**Reflexão sobre a Secção 6.15 do *draft* ISSO 27552**

De acordo com o *draft* do ISO 27552, secção 6.15 (*Compliance*), qualquer organização cujas atividades envolvam de alguma forma a manipulação de dados pessoais identificáveis (*Personally Identifiable Information* ou *PII*) deve respeitar, e agir em conformidade com, três pontos distintos.

O primeiro ponto está relacionado com a proteção de registos de dados. Cada organização deve manter cópias das suas políticas de segurança e privacidade durante um período de tempo específico, que deve estar documentado, incluindo versões anteriores dessas políticas.

A existência obrigatória de documentos que especifiquem pormenorizadamente como cada organização lida com a segurança e privacidade de todos os dados pessoais resulta na maior facilidade de supervisão por uma autoridade competente que investigue a organização no sentido de averiguar se esta está a agir em conformidade com as normas estabelecidas.

Na produção de *software,* como consequência, deverá haver a especial atenção acerca de quais os protocolos especificados pela organização, tentando garantir que os algoritmos que processam e guardam informação pessoal os seguem com rigor. Esta nova necessidade de rigor de documentação e produção de *software* poderão implicar um desafio considerável para organizações que não possuam os cuidados necessários quando manipulam dados pessoais, uma vez que poderá, em último caso, resultar na necessidade de reescrever todo o código responsável pelo processamento dos mesmos (e essa tarefa pode nem sequer ser viável, tanto do ponto de vista financeiro como do ponto de vista mais prático).

O segundo ponto está relacionado com a transparência que deve existir entre uma organização e cada um dos seus clientes relativamente às suas políticas de segurança e privacidade. Sempre que a solicitação de informações relativas à manipulação ou manutenção de dados pessoais por um cliente é impraticável ou pode resultar em riscos de segurança, a organização em questão deve disponibilizar provas independentes, como auditorias levadas a cabo por terceiros, de que as políticas de segurança e privacidade estão a ser corretamente aplicadas. Essas provas devem ser disponibilizadas antes e durante todo o período do contrato.

Uma vez que a necessidade de apresentação de provas da correta aplicação das políticas da organização implicam, de uma forma ou outra, que estas sejam verificadas por alguma entidade terceira, as implicações no que toca ao desenvolvimento de *software* coincidem com as especificadas no primeiro ponto.

O terceiro ponto é referente à monitorização das políticas de manipulação de dados pessoais feita pela própria organização.

Esta deve ser capaz de monitorizar constantemente a sua atividade de forma a garantir que não é feito qualquer processamento de dados indevido e deve também levar a cabo testes de vulnerabilidades dos seus sistemas.

A nível de produção de *software*, a constante monitorização dos seus próprios sistemas e protocolos pode implicar um investimento considerável a nível de gestão de segurança (uma empresa poderá não ter recursos suficientes para fazer testes de segurança adequados, pelo que poderá recorrer a serviços externos). Mesmo que uma organização possua recursos internos para gerir toda a infraestrutura de segurança, continua a poder ser necessário dedicar recursos única e exclusivamente a fazer auditorias ao sistema de segurança, o que poderá ser impraticável para organizações mais pequenas que não possuam os recursos necessários.