Vêm aí as novas regras de proteção de dados. Está preparado?

Regulamento Geral da Proteção de Dados entra em vigor a 25 de maio e aplica-se a todas as empresas e organizações. A três meses das novas regras, saiba o que tem de fazer para evitar multas pesadas.

Por **FÁVIO NUNES**

Há um elefante na sala. E vamos ter de falar sobre ele. Chama-se Regulamento Geral de Proteção de Dados (RGPD) e, a partir de 25 de maio, poderá resultar em multas pesadas para as entidades que não cumpram a nova legislação: coimas até 20 milhões de euros ou 4% do volume de negócios anual da companhia. Mas este não é um artigo normal, nem uma tentativa de incutir medo. Ao longo das próximas linhas, tentaremos desmistificar o que muda realmente, bem como dar algumas orientações sobre o que as empresas devem fazer nos meses que se seguem.

Atualmente, o que as empresas têm de fazer em matéria de dados é pedir um parecer à Comissão Nacional de Proteção de Dados (CNPD), que autoriza ou não a recolha, tratamento e armazenamento desses mesmos dados - e só em ocasiões específicas. "As empresas pedem uma autorização e fazem pouco mais", reconhece Cláudia Martins, advogada da Macedo Vitorino & Associados, especializada nesta matéria. "Mas vai deixar de ser assim. O ónus vai passar para as empresas. Vamos passar a um modelo de auto-regulação", sublinha à Advocatus. Por outras palavras, cai sob as organizações a responsabilidade de interpretar e cumprir o novo regulamento. Mais: terão de conseguir provar que o cumprem, que estão em compliance. E que gerem a questão internamente, de forma contínua.

"Numa lógica de processo de negócio, as empresas não estavam preocupadas com isto e agora têm de se preocupar. Têm de nomear uma pessoa para tratar do assunto, ou um grupo de pessoas", resume Daniel Reis, advogado da PLMJ. "O que significa auto-regulação? Significa olhar para os tratamentos de dados. Perceber como é que a privacidade das pessoas é afetada", acrescenta o especialista. Há ainda uma nova função "que não existia". Essa função é a do Encarregado de Proteção de Dados, ou DPO, que algumas empresas vão ser obrigadas a nomear (ver caixa). Será o responsável máximo por garantir que a empresa cumpre o RGPD.

PIXABAY

PREPARAÇÃO? É CASO A CASO

Muitas empresas ainda não começaram a olhar para as novas regras, reconhecem os peritos na área. O problema não vem de agora. Em março de 2017, um estudo da KPMG dava alguns números: 65% das empresas inquiridas "consideram ter um grau de consciência médio ou alto sobre as obrigações e impacto do RGPD", enquanto 85% "ainda não começaram a implementar medidas efetivas para garantir a conformidade". À Advocatus, João Costa Quinta, advogado da DLA Piper ABBC, arrisca um número: só um terço das empresas portuguesas estará "mais ou menos ciente" das novidades que aí vêm.

A boa notícia é que, a três meses da entrada em vigor do regulamento, ainda é possível alisar terreno para estar tudo pronto a 25 de maio. Pelo menos para a generalidade das companhias. A notícia menos boa é que não há uma solução do tipo pronto-a-vestir. "Não há um modelo one-fits-all", reconhece Daniel Reis, da PLMJ. Por isso, deixa algumas questões a que as empresas devem responder para completar a primeira fase

<< **João Costa Quinta**
sócio da DLA Piper ABBC

< **Cláudia Fernandes Martins**
Associada sénior da Macedo Vitorino & Associados

Cumprir o RGPD, passo a passo

1 - Fase de Diagnóstico
Ler o regulamento. Identificar os dados que existem na empresa e o tratamento que é feito. Que tipos de dados existem? Para que finalidade? E qual o prazo de conservação? Perceber quais os fluxos de dados existentes. Há fornecedores com acesso aos mesmos?

2 - Fase de Revisão
Rever se há consentimento dos titulares para uso e tratamento dos dados que já existem. Verificar os documentos de consentimento. Rever políticas de privacidade e termos de utilização, assim como contratos com fornecedores e outras entidades subcontratantes. Colocar toda a documentação em cumprimento com o RGPD.

3 - Fase do DPO
Perceber se a empresa cumpre os requisitos (ver caixa) para ter de nomear um Encarregado de Proteção de Dados (DPO). Nomear um DPO caso seja necessário e envolvê-lo no processo de preparação.

4 - Fase de Implementação
Identificar as medidas a adotar. Avaliar se é preciso substituir sistemas informáticos. Adquirir os sistemas necessários. Desenhar um plano de implementação. Executar as novas medidas e avaliar se tudo ficou em conformidade.

5 - Fase de compliance
Formação aos funcionários. Garantir a contínua conformidade com o RGPD. Business as usual a partir de 25 de maio.

do processo de preparação: "Como estão organizadas? Onde é que estão os dados? Estão dentro da empresa? Estão num fornecedor? Estão na cloud? Onde estão os pontos de risco? Há três processos de tratamento de dados, ou há 53? É fundamental olhar para dentro da organização para encontrar formas de começar a criar um sistema de compliance", recomenda o advogado.

Nos próximos três meses, as empresas portuguesas vão ter de ler o Regulamento, efetuar um diagnóstico interno e encontrar medidas para tapar as lacunas.

Ou seja, o primeiro passo é realizar um diagnóstico. Saber que dados estão na posse da empresa, que podem ser tão diversos como os endereços de e-mail inscritos numa newsletter como os dados pessoais dos trabalhadores que a empresa transmite ao fisco e à Segurança Social - mais os dados dos clientes, dos visitantes do website e por aí em diante. O que muda? Em suma, é preciso minimizar o risco para o titular dos dados, que tem de dar autorização expressa para a organização os poder tratar e guardar. "As opções pré-preenchidas deixam de ser possíveis. Terá de ser a própria pessoa a preencher", nota a advogada Cláudia Martins. O titular dos dados também tem de saber o fim que será dado a esses dados e a empresa só os poderá usar nesse sentido. Tem de ser tão fácil aceitar como revogar a permissão.

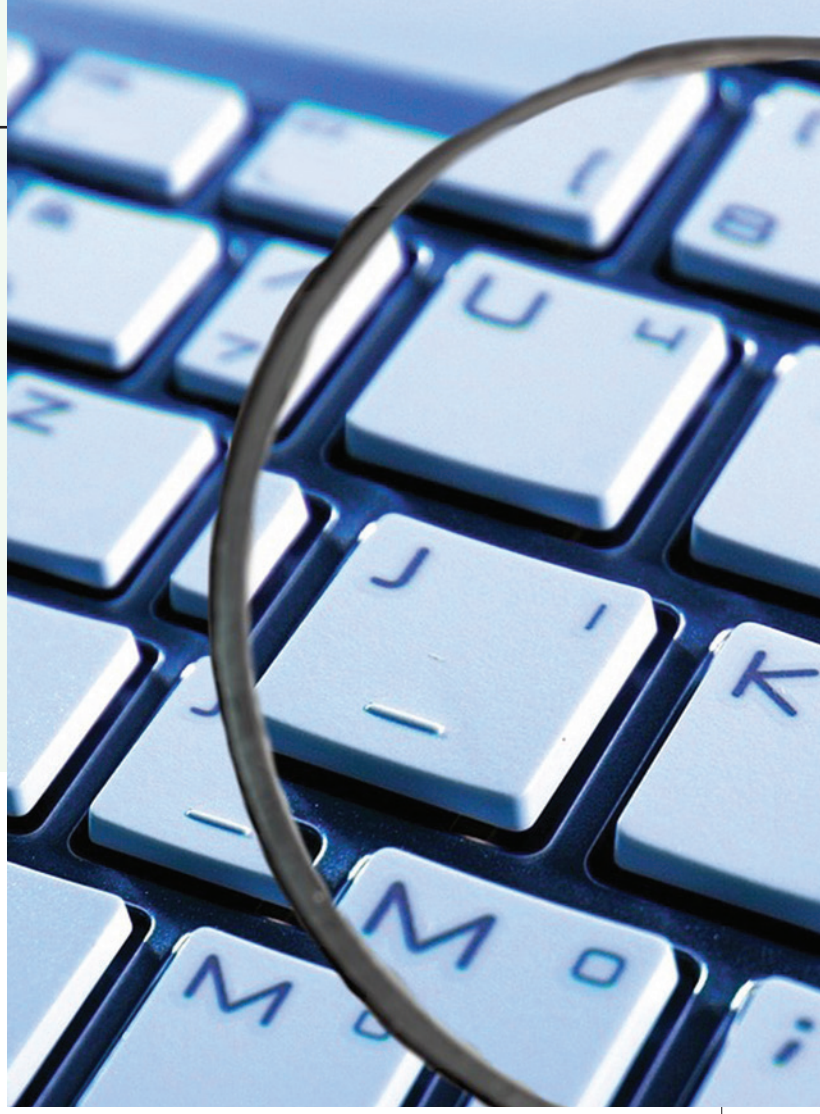
PREPARAÇÃO PODE ENVOLVER CUSTOS

Dos três profissionais com quem a Advocatus falou, nenhum pôde avançar com um valor médio de investimento que a preparação para o regulamento poderá acarretar. Como não há uma solução para todos, os custos podem variar muito. Algumas empresas poderão estar muito perto do total cumprimento, enquanto outras poderão ter de atualizar toda a infraestrutura informática, ou repensar totalmente os processos de tratamento de dados pessoais. No entanto, no caso das empresas mais longe do compliance, o investimento necessário será, naturalmente, superior. "Alguns milhares de euros vão ter de ser gastos pelas empresas. É difícil dar um número fixo", admite o especialista João Costa Quinta. Mas lembra: "Todo o custo é pouco comparativamente com o quadro sancionatório."

Resumindo, nos próximos três meses, as empresas portuguesas vão ter ler o regulamento, efetuar um diagnóstico interno, encontrar medidas para tapar as lacunas, implementá-las na companhia e, por fim, criar um processo de gestão de dados contínuo, em concordância com o RGPD. Em todo este processo, os advogados garantem que podem ajudar, mas indicam que qualquer solução tem de abranger duas vertentes: a parte técnica e a parte jurídica. Ambas terão de conviver e falar a mesma língua, o que poderá ser um desafio.

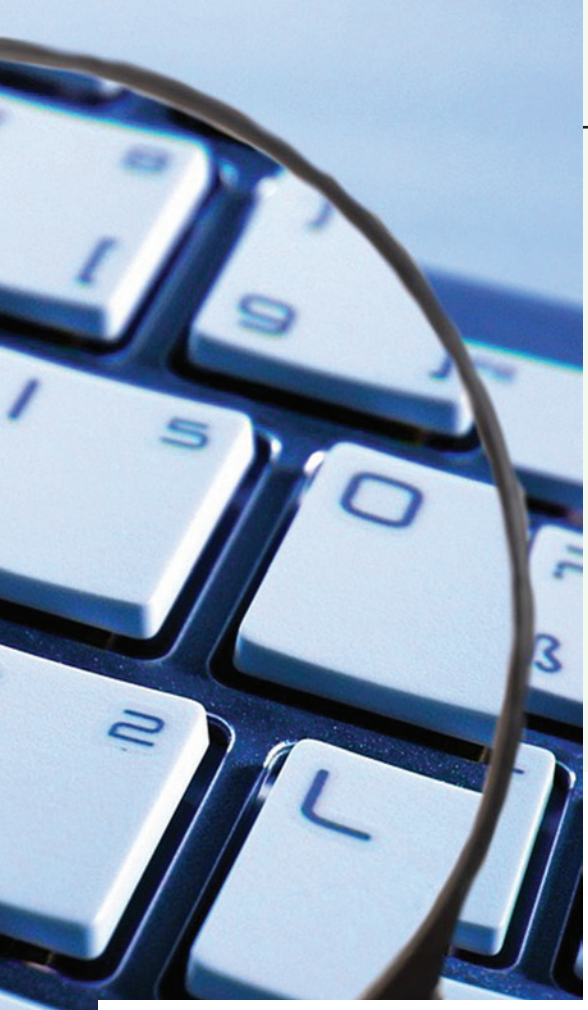
A ADVOCATUS sondou algumas empresas portuguesas para perceber se já se debruçaram sobre este assunto. Gonçalo Rebelo de Almeida, administrador do grupo Vila Galé, revela: "Desde há um ano que temos vindo a preparar-nos para as mudanças que a nova legislação implicará. Desde logo, foi criado um grupo de trabalho multidisciplinar com representação de departamentos como jurídico, informático, qualidade e segurança, marketing e outros, com o objetivo de adaptar a política de proteção de dados e de privacidade às exigências do novo regulamento."

O grupo hoteleiro já está mesmo a implementar medidas, como "reconfigurar os processos de negócio", tais como os pedidos de reservas, "para diminuir o volume de dados solicitados aos clientes". A empresa vai ainda encriptar alguns dados para os proteger, bem como reavaliar contratos com fornecedores que lidem com os dados dos clientes do grupo. Outras medidas abrangem o reforço dos "processos de recolha de consentimento junto dos clientes", assim como a



PIXABAY

> **Daniel Reis**
> sócio PLMJ



Requisitos para nomear um DPO

Segundo o RGPD, é obrigatória a figura do Encarregado de Proteção de Dados (DPO) nas seguintes organizações:

1 - Empresas que tratem dados sensíveis em grande escala como atividade principal.

2 - Organismos públicos, exceto tribunais no exercício da sua função jurisdicional.

3 - Empresas que façam "controlo regular e sistemático" dos titulares dos dados.

contratação de um DPO. "Acreditamos que a empresa estará devidamente preparada para cumprir a nova lei quando esta entrar em vigor", conclui o gestor.

Miguel Sousa, diretor de Sistemas de Informação do Super Bock Group, indica que a empresa encara o RGPD "como um enorme desafio mas, simultaneamente, uma grande oportunidade". As medidas que estão a ser alinhavadas abrangem a "implementação de um conjunto de mudanças ao nível dos processos de gestão de informação, de adoção e ajuste de múltiplas tecnologias envolvidas, com impactos em aspetos culturais da própria organização", refere. Segundo o diretor, o RGPD encontra-se "no topo das prioridades" da "agenda tecnológica" do grupo cervejeiro, que reconhece que "os dados serão o combustível que irá alimentar a nova economia".

QUEM VAI FISCALIZAR?

Se as empresas vão ter de cumprir, quem vai fiscalizar? Em teoria, será a CNPD. Mas ninguém parece saber ao certo, até porque há legislação própria que vai ser criada nos Estados-membros e que, em Portugal, ainda é desconhecida. "O Governo nomeou um grupo de trabalho que preparou um anteprojeto. O que me disseram é que já está na Presidência do Conselho de Ministros, mas não sei o que está lá. Alguma coisa vai sair daí", aponta Daniel Reis. Dúvidas que também são reconhecidas por Cláudia Martins: "Ainda não sabemos muito bem se será a CNPD ou uma outra entidade que, entretanto, possa ser criada e que vá substituir ou complementar a CNPD. Ainda não há nenhuma novidade em relação a este aspeto. E continuamos à espera." João Costa Quinta reconhece as dúvidas, mas dá um passo em frente: "Se não for a CNPD, o que é que ficará cá a fazer?" Para o especialista, o que poderá acontecer é uma "reconfiguração" da comissão, ou a criação de uma Autoridade Nacional de Proteção de Dados.

Há também dúvidas sobre o grau de preparação da própria CNPD no que toca ao novo regulamento. A ADVOCATUS enviou um conjunto de questões à comissão. Mesmo após várias insistências, a CNPD não deu qualquer tipo de resposta. "Eu não acho que a própria CNPD vá estar preparada" a 25 de maio, reconhece Daniel Reis, notando que a entidade necessitará de meios para ser capaz de "fiscalizar o mercado todo". Questionada sobre um possível atraso da própria comissão, a advogada Cláudia Martins indica: "Acho que a própria CNPD foi colocada um bocadinho de parte nas novidades que podem ser trazidas." Porquê? "Quando foi criado o grupo de trabalho que está a preparar a legislação, a CNPD não só não foi ouvida como não tem qualquer papel a esse nível. Na minha opinião, pode ser um erro."Atualmente, a comissão conta com um espaço próprio no website dedicado ao RGPD e lançou, há algum tempo, um documento com dez medidas que resumem as novas regras.

● **COM ELISABETE FELISMINO**