Aurélio Maia, diretor de serviços de consultoria na INTEGRITY S.A., foi o convidado da edição de 22 de setembro do It's Time To Talk About, e começou por justificar a premência da discussão sobre a ISO 27701 com o facto de **não haver um dia sem que haja uma violação de dados pessoais, seja em organizações, operadores de telecomunicações ou até nalgum serviço público**. Isso faz com que as organizações tenham uma preocupação acrescida sobre como proteger a informação pessoal.

Por outro lado, também nós, enquanto cidadãos, estamos cada vez mais consciencializados da utilização dos nossos dados e vamos ficando mais preocupados e exigentes.

A própria União Europeia através de regulamentação transnacional e a legislação nacional estão a impor um conjunto de obrigações que fazem com que as organizações tenham de ter cuidados crescentes na proteção dos dados pessoais e na gestão da privacidade.

Assim, a ISO 27701 surgiu, tentando antecipar-se e apoiar no alinhamento com este enquadramento regulatório, preparando, previamente, uma série de normas sobre proteção de dados pessoais que começaram a ser implementadas desde 2018 e tinham por objetivo levar à sua apresentação em janeiro de 2020. Este calendário foi antecipado e a norma acabou por ser publicada até um pouco antes do tempo previsto: a 6 de agosto de 2019

Baseada na ISO 27001, enquanto membro da respetiva "família", a 27701 é orientada para a privacidade, foca-se em novos requisitos de controlo assentes nesta temática, pode ser usada como instrumento da demonstração da conformidade e aplica-se nomeadamente às organizações nos seus papéis de responsável pelo tratamento de dados e/ou de subcontratante; são as novas figuras que surgem no âmbito da proteção de dados pessoais. De alguma forma, está associada à ISO 27001 que tem de estar já certificada na organização, ou ser obtida em simultâneo, ou seja, se as organizações optarem pela certificação ISO 27701, tal exige também uma certificação ISO 27001. Posteriormente, acrescenta vários controlos que devem ser endereçados quer pelos responsáveis pelo tratamento quer pelos subcontratantes. **É, resumidamente, a extensão para a proteção da informação pessoal e privada.**

Esta norma introduz dois novos papéis que derivam do RGPD e que devem ter sempre em consideração a legislação nacional: o responsável pelo tratamento de dados e o subcontratante.

A estrutura da ISO 27701

Esta norma segue a estrutura *standard* de todas as ISO: tem um capítulo dedicado aos requisitos que a norma impõe às organizações e tem um conjunto de anexos onde se encontram os novos controlos que devem ser seguidos no âmbito da adoção desta norma.

Para além de novos controlos, a diferença está em dois capítulos que endereçam novos requisitos à 27001 – contexto da organização (o seu papel no tratamento de dados pessoais) e planeamento.

Esta norma exige que, embora se possa utilizar a mesma metodologia associada à gestão de risco patente na ISO 27001, se acrescente, agora, a identificação de riscos relacionados com a privacidade. Ao fazê-lo terão de ser mapeados os objetivos de controlo e a aplicabilidade dos mesmos relativamente à mitigação dos riscos da privacidade.

São requisitos específicos da nova ISO 27701:

- Atualizar políticas para incluir um compromisso de cumprimento com os regulamentos relevantes de dados pessoais e com acordos contratuais com clientes e terceiros;

- Designar um ponto de contacto para consultas sobre dados pessoais;

- Responsabilizar uma pessoa ou equipa pela implementação e manutenção de um programa de governança e privacidade para garantir a conformidade com os regulamentos;

- Garantir que toda a equipa relevante seja devidamente formada sobre como é feito o tratamento de dados pessoais;

- Considerar especificamente dados pessoais em sistemas de classificação de informação.

Todas as pessoas de determinada organização que tenham acesso aos dados pessoais têm que ser bem conhecidas e estar devidamente registadas pela organização.

Para se implementar esta ISO a organização tem de saber, desde logo, em que ponto está relativamente aos requisitos e controlos para a proteção da privacidade e fazer uma análise prévia, saber onde está essa informação de dados pessoais e qual o fluxo na organização, o papel do responsável pela proteção dos dados, dotar a sua estrutura documental de formação e operacionalizar todo o acervo que possui em matéria documental.

A conformidade da ISO 27701 com o RGPD

A criação de esquemas de certificação foi contemplada para aumentar a transparência e a conformidade com o RGPD mas ainda não foram determinados quais os sistemas de certificação que vão avançar. Ainda assim, **a norma apresenta-se como uma das que trará maior credibilidade e relevância por ser um *standard* internacional reconhecido.**

Deste modo, a sua adoção trará benefícios para as organizações como:

- A criação de evidências documentais de como é realizado o processamento de dados pessoais;

- Pode vir a ser utilizada como método de certificação credenciado para efeitos de RGPD;

- Ajuda a criar confiança nas práticas de gestão de dados pessoais;

- Facilita acordos com parceiros de negócios.

Perguntas e respostas

- Na reta final da sessão de IT2TA surgiram questões como a **validade e prazos de renovação** da ISO 27701 e a possibilidade de renovação em simultâneo com a 27001. A resposta é "sim" e durante os três anos é feita uma auditoria de acompanhamento.

- Havendo um *deficit* de consciencialização para esta matéria, **como se pode alavancar a consciência dos papéis de cada um de nós?** Por duas vias: a ISO 27701 confere credibilidade à temática e a própria norma segue as orientações do RGPD.

- Como se pode formar uma equipa para lidar com esta norma? Através de um programa em segurança da informação e proteção de dados e estender essas formações já existentes à questão da privacidade.

- **A certificação por entidades não europeias garante automaticamente a sua conformidade com o RGPD? Poderá legitimar transferências transfronteiriças em dados pessoais?** Não; o próprio RGPD ainda não "certificou o sistema de certificação ISO".

- **Que impulso este referencial pode dar aos encarregados de proteção de dados?** A capacidade de estruturar as temáticas relevantes por via de uma estrutura ISO; ao adotar esta norma nenhum requisito fica esquecido. Assim, o DPO tem aqui uma *checklist* ideal.

- **Há cláusulas que podem ser excluídas?** Nos anexos com requisitos (A e B), para os controlos não aplicáveis à organização, como p.ex. o das transferências internacionais, é possível; nas cláusulas de requisitos, não.

- A Administração Pública pode ganhar uma **nova motivação** nesta fase para se preocupar com estes temas? Sim, porque esta norma vem facilitar a estruturação do trabalho.

- **Qual a recetividade a estes temas por parte das empresas**, passada a "febre" de implementação inicial? "Não sinto que existam muitas implementações completas endereçando todos os aspetos relevantes do que é ser conforme com o RGPD", concluiu Aurélio Maia.

O próximo evento da itSMF Portugal é o HOT – Hands on Talk, a 20 de outubro, intitulado "**5in1: Construção e certificação de um sistema de gestão – da qualidade, serviços e segurança da informação à proteção de dados**".