconhecimento da Lei leva clientes a não aceitarem o consentimento de partilha de dados essenciais à realização de campanhas, o acréscimo de burocracia e dos processos administrativos e o aumento dos custos, em especial com a adaptação como os mais nefastos.

DESAFIOS

A responsável da DPO Consulting acredita que os desafios para as empresas «permanecem iguais aos que existiam desde o início da entrada em vigor do RGPD em 2016 e a sua aplicabilidade plena em 2018» e destaca «a necessidade das empresas identificarem os tratamentos de dados que ocorrem no seio de cada organização, perceber que processos, políticas e procedimentos precisam de implementar, que tipo de formação deverão dar aos seus colaboradores e, muito importante, que segurança da informação têm implementada e o que é preciso fazer para a melhorar». Acresce, ainda, a questão da «necessidade, ou não, da nomeação do DPO, e quem nomear». Margarida Ferreira enumera o mesmo tipo de desafios acrescentando «os grandes investimentos necessários» e o business development manager





Durante o primeiro ano de RGPD, a CNPD usou 31 recursos humanos para tratar das situações referentes ao regulamento.

da Axians Portugal, Miguel Gonçalves, acrescenta a «alteração comportamental». O responsável diz que não são só mudanças de comportamentos, mas «culturais e sociais». Para a Gabriel Coimbra, «o grande desafio das organizações portuguesas é gerirem os dados como um activo estratégico, e serem capazes de facto de monetizarem a informação, garantindo a segurança e privacidade dos dados» mas de acordo com o que o executivo disse numa recente conferência organizada pela IDC em que a businessIT esteve presente, este não é um problema só nacional.

A LEI NACIONAL

Portugal era, até Junho, um dos três países, a par da Grécia e Eslovénia, que ainda não tinha transposto o RGPD para uma lei nacional. A Lei de Execução do Regulamento Geral sobre a Protecção de Dados em Portugal já foi aprovada pela Assembleia da República mas terá agora de ser promulgada antes que entre, efectivamente, em vigor. Isto não inviabiliza a aplicação do que é indicado no regulamento europeu; vem é colmatar algumas necessidades específicas e resolver «alguns temas que o RGPD tinha deixado em aberto e que careciam desta intervenção legislativa», indica Ricardo Henriques. A porta-voz da CNPD corrobora este facto e indica que «a Lei de Execução visa apenas regular ou adaptar algumas matérias específicas que o RGPD admite que sejam os Estados-Membros a legislar, sem contrariar o direito europeu. Em alguns casos, a Lei de Execução é essencial para dar fundamento de legitimidade a tratamentos de dados que o RGPD não contempla directamente ou para regular aspectos que o RGPD não faz para que seja possível um ajustamento a outra legislação nacional». O advogado salienta que as principais mudanças são ao nível das «regras relativas a entidades públicas (designação de DPO

/EPD e a possibilidade de dispensa de aplicação de coimas), a fixação da idade de consentimento para menores de treze anos, regras específicas relativas ao tratamento de dados dos trabalhadores no âmbito de relações laborais (em especial, quanto ao consentimento do trabalhador, sistemas de video-vigilância e dados biométricos) e regras quanto ao tratamento de dados de saúde e dados genéticos». Por outro lado, a lei nacional vai também definir as regras referentes aos processos de contraordenação e aos montantes e critérios de determinação das coimas a aplicar. Mas Clara Guerra alerta que o «texto actual aprovado na AR continua a ter muitas das deficiências que a CNPD já assinalou e explicou» num parecer.

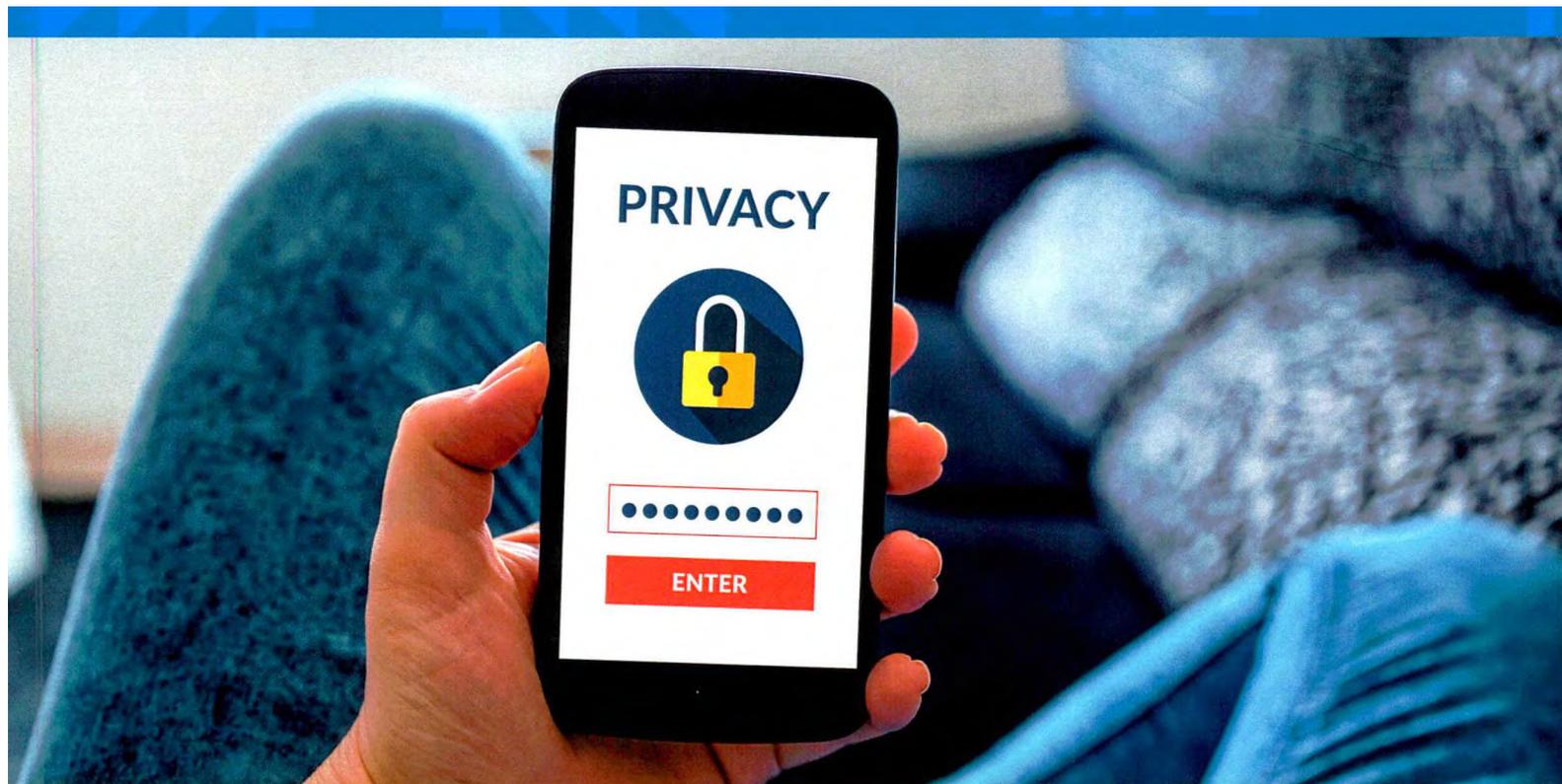
LEGITIMAR É A PALAVRA DE ORDEM

Elsa Raposo considera que a Lei de Execução «vai mudar, essencialmente, a perspectiva de que o RGPD tem de ser cumprido» e que vai trazer o regulamento «para a linha da frente no que às preocupações imediatas das empresas diz respeito». 'Legitimar' - é também esta a convicção de Miguel Gonçalves e da Axians: «Se por um lado consideramos que a existência (finalmente) de uma lei vai "oficializar" a urgência e a necessidade junto de muitas organizações, (isto apesar de já existir um regulamento de aplicabilidade directa à data de 25 de maio de 2018), em especial das entidades públicas, que aguardavam por uma lei nacional para tomar decisões, por outro lado junto das entidades em que o investimento começou a ser feito há dois ou três anos, existirá agora uma legitimação nacional, que corrobora o trabalho já realizado». O responsável vai mais longe e afirma que a nova lei «transmite uma mensagem de justiça e igualdade entre as organizações públicas e privadas».

SUPERVISÃO

A CNPD é a entidade responsável em Portugal pela execução do RGPD e em Maio de 2018 disse claramente que não dispunha dos meios necessários para tal. Passado um ano será que algo se alterou? Clara Guerra é peremptória e diz que não: «Os meios da CNPD não se alteraram, são claramente insuficientes há vários anos, o que impede uma supervisão plena dos tratamentos de dados pessoais». A responsável afirma mesmo que a entidade se debate com «grandes dificuldades» no seu quotidiano, com «prejuízo» para as organizações e para os cidadãos: «Para as organizações, porque têm direito a ter uma autoridade de supervisão forte e interventiva para que não haja impacto na concorrência, entre os que investem em protecção de dados e os que não investem e não são penalizados. Para os cidadãos, porque uma intervenção morosa da nossa parte põe em causa a garantia dos direitos». E deixa uma crítica ao Governo: «O RGPD veio acabar com as autorizações prévias, mas veio trazer um conjunto de novas tarefas, algumas das quais muito burocráticas, que exigem muito tempo





Ricardo Henriques afirma que embora «existam alguns novos direitos dos titulares dos dados (ex.: portabilidade e apagamento) e obrigações dos responsáveis pelo tratamento, a verdade é que a grande maioria dos princípios consagrados no RGPD já constavam da anterior legislação».

e recursos. Faz parte das obrigações do Estado Português dotar a autoridade de proteção de dados dos recursos necessários para desempenhar as suas competências».

O QUE FALTA FAZER

A formação é a grande área em que as empresas devem apostar e o que está em falta na implementação do RGPD. É isto que dizem Miguel Gonçalves, Elsa Veloso e Ricardo Henriques.

QUEIXA E MULTAS EM PORTUGAL

A CNDP fez um resumo da sua actividade entre 25 de Maio de 2018 e 30 de Abril de 2019. Neste período foram iniciados 864 processos de averiguação, foram realizadas 274 notificações de violações de (segurança) proteção de dados (data breach) e foram feitas 263 fiscalizações. A decorrer de momento estão 416 casos dos quais 295 tem origem em queixas e 121 em outras fontes. Além disso, foram ainda enviadas 2569 notificações de DPO à CNPD e existiram cinco casos transfronteiriços. O valor das coimas aplicado neste primeiro ano de RGPD foi de 424 mil euros, a quatro entidades.

O responsável da Axians esclarece que «falta, acima de tudo, formar as pessoas». Para Miguel Gonçalves tecnologia é «unicamente uma maneira de apoiar as organizações, de tornar os seus processos e procedimentos mais eficazes e eficientes, mas não os substitui em momento algum»; este manager falou também da «necessidade de promover conceitos como a ética». Já o advogado salienta que é preciso «formação de todos os envolvidos no tratamento de dados, aproveitando a oportunidade para repensar alguns dos processos de negócio, aplicando o princípio do privacy by design». O sócio da Abreu Advogados diz que isso trará ganhos às organizações já que promove a «redução de riscos legais relacionados com o incumprimento do RGPD» e a «confiança dos clientes que vêm com mais transparência aquilo que a empresa faz com os seus dados». Por seu lado Elsa Veloso, acrescenta que «falta aprofundar junto dos órgãos de gestão e decisórios das organizações que a protecção de dados, a privacidade e a segurança da informação são factores essenciais, no tempo actual, de qualquer organização».

MAIS SEGURANÇA

Será que os dados pessoais dos portugueses estão mais seguros após um ano de implementação do RGPD?





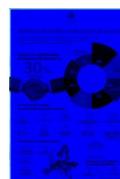
Aparentemente, sim mas talvez tenhamos de aguardar mais algum tempo para ver os verdadeiros benefícios - Clara Guerra é desta opinião. «Penso que teremos de esperar pelo menos cinco anos para poder fazer um primeiro balanço quanto ao nível de protecção oferecido pelo novo quadro legal e quanto à efectividade dessa protecção na prática». O RGPD contribui para uma mudança de abordagem «quer por parte dos reguladores, quer por parte da sociedade, o que traz uma necessária mudança na forma como as empresas devem endereçar as suas responsabilidades» refere Ricardo Henriques. É por isso que «se pode dizer que o regulamento tem contribuído para a criação de cultura de proteção de dados pessoais, isto é, de uma maior consciencialização dos direitos pelos titulares, da procura de uma maior garantia desses mesmos direitos pelos reguladores e de uma maior perceção do valor que uma actuação responsável por parte das empresas em relação ao tratamento de dados pessoais poderá trazer». Já a fundadora da DPO Consulting considera que «depende do grau de maturidade da organização, do seu timing de implementação do RGPD, do que já fez e continua a fazer e se considera que esta é sempre um processo contínuo». Neste caso os titulares de dados estão «mais protegidos».

O Regulamento Geral de Protecção de Dados (RGPD) da União Europeia (UE) é «a maior e mais importante regulamentação referente à privacidade e aos dados pessoais das últimas duas décadas». Foi assim que a própria instituição que a criou se referiu à legislação, que entrou em vigor na sua plenitude a 25 de Maio de 2018.

O business manager da Axians Portugal destaca que «deverá existir uma monitorização constante e um trabalho por um nível de conformidade com o RGPD e de protecção pela segurança constante e ininterrupto». Além disso, «as organizações devem assumir que a preocupação com a privacidade e segurança dos dados é e será uma preocupação contínua, com momentos de atingimento muito próximos da segurança total». Inegável é que o RGPD veio trazer um maior alerta para a questão da protecção dos dados e da privacidade e que as empresas estão mais atentas a estes assuntos (muito por culpa das multas) o que é bom para todos em Portugal, na Europa e um pouco por todo o mundo.

«A protecção de dados pessoais tem de ser pensada. Não vale a pena fingir que não existe. Mas é preciso não entrar em pânico, respirar e ter bom senso» lembra Clara Guerra.





Infografia

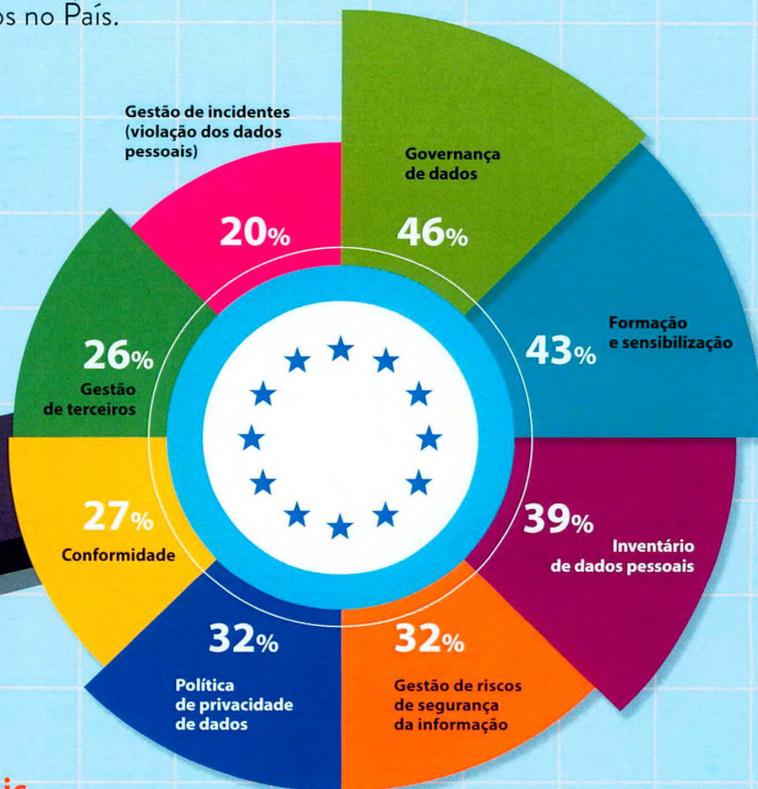
RGPD EM NÚMEROS: O BALANÇO DE UM ANO

Depois de sabermos que nem todas as organizações que operam em Portugal estão em conformidade, esta é a radiografia dos primeiros 365 dias do Regulamento Geral de Protecção de Dados no País.

ESTADO DE CONFORMIDADE EM RELAÇÃO AOS REQUISITOS

30%

nível médio de adesão aos requisitos do RGPD



As 10 maiores ameaças à privacidade dos dados pessoais

- Retenção desnecessariamente prolongada
- Acesso não autorizado
- Recolha excessiva
- Processamento sem o conhecimento ou consentimento do titular dos dados
- Relacionamento não autorizado de dados
- Modificação não autorizada
- Perda, roubo ou remoção não autorizada
- Incumprimento dos direitos do titular dos dados
- Informação insuficiente sobre o propósito do processamento
- Partilha ou alteração do propósito de processamento de dados pessoais com terceiros sem o consentimento do titular

Panorama na União Europeia

144 376

Queixas feitas às autoridades nacionais dos países europeus

+ 375 mil

DPO (data protection officers) existentes

89 271

Violações de dados comunicadas

+56

milhões de euros
Valor global de multas aplicadas



Queixas mais habituais à violação do RGPD

- Promoções de telemarketing
- E-mails
- Video-vigilância/CCTV



ID: 81803135

31-07-2019



20

TEMA DE CAPA

O RGPD entrou em vigor há um ano. As empresas nacionais ainda se estão a adaptar, como explicaram, à businessIT, a CNPD e algumas entidades que acompanham a implementação do regulamento em Portugal

Um produto Fidemo - PCGuia / Julho - 2019

business.IT
PROFESSIONAL MAGAZINE**ENTREVISTA**

Ricardo Pires Silva, SAS
«Transformação digital
sem transformação
analógica é um desastre»

**ALÉM-FRONTEIRAS**

Lenovo aposta
em equipamentos
inteligentes
e na segurança

**REPORTAGEM**

Dell Technologies Forum:
Mais que novidades,
consistência no negócio

**SEGURANÇA**

Mastercard:
PSD2 vai obrigar
a alterações nos
pagamentos digitais

UM ANO DE
RGPD

O Regulamento Geral sobre a Proteção de Dados
entrou em vigor há um ano, mas as empresas nacionais
ainda estão a adaptar-se à nova realidade.