Last Call para o RGPD
As oportunidades ao alcance do Canal

O novo Regulamento é um incentivo de peso à mudança na forma como as organizações recolhem, processam e armazenam dados de natureza pessoal. Esta alteração no relacionamento com a informação, a garantia da sua privacidade e a sua proteção terá inevitavelmente de ser suportada por um conjunto de processos tecnológicos

Vânia Penedo

Falta pouco mais de um mês para a entrada em vigor do novo Regulamento Geral de Proteção de Dados (RGPD). A nova diretiva, que a partir de 25 de maio é de cumprimento obrigatório, exigirá às empresas novas formas de lidar com a informação pessoal, já que a salvaguarda da privacidade terá de estar enraizada nos processos de tratamento de dados, quer tecnológicos quer humanos. A diretiva uniformiza a proteção dos dados pessoais e substitui o Regulamento atualmente em vigor, que data de 1995 (Diretiva de Proteção de Dados) e que está desadequado da realidade de hoje.

Assim, apesar de o novo RGPD dizer sobretudo respeito aos processos das organizações, a verdade é que, do ponto de vista tecnológico, trará mudanças. Num white paper que data de outubro de 2017, intitulado "Technology's role in data protection - the missing link in GDPR transformation", a PwC sublinha que "ao invés de um add-on ou de uma consideração *a posteriori* no seio das operações de negócio, a proteção dos dados pessoais terá, agora, de ser projetada de raiz nos sistemas de processamento de dados, o que significa que as entidades terão de reexaminar a forma como abordam a utilização da tecnologia nas suas organizações".

Fotografia: © santiago silver - stock.adobe.com

Nova forma de olhar para a gestão e tratamento dos dados

Segundo Daniel Reis, sócio e coordenador da sociedade de advogados PLMJ TMT, de entre todas as alterações trazidas pelo RGPD, o que é "verdadeiramente essencial e talvez menos evidente" é a transição de um sistema em que as organizações seguem as orientações do Regulador, em Portugal a Comissão Nacional de Proteção de Dados, para um sistema de autorregulação. "Isto significa cumprir determinadas obrigações que hoje não cumprem. Estamos a falar de saber olhar para os tratamentos de dados pessoais, perceber qual o impacto desses tratamentos na privacidade das pessoas e, em função desse impacto, tomar decisões sobre a organização e sobre a segurança dos dados".

Nesta fase, já tão próxima do cumprimento obrigatório, é fundamental estabelecer prioridades, porque estão em causa coimas que podem ascender aos 20 milhões de euros ou a 4% do volume global de negócios. A primeira medida, indica Daniel Reis, é "identificar onde está o risco e tratar das situações onde este é superior". Importa ainda "olhar para o tratamento de dados que é realizado pela organização, onde é que esses dados estão, de onde vêm, para onde estão a ser transmitidos, e perceber todos os aspetos logísticos, tecnológicos e organizacionais relacionados com o tratamento dos mesmos".

O advogado da PLMJ alerta ainda para a importância de "alterar os sistemas de informação para garantir que os dados são apagados, bem como criar rotinas para evitar a duplicação de dados". Porém, qualquer implementação tecnológica, diz, "terá de ter como ponto de partida o conhecimento da situação atual das empresas".

Ao IT Channel, a ASSOFT – Associação Portuguesa de Software, sublinhou ser fundamental elaborar um Estudo de Impacto da Privacidade, "que se resume a compreender o nível de exposição da organização, a sua capacidade de garantir a privacidade e proteção dos dados que trata e, desta forma, perceber que processos deve a organização implementar ou alterar para garantir a conformidade com o Regulamento".

A tecnologia ao serviço dos novos direitos individuais

Na sua essência, o RGPD dotará o cidadão de ferramentas que lhe permitem ter uma palavra a dizer sobre a manipulação dos seus dados. A diretiva contempla, deste modo, o direito a ser esquecido, o acesso facilitado aos próprios dados e à forma como estes são tratados, bem como o direito a ser-se informado se os dados estiverem comprometidos devido a uma falha de segurança. Na categoria de dados pessoais, importa recordar, o RGPD contempla nomes, moradas, números de telefone, números de identificação fiscal, e-mails e até endereços IP, mas também dados de natureza médica ou financeiros.

Os titulares passam também a ter o direito de solicitar que os seus dados sejam eliminados por determinada empresa/organização sempre que: já não sejam necessários para o propósito para o qual foram recolhidos; que o período de consentimento tiver expirado; quando o consentimento for revogado. Cada cidadão passa ainda a ter o direito à

portabilidade dos dados, o que significa que pode mais facilmente "reutilizá-los" junto de diferentes organizações.
O white paper da PwC é bastante esclarecedor a este respeito, dizendo que todos estes direitos expressos no Regulamento exigem que as organizações estejam dotadas de tecnologia que permita:

- A categorização dos dados pessoais por tipo e propósito de processamento;
- A possibilidade de retificar, apagar ou anonimizar os dados;
- O mapeamento e rastreio da vida útil da informação;
- A possibilidade de transmitir dados pessoais de uma tecnologia para outra;
- O congelamento ou supressão dos dados;
- A proteção adequada dos dados;

Níveis baixos de preparação entre as PME

Para a jp.di, o RGPD marca "o início de uma nova era na gestão de dados pessoais na União Europeia", nas palavras de Helder Miranda, head of marketing. "Nos últimos meses tem existido um aumento da procura por soluções tecnológicas que vão ao encontro do cumprimento do RGPD", refere, reflexo de um aumento da preocupação, por parte dos gestores portugueses. "Verificamos com satisfação que existem várias empresas portuguesas que encaram este momento como uma oportunidade para realizarem a tão necessária transformação digital".
O Regulamento impõe uma nova forma de estar perante a informação, pelo que o tema promete não mais abandonar a agenda dos decisores. "As organizações não precisam estar compliant para o dia 25 de maio, mas daí para a frente", destaca Helder Miranda. "Será certamente gerador de oportunidades comerciais para quem oferece soluções tecnológicas de segurança, armazenamento, entre outras".

Nos próximos meses a jp.di acredita que assistiremos a um "contágio positivo" por parte das empresas mais avançadas no processo de compliance. A ASSOFT realça, porém, que "as micro e as pequenas empresas não estão de todo preparadas", por oposição às empresas de média e grande dimensão.
Apesar do aumento do número de sessões de esclarecimento realizadas nos últimos tempos, as dúvidas sobre o novo Regulamento persistem. Segundo Sónia Casaca, business unit manager de Security da Arrow ECS, continua a ser imperativo sensibilizar tanto as organizações como os colaboradores. "Dadas as ações que temos vindo a realizar, verificamos que grande parte das empresas não estão preparadas".
Segundo a SAP, as empresas "ou estão a ultimar a definição do plano de implementação do RGPD ou no início da implementação do plano que definiram para a sua organização", indica Ilda Freitas, pre-sales business architect. O fornecedor tem observado que as empresas mais sensibilizadas para o tema têm realizado três ações: a inventariação e catalogação dos dados pessoais; a definição de regras de acesso dos utilizadores às aplicações, "a fim de garantirem a adequada proteção no acesso e manuseamento dos dados pessoais"; e a criação de mecanismos de "mascaramento da informação em ecrãs", acrescenta, "para se assegurar a máxima privacidade relativamente aos dados mais sensíveis".

Mas existem até empresas, segundo José Fonseca, data management expert no SAS, que "admitem que só vão começar a funcionar de acordo com a nova regulamentação após 25 de maio, mesmo correndo risco de incorrerem em multas avultadas".
O atraso, defende, explica-se pela "falta de orçamento" e pela "inexistência de um responsável pela proteção de dados, de um Data Protection Officer".

Parceiros enquanto advisor da compliance

Nas empresas de menor dimensão, os Parceiros de Canal podem assumir esta posição. Uma das estatísticas mais recentes, e reveladoras, foi divulgada pela Sage no final de fevereiro, fruto de um inquérito que o fornecedor de software de gestão realizou junto dos seus clientes, em Portugal, e que indicava que 67% das PME nunca ouviram falar ou não estão familiarizadas com o novo Regulamento. Mais de metade admitiam mesmo não perceber inteiramente o impacto que teria no seu negócio e 36% não sabiam ou não estavam confiantes em ter os recursos necessários para se prepararem para a nova Regulamentação.

Os Parceiros, da área de software de gestão, mas não só, encontram por isso no RGPD uma importante janela de oportunidade para se aproximarem ainda mais do negócio dos seus clientes. "Os Parceiros são por excelência o advisor das empresas quando se trata de alterações legais, e esta mudança é mais uma oportunidade para ajudarem os seus clientes no que diz respeito ao software, mas mais do que isso para os alertarem para as mudanças nas tarefas do dia-a-dia", afirma Cristina Francisco, product marketing da Sage Portugal. O RGPD é também o pretexto ideal para que os Parceiros "acrescentem valor nos serviços que prestam e se afirmem como Parceiro de negócio 360º".
A este respeito, Ilda Freitas destaca que alguns Parceiros da SAP Portugal têm já disponível "o próprio serviço de avaliação dos processos de negócio e das aplicações existentes, através do qual obtêm um plano de recomendações para ajudar as empresas na sua jornada de conformidade". A jusante desta avaliação realizada pelos Parceiros, a SAP prevê que as maiores oportunidades residam na "implementação de produtos de portfólios de data base & data management e de governance risk & compliance".
Para a Microsoft Portugal, as maiores oportunidades estão no "desenvolvimento de projetos de avaliação

e implementação de requisitos de conformidade com o RGPD, nas suas diferentes dimensões – processuais, legais e tecnológicas", indica André Azevedo, diretor nacional de tecnologia. "Cada Parceiro, em função do seu ADN e das suas competências técnicas, estará habilitado a encontrar o seu espaço no mercado, optando por uma abordagem mais focada ou mais holística. Dada a premência da data, começa a ser fulcral não nos cingirmos ao diagnóstico, mas ser consequentes na implementação de medidas corretivas". A única opção "inviável", por parte dos Parceiros, "é considerar que não existem oportunidades com este Regulamento". André Azevedo sublinha que a tecnologia "pode desempenhar o papel de acelerador do caminho para a conformidade com o RGPD", e que, "quer por uma questão de celeridade quer por uma questão de custo, a opção cloud deve ser ponderada", tanto por clientes como por Parceiros.

Rui Duro, sales manager da Check Point para Portugal, entende que os Parceiros que souberem especializar-se "e dar uma resposta concreta às necessidades de proteção de dados das empresas serão os primeiros a beneficiar das oportunidades comerciais geradas pelo RGPD", lembrando que o facto de ser legalmente obrigatório "comunicar atempadamente, em 72 horas, as falhas de segurança" dá a oportunidade de "propor uma visão holística sobre a segurança das infraestruturas".

Aferir o risco

O RGPD coloca um enfoque particular na gestão do risco. Antes de serem tomadas medidas de cariz mais técnico ou até mesmo organizacional relacionadas com a proteção dos dados, é vital avaliar o risco que o processamento dos dados implica para os direitos individuais de cada cidadão.

A verdade é que todas as organizações, sem exeção, devem, como sublinha Rui Barata Ribeiro, security software sales da IBM Portugal, concentrar-se em reduzir a sua superfície de risco. "Destruindo, por exemplo, documentação e informação para lá dos prazos de retenção obrigatória – ter informação desatualizada, mas ainda assim relevante do ponto de vista de dados pessoais é uma componente de risco que pode ser mitigada", indica, chamando a atenção para a necessidade de "rever todos os acessos possíveis à informação existente", que deriva da aplicação do princípio de 'need to know'. Por outro lado, conhecer os fluxos de dados e da informação é imperativo e, defende, "a maioria das organizações conhece-os pouco". A implementação de tecnologias de monitorização, ao nível das aplicações, bases de dados, ambiente de rede ou dos utilizadores, serão uma forma de mitigar esta realidade. "Tecnologias de security information and events management,

database activity monitoring, network anomaly detection ou user behavious analytics poderão fazer parte das iniciativas lançáveis no curto prazo, mas que têm efeitos a médio/longo prazo", observa.

A necessidade de uma segurança end-to-end

Além da implementação de procedimentos de classificação da informação e de "uma boa política de análise de dados", Sónia Casaca, da Arrow ECS, chama a atenção para a importância de as organizações terem de "prevenir e detetar fugas de dados" e de "dotar-se de ferramentas de segurança que tenham a capacidade de ajudar a notificar as autoridades rapidamente e de forma correta, no caso de existir algum incumprimento".
O Regulamento, no âmbito da segurança, combina a obrigatoriedade de notificação de violações de dados em 72 horas – ao Regulador e aos titulares – com a exigência de tecnologia que previna as falhas de segurança, que as detete quando estas ocorrem e que auxilie na restauração dos sistemas após estas acontecerem.
Sem surpresas, a área da segurança será uma das maiores beneficiárias do RGPD. Rui Duro, da Check Point, lembra que este, por aumentar a responsabilidade das organizações, "representa uma boa oportunidade para que revejam as suas práticas em matéria de cibersegurança" e que tal irá "necessariamente gerar mais negócio". Até porque o novo enquadramento legal, defende, "tornará mais simples para os CIOs e CISOs a missão de justificar futuros investimentos em tecnologia e formação para a proteção e segurança dos dados, o que poderá ajudar a desbloquear negócios que, até então, estavam em suspenso".

Assim, existem dois tipos de soluções relevantes para a proteção da informação. Por um lado, a encriptação de dados, medida que é o único requisito tecnológico explícito no Regulamento, com ênfase para a capacidade de "saber exatamente quem acede e como acede a esses dados, se há consulta dos mesmos, manipulação ou alteração", explica Rui Duro, e também tecnologia para prevenção e mitigação de falhas de segurança, além da que possibilite "a pronta comunicação de incidentes".

A Sophos, por sua vez, realça que uma estratégia de proteção de dados adequada ao novo Regulamento tem de incluir "capacidades avançadas de encriptação e segurança antimalware", segundo Ricardo Maté, country manager da Sophos Iberia. Estas proteções devem estender-se aos dispositivos, às informações presentes nos discos e aos endpoints, como forma de "conter as principais causas de perda de dados". O country manager nota que, para deter ameaças à entrada, há que "bloquear os ataques de roubo de informação antes destes chegarem aos dispositivos dos utilizadores e cifrar ou negar acesso automaticamente às caixas de correio eletrónico que contenham arquivos confidenciais". Dado que o fator humano é, quase sempre, o elo mais fraco, Ricardo Maté sublinha que "é essencial que as empresas mantenham a informação que está na posse dos colaboradores segura e protegida, inclusivamente quando é partilhada por engano".
Ao alterar a forma como se lida com a informação, a nova diretiva "vai alterar as regras de gestão e armazenamento da informação", indica David Benito, responsável de Canal da Commvault, sendo essencial que cada empresa "conheça todos os seus dados, independentemente do local onde residam", o que significa "saber que dados não estruturados estão disponíveis, como ficheiros ou e-mails, que são mais problemáticos, uma vez que não são indexados, ao contrário dos bancos de dados", recorda. Adotar ferramentas que sejam capazes de "gerir e proteger as informações", independentemente de onde estejam armazenadas – on-premises, na nuvem, em ambientes virtualizados, em dispositivos do utilizador –, diz, "é a única maneira de garantir que muitos dos requisitos impostos pelo Regulamento possam ser cumpridos".