



MeetOn “Maturidade no RGPD @ Administração Local” CONCLUSÕES

01 de fevereiro de 2021

A APDSI começou 2021 com o MeetOn / Webinar “Maturidade no RGPD @ Administração Local”, no dia 27 de janeiro. Esta foi a primeira iniciativa do ano a decorrer online e que juntou cerca de 180 participantes.

Orlando Colaço, Co-Coordenador do Grupo de Missão da APDSI “RGPD Implementação” – o responsável por este MeetOn, foi o moderador da sessão e quem apresentou os oradores que deram os seus testemunhos sobre o estado atual do RGPD. O Grupo pretende estabelecer um modelo de rating de maturidade na proteção de dados e, com essa finalidade, construiu um questionário disponibilizado no sítio na web da APDSI que é detalhado mais à frente neste documento.

Os oradores do evento foram:

- **Alexandre de Sousa Pinheiro**, Doutor em Direito e Professor universitário na Universidade Europeia e Diretor da ASP - Consultoria e Formação, é também

advogado. Foi vogal da CNPD – Comissão Nacional de Proteção de Dados e apresentou uma tese de doutoramento sobre Privacidade e Proteção de Dados. É coordenador do Comentário sobre o RGPD publicado em 2018. É participante habitual em conferências sobre proteção de dados tendo publicado mais de 40 títulos.

- **Luis Neto Galvão**, é sócio da SRS Advogados, sendo responsável pela prática de Proteção de Dados e co-responsável pelo departamento de Telecomunicações, media e tecnologia. É licenciado em Direito pela Universidade Católica Portuguesa de Lisboa, tem um mestrado em estudos europeus, política e administração pelo colégio da Europa/Bélgica. Entre outras funções, foi consultor do Conselho da Europa e perito na Comissão Europeia na área da proteção de dados pessoais.
- **Filipe Barata Pereira**, Head of Digital Lead & Protection na LCG Consulting; é responsável pela proteção de dados e segurança da informação e tem acompanhado diversas organizações, incluindo algumas autarquias no seu caminho para a conformidade.
- **Cristina Máximo dos Santos**, Data Protection Officer (DPO) da Caixa Geral de Depósitos; é vogal da direção da Associação de Encarregados de Proteção de Dados. Tem uma longa carreira no setor bancário, nos departamentos de compliance e assuntos jurídicos da CGD e do Caixa-Banco de Investimento. Foi assessora do gabinete do Presidente do Tribunal Constitucional e, anteriormente, do respetivo Gabinete de Juízes. Leciona em várias instituições de ensino superior e é autora de várias publicações nas áreas da sua especialidade.
- **Wilson Lucas**, Coordenador do Grupo de Missão da APDSI “RGPD Implementação”. É DPO no Instituto de Informática, IP.

Alexandre de Sousa Pinheiro falou sobre as expectativas que existem à volta do RGPD para 2021. O Regulamento é aplicado a todos os indivíduos na União Europeia e no Espaço Económico Europeu.

De que modo é que o RGPD tem sido menos cumprido ou tem havido mais aplicação de sanções? Este foi o ponto de partida para a apresentação do professor que nota que é essencialmente sobre a segurança da informação e medidas organizativas que tem havido um maior acervo de sanções por parte das autoridades nacionais e coimas aplicadas a grandes tratadores de informação frequentemente relacionadas com o consentimento, o que também tem inspirados mais cuidados quer por parte de entidades públicas, quer por parte de entidades privadas.

As empresas de Big Tech também foram alvo de aplicação de sanções por autoridades de controlo nacionais, mas nenhuma chegou a decisão pelo Tribunal de Justiça da União Europeia. O que se tem verificado é que o incumprimento do regulamento se baseia nas regras de minimização do tratamento de dados e no incumprimento de regras sobre consentimento (artigo 5.º).

O professor nota que há uma expectativa muito forte para 2021 relacionada com modo como as empresas vão reagir ao acórdão C-311/18 - Schrems II sobre a declaração de invalidade do Privacy Shield e afetando, essencialmente, a transferência de dados para os Estados Unidos. O Acórdão vai levantar questões na transmissão de dados para outros Estados que não apenas os Estados Unidos. “Vamos ter um conjunto de necessidades de articulação para 2021 com uma dimensão muito significativa”, salientou.

Temos ainda matéria relativa à proteção de dados no ambiente das comunicações eletrónicas. E com Portugal na Presidência do Conselho da União Europeia “é expectável que exista intervenção do Estado Português no sentido de alterar o legado da presidência que foi deixado pela Alemanha”.

Na fase de perguntas e respostas por parte dos participantes no MeetOn, o professor Referiu que por vezes na legislação interna encontramos atos que podem ser considerados incompatíveis com o RGPD, como, por exemplo, portarias na área da contratação pública que versam sobre a conservação de dados pessoais.

Luis Neto Galvão, tem uma perspetiva sobre a Proteção de Dados para 2021 que engloba múltiplos desafios, devido à pandemia que, acredita, vai manter-se sem exceções ao longo deste ano, continuando a levantar questões como o trabalho

remoto e a sua monitorização, bem como vários outros problemas que vão continuar a surgir no contexto laboral e a exigir uma resposta no que respeita à proteção de dados.

2021 será, para o advogado, mais desafiante com uma crescente exigência por parte dos cidadãos em matéria de proteção de dados, ajudada pela implementação do 5G: “Estamos na fase de leilão para atribuição de espectro e vamos, provavelmente, ter um novo operador”. 5G é sinónimo de Internet das coisas e de uma nova fase na qual os dados pessoais vão explodir com o desenvolvimento dos carros autónomos, *weareables* e domótica, logo é um enorme desafio para a proteção de dados.

As grandes tecnológicas vão continuar a ter uma expansão muito significativa enfrentando, a par disso, uma maior exigência por parte dos titulares dos dados. Exemplo dessa crescente exigência no que concerne à proteção de dados verificou-se muito recentemente quando o WhatsApp perdeu alguns dos seus utilizadores devido a uma estratégia de atualização dos seus termos e condições e política de privacidade que Luís Neto Galvão considerou “pouco inteligente”.

Ainda no que toca ao poder das grandes tecnológicas, está em curso uma resposta das autoridades europeias à enorme quantidade de dados gerados por aquelas empresas baseada no direito da concorrência. “A Comissão Europeia, através do Digital Markets Act, procura aplicar uma às tecnológicas uma lógica de silos de modo que permitir a separação entre dados gerados nas diversas áreas de negócio que me parece uma abordagem interessante na proteção de dados das pessoas singulares”, aponta.

Até 2023 vamos continuar a ter novas leis de proteção de dados e 65% da população mundial vai estar abrangida por elas, sendo “importante para nós que existam leis que nos deem garantias de que os nossos dados estão protegidos quando vão para fora do espaço europeu. Porque efetivamente circulam por todo o lado”, resumiu Luís Neto Galvão.

Por seu turno, o Acordo Schrems II veio impor uma muito maior responsabilização de todas as entidades que exportam dados pessoais para fora da União Europeia

Sobre o Brexit, foi feito um acordo de última hora que nos vai permitir continuar a exportar dados até ao final deste semestre, mas depois disso vai gerar-se uma situação

particularmente desafiante, dado que, ao dia de hoje, ainda não se sabe se haverá uma decisão de adequação da Comissão Europeia. 2021 também será o ano de aprovação das novas cláusulas *standard* da União Europeia relativas à legitimação da exportação de dados.

A Presidência Portuguesa apresentou uma proposta de regulamento de *e-privacy*, mas, provavelmente, seis meses não vão chegar para completar o processo decisório europeu. Fica, todavia, um impulso importante a esta lei especial no contexto das comunicações eletrónicas e o apelo à necessidade urgente de cooperação entre as várias autoridades europeias de proteção de dados: “Grandes tecnológicas concentram-se apenas nalguns Estados Membros, daí ser importante que haja colaboração entre todas, incluindo a nossa CNPD”.

No nosso Governo, em termos de segurança, Luís Neto Galvão considera que falta ainda uma portaria que regule certos aspetos do tratamento de dados na Saúde e que ainda não há qualquer pista sobre quando surgirá.

Filipe Barata Pereira abordou neste MeetOn os modelos de maturidade que têm como vantagem estabelecer uma análise da adoção do RGPD na Administração Pública.

Quanto às expectativas para 2021, Filipe Barata Pereira considera que a Transição Energética, que à partida não parece relacionada com a proteção de dados, vai trazer uma carga adicional às autarquias que estão a iniciar um caminho rumo às cidades inteligentes, pois obriga a uma transformação na forma como as próprias organizações vão pensar o modelo de relacionamento com os cidadãos.

Quanto aos modelos de maturidade em relação à privacidade, estes não são em si mesmo um objetivo final, mas permitem entender o caminho que está a ser feito para a conformidade. Há vários níveis e modelos de maturidade de uma organização que estão diretamente relacionados com a capacidade que a mesma tem de medir e estabelecer uma melhoria contínua nos seus objetivos e, neste caso em particular, em termos de conformidade e privacidade nos seus processos.

Entender o quanto não se sabe é um sinal de maturidade, tal como aceitar que se tem mais a ganhar a ouvir que a falar, respeitar o outro, e não assumir um lado pessoal ficando facilmente ofendido.

Organizações e autarquias não são alheias à necessidade de recolher *feedback* dos munícipes, bem como de entender como a mensagem deve ser passada em termos comunicacionais. Tem de existir uma relação madura de relacionamento entre todos os envolvidos e os municípios têm de analisar muito bem como as mensagens estão a ser transmitidas, de modo a que o cumprimento das normas também os diferencie e seja visto como mais um modelo de qualidade e confiança por parte dos munícipes.

O primeiro confronto das autarquias com o RGPD é com os riscos porque “no aferir dos riscos temos noção das vulnerabilidades a que estamos sujeitos. O dano reputacional pode até ser mais danoso do que determinada coima aplicada”, frisa Filipe Barata Pereira, esclarecendo que a necessidade de reajuste surge acompanhada de uma necessidade de adaptação da própria organização.

Se não olharmos para a proteção de dados apenas como uma legislação que deve ser aplicada, mas sim como algo transversal à organização e visível na forma como todos se comportam relativamente aos direitos dos titulares, parte do percurso para se atingir a maturidade estará feito.

Neste percurso, o primeiro estágio é de não consciência da importância e necessidade de respeitar o utente enquanto titular dos dados. Muitas vezes não há uma pessoa que desempenhe esse papel de controlo na organização e frequentemente é atribuída a tarefa sem disponibilizar as condições necessárias, e sem uma reflexão da importância da conformidade nos processos.

Num nível de maior maturidade, a organização aprende com os seus erros. Estar em conformidade pode resultar até num voto de confiança dos munícipes que têm consciência da importância da privacidade e observam um procedimento orgânico que trespassa a organização e em que todos os elementos percebem o respeito que implica a proteção de dados. Tudo isto pode ser um fator de diferenciação, destaca Filipe Barata Pereira.

Para as cidades do futuro e a transformação inerente, a proteção de dados não pode ser vista como um entrave à inovação. A clareza do que é feito e os seus benefícios devem, isso sim, ser frontalmente comunicadas ao munícipe.

Os territórios inteligentes vão implicar a captação de um elevado volume de informação, com a dificuldade em cumprir todas as regras do RGPD e consentimento a surgir no horizonte como uma forte possibilidade. A lei é comum a todos os municípios, mas em todos eles verifica-se um grande ímpeto no tratamento de dados pessoais – sensíveis e comuns – e deve procurar-se uma maior sensibilização de quem trabalha estes dados.

Também no momento de perguntas e respostas, Filipe Barata Pereira respondeu sobre como o modelo de maturidade de *compliance* ao RGPD se aplica a uma comunidade intermunicipal. É possível tipificar documentos entre autarquias, mas cada uma terá uma especificidade que carece de análise granular específica. Parte do programa de proteção de dados pode ser partilhado entre municípios, mas haverá sempre a necessidade de adequação à conformidade, realizada especificamente por cada município.

Genericamente, mesmo dentro de um grupo com regras semelhantes, existem especificidades de negócio distintas que acabam por intervir e promover algum risco, esclareceu.

Cristina Máximo dos Santos, Data Protection Officer (DPO) da Caixa Geral de Depósitos, destacou vários desafios na implementação do RGPD desde 2018; inicialmente, para se atingirem valores mínimos de conformidade; em 2019, com a publicação da Lei nacional de proteção de dados que consagrou requisitos regulatórios complementares sobre proteção de dados, não esquecendo as duas importantes deliberações da CNPD relativas à desaplicação de algumas normas da Lei nacional (Deliberação 2019/494) e à dispensa de aplicação de coimas às entidades públicas no âmbito de processos de contraordenação concretamente instaurados (Deliberação 2019/495). Os desafios do RGPD em 2020 e 2021 centram-se essencialmente no âmbito da crise pandémica que atravessamos (prestação de serviços à distância, regime de teletrabalho, leitura da temperatura corporal de trabalhadores e utentes de

serviços públicos, dados de saúde e prevenção de propagação da doença). Destacou que, em agosto de 2022, termina o prazo de três anos durante o qual - mediante pedido fundamentado à CNPD e decisão, também fundamentada, desta autoridade de controlo - as entidades públicas estão dispensadas da aplicação de coimas por violação de princípios e regras do RGPD.

“Esperemos que 2021 seja o derradeiro ano de pandemia, mas ainda há alguns desafios que obrigam a uma dupla reflexão à prestação de serviços à distância, não só aos munícipes, mas às empresas como um todo que adotaram o trabalho à distância para continuarem a entregar produtos e serviços aos seus clientes”, afirma Cristina Máximo dos Santos.

O Regulamento Geral sobre a Proteção de Dados assenta em três fatores – jurídico, tecnológico e processos internos, os quais exigem e implicam conhecer a organização.

Como DPO e co-criadora do modelo de maturidade, assinalou como quarto fator do RGPD, a gestão da mudança associada à mudança de paradigma para organizações e as pessoas que o RGPD introduziu. Para a conformidade das organizações com o RGPD, o contributo individual de todos os membros da organização é decisivo, mas a pedra de toque está no compromisso da gestão de topo com a conformidade, para se conseguir uma mudança de mentalidade e uma adesão plena aos princípios da proteção de dados: uma cultura organizacional de proteção de dados.

Como se consegue a conformidade e as tão desejadas vantagens para as organizações? Do ponto de vista interno de uma organização, a conformidade assenta no princípio da responsabilização. É muito importante sublinhar que mesmo havendo prestadores de serviços e DPO externo (vulgarmente, “DPO as a service”), a responsabilidade é sempre da organização. Não é o DPO que responde perante as autoridades de controlo e titulares dos dados. O DPO informa e aconselha o responsável pelo tratamento e os seus colaboradores, sendo ponto de contacto com a autoridade de controlo. O RGPD consagra a responsabilidade das organizações, enquanto responsáveis pelo tratamento de dados. A designação de DPO é de enorme importância e uma mais valia para o aconselhamento quanto ao cumprimento deste

princípio da responsabilidade das organizações, mesmo nas situações em que tal designação não resulta de uma obrigação legal.

Atingir um patamar superior de conformidade pode não ser fácil, mas é mais exigente ainda a organização manter-se nesse patamar superior. As organizações devem, todavia, entender que a conformidade é uma melhoria contínua, integrando um “ciclo virtuoso”, que exige planejar, fazer, verificar, agir e validar/avaliar o que se fez.

Sobre a necessidade de medir o grau de conformidade com o RGPD por parte de uma organização, e destacando que a fiabilidade do resultado apurado no modelo de maturidade depende da qualidade e veracidade da informação fornecida, Cristina Máximo dos Santos finalizou a sua intervenção, resumindo as vantagens dos métodos de maturidade:

- São um instrumento de navegação para se chegar à meta da conformidade;
- Ajudam a conhecer a organização (pontos fortes e menos fortes) e as pessoas;
- Fornecem alertas e indicadores;
- Facilitam o diagnóstico;
- Indicam onde intervir e estabelecer prioridades;
- Ajudam a definir e implementar planos de ação e revisão;
- Apoiam a avaliação do que se fez, do que falta fazer e dos respetivos resultados;
- Auxiliam o governo da organização.

“É preciso um rigoroso exercício de auto-avaliação e perceber as nossas fraquezas e forças, a par de ajuda especializada para melhorar”, respondeu Cristina Máximo dos Santos, quando questionada sobre o que fazer quando determinada organização deteta fragilidades na sua atuação.

Wilson Lucas, Coordenador do Grupo de Missão da APDSI “RGPD Implementação” apresentou, precisamente, o modelo de maturidade do RGPD com uma demonstração prática de um questionário que produz como resultado um rating, ajudando as organizações a fazer um exercício contínuo de melhoria.

O RGPD tem que fazer parte da cultura da organização e o objetivo tem de passar a ser *business as usual* – encarar a privacidade como um reflexo e não como um incómodo.

A ideia de lançar este questionário surgiu em 2019, numa análise ao rating associado à cibersegurança, de onde veio a intenção de avaliar a postura das organizações face ao RGPD do ponto de vista jurídico, tecnológico, processual e comportamental.

As respostas dadas são da responsabilidade da organização que a utiliza. A fiabilidade do modelo tem a ver com a fiabilidade das respostas ao questionário que pretendem demonstrar que a mudança que tem de ser incentivada e gerida, devendo ir além do mero cumprimento do RGPD.

Todos os temas ou requisitos regulatórios estão contemplados neste questionário que está disponível na página oficial da APDSI, através de um link associado ao Grupo de Missão (<https://apdsi.pt/grupo/rgpd-implementacao/>). Este questionário aplica-se a entidades da Administração Pública Local.

SOBRE A APDSI

Criada em 2001, a Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI) tem por objetivo a promoção e desenvolvimento da transformação e inclusão digital em Portugal, reunindo com este interesse comum profissionais, académicos, empresas, organismos públicos e cidadãos em geral.

Na linha destes propósitos a APDSI tem vindo a desenvolver diversas atividades em torno de causas tecnológicas e sociais, que se traduzem num conjunto de eventos, recomendações e estudos realizados por grupos de trabalho multidisciplinares em diversas áreas de intervenção, como a Segurança, os Serviços Públicos Digitais, a Saúde, a Cidadania e Inovação Social, o Território Inteligente, a Governação das TIC, a Inteligência Digital, a Política Digital e Governança, os Futuros da Sociedade da Informação e as Competências digitais.

Em todos estes trabalhos a APDSI procura identificar as tendências de evolução e também as interações entre as tecnologias e outras dimensões sociais e económicas, contribuindo com uma visão mais aberta para a discussão e tendo como meta a eficaz perceção e implementação destes conceitos na Sociedade Portuguesa. A APDSI tem o Estatuto de Utilidade Pública e foi em 2008 reconhecida como ONGD.

ASSOCIE-SE

URL | www.apdsi.pt

email | secretariado@apdsi.pt

APDSI

ASSOCIAÇÃO
PARA A PROMOÇÃO E DESENVOLVIMENTO
DA SOCIEDADE DA INFORMAÇÃO



Associação de Utilidade Pública
ONG – Organização Não Governamental

Rua Alexandre Cabral, 2C – Loja A
1600-803 Lisboa – Portugal
URL: www.apdsi.pt

Tel.: (+351) 217 510 762
Fax: (+351) 217 570 516
E-mail: secretariado@apdsi.pt

Apoio



Patrocínio

ORACLE

Patrocinadores Globais da APDSI

accenture



Google