

# Fechar os olhos ao *Big Brother*

➤ Em 2018, entra em vigor o Regulamento Europeu de Proteção de Dados. Muitas empresas ainda desconhecem os contornos do diploma, que promete fechar os olhos ao *Big Brother*. O Grupo Sendys realizou uma sessão de esclarecimento sobre o tema e o Jornal das Oficinas esteve presente

Por: **Jorge Flores**



# O

O novo Regulamento Europeu de Proteção de Dados Pessoais (RGPD) está quase a entrar em vigor. No próximo dia 28 de maio de 2018, muito vai mudar na relação como as empresas terão de gerir as suas bases de dados. E a grande maioria ainda não está devidamente informada sobre os passos a dar para que esta mudança do quadro legal seja pacífica e possa, inclusivamente, abrir perspectivas positivas para o negócio.

Refira-se que o regulamento tem aplicabilidade direta em todos os países da União Europeia e é válido para todas as empresas que operem na UE e para todos os cidadãos. As empresas do *aftermarket* nacional não estão isentas desta realidade. A esse propósito, o Grupo Sendys, do qual faz parte a Alidata, organizou uma sessão de esclarecimento, onde convocou algumas personalidades, de diferentes áreas, para ajudar as empresas a compreenderem melhor os contornos do novo RGPD. Colocando questões (aparentemente) tão simples como esta: um endereço de *email* do trabalho é um dado pessoal ou é um

para tratar de negócios, então não caia na tentação de colocá-lo na sua *mailing list* comercial, pois o resultado pode ser negativo para o seu lado”.

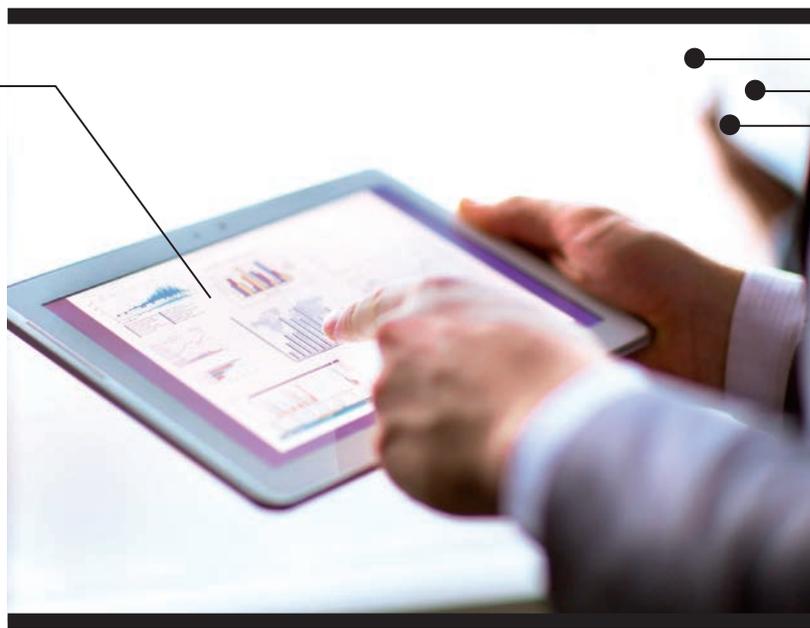
Separar as águas é crucial. Segundo afirmou ainda Fernando Amaral, diretor executivo do Grupo Sendys, “o que estamos aqui a falar é de uma questão de processos, não de *software*. Não é com uma atualização de *software* que se vai resolver a adaptação destas normas”. De

---

**O regulamento, que entrará em vigor a 28 de maio de 2018, tem aplicabilidade direta em todos os países da União Europeia e é válido para todas as empresas que nela operem e para todos os cidadãos**

---

acordo com os responsáveis do Grupo Sendys, o RGPD não está, diretamente, relacionado com a alteração de práticas que sejam executadas com *software*, “mas tenta colocar um travão naquelas que são más práticas comportamentais das empresas e dos seus colaboradores, relativamente à recolha e tratamento de



dado coletivo? A resposta obriga a alguma reflexão. “É pessoal, no sentido em que permite identificar uma pessoa. E é coletivo, no sentido em que é um veículo de comunicação com a empresa”. Todo o cuidado é pouco, uma vez que este “pormenor” poderá ter implicações legais para a empresa. Daí que o conselho deixado para a plateia pela organização da conferência seja o de usar apenas o *email* para aquilo que lhe foi dado; se foi

dados pessoais dos seus utilizadores”. E que não haja dúvidas. “Sim, o *software* pode ajudar a atenuar esta transição, mas o grande problema está mesmo na cultura empresarial”.

#### ■ OLHAR DA LEI

Foram vários os especialistas a intervir na sessão de esclarecimento do Grupo Sendys. “Se tivermos a consciência da importância que isto tem para o nosso

## Sete chaves a reter do RGPD

### 1 Registo de dados

Importa criar um sistema de registo de dados. É essencial identificar os dados que são recolhidos, deixando claro de onde vêm, como, porquê e com quem são partilhados. O objetivo é “mapear” todos os dados utilizados pela empresa e deixá-los ordenados em conjuntos fáceis de identificar. O nível de conservação e de proteção deverá ser idêntico para todos.

### 2 Política de privacidade

Repensar os princípios da privacidade, os procedimentos administrativos e a documentação, é outra das prioridades. O consentimento dos titulares dos dados deverá ser livre, específico, informado e corresponder a uma clara ação afirmativa do titular dos dados (na forma oral ou escrita). O silêncio, opções pré-validadas ou omissão do titular dos dados, não constituem consentimento. O novo regulamento impõe a criação de um registo das atividades de tratamento, caso a empresa tenha mais de 250 trabalhadores, se o tratamento de dados implicar um risco para os direitos do titular, se não for ocasional ou se incluírem dados sensíveis ou relativos a condenações penais e infrações.

### 3 Direitos dos titulares

Os novos direitos dos titulares dos dados não podem ser esquecidos. As empresas terão de garantir o cumprimento de dois direitos fundamentais: o direito de portabilidade e o direito a ser esquecido. O primeiro, reforça o já existente direito de acesso dos titulares aos seus dados pessoais através de um pedido de acesso, podendo ainda ser pedidos os mesmos, num formato estruturado, de uso correntes e de leitura automática. O titular poderá transmitir esses dados, de forma gratuita, a outro responsável pelo tratamento e sem que o primeiro responsável a quem foram fornecidos o possa impedir. O segundo direito, “a poder ser esquecido”, significa que os titulares dos dados podem exigir a eliminação da informação e a abstenção de qualquer disseminação futura desses dados.

### 4 Conhecimento da lei

Os recursos humanos devem estar devidamente conscientes das implicações do RGPD e obter formação sobre as novas regras. As organizações devem estar atentas e verificar se cumprem os requisitos para ser obrigatório designar um DPO e de que forma esta função se enquadrará no seio da empresa. Para esse efeito, poderá ser necessário criar uma função específica para desempenhar a função de DPO. Em determinados casos, poderá ser necessário nomear um responsável por cada empresa ou jurisdição do grupo. A designação de um DPO, quando seja obrigatória, aplica-se aos responsáveis pelo tratamento e subcontratantes.

### 5 Requisitos de proteção

As empresas devem adotar medidas internas que cumpram os requisitos de proteção, “desde a conceção” e proteção “por defeito”. A primeira, requer que o responsável pelo tratamento de dados aplique, quer no momento de definição dos meios de tratamento quer no momento do próprio tratamento, medidas técnicas e organizativas adequadas. Como, por exemplo: minimização do tratamento de dados; pseudonimização de dados pessoais o mais cedo possível; adoção de medida de transparência relativas às funções e ao tratamento de dados pessoais; possibilidade de o titular dos dados controlar o tratamento de dados; possibilidade de o responsável pelo tratamento criar e melhorar medidas de segurança. Por sua vez, a “proteção por defeito” →



futuro, para o futuro dos nossos filhos, vamos tomar medidas para que os dados pessoais dos cidadãos sejam, efetivamente, protegidos”, alertou Paulo Calçada, da Calçada Advogados. Para, de seguida, chamar a atenção para uma necessidade: “As organizações têm de entender que informação pessoal dispõem, para que é utilizada, onde e como é armazenada. Depois, as empresas precisam de entender o regulamento e garantir que o mesmo é cumprido”, sublinhou o advogado na conferência de esclarecimento.

Sandra Veloso, da Data Privacy ON, explicou que o novo RGPD “é uma questão que deve dizer respeito a todas as pessoas das empresas, desde os executivos e altos quadros até aos profissionais com

móveis, em serviços *web* ou em formato *excel*, esquecida numa *pen*, algures no escritório ou em casa. Rui Batista deixou ainda um aviso: “Onde estão as cópias de segurança, quem lhe acede, em que data? É preciso saber mesmo tudo. O próprio controlo de acesso à infraestrutura de TI tem de ser revisto”, reforçou, tratando, depois, de explicar como deve funcionar uma gestão “assente na rastreabilidade” e como se deve acabar com as “contas de acesso genéricas e implementar permissões para a exportação de dados e até de impressão”, afirmou ainda o mesmo responsável do Grupo Sendys.

#### ■ MULTAS ELEVADAS

Para melhor compreensão das obrigações inscritas no RGPD, os responsáveis



**A negligência aos contornos do RGPD poderá ter consequências muito nefastas para as organizações. A multa para incumprimentos pode chegar aos 20 milhões de euros ou até 4% da faturação**

menores poderes de decisão, mas pelas mãos dos quais passam dados pessoais. Não é necessário que todos sejam especialistas em RGPD, ainda que seja aconselhável que todos tenham, pelo menos, uma noção deste regulamento”, disse.

Qual deverá, neste caso, ser o primeiro passo a dar pelas empresas? “Identificar os dados!”, garantiu Rui Batista, gestor de desenvolvimento do Grupo Sendys, sem esquecer que estamos perante um processo complexo, uma vez que dados pessoais podem estar guardados em folhas de papel, na *cloud*, em dispositivos

do Grupo Sendys trataram de esclarecer algumas questões fulcrais do diploma, que entra em vigor este ano. Desde logo, responde a uma dúvida basilar, na mente de muitas organizações: o que são considerados dados pessoais ao abrigo do RGPD? “Todos os dados que possam identificar, direta ou indiretamente, uma pessoa, seja o nome, o *email*, identificadores eletrónicos, o IP ou até dados biométricos”. De acordo com muitas intervenções ouvidas na sessão de esclarecimento, convém deixar claro que as autoridades competentes não serão

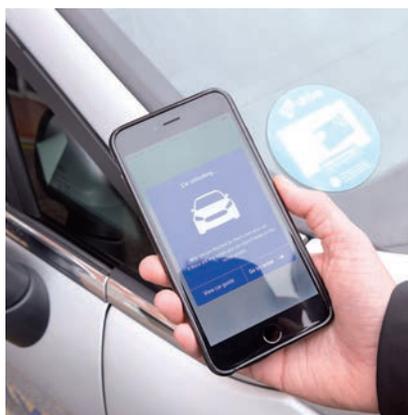
tolerantes com desculpas de “falta de tempo” ou de “orçamento” para cumprir com as obrigações.

Por outro lado, importa nomear um encarregado de proteção de dados (DPO na sigla em inglês). Com um detalhe: “Nem todas as organizações são obrigadas por lei a ter um DPO, mas alguém dentro da empresa deve ser nomeado como pessoa responsável para gerir futuros pedidos de dados por parte dos utilizadores. Ou para trabalhar com a Comissão Nacional de Proteção de Dados em caso de auditoria”. O referido responsável deve primar pela “independência dentro da organização, mas tendo em conta que, em Portugal, o tecido empresarial é, acima de tudo, constituído por PME, o que leva a que

exista uma acumulação de funções. Empresas públicas, empresas com mais de 250 funcionários ou que trabalhem com tipologias de dados sensíveis, são sempre obrigadas a ter um DPO”, explicou ainda a mesma fonte.

Aconselhável será ainda procurar integrar ferramentas de *software* que facilitem a realização de auditorias técnicas. Significa isto que as organizações devem dispor de registo detalhado de quem acedeu a determinada informação, quando e em que circunstâncias. Tais dados poderão revelar-se vitais para detetar eventuais incumprimentos do RGPD e ajudam nos processos de auditoria das entidades reguladoras.

A negligência aos contornos do RGPD poderá ter consequências muito nefastas para as organizações. “A multa para incumprimentos pode chegar aos 20 milhões de euros ou até 4% da faturação global da empresa, mas as coimas não serão estanques. As entidades terão em consideração diversos pontos de conformidade, pelo que a multa será mais pesada quantos mais pontos não estiverem a ser respeitados”, alertaram, na sessão de esclarecimento, os especialistas jurídicos. Já em caso de violação da privacidade ou do tratamento dos dados, um utilizador poderá pedir uma indemnização, caso consiga provar os danos ou prejuízos decorrentes do incumprimento do RGPD. \*



➔ requer que o responsável pelo tratamento implemente medidas técnicas e organizativas adequadas destinadas a assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento.

## 6 Medidas de segurança

O novo regulamento prevê a aplicação de várias medidas organizativas. Antes de mais, a pseudonimização e cifragem dos dados pessoais e a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento. Também a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada em caso de incidente físico ou técnico e ter um processo para testar, apreciar e avaliar regularmente a eficácia das medidas adotadas para garantir a segurança do tratamento, são vinculativas. Estas medidas não são obrigatórias em todos os casos, dado que a empresa tem o direito de optar por outras soluções.

## 7 Transferências transfronteiriças

As atuais regras sobre transferências internacionais de dados saem reforçadas com o novo diploma. Estas são permitidas, desde que apresentem garantias. A juntar às conhecidas cláusulas contratuais-tipo e ao consentimento do titular, o novo RGPD acrescenta outras soluções. As já existentes cláusulas contratuais-tipo deixam de requerer a autorização prévia da CNPD. Contudo, apesar desta “dispensa”, a CNPD poderá exigir à organização uma notificação prévia para essas operações de tratamento. As regras vinculativas aplicáveis às empresas

são outra das soluções ao abrigo da qual as entidades de um grupo empresarial se obrigam a realizar entre si transferências de dados. \*

Publicidade

# O Óleo da Oficina



FUCHS LUBRIFICANTES, Unip. Lda. | Zona Industrial Maia 1 | Sector VII  
Trav. Eng. Nobre da Costa | 4470-435 Moreira - Maia  
Tel. 229 479 360 | fuchs@fuchs.pt | [www.fuchs.com/pt](http://www.fuchs.com/pt)

LUBRICANTS.  
TECHNOLOGY.  
PEOPLE.

