A Gestão da Privacidade nas Organizações

O papel do standard ISO/IEC 27701 na garantia de conformidade com o Regulamento Geral de Proteção de Dados

Catarina Conde Nogueira

Dissertação para obtenção do Grau de Mestre em

Segurança de Informação e Direito no Ciberespaço

Orientador: Capitão de Fragata EN-MEC Gonçalo Baptista de Sousa
Co-orientador: Prof. Doutor Carlos Manuel Costa Lourenço Caleiro

Júri

Presidente: Prof. Doutor Paulo Alexandre Carreira Mateus
Vogais: Capitão de Fragata EN-MEC Gonçalo Baptista de Sousa
Prof. Doutor Anacleto Cortez Correia

9 de dezembro de 2022

Agradecimentos

Em primeiro lugar, gostaria de agradecer ao Engenheiro Hélder Gonçalves por todo o apoio prestado ao longo dos dois anos letivos do Mestrado em Segurança de Informação e Direito no Ciberespaço e pelo incentivo de prosseguir com os meus objetivos numa área que estimo. Sobretudo, agradeço-lhe a constante partilha de conhecimentos e conselhos, os quais me orientaram na realização deste trabalho, mas mais importante ainda mudaram o meu rumo a nível profissional, proporcionando-me a oportunidade de trabalhar numa área desafiante e em constante evolução. Estou eternamente grata por tê-lo como meu mentor e sei que hoje sou uma profissional mais competente e informada graças à sua orientação.

Gostaria também de agradecer ao Professor e Capitão de Fragata EN-MEC Gonçalo Baptista de Sousa, orientador da minha dissertação, a disponibilidade para qualquer esclarecimento e celeridade nas respostas a cada interação, tendo partilhado o seu saber e experiência, apoiando *step by step* o desenvolvimento do presente trabalho.

Agradeço ao Professor Doutor Carlos Caleiro, coordenador do Mestrado, por me ter concedido a oportunidade de realizar esta dissertação sob a sua co-orientação.

Como não poderia deixar de ser, queria também agradecer à Celfocus, S.A., empresa onde trabalho desde 2019, por me ter dado a oportunidade de desenvolver parte deste trabalho *in loco*, perante uma situação real do sector das tecnologias da informação, o que, sem dúvida, enriqueceu este trabalho, mas também por me proporcionar um ambiente de trabalho propício ao desenvolvimento das minhas competências a vários níveis.

Queria especialmente agradecer aos meus colegas Luís Anselmo e Daniel Caldeira, a partilha dos seus conhecimentos, que muito me ajudaram durante o Mestrado e contribuíram para a construção deste trabalho, mas também pelo companheirismo e boa disposição sempre presentes, sem os quais esta etapa teria sido muito mais difícil de ultrapassar.

Um agradecimento gigante aos meus pais por me terem incutido o valor do trabalho e incentivado a minha formação académica, tendo apoiado desde o primeiro minuto o atingimento de mais um objetivo – concluir o segundo Mestrado. Obrigada por todo o apoio, pela força e compreensão incansáveis e, acima de tudo, por me tornarem na mulher que sou hoje. Sem vocês, nada disto seria possível. Agradeço também com muito carinho à minha tia Carla, ao meu primo Carlos e ao meu namorado Pedro por estarem sempre presentes, por todo apoio e paciência demonstrados, e por me animarem sempre que a ansiedade levava a melhor de mim.

Por último, um agradecimento muito especial à minha mãe que, por estar sempre aqui, foi a minha ajuda mais preciosa durante esta etapa. Obrigada por seres a mulher que és, e por me mostrares que “eu sou capaz”.

Resumo

A era digital em que vivemos potencia o crescente volume de dados pessoais processados, resultando num risco acrescido para as organizações e numa ameaça para a Privacidade dos titulares, no geral.

A garantia de um tratamento seguro continua a representar um desafio para as organizações, as quais têm de atuar em conformidade com os requisitos legais e regulamentares nesta matéria, com destaque para o Regulamento Geral de Proteção de Dados (RGPD), que veio introduzir um conjunto de imposições relativas ao armazenamento, processamento e recolha de dados pessoais com o intuito de reivindicar o direito fundamental à proteção destes dados.

As organizações, a fim de se adaptarem às exigências deste Regulamento e evitar as penalizações previstas, tiveram de investir na implementação de práticas em consonância com os seus requisitos, tendo sido confrontadas com a necessidade de interpretação de um documento jurídico que não especifica, na prática, quais as soluções a implementar.

A norma ISO/IEC 27701:2019 fornece *guidance* para o estabelecimento de um Sistema de Gestão da Privacidade, alinhado com a ISO/IEC 27001:2013 para a gestão da Segurança da Informação, cujos requisitos de proteção de dados estão muito em linha com os do RGPD.

De forma a compreender qual o papel da ISO/IEC 27701:2019 na garantia de conformidade com os requisitos do RGPD, realizou-se uma análise comparativa entre os requisitos de ambos os documentos, que foi comprovada num caso de estudo real na empresa Celfocus, S.A, cujo Sistema de Gestão da Privacidade obteve, recentemente, a certificação na norma em estudo.

Palavras-chave: Sistema de Gestão da Privacidade; ISO/IEC 27701:2019; Segurança da Informação; Proteção de Dados; RGPD.

Abstract

The digital era in which we live enhances a continuous increase in the volume of personal data processed, resulting in a higher risk for organisations and in a threat to the Privacy of data subjects in general.

Ensure a secure personal data processing is still a challenge for organisations that must act in accordance with legal and regulatory requirements in this matter, especially the General Data Protection Regulation (GDPR), which introduced a set of requirements to store, process and collect personal data aiming to claim the fundamental right of data protection.

In order to adapt to the requirements of this Regulation, and avoid the defined penalties, organisations had to invest in implementing practices in line with its demands and have been faced with the need to interpret a legal document that does not specify, in practice, which solutions should be implemented.

The ISO/IEC 27701:2019 standard provides guidance for the establishment of a Privacy Management System, aligned with ISO/IEC 27001:2013 for Information Security management, whose data protection requirements are much in line with those established in the GDPR.

To understand the role of ISO/IEC 27701:2019 in ensuring compliance with GDPR's requirements, a comparative analysis was carried out between the requirements of both documents, which was proven in a real case study in the company Celfocus, S.A, whose Privacy Management System has recently obtained certification in the standard in study.

Keywords: Privacy Management System; ISO/IEC 27701:2019; Information Security; Data Protection; GDPR.

Índice

Lista de Tabelas

Lista de Figuras

Lista de Abreviaturas

CCPA - California Consumer Privacy Act

CE – Comissão Europeia

CNCS - Centro Nacional de Cibersegurança

CNPD – Comissão Nacional de Proteção de Dados

DPA - Data Processing Agreement

DPO - Data Protection Officer

EDPB - European Data Protection Board

EEE – Espaço Económico Europeu

EDP – Encarregado de Proteção de Dados

IEC - International Electrotechnical Commission

ISO - International Organisation for Standardization

LGPD - Lei Geral de Proteção de Dados Pessoais

PDCA - Plan-Do-Check-Act

PIAs - Privacy Impact Assessments

PIMS – Privacy Information Management System

RGPD – Regulamento Geral de Proteção de Dados

SCC - Standard Contratual Clauses

SGP – Sistema de Gestão da Privacidade

SGSI - Sistema de Gestão da Segurança da Informação

SoA - Statement of Aplicability

UE - União Europeia

1. Introdução

1.1. Breve enquadramento

A garantia de Privacidade é o processo de salvaguardar informação importante contra corrupção, comprometimento ou perda, cuja adequada gestão para as organizações tem grande importância, especialmente tendo em conta a quantidade de dados gerados e armazenados que continua a crescer a um ritmo sem precedentes[1]. O desenvolvimento de novas ferramentas e técnicas, tais como *Big Data*[2], *Data Mining*[3] e *Machine Learning*[4], assim como a computação em *cloud*[5] e o conceito da *Internet of Things*[6] (IoT), vieram alavancar o consumo de dados pessoais para um patamar completamente novo e revolucionar os modelos de negócio[7]. Esta revolução digital e o crescente processamento de dados pessoais pelas organizações tem riscos associados, nomeadamente tornando-as mais vulneráveis a violações de privacidade, uma vez que o tratamento de dados em larga escala se encontra facilitado, o que pode atrair as organizações a recolherem mais dados que os necessários, levando, eventualmente, ao seu uso indevido[8].

A entrada em vigor do Regulamento Geral para a Proteção de Dados (RGPD), mais precisamente a 25 de maio de 2018, veio contribuir para a alteração da mentalidade sobre a forma como as organizações recolhem, processam e armazenam os dados pessoais de cidadãos europeus, as quais passaram a ter de cumprir obrigatoriamente com os seus requisitos[9]. O RGPD veio substituir a Diretiva 95/46/CE[10], a qual já não satisfazia os requisitos de Privacidade da nova economia digital, tendo introduzido alterações significativas nas regras para o tratamento de dados pessoais, assegurando uma abordagem uniforme dentro do âmbito material e territorial definidos, e colocando o titular dos dados numa posição de destaque ao atribuir-lhe direitos que fornecem um maior controlo

[1] Crocetti, *et al*, 2021.

[2] Conjuntos de dados extremamente grandes, os quais podem ser analisados computacionalmente de modo a revelar padrões, tendências e associações, especialmente relacionados com o comportamento e interações humanas.

[3] Técnica de análise utilizada para explorar grandes bases de dados com informação dispersa, com o intuito de dar sentido à mesma, transformando-a em conhecimento. Esta análise tem o objetivo de encontrar anomalias, padrões ou correlações entre milhões de registos para prever resultados.

[4] Trata-se de uma aplicação da inteligência artificial que fornece aos sistemas informáticos a capacidade de aprendizagem e adaptação. São utilizados algoritmos e modelos estatísticos para analisar padrões existentes nos dados para de certa forma imitar o modo como os seres humanos aprendem, melhorando gradualmente a sua precisão com a experiência sem seguirem instruções específicas.

[5] O termo *cloud* é utilizado para descrever uma rede global de servidores interligados, os quais foram concebidos para executar aplicações, fornecer serviços, armazenar e gerir dados, entre outras funcionalidades. A utilização da *cloud* é feita *online*, ou seja, em vez de se aceder aos ficheiros no computador local, o acesso é feito através da *internet*, estando o conteúdo disponível através de qualquer dispositivo conectado.

[6] Conceito de interligação, através da *internet*, de dispositivos informáticos incorporados em objetos do quotidiano, os quais possuem sensores, *software* e outras tecnologias que lhes permite enviar e receber dados estando conectados entre si.

[7] Almeida Teixeira, 2019: 1-2.

[8] Agarwal, 2016: 1.

[9] Lameiras, 2022.

[10] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

sobre os seus dados pessoais[11]. Na verdade, o RGPD veio impor vários desafios para as organizações, incluindo um complexo conjunto de alterações a nível funcional, tecnológico e também jurídico, para que estas possam demonstrar que o tratamento de dados pessoais efetuado está em conformidade com o Regulamento, o que, na prática, resulta num compromisso a longo prazo[12].

Para alcançar a plena conformidade com os requisitos do Regulamento, e evitar as penalizações previstas, as organizações tiveram forçosamente de investir na implementação de boas práticas de proteção de dados pessoais, passando pela revisão das suas Políticas, Processos e Procedimentos relacionados. Sendo um documento jurídico, o Regulamento não é descritivo ao ponto de especificar quais as soluções a implementar pelas organizações, o que aliado ao desafio de interpretação do mesmo, dificulta a aplicação dos requisitos[13].

Com o intuito de fornecer as ferramentas necessárias para a garantia de conformidade com os requisitos para a gestão da Privacidade nas organizações, foi publicada a norma em estudo - ISO/IEC 27701:2019 - a qual providencia *guidance* para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão da Privacidade, em cumprimento com os requisitos globais para a proteção de dados, de salientar os do RGPD[14]. Esta norma, conforme explicado com maior detalhe no segundo capítulo, trata-se de uma extensão da ISO/IEC 27001:2013, o standard para a gestão da Segurança da Informação por excelência, pelo que os seus requisitos para a proteção de dados estão intimamente relacionados com os da segurança, sendo estes dois domínios indissociáveis nas organizações na garantia de um processamento seguro[15]. Assim, a abordagem da ISO/IEC 27701:2019, visto que a Segurança da Informação e a Privacidade se complementam nas organizações, passa pelo atingimento da plena conformidade com os requisitos legais e regulamentares aplicáveis de proteção de dados, através da sua gestão integrada, onde os controlos implementados para assegurar a proteção adequada da informação organizacional no seu todo, com a devida adaptação e implementação de requisitos específicos, servem de base para a garantia de um processamento seguro de uma categoria especial de informação – os dados pessoais[16].

Contudo, a norma ISO/IEC 27701 não foi desenvolvida especificamente de acordo com o RGPD, sendo abrangente à aplicação de outras legislações de proteção de dados, cabendo às organizações a devida adaptação do sistema de gestão às suas exigências, sendo essencial a análise comparativa entre os requisitos normativos e as exigências regulamentares, de modo a que o alinhamento das práticas de proteção de dados com a norma sirva também o propósito de garantir a conformidade com o RGPD.

Na Celfocus S.A., onde tive oportunidade de realizar um caso de estudo relevante para a empresa, os Sistemas de Gestão da Segurança da Informação e Privacidade são recém certificados na ISO/IEC 27001:2013 e ISO/IEC 27701:2019, respetivamente, tendo sido possível verificar o impacto da aplicação dos seus controlos na melhoria da conformidade com o RGPD, precisamente no decorrer

[11] Lopes, 2016: 33-42.
[12] Teixeira, 2019: 8-9.
[13] Lachaud, 2020: 11.
[14] International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 1.
[15] Anwar e Gill, 2020: 3; Alves, 2021: 122.
[16] Soenen, 2019: 1-2.

do processo de preparação para a certificação dos sistemas, o momento ideal para realizar esta análise.

1.2. Objetivos

O objetivo do presente trabalho, prende-se, sobretudo, com a realização de uma análise comparativa entre os requisitos do Regulamento Geral para a Proteção de Dados (RGPD) e os controlos da ISO/IEC 27701:2019, de forma a compreender, por um lado, o benefício que o alinhamento nesta norma traz para a gestão da Privacidade nas organizações e, por outro lado, compreender qual o papel da mesma na garantia de conformidade com os requisitos regulamentares previstos no RGPD, transpostos para a legislação portuguesa através da Lei n.º 58 de 2019.

Primeiramente, é efetuada a análise dos pontos de convergência e de divergência das abordagens da norma e do Regulamento, materializando-se depois esta análise num caso real ao levar a cabo a apresentação de um *case-study* na empresa Celfocus, S.A, cujo Sistema de Gestão da Privacidade (SGP) obteve, em julho de 2022, a certificação na norma em estudo - ISO/IEC 27701:2019 – com o objetivo de averiguar o papel da aplicação dos controlos da norma na garantia de conformidade com o RGPD.

1.3. Estrutura do documento

No primeiro capítulo deste documento é feita uma breve introdução sobre a temática da Privacidade, a sua importância e constante evolução na atualidade, em que a quantidade de dados pessoais gerados multiplica-se de dia para dia, resultando no processamento de um volume crescente de dados pelas organizações, as quais veem as suas responsabilidades relativamente à proteção de dados significativamente aumentadas, sobretudo desde a entrada em vigor do RGPD. Neste capítulo são ainda apresentados os objetivos do trabalho e a estrutura do presente documento.

O segundo capítulo assenta, essencialmente, na explicitação da importância que a Privacidade e a Segurança da Informação têm nos dias de hoje para as organizações, tendo em conta a crescente dependência das tecnologias da informação e os perigos que isso acarreta e também do papel que os standards desempenham na sua adequada gestão. Para além disto, encontra-se a descrição exaustiva dos controlos das cláusulas 5, 6, 7 e 8 da ISO/IEC 27701:2019, bem como dos requisitos do RGPD.

No terceiro capítulo, é explicado o papel da ISO/IEC 27701:2019 na garantia de conformidade com o RGPD e apresentada a análise comparativa, ponto a ponto da norma, com os respetivos artigos do Regulamento, incluindo os anexos A e B, e, no final, o estudo dos pontos de convergência e de divergência entre ambos.

O quarto capítulo, inicia-se com uma breve descrição da empresa Celfocus, S.A., na qual foi realizado o *case-study*, mais precisamente da sua história, desde a criação até aos dias de hoje, assim como mencionados os domínios tecnológicos em que se especializa e os mercados em que atua. De seguida, encontra-se o enquadramento relativo ao seu SGP e respetivo alinhamento com o Sistema de Gestão da Segurança da Informação (SGSI) e, posteriormente, é demonstrado todo o trabalho que foi

realizado no sentido de alinhar o SGP com a ISO/IEC 27701:2019, preparando-o para a certificação. Este capítulo termina com a análise da perceção de melhoria na conformidade com o RGPD na Celfocus, como consequência da aplicação dos controlos da norma para a gestão da Privacidade.

Por último, são apresentadas as conclusões relativas à análise comparativa entre os controlos da ISO/IEC 27701:2019 e os requisitos do RGPD e ainda algumas considerações sobre o trabalho realizado no âmbito do *case-study* na empresa Celfocus, S.A.

2. A Privacidade e a Segurança da Informação nas Organizações

A progressiva dependência das organizações relativamente às tecnologias de informação, em conjunto com o agravamento registado de incidentes de segurança, tem elevado a preocupação da gestão de topo relativamente à segurança da informação. De acordo com os dois últimos relatórios "Riscos & Conflitos", desenvolvidos pelo Centro Nacional de Cibersegurança (CNCS), sobre a cibersegurança em Portugal, a principal diferença registada, em relação aos períodos passados analisados, prende-se com o facto de se verificar um aumento do número de atividades ilícitas *online* e a sofisticação dos modos de atuação dos cibercriminosos, sendo que o volume de incidentes de cibersegurança e os indicadores de cibercrime sofreram um incremento significativo em 2021 e 2022, com destaque para os esquemas de *phishing*[17]/*smishing*[18] e infeção de sistemas por *malware*[19] e *ransomware*[20], bem como de fraude e burla *online*. No que diz respeito às notificações enviadas à Comissão Nacional de Proteção de Dados (CNPD) por violação de dados pessoais[21], registou-se, em comparação com o ano anterior, um aumento de 25% em 2020 e de 6% no ano de 2021[22]. Neste contexto, a perceção do risco de sofrer um incidente que coloque em causa a segurança da informação é aumentada, o que desperta as organizações para melhorar o nível de consciência dos seus colaboradores e promover ações preventivas adequadas.

Nos últimos anos, a proteção dos dados pessoais, os quais, regra geral, fazem parte da informação que as organizações processam, tornou-se uma questão prioritária para a segurança da informação organizacional na sequência da entrada em vigor do Regulamento Geral para a Proteção de Dados (RGPD). Na verdade, com a globalização do processamento de dados pessoais e com a evolução da sensibilização para a temática da proteção de dados, sustentada pela Carta dos Direitos Fundamentais da União Europeia (UE), mais especificamente no seu artigo 8.º, o qual estabelece o direito à proteção dos dados pessoais[23], têm surgido em todo o mundo leis para proteger esse direito fundamental, com as quais as organizações, que operam num ambiente global, se têm de alinhar e garantir que estão em conformidade. A Convenção para a Proteção dos Direitos do Homem e das

[17] O *phishing* é uma forma de crime informático que recorre a métodos enganadores/fraudulentos de criação e distribuição de *e-mails* com o objetivo de iludir os utilizadores, fazendo-os partilhar informações confidenciais, tais como a sua identificação pessoal, informações financeiras ou outros dados sensíveis. De acordo com o Observatório de Cibersegurança 2021, durante o ano de 2020, foi a ciberameaça mais predominante em Portugal, contribuindo para 43% dos incidentes registados pelo CERT.PT (serviço integrante do CNCS que coordena a resposta a incidentes que envolvam entidades do Estado, operadores de serviços essenciais, operadores de infraestruturas críticas nacionais e prestadores de serviços digitais).
[18] O termo *smishing* trata-se de uma combinação entre *phishing* e SMS (*short message services*). Enquanto o *phishing* utiliza *e-mails* como forma de disseminação do conteúdo fraudulento, o *smishing* usa mensagens de texto.
[19] *Malware*, ou *software* malicioso, trata-se de um termo genérico que descreve qualquer programa ou código que seja prejudicial para os sistemas informáticos, através do qual seja possível invadir, danificar ou incapacitar os sistemas, podendo inclusive assumir o controlo parcial das operações, interferindo obviamente com o seu normal funcionamento. Este tipo de *software* pode ser utilizado para roubar, encriptar ou apagar os dados das vítimas do ataque e ainda espiar as suas atividades sem que se apercebam.
[20] Observatório de Cibersegurança. 2021: 5; Observatório de Cibersegurança. 2022: 4.
O *Ransomware* é um tipo *de software* malicioso que impede os utilizadores de aceder ao seu sistema ou aos seus ficheiros pessoais, exigindo às vítimas o pagamento de um resgate (*ransom*) para devolver o acesso aos mesmos.
[21] Uma violação de dados pessoais, ou *data breach*, ocorre quando a organização sofre um incidente de segurança que provoque a destruição, perda, alteração ou divulgação não autorizada de dados pessoais.
[22] Observatório de Cibersegurança. 2021: 47-48; Observatório de Cibersegurança. 2022: 10-14.
[23] Carta dos Direitos Fundamentais da União Europeia, 2016: 7.

Liberdades Fundamentais, que teve lugar em Roma a 4 de novembro de 1950, já contemplava no capítulo respeitante aos direitos e liberdades, um artigo sobre o direito ao respeito pela vida privada e familiar, do seu domicílio e da sua correspondência, o que demonstra que a preocupação com a preservação da privacidade não é uma temática recente, embora o conceito tenha evoluído ao longo dos anos. Na atual Carta dos Direitos Fundamentais, encontra-se estabelecido que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito" e que esses dados devem ser processados de forma legal, para um propósito específico e de acordo com o consentimento do titular, ou com outro fundamento legítimo previsto na lei[24]. O exercício deste direito fundamental e o cumprimento do RGPD, que vem estabelecer requisitos para o processamento legal de dados pessoais, implica responsabilidades e deveres por parte das organizações, tanto para com os titulares individualmente envolvidos, como para a comunidade em geral e respetivas gerações futuras[25].

A segurança da informação e o cumprimento dos requisitos de privacidade continuam, nos dias de hoje, a representar uma tarefa desafiante para as organizações, por um lado, devido às crescentes exigências regulamentares e alterações na legislação e, por outro, como consequência da evolução tecnológica e expansão mundial do acesso à *internet*. O conjunto destes fatores permitiu o surgimento de crimes de natureza virtual cada vez mais sofisticados, com consequências potencialmente nefastas para a segurança e privacidade, os quais são levados a cabo para obtenção de lucro fácil, por exemplo através do roubo de informação, incluindo dados pessoais, e respetivo pedido de resgate[26]. De facto, os incidentes de segurança, em conjunto com a crescente digitalização, tornaram-se, na última década, uma preocupação mundial que totaliza, até 2024, 5,2 milhões de biliões de dólares em risco decorrentes de ciberataques, sendo, portanto, essencial e cada vez mais urgente que as organizações tomem medidas adequadas para assegurar a segurança da sua informação e a privacidade das pessoas envolvidas[27]. Os ciberataques podem ser altamente prejudiciais para as organizações, para os colaboradores e outras partes interessadas no negócio, uma vez que, ao serem cometidos através da *internet*, beneficiam de uma camada adicional de anonimato, ou até mesmo invisibilidade, tornando muito mais difícil a identificação da fonte ou autor do esquema, ou, em alguns casos, mascarando, inclusive, o facto de um esquema ter sido perpetrado, dificultando o seu combate nas organizações que necessitam de proteger o seu ativo mais valioso – a informação[28].

Assim, a proteção da informação nas organizações, tendencialmente cada vez mais digital (armazenada e processada em sistemas informáticos[29] e *clouds*), requer forçosamente uma abordagem interdisciplinar para a implementação de um sistema capaz de satisfazer simultaneamente os diferentes requisitos legais, no que concerne à proteção de dados pessoais, garantir a confidencialidade, a integridade e a disponibilidade da informação e ainda acompanhar as necessidades do negócio[30].

[24] Carta dos Direitos Fundamentais da União Europeia, 2016: 7.
[25] Veiga, 2020: 67-68.
[26] Anwar e Gill, 2020: 1; Santos, 2015: 18.
[27] Accenture Security, 2019: 15.
[28] Miller, *et al.*, 2020: 1-2.
[29] Um sistema informático é constituído por um ou mais computadores, *software* e dispositivos periféricos, que executam um processamento de dados.
[30] Anwar e Gill, 2020: 1.

A Segurança da Informação e a Privacidade são áreas complementares numa organização, na medida em que a privacidade sem a segurança acaba por tornar-se apenas num exercício de direito, sem um verdadeiro suporte para a sua implementação prática, o qual permita ao responsável pelo tratamento de dados garantir um processamento seguro e adequado e ao titular dos dados o exercício dos seus direitos, enquanto que a segurança sem a privacidade trata-se de uma disciplina de proteção da informação, a qual se foca na proteção de um ativo fundamental para as organizações, mas não abrangendo as implicações do exercício do direito à privacidade pelos titulares. Tanto a Privacidade como a Segurança da Informação requerem um exercício de construção conjunta, que permita conciliar a relevância dos dois domínios, fazendo com que a informação prevaleça como fonte de vantagem competitiva, passando pela articulação da relação entre as pessoas, os processos e as tecnologias, de forma a incorporar as práticas necessárias para orientar a cultura da organização no sentido da preservação da informação, incluindo dados pessoais, como base para a estratégia de negócio[31].

O recentemente publicado standard ISO/IEC 27701:2019, uma extensão à ISO/IEC 27001 e ISO/IEC 27002, relativamente à gestão da privacidade, fornece as ferramentas chave para as organizações estarem em conformidade com os requisitos de privacidade globais, nomeadamente com o internacionalmente reconhecido RGPD. Este standard, conforme explicado com maior detalhe no ponto 2.2 deste trabalho, fornece o *guidance* necessário para o estabelecimento, implementação, manutenção e melhoria contínua do *Privacy Information Management System* (PIMS), ou do Sistema de Gestão da Privacidade (SGP), bem como dos respetivos controlos para garantir a proteção dos dados pessoais e seus titulares, independentemente do papel da organização relativamente ao processamento dos dados pessoais. Tratando-se de uma extensão à ISO/IEC 27001:2013, os requisitos apresentados para o SGP são complementares aos requisitos para o Sistema de Gestão da Segurança da Informação (SGSI), os quais se materializam nos requisitos adicionais apresentados nas subcláusulas 5.2 a 5.8 e 6.2 a 6.15, nos controlos normativos específicos para os *Controllers* apresentados na cláusula 7 (7.1 a 7.5) e no Anexo A (A.7.2 a A.7.5) e, por último, nos controlos normativos para os *Processors* apresentados na cláusula 8 (8.1 a 8.5) e no Anexo B (B.8.2 a B.8.5)[32].

As certificações ISO 27001 e ISO 27701 oferecem muitas vantagens operacionais às empresas, que procuram uma solução viável para agilizar a segurança da informação e a proteção de dados pessoais na sua organização, estabelecendo uma relação de confiança entre a organização e as suas partes interessadas, nomeadamente clientes, parceiros e autoridades governamentais. Os principais benefícios associados à certificação prendem-se, essencialmente, com o aumento da sensibilização das partes interessadas, no que diz respeito à Segurança da Informação e Privacidade, com a melhoria do conhecimento da organização e o maior controlo sobre os seus ativos, com especial atenção para a informação sensível e dados pessoais, com o fornecimento de métodos eficazes para a implementação dos controlos, com a melhoria da organização em processos e mecanismos de gestão, de forma a promover a redução de custos e o cumprimento da legislação em vigor, bem como a prevenir a ocorrência de incidentes de segurança e privacidade[33]. De destacar ainda, o conhecimento

[31] Cano, 2014.
[32] Knuuti *et al*., 2020: 17; International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 4.
[33] Almeida, 2018: 15.

real dos riscos, a identificação e eliminação de ameaças e vulnerabilidades e o aumento da capacidade de previsão e gestão perante uma situação de disrupção, assegurando a continuidade do negócio[34]. A ISO 27701, especificamente, assegura ainda a conformidade com as leis e regulamentos de privacidade aplicáveis, quer seja o RGPD ou outra legislação local, e melhora a gestão da privacidade, reduzindo os riscos relacionados, como, por exemplo, a ocorrência de *privacy breaches*[35].

Recentemente, tem sido estudada a aplicabilidade da certificação ISO 27701 para atestar a conformidade das organizações com os requisitos do RGPD, como alternativa ao regime estabelecido nos Artigos 42.º (Certificação) e 43.º (Organismos de Certificação) do Regulamento, o qual ainda não se encontra efetivo. Visto que a certificação ISO é globalmente reconhecida, sendo inclusive adotadas certificações em larga escala nas normas da família ISO 27000, em especial na ISO/IEC 27001:2013, o mercado de auditores e organismos de certificação está totalmente consolidado, tratando-se por isso de um sistema de certificação robusto e confiável. Apesar de não ser de todo equivalente ao regime estabelecido no RGPD, é consensual que as certificações ISO/IEC 27701:2019 e ISO/IEC 27001:2013 oferecem um conjunto de *guidelines*, quer para *Controllers* quer para *Processors*, as quais podem ajudar a agilizar e otimizar o processamento de dados pessoais e, em simultâneo, gerar uma relação de confiança com os clientes e outras partes interessadas, o que pode contribuir largamente para a difusão da conformidade com os requisitos de proteção de dados pessoais em todo o mundo[36].

2.1. Standard ISO/IEC 27001:2013

A ISO/IEC 27001:2013 é a norma para a gestão da Segurança da Informação, criada pela *International Organization for Standardization* (ISO) em conjunto com a *International Electro-technical Comission* (IEC), a qual é aplicável a todos os setores de atividade. Trata-se de um standard globalmente reconhecido, que especifica os requisitos para estabelecer, implementar, documentar, monitorizar, manter e melhorar o Sistema de Gestão de Segurança da Informação (SGSI) das organizações, bem como definir os requisitos para os controlos de segurança a serem implementados, de acordo com as suas necessidades individuais[37].

A norma ISO/IEC 27001 define os três aspetos essenciais para a Segurança da Informação: as pessoas, os processos e a tecnologia. Esta abordagem, em três níveis, ajuda as organizações a protegerem-se, tanto de ataques externos como de ameaças internas comuns[38]. A necessidade da melhoria contínua do SGSI está no centro das preocupações da ISO 27001, sendo a cláusula 10, "*Improvement*", dedicada a este tema. Tendo em consideração a velocidade em que atualmente ocorrem alterações ao contexto em que as organizações atuam, nomeadamente a diversidade crescente das ameaças que podem colocar a Segurança da Informação em causa, esta é, sem dúvida, um dos princípios mais importantes da norma, que garante a atualização e adequação constante do

[34] Lopes et. al, 2019: 3-4.
[35] Knuuti *et al*., 2020: 21.
[36] Lachaud, 2020: 2-4.
[37] ISO, 2020.
[38] Lopes *et. al*, 2019: 3.

SGSI[39]. Outro dos fatores que contribuem para uma melhor gestão da informação é a abordagem baseada no risco (cláusula 6, "*Planning*"), a qual, em conjunto com o conhecimento do contexto da organização e seu negócio (cláusula 4, "*Context of the organization*"), é essencial na identificação dos riscos que podem colocar em causa a Segurança da Informação e na definição de políticas. Depois de serem reconhecidos os riscos, é importante analisar cada um em pormenor, incluindo a apreciação da sua probabilidade de ocorrência, o seu potencial impacto e respetiva consequência e ainda a identificação de estratégias para a gestão dos mesmos[40]. Todos os fatores referidos anteriormente, requerem o comprometimento da gestão de topo, exigido na cláusula 5 ("*Leadership*") da norma, na qual são elencadas as funções esperadas da gestão, como, por exemplo, assegurar que a política e os objetivos definidos sejam compatíveis com o contexto e orientação estratégica da organização; proporcionar os recursos necessários para tal; e assegurar a integração do SGSI nos processos de negócio[41]. Além do comprometimento da gestão de topo, o envolvimento de todos os colaboradores no cumprimento dos requisitos anteriormente referidos é crucial, uma vez que o estabelecimento de uma cultura de Segurança da Informação nas organizações tem impacto na perceção e comportamento de todos os colaboradores, ao ponto de alterar o seu grau de sensibilização para as ameaças que possam colocar a proteção da informação em causa[42]. O ciclo *Plan-Do-Check-Act* (PDCA) encontra-se subentendido e incorporado ao longo das várias cláusulas da ISO/IEC 27001:2013, o qual descreve o procedimento a adotar para a gestão da Segurança da Informação, de acordo com a Figura 1, que proporciona uma maior organização e coesão no estabelecimento do SGSI[43].

A implementação dos controlos de segurança, presentes no Anexo A da ISO/IEC 27001:2013, conduz ao estabelecimento de um SGSI eficiente e robusto, no qual as responsabilidades são adequadamente definidas e comunicadas e os controlos de segurança são rigorosamente aplicados, resultando numa gestão competente dos ativos da organização e numa relação de maior confiança com todas as partes interessadas, ao demonstrar a preocupação em manter a confidencialidade, a integridade e a disponibilidade da informação[44].

A certificação neste standard pode também ser encarada como uma vantagem competitiva para as organizações, uma vez que comprova o cumprimento das boas práticas de Segurança da Informação, o que, por si só, melhora a reputação da organização nesta temática, como também oferece garantias relativas à proteção de dados pessoais contra *data breaches*, podendo, com a devida adaptação, ir ao encontro das exigências do RGPD, o que, sem dúvida, resulta em benefícios de *marketing* para as empresas[45].

[39] Lopes *et. al*, 2019: 4.
[40] International Standard, ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements: 1-3.
[41] International Standard, ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements: 2.
[42] AlHogail, 2015: 2.
[43] Mattes e Petri, 2015: 97.
[44] Irwin, 2018.
[45] IT Governance, 2020.

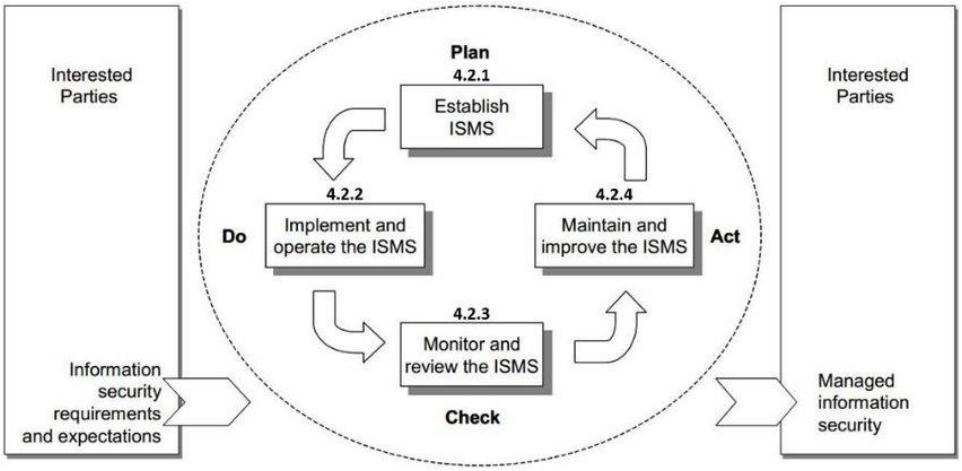

Figura 1 - Ciclo *Plan-Do-Check-Act* aplicado ao SGSI (Proença e Borbinha, 2018 – com base no Ciclo de *Deming*).

2.2. Standard ISO/IEC 27701:2019

Ao identificar a necessidade de existir um conjunto de requisitos para gerir e garantir a segurança dos dados pessoais, independentemente dos requisitos legais e regulamentares aplicáveis, a ISO e a IEC desenvolveram e publicaram recentemente um standard que oferece, precisamente, o *guidance* necessário para as organizações implementarem um SGP com os controlos adequados para assegurar a proteção dos dados pessoais e seus titulares – a ISO/IEC 27701:2019.

O standard ISO/IEC 27701:2019 é uma das mais recentes normas da família ISO/IEC 27000, tratando-se de uma extensão da ISO/IEC 27001 e da ISO/IEC 27002, a qual apresenta requisitos e *guidelines* para a implementação, manutenção e melhoria contínua de um SGP, o qual tem o intuito de melhor gerir os processos que garantam a recolha segura de dados pessoais, bem como aqueles que assegurem a disponibilidade, a integridade e a confidencialidade dos mesmos nas organizações[46]. Tratando-se de uma extensão da ISO/IEC 27001, esta norma foi concebida de forma a permitir a adição de requisitos específicos, relacionados com o processamento de dados pessoais, sem a necessidade de desenvolver um novo Sistema de Gestão, ou seja, proporcionando a oportunidade às organizações interessadas de conciliarem os seus Sistemas de Gestão da Segurança da Informação e da Privacidade[47]. Dito isto, a certificação ISO/IEC 27701 é apenas possível nas organizações que também tenham o seu SGSI certificado pela ISO/IEC 27001.

A implementação de um SGP, de acordo com a ISO/IEC 27701:2019, possibilita a conformidade com múltiplas legislações de privacidade, o que é particularmente interessante para as organizações que atuam em diversos países, nas quais a *compliance* com as respetivas legislações é essencial para o negócio. Assim, os requisitos para a proteção dos dados pessoais podem variar de acordo com o contexto onde as organizações operam, sendo essencial a sua plena compreensão, em particular das diferentes legislações ou regulamentos nacionais, pois a ISO/IEC 27701 apenas inclui

[46] ISO, 2019.
[47] International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 7

mapeamento direto para os requisitos do RGPD (e também para outros standards da ISO, nomeadamente a ISO/IEC 29100, 27018 e 29151), pelo que os requisitos da norma devem ser interpretados de forma a incluir as exigências de outra legislação de privacidade, relevante no Sistema de Gestão[48]. Conforme anteriormente mencionado, este standard de referência tanto pode ser utilizado por organizações que tenham o papel de *Controller*[49], como por organizações que atuam como *Processor*[50]. Ambas as entidades têm responsabilidade no processamento de dados pessoais, sendo que qualquer organização que siga os princípios estabelecidos na ISO/IEC 27701 e cumpra os seus requisitos, irá ter na sua posse evidências documentadas da forma como processa os dados pessoais, bem como do cumprimento das exigências do RGPD, ou outra legislação de privacidade relevante que seja incluída no âmbito do Sistema de Gestão.

O foco da ISO/IEC 27701 prende-se com a adição de requisitos específicos de privacidade, aos definidos pelos standards ISO/IEC 27001 e 27002, sendo a organização do documento idêntica, onde pontualmente vão surgindo extensões aos requisitos de segurança da informação, de forma a também incluir no âmbito do Sistema de Gestão a proteção dos titulares de dados, os quais são potencialmente afetados pelo processamento dos seus dados pessoais. Aliás, no próprio standard é mencionado que os requisitos da ISO/IEC 27001:2013 que mencionam "segurança da informação", devem ser alargados à proteção da privacidade, devendo, na prática, passar a aplicar-se "segurança da informação e privacidade" nesses mesmos requisitos[51]. Abaixo, encontra-se uma figura que representa a abordagem da ISO/IEC 27701, nomeadamente a sua relação com a norma ISO 27001.

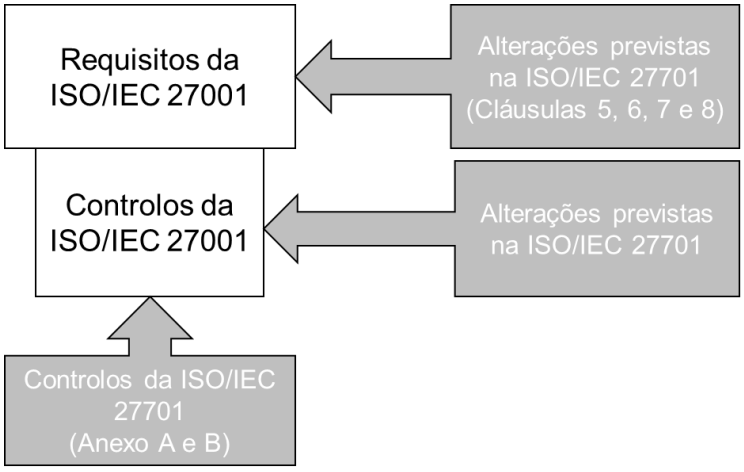

Figura 2 - Representação da relação dos standards ISO/IEC 27001 e ISO/IEC 27701.

[48] International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 7

[49] O *Controller*, de acordo com o RGPD, trata-se da pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que, sozinho ou em conjunto com outros, determina as finalidades e os meios do tratamento de Dados Pessoais (em português é designado por responsável pelo tratamento).

50 O *Processor*, de acordo com o RGPD, trata-se da pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que trate dados pessoais em nome do responsável pelo tratamento (em português é designado por subcontratante).

[51] International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 4

No que diz respeito à organização da ISO/IEC 27701, são acrescentados requisitos de privacidade nas cláusulas 5, 6, 7 e 8, bem como nos anexos A e B. Na cláusula 5, intitulada de "*PIMS-specific requirements related to ISO/IEC 27001*", são fornecidos requisitos adicionais e outras informações relativas aos requisitos de segurança da informação da ISO/IEC 27001, os quais são aplicáveis tanto às organizações que atuam como *Controller* como àquelas que atuam como *Processor*, tendo sido adicionadas subcláusulas para cada uma das cláusulas apresentadas na ISO/IEC 27001. Já a cláusula 6, cujo título é "*PIMS-specific guidance related to ISO/IEC 27002*", dá orientações específicas e informações adicionais aos controlos de segurança da informação da ISO/IEC 27002, os quais também são aplicáveis às organizações que atuam como *Controller* e como *Processor.* No que concerne à cláusula 7, "*Additional ISO/IEC 27002 guidance for PII controllers*", conforme o próprio título indica, são fornecidas orientações adicionais às estabelecidas na ISO/IEC 27002 para as organizações que atuam como *Controller*, enquanto a cláusula 8, "*Additional ISO/IEC 27002 guidance for PII processors*" dá *guidance* adicional especificamente para as organizações que atuam como *Processor.* No que diz respeito ao Anexo A, "*PIMS-specific reference control objectives and controls (PII Controllers)*", este apresenta a lista dos objetivos dos controlos e os controlos específicos de privacidade, respeitantes às organizações que atuam como *Controller,* e o Anexo B, "*PIMS-specific reference control objectives and controls (PII Processors)*", apresenta a mesma lista para as organizações que atuam como *Processor.* Adicionalmente, existem ainda os Anexos C e D, os quais fornecem o mapeamento dos requisitos de privacidade específicos desta ISO com outros standards e regulamentos. Portanto, o Anexo C apresenta o mapeamento entre as disposições da ISO/IEC 27701 e os princípios de privacidade da ISO/IEC 29100. Já o Anexo D, apresenta o mapeamento entre as disposições da ISO/IEC 27701 com os requisitos dos artigos 5.º ao 49.º (com exceção do artigo 43.º, "Organismos de certificação") do RGPD, demonstrando como o cumprimento dos requisitos desta ISO pode ser relevante para garantir a conformidade com as obrigações impostas às organizações pela entrada em vigor do RGPD[52].

Todas as cláusulas que acrescentam informação relevante para o SGP vão ser alvo de escrutínio no presente trabalho, com o intuito de compreender o papel real da ISO/IEC 27701 na garantia de conformidade com o RGPD nas organizações.

2.2.1. Visão geral das cláusulas relevantes

2.2.1.1. Cláusula 5 – Requisitos de privacidade específicos relacionados com a ISO/IEC 27001

Na cláusula 5 da ISO/IEC 27701:2019 estão inseridos os requisitos auditáveis da ISO/IEC 27001:2013, nomeadamente os presentes nas cláusulas "4. *Context of the organization*", "5. *Leadership*", "6. *Planning*"; "7. *Support*", "8. *Operation*", "9. *Performance evaluation*" e "10.

[52] International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 2.

Improvement", com o objetivo de alargar a sua aplicação nas organizações, de forma a garantir um nível de segurança adequado nas atividades de processamento de dados pessoais levadas a cabo.

Assim, no que diz respeito à cláusula "4. *Context of the organization*", esta norma vem acrescentar a necessidade de a organização determinar o seu papel enquanto *Controller*, *Processor*, ou eventualmente *joint-controller*[53], assim como determinar os fatores externos e internos relevantes, para o seu contexto, que possam afetar a capacidade de alcançar os resultados pretendidos pelo seu *Privacy Information Management System* (PIMS), equivalente ao comumente designado SGP. Para tal, são sugeridos alguns fatores a ter em consideração, nomeadamente: legislação aplicável em matéria de privacidade; regulamentos aplicáveis; decisões judiciais aplicáveis; contexto da organização, *governance*, políticas e procedimentos aplicáveis; e ainda requisitos contratuais aplicáveis. Quando a organização atua como *Controller* e como *Processor*, de acordo com esta norma, devem ser determinadas funções separadas, cada uma delas com o seu conjunto próprio de controlos aplicáveis. Ainda sobre a cláusula "4. *Context of the organization*" é acrescentado um requisito relativo às partes interessadas, as quais devem passar a incluir as entidades com interesse e responsabilidade no processamento de dados pessoais, incluindo os próprios titulares dos dados. Por exemplo, estas partes interessadas a acrescentar podem incluir as autoridades de controlo, outros *Controllers*, *Processors* e seus subcontratados. Nesta cláusula são ainda adicionados requisitos para a identificação do âmbito do Sistema de Gestão, o qual deve passar a ter em consideração o processamento de dados pessoais, pelo que a organização o deve estabelecer, implementar, manter e melhorar de forma contínua de acordo com os requisitos das cláusulas 4 a 10 da ISO/IEC 27001:2013, anteriormente identificadas, tendo também em conta a extensão aos requisitos apresentada ao longo da cláusula 5 da ISO/IEC 27701:2019[54].

Na ISO/IEC 27701:2019 são acrescentados vários requisitos de privacidade à cláusula "6. *Planning*", sendo o primeiro deles relativo à avaliação de risco. Para cumprir com este requisito, as organizações devem passar a aplicar o seu processo de avaliação de risco na identificação dos riscos que caem dentro do âmbito do SGP, ou seja, aqueles relacionados com o processamento de dados pessoais, devendo para tal levar a cabo *Privacy Risk Assessments.* Através destas avaliações, devem ser analisadas as potenciais consequências, quer para a organização quer para os titulares dos dados, no caso de os riscos identificados se materializarem. A organização deve também assegurar, através do processo de avaliação de risco, que a relação entre a segurança da informação e a privacidade é gerida adequadamente, podendo para tal definir um processo integrado para a avaliação de riscos de segurança da informação e privacidade. No que diz respeito ao tratamento do risco, a aplicabilidade dos controlos considerados no contexto dos riscos para a segurança da informação deve ser avaliada no contexto dos riscos relacionados com o processamento de dados pessoais, incluindo os riscos para os titulares dos dados. Desta forma, deve ser estabelecido um *Statement of Aplicability* (SoA), no qual são apresentados os controlos aplicáveis, determinados no Anexo A e/ou B assim como no Anexo A

[53] O *joint-controller*, de acordo com o RGPD, é o nome que se utiliza quando existem dois ou mais responsáveis pelo tratamento, os quais determinam em conjunto as finalidades e os meios desse tratamento, sendo ambos responsáveis conjuntos pelo tratamento, pelo que determinam, por acordo entre si e de modo transparente, as respetivas responsabilidades pelo cumprimento do RGPD.

[54] International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 4-5.

da ISO 27001, e a justificação da sua inclusão no Sistema de Gestão, bem como a informação relativa à implementação dos controlos e ainda a justificação para a sua exclusão quando estes não são aplicáveis[55]. Na Tabela 1, encontra-se o resumo da extensão aos requisitos da ISO/IEC 27001:2013 apresentada na cláusula 5 da ISO/IEC 27701:2019.

Tabela 1 - Resumo da extensão aos requisitos da ISO/IEC 27001:2013 apresentada na cláusula 5 da ISO/IEC 27701:2019

Sub-cláusulas ISO/IEC 27001:2013	**Sub-cláusulas ISO/IEC 27701:2019**	**Extensão**
1. *General*	5.1 *General*	Todos os requisitos da ISO/IEC 27001:2013 que mencionam "*information security*" devem ser alargados a "*information security and privacy*".
4. *Context of the organization*	5.2 *Context of the organization*	Indicação do papel da organização enquanto *Controller* e/ou *Processor.*
5. *Leadership*	5.3 *Leadership*	Compromisso da Gestão de Topo para com a Política de Privacidade e garantia de integração do SGP no SGSI.
6. *Planning*	5.4 *Planning*	Identificação dos riscos relacionados com o processamento de dados pessoais (*privacy risk assessment*) e respetivo tratamento. Realização do *Statement of Applicability* (justificação de inclusão ou exclusão de controlos).

2.2.1.2. Cláusula 6 – Requisitos de privacidade específicos relacionados com a ISO/IEC 27002

Na sexta cláusula da ISO/IEC 27701, intitulada de "*PIMS-specific guidance related to ISO/IEC 27002*", é referido que, à semelhança do *guidance* específico para a ISO/IEC 27001 apresentado na cláusula anterior, quando se lê *information security* nos requisitos da ISO 27002, deve passar a ler-se *information security and privacy*. Apesar dos requisitos apresentados nesta cláusula não serem requisitos normativos, acrescentam grande valor para as organizações que pretendam certificar o seu SGP na ISO/IEC 27701, uma vez que a ISO/IEC 27002 estabelece o código de melhores práticas para apoiar a gestão da segurança da informação e a certificação do SGSI e, consequentemente, do SGP.

No que diz respeito à cláusula "5. *Information Security Policies*" da ISO/IEC 27002, é adicionada a necessidade de as organizações produzirem uma declaração sobre o compromisso do cumprimento da legislação de privacidade aplicável, assim como com os termos contratuais acordados entre a

[55] International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 6-7.

organização e outras partes interessadas, sendo que tal pode ser atingido pela produção de políticas de privacidade ou pela extensão das políticas de segurança da informação. Para além disto, é adicionada a preocupação de se ter em linha de conta a legislação de privacidade, no desenvolvimento e manutenção das políticas de segurança da informação da organização.

No que concerne à cláusula seguinte da ISO/IEC 27002, "6. *Organization of information security*", mais precisamente no ponto relativo aos papéis e responsabilidades dentro da organização, é acrescentada a necessidade de esta designar um ponto de contacto para os clientes tratarem de questões relacionadas com o processamento de dados pessoais, assim como um contacto para os titulares dos dados (caso a empresa tenha também o papel de *Controller*). Adicionalmente, devem ser nomeadas as pessoas responsáveis pelo desenvolvimento, implementação, manutenção e monitorização do programa de privacidade e *governance* da organização, o qual deve assegurar o cumprimento das leis e regulamentos aplicáveis relativos ao processamento de dados pessoais. São ainda acrescentados neste ponto alguns requisitos para a pessoa responsável, os quais estão totalmente alinhados com as funções designadas no RGPD para o *Data Protection Officer* (DPO)[56], nomeadamente ser independente e reportar diretamente à gestão de topo, estar envolvido na gestão de todas as questões relacionadas com o processamento de dados pessoais, ser conhecedor da legislação em matéria de proteção de dados, atuar como ponto de contacto para as autoridades de controlo, informar o *top management* e os colaboradores da organização das suas obrigações relacionadas com o processamento de dados pessoais e, ainda, prestar aconselhamento relativamente aos *Privacy Impact Assessments* (PIAs) a ser conduzidos pela organização. Nesta cláusula, é apenas acrescentado mais um requisito no âmbito da política de dispositivos móveis, o qual refere que deve ser garantido que a utilização de dispositivos móveis não pode levar ao comprometimento de dados pessoais.

Na cláusula "7. *Human resource security*" da ISO/IEC 27002, a ISO/IEC 27701 vem acrescentar requisitos de privacidade relativamente à sensibilização, educação e formação em matéria de segurança da informação. Assim, de acordo com esta norma, devem ser implementadas medidas que assegurem que os colaboradores que processam dados pessoais estejam cientes das possíveis consequências para a organização, decorrentes da violação das regras e procedimentos de privacidade ou segurança, em especial aqueles que se referem ao processamento de dados pessoais. Estes colaboradores devem estar a par das consequências legais, da eventual perda de negócios associada, bem como dos possíveis danos para a reputação da empresa, mas também das potenciais consequências para os colaboradores, por exemplo consequências disciplinares, e para os titulares dos dados, tais como consequências físicas, materiais e emocionais. As medidas a implementar devem incluir a sensibilização de todos os colaboradores para a comunicação de incidentes de privacidade.

Sobre a cláusula "8. *Asset Management*" da ISO/IEC 27002, mais precisamente no que concerne à classificação e rotulagem da informação, há a acrescentar que a organização deve ter em conta a inclusão dos dados pessoais no seu esquema de classificação, bem como assegurar que os

[56] O *Data Protection Officer*, de acordo com o RGPD, auxilia o *Controller* ou o *Processor* em todas as questões relacionadas com a proteção de dados pessoais, devendo informar e aconselhar sobre as respetivas obrigações nos termos da lei da proteção de dados, controlar o cumprimento da legislação relacionada com a proteção de dados e, entre outras funções, cooperar com a autoridade de controlo.

seus colaboradores estão sensibilizados para a definição de dados pessoais, sabendo reconhecer quando uma informação se trata de um dado pessoal, de forma a conseguirem classificar e rotular a informação corretamente. Relativamente ao manuseamento de *media*, a ISO 27701 vem acrescentar que deve ser documentada qualquer utilização de dispositivos amovíveis, ou outros dispositivos, para o armazenamento de dados pessoais e, sempre que possível, os dispositivos a utilizar devem permitir a encriptação dos dados. De acordo com este requisito, o uso de dispositivos não encriptados apenas deve acontecer em situações totalmente inevitáveis e, nestes casos, a organização deve implementar os procedimentos e controlos apropriados para mitigar os riscos para os dados pessoais e seus titulares, caso os dispositivos fossem comprometidos. Sobre a eliminação dos *media*, a ISO 27701 adiciona a preocupação de documentar e implementar procedimentos de eliminação segura dos dados pessoais, de forma que estes não possam ser acedidos novamente. Se forem utilizados dispositivos móveis para a transferência de informação, deve ser criado um sistema para o registo dos dispositivos utilizados para receção e divulgação de dados pessoais, incluindo o tipo de dispositivos, a identificação do remetente e do recetor autorizados e a data e hora da transferência. Sempre que possível, devem ser implementadas medidas adicionais, nomeadamente a encriptação, para assegurar que os dados só podem ser acedidos no ponto de destino e não em trânsito.

A cláusula "9. *Access Control*" da ISO/IEC 27002 também tem requisitos adicionais na ISO 27701. Por exemplo, no ponto *user access management*, em relação aos procedimentos de registo e cancelamento de registo de *users*, estes devem ter em conta as situações em que o controlo de acesso é comprometido, nomeadamente através do comprometimento de *passwords*. Assim, as organizações não devem reativar *users* para dar acesso a sistemas onde são processados dados pessoais, sem que previamente tenham sido revistos esses acessos. Ao ponto "9.2.2 *User access provisioning*", é acrescentado que a organização deve manter um registo preciso e atualizado dos perfis de utilizadores criados para aceder aos sistemas, onde existem dados pessoais de forma a ser possível identificar quem acedeu, a que dados acedeu e que alterações foram efetuadas. No caso de a organização estar a prestar um serviço onde existe processamento de dados pessoais, poderá fornecer ao cliente, quando apropriado, os meios para ele próprio efetuar a gestão dos acessos.

Na cláusula "10. *Cryptography*" da ISO/IEC 27002 é acrescentada a noção de que em algumas jurisdições pode ser exigida a utilização de criptografia para proteger algumas categorias de dados pessoais, como por exemplo dados de saúde ou outros dados sensíveis[57]. As organizações devem informar os seus clientes das situações em que recorrem à encriptação, para proteger os dados pessoais, e ainda providenciar informação aos mesmos sobre o seu conhecimento na matéria, de forma a ajudá-los a aplicar esta medida de proteção.

Na cláusula "11. *Physical and environmental security*" da ISO/IEC 27002, mais precisamente no ponto "11.2.7 *Secure disposal or re-use of equipment*" é acrescentado que, sempre que seja reatribuído espaço de armazenamento, deve ser assegurado que quaisquer dados pessoais

[57] Dados sensíveis, de acordo com o RGPD, são dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como dados genéticos, dados biométricos que identifiquem inequivocamente uma pessoa, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa, bem como dados pessoais relacionados com condenações penais e infrações.

previamente armazenados não sejam acessíveis. No que diz respeito à política de *clear desk*, deve haver um cuidado acrescido para restringir a criação de cópias de documentos, que contenham dados pessoais, ao estritamente necessário.

Na cláusula "12. *Operations security*" da ISO/IEC 27002, no ponto referente ao *backup* da informação, é adicionado o requisito de existir uma política que aborde os requisitos de *backup*, recuperação e reposição de dados pessoais, e quaisquer outros requisitos para o seu apagamento, nomeadamente requisitos legais ou contratuais. Esta política pode ser parte integrante da política geral de *backup*. Algumas jurisdições impõem requisitos específicos relativamente à frequência das cópias de segurança dos dados pessoais, à frequência das revisões e testes das cópias de segurança, ou até mesmo relativamente aos procedimentos de recuperação de dados pessoais, pelo que as organizações que operam nestas jurisdições devem demonstrar conformidade com estes requisitos. Nas situações em que haja recuperação de dados pessoais, devem existir processos que assegurem que estes dados são recuperados num estado em que a sua integridade seja garantida e/ou em que seja possível identificar qualquer inexatidão para que possa ser resolvida. A organização deve ter um procedimento para as atividades de recuperação de dados pessoais e um registo das atividades, o qual deve conter, pelo menos, o nome do responsável pela recuperação da informação e a descrição dos dados pessoais envolvidos. No que diz respeito ao ponto "12.4.1 *Event logging*", existem também requisitos adicionais, nomeadamente a implementação de um processo de revisão de *event logs*, sendo que estes devem registar quem acedeu aos dados pessoais, quando ocorreu esse acesso, quais os dados acedidos e eventuais alterações efetuadas. Sendo que a própria informação registada nos *logs* pode conter dados pessoais, devem ser implementadas medidas de controlo de acesso, que assegurem que esta informação é apenas utilizada para os fins pretendidos.

Na cláusula "13. *Communications security*" da ISO/IEC 27002, no que diz respeito às políticas e procedimentos de transferência de informação, é acrescentado que a organização deve implementar procedimentos para assegurar que as regras relacionadas com o processamento de dados pessoais, aplicadas em todo o sistema, são também usadas na sua transferência, quando aplicável. Relativamente ao ponto "13.2.4 *Confidentiality or non-disclosure agreements*", existe o requisito adicional de assegurar que todas as pessoas, que acedam a dados pessoais no âmbito do seu trabalho, estejam sujeitas a um acordo de confidencialidade.

A ISO/IEC 27701 também apresenta requisitos adicionais à cláusula "14. *Systems acquisition, development and maintenance*" da ISO/IEC 27002. No ponto "14.1.2 *Securing application services on public networks*" é adicionada a preocupação de garantir que a transmissão de dados pessoais, através de redes não confiáveis, como por exemplo redes *free wi-fi*, é feita com recurso à encriptação dos dados. Ao ponto "14.2.1*Secure development policy*" é adicionada a necessidade de as políticas de desenvolvimento e *design* de sistemas incluírem orientações relativas ao processamento de dados pessoais, as quais devem estar alinhadas com os requisitos da legislação aplicável e de acordo com as atividades de processamento levadas a cabo pela organização. As políticas de *privacy by design and by default* devem ter em consideração os seguintes pontos: orientações para a proteção de dados pessoais e implementação de princípios de privacidade ao longo do ciclo de vida do desenvolvimento de *software*; requisitos de proteção de dados pessoais na fase de *design*, os quais podem ser baseados

nos resultados das avaliações de risco de privacidade; conhecimentos necessários em matéria de proteção de dados; e o princípio da minimização de dados. Relativamente ao ponto "14.2.5 *Secure systems engineering principles*" é acrescentado que os sistemas, relacionados com o processamento de dados pessoais, devem ser concebidos segundo os princípios de *privacy by design and by default* e de forma a facilitar a implementação dos controlos relevantes (descritos nas cláusulas 7 e 8 da ISO/IEC 27701, em análise nos pontos seguintes), nomeadamente aqueles que limitam a recolha e o processamento de dados pessoais ao estritamente necessário, garantindo ainda a eliminação facilitada dos mesmos quando já não são necessários. Ao ponto "14.2.7, *Outsourced Development*" é apenas adicionada a noção de que o princípio de *privacy by design and by default* deve ser também aplicado aos sistemas de informação subcontratados. Por último, o ponto "14.3.1, *Protection of test data*" passa a incluir o requisito de não serem utilizados dados pessoais em testes. Quando o recurso a dados pessoais em testes é completamente inevitável, devem ser implementadas medidas técnicas e organizativas equivalentes às utilizadas no ambiente de produção, com o objetivo de minimizar os riscos e, quando a implementação de medidas equivalentes não for viável, deve ser realizada uma avaliação de risco para determinar os controlos adequados para mitigar o risco da utilização dos dados pessoais.

Na ISO/IEC 27701 também são adicionados requisitos à cláusula "15. *Supplier relationships*" da ISO/IEC 27002. A extensão ao ponto "15.1.2 *Addressing security within supplier agreements*" diz que a organização deve estabelecer acordos com os fornecedores, sempre que sejam processados dados pessoais, os quais devem incluir as medidas mínimas técnicas e organizativas que o fornecedor precisa de cumprir. Estes acordos com fornecedores devem atribuir claramente responsabilidades entre a organização e os seus parceiros e fornecedores, tendo em consideração as atividades de processamento e as categorias de dados pessoais envolvidas. Além disto, devem ainda estabelecer um mecanismo para assegurar que a organização apoia e gere o cumprimento de toda a legislação aplicável, assim como a exigência de auditorias independentes que verifiquem a conformidade com as obrigações relativas ao processamento de dados pessoais.

Na cláusula "16. *Information security incident management*" é acrescentado que, como parte do processo global de gestão de incidentes de segurança da informação, a organização deve estabelecer responsabilidades e procedimentos para a identificação e registo de violações de dados pessoais. Adicionalmente, a organização, enquanto *Controller,* deve ainda estabelecer procedimentos relacionados com a notificação das violações de dados pessoais (por exemplo ao titular dos dados), bem como com a divulgação às respetivas autoridades, tendo em consideração a legislação aplicável. Tais notificações devem ser claras e conter o ponto de contacto para informações adicionais, a descrição da violação e as suas potenciais consequências, a quantidade de pessoas e dados pessoais afetados, assim como as medidas tomadas e planeadas. Quando ocorre um incidente com violação de dados pessoais, a organização deve manter o registo completo do mesmo, incluindo a descrição do incidente, o período de tempo em que ocorreu, as consequências do incidente, o nome do relator, a identificação de a quem o incidente foi reportado, os dados pessoais afetados, se houve ou não necessidade de notificar os titulares ou as autoridades competentes, as medidas tomadas para resolver o incidente e a descrição do resultado do mesmo, nomeadamente se este resultou na indisponibilidade,

perda, divulgação ou alteração de dados pessoais. Enquanto *Processor*, não cabe à organização a responsabilidade de notificar os incidentes às respetivas autoridades, no entanto, deve comunicar prontamente ao *Controller* sempre que tais incidentes ocorram, sendo necessário incluir cláusulas sobre a gestão de incidentes no contrato estabelecido entre as partes, com detalhe relativamente à informação a disponibilizar e o período máximo para tal.

Na última cláusula da ISO/IEC 27002 "18. *Compliance*" é acrescentado que a organização deve identificar quaisquer potenciais sanções legais, relacionadas com o processamento de dados pessoais, incluindo eventuais multas da autoridade de controlo competente. No que concerne ao ponto "18.2.1 *Independent review of information security*", é acrescentado que as organizações, que atuam como *Processor*, devem disponibilizar aos clientes evidências, obtidas de forma independente, de que a segurança da informação é implementada de acordo com as políticas e procedimentos definidos, sempre que as auditorias individuais dos clientes sejam impraticáveis. Por exemplo, a realização de uma auditoria independente é geralmente um método aceitável para satisfazer os interesses do cliente a este respeito. Por último, relativamente às *technical compliance reviews* com as políticas e standards de segurança da informação, a organização deve também incluir a revisão das atividades de processamento de dados pessoais levadas a cabo. Na Tabela 2, encontra-se o resumo da extensão aos requisitos da ISO/IEC 27002:2013 apresentada na cláusula 6 da ISO/IEC 27701:2019.

Tabela 2 - Resumo da extensão aos requisitos da ISO/IEC 27002:2013 apresentada na cláusula 6 da ISO/IEC 27701:2019

Sub-cláusulas ISO/IEC 27002:2013	**Sub-cláusulas ISO/IEC 27701:2019**	**Extensão**
	6.1 *General*	Todos os requisitos da ISO/IEC 27002:2013 que mencionam "*information security*" devem ser alargados a "*information security and privacy*".
5. *Information security policies*	6.2 *Information security policies*	Desenvolvimento de Políticas de Privacidade e declaração de compromisso (cumprimento da legislação de privacidade aplicável e dos termos contratuais).
6.*Organization of information security*	6.3 *Organization of information security*	Designação do ponto de contacto relativo ao processamento de dados pessoais *(Data Protection Officer*). Nomeação das pessoas responsáveis pelo desenvolvimento, implementação, manutenção e monitorização do programa de privacidade.
7. *Human resource security*	6.4 *Human resource security*	Inclusão dos requisitos de privacidade na sensibilização, educação e formação.
8. *Asset management*	6.5 *Asset management*	Estabelecimento de um sistema de classificação da informação que considere os dados pessoais.

		Registo da utilização de dispositivos amovíveis para armazenamento de dados pessoais. Utilização de métodos de apagamento seguro para a eliminação de dados pessoais.
9. *Access control*	6.6 *Access control*	Implementação de procedimentos de registo e cancelamento de registo de *users* para os sistemas onde são processados dados pessoais. Não reativação de *users* para acesso a sistemas onde são processados dados pessoais. Registo dos perfis criados para *users* com acesso a dados pessoais.
10. *Cryptography*	6.7 *Cryptography*	Utilização de encriptação para proteger algumas categorias de dados pessoais.
11. *Physical and environmental security*	6.8 *Physical and environmental security*	Reatribuição de espaço de armazenamento apenas após garantir que os dados pessoais previamente armazenados não estão acessíveis.
12. *Operations security*	6.9 *Operations security*	Inclusão dos requisitos para a recuperação e reposição de dados pessoais na política de *backups*. Recuperação de dados pessoais num estado em que a sua integridade seja garantida. Revisão de *event logs* respetivos ao acesso e alterações efetuadas nos dados pessoais.
13. *Communications security*	6.10 *Communications security*	Garantia de que todos os colaboradores que acedem a dados pessoais estão sujeitos a um acordo de confidencialidade.
14. *Systems acquisition, development and maintenance*	6.11 *Systems acquisition, development and maintenance*	Recurso a encriptação para a transmissão de dados pessoais através de redes não confiáveis. Desenvolvimento de políticas que contribuam para a conformidade com os princípios de *privacy by design and by default*. Desenvolvimento de sistemas de acordo com os princípios de *privacy by design and by default.* Não utilização de dados pessoais reais em testes.
15. *Supplier relationships*	6.12 *Supplier relationships*	Estabelecimento de acordos com os fornecedores que incluam as medidas técnicas e organizativas mínimas que o fornecedor deve cumprir, bem como a definição de responsabilidades.

16. *Information security incident management*	6.13 *Information security incident management*	Estabelecimento de responsabilidades e procedimentos para a identificação e registo de violações de dados pessoais. Estabelecimento de procedimentos para a notificação das violações de dados pessoais e divulgação às respetivas autoridades. Inclusão de cláusulas sobre gestão de incidentes nos contratos com os *Processors*.
18. *Compliance*	6.15 *Compliance*	Identificação das sanções legais relacionadas com o processamento de dados pessoais, incluindo multas da autoridade de controlo competente. Inclusão da revisão das atividades de processamento de dados pessoais, no âmbito das *technical compliance reviews,*

2.2.1.3. Cláusula 7 – Orientações adicionais para *Controllers*

Nesta cláusula da ISO/IEC 27701 são apresentados os requisitos de privacidade específicos, para as organizações que atuam enquanto *Controllers*, os quais, em conjunto com as extensões aos controlos da ISO/IEC 27002 apresentadas na cláusula 6, resultam no *guidance* de privacidade completo a considerar, cujos controlos e objetivos de controlo se encontram enumerados no Anexo A[58].

De seguida, são apresentados os principais tópicos tratados na cláusula 7. Contudo, no capítulo seguinte do presente trabalho, no qual se inclui a análise comparativa dos requisitos do RGPD e da ISO/IEC 27701, será apresentado maior detalhe relativamente às sub-cláusulas e aos controlos e objetivos de controlo apresentados no Anexo A.

A cláusula 7 contém cinco sub-cláusulas, mais precisamente "7.1 *General*", "7.2 *Conditions for collection and processing*", "7.3 *Obligations to PII principals*", "7.4 *Privacy by design and privacy by default*" e "7.5 *PII sharing, transfer, and disclosure*". De uma forma resumida, esta cláusula dita que é necessário identificar e documentar os propósitos específicos para o processamento de dados pessoais, bem como a base legal para tal, de forma a assegurar que o processamento cumpre a legislação e regulamentos relevantes, e que quaisquer alterações ao propósito do processamento definido resultam numa atualização do tratamento de dados pessoais. Adicionalmente, são apresentadas algumas orientações sobre as categorias especiais de dados pessoais, nomeadamente dados sensíveis. No que diz respeito ao consentimento, inclui detalhe sobre quando e como o obter, devendo existir um processo documentado para tal, bem como um registo dos consentimentos obtidos dos titulares dos dados. Também são apresentados os requisitos para a realização de *privacy impact assessments*, de forma a minimizar o risco para os titulares dos dados, assim como para o estabelecimento de contratos com os *Processors* e a definição de responsabilidades, sempre que

[58] International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 29.

existam *joint-controllers*. Para além disto, refere ainda que a organização deve determinar quais os registos necessários a manter, os quais devem servir de suporte às suas obrigações, relativas ao processamento de dados pessoais. Inclui também orientação detalhada sobre as obrigações para com os titulares dos dados, incluindo a informação a fornecer aos titulares, orientação detalhada sobre o acesso a dados pessoais, a correção dos mesmos ou eventual apagamento e, ainda, sobre a retirada de consentimento, bem como obrigações com terceiras-partes e *guidance* relativo às decisões automatizadas que envolvam dados pessoais. Apresenta também requisitos relativos ao conceito de *privacy by design and by default*, mais precisamente relacionados com a limitação da recolha e processamento de dados pessoais nos sistemas, assim como requisitos para garantir a exatidão, a qualidade e a minimização dos dados pessoais, e ainda requisitos para a sua retenção e eliminação. Por último, são fornecidas também linhas guia para a partilha, transferência e divulgação de dados pessoais entre vários países ou jurisdições, as quais são forçosamente pautadas pela legislação aplicável, devendo existir registos que as suportem[59].

2.2.1.4. Cláusula 8 – Orientações adicionais para *Processors*

Na oitava cláusula da ISO/IEC 27701, encontram-se os requisitos de privacidade específicos para as organizações que atuam enquanto *Processors*, os quais, em conjunto com as extensões aos controlos da ISO/IEC 27002 apresentadas na cláusula 6, totalizam os requisitos de privacidade a ter em consideração no Sistema de Gestão, cuja listagem dos controlos e objetivos de controlo se encontra no Anexo B da norma[60].

À semelhança da cláusula anterior, a cláusula 8 está dividida nas mesmas cinco sub-cláusulas, mais precisamente "8.1 *General*", "8.2 *Conditions for collection and processing*", "8.3 *Obligations to PII principals*", "8.4 *Privacy by design and privacy by default*" e "8.5 *PII sharing, transfer, and disclosure*", no entanto, os requisitos são aplicáveis na perspetiva das organizações que processam dados pessoais em nome de outrem, segundo as suas instruções.

De seguida, encontra-se a visão geral dos tópicos da cláusula 8, embora seja apresentado no capítulo seguinte maior detalhe relativamente às sub-cláusulas e aos controlos e objetivos de controlo do Anexo B, como parte integrante da análise comparativa dos requisitos do RGPD e da ISO/IEC 27701.

Portanto, esta cláusula dita que as organizações que atuam enquanto *Processors* devem ter contratos estabelecidos com os clientes (*Controllers*), relativamente ao processamento de dados pessoais, que impõem que os dados pessoais apenas são processados de acordo com as instruções do cliente e esclareçam o papel e as responsabilidades da organização, no que diz respeito à assistência a dar ao cliente para que este cumpra as suas obrigações para com os titulares dos dados. Enquanto *Processor*, a organização deve também ter a capacidade de informar o cliente quando, na

[59] British Standards Institution (BSI), 2019: 5 e International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 29-42.
[60] International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 42.

sua opinião, o processamento de dados pessoais está, de alguma forma, a infringir a legislação aplicável, sem esquecer que deve ser obtido previamente o consentimento para a utilização dos dados pessoais, que identifiquem os clientes, para fins de *marketing* e publicidade. Relativamente aos registos de suporte ao tratamento de dados pessoais, as organizações devem determinar os registos necessários que as ajudem a demonstrar conformidade com as obrigações acordadas. No que diz respeito às obrigações para com os titulares dos dados, são apresentadas orientações detalhadas sobre como as organizações devem proceder para ajudar os clientes a responder a pedidos dos titulares. Quanto ao conceito de *privacy by design and by default*, são dadas orientações específicas para assegurar que os processos e os sistemas são desenhados, de forma a que a recolha e o processamento de dados pessoais seja limitado ao estritamente necessário e de acordo com o propósito definido, gerindo apropriadamente os ficheiros temporários criados durante o processamento, assim como a devolução, transferência ou eliminação segura de dados pessoais, incluindo os controlos adequados para a transferência de dados pessoais. Por último, nesta cláusula, são fornecidas orientações, relativas à partilha, transferência e divulgação de dados pessoais, para as organizações lidarem com as transferências entre vários países ou jurisdições, incluindo instruções sobre os registos necessários de suporte à divulgação de dados pessoais a terceiras partes, assim como instruções para a notificação ao cliente dos pedidos legítimos de partilha de dados, para o compromisso com outros subcontratantes e eventuais alterações de subcontratantes e divulgação dos mesmos ao cliente[61].

2.3. Perspetiva global da legislação de privacidade

Nos últimos quatro anos, mais precisamente desde a implementação do RGPD, a 25 de maio de 2018, tem existido um maior interesse e uma preocupação crescente, tanto por parte dos cidadãos como das empresas, no que diz respeito à privacidade e à proteção dos dados pessoais, bem como a aspiração notória da União Europeia em afirmar-se como uma referência na proteção jurídica dos titulares de dados. Os princípios basilares da proteção de dados pessoais assentam na garantia de que a informação de caráter pessoal é utilizada de forma justa, legal e transparente, bem como adequada, relevante e limitada ao estritamente necessário, de acordo com um propósito específico e explícito, sendo todo o processamento assente no consentimento do titular dos dados[62]. A proteção da privacidade e dos dados pessoais trata-se de um pilar fundamental numa sociedade evoluída e conhecedora do valor dos seus dados, pelo que as leis e regulamentos, com especial destaque para o RGPD, procuram assegurar a total e efetiva aplicação desse direito[63].

No novo mundo virtual em que vivemos, a informação tende a circular sem constrangimentos espaciais, fruto do avanço tecnológico, do qual beneficiam não só os cidadãos, mas também as empresas. Atualmente, a transação de dados pessoais integra as atividades diárias das empresas em todos os setores da economia, tratando-se de uma tendência em crescimento, pelo que a entrada em

[61] British Standards Institution (BSI), 2019: 6 e International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 42-48.
[62] Governo do Reino Unido, s.d.
[63] Alves, 2021: 124-125.

vigor do RGPD, pioneiro no que diz respeito à proteção de dados, trouxe novas preocupações a todas as empresas que, no âmbito do seu negócio, processam e transferem dados pessoais[64]. De acordo com este Regulamento, quando são transferidos dados pessoais para fora da UE, a proteção por este assegurada deve manter-se e, neste sentido, vários países, pautados pelo nível de exigência que a aplicação do RGPD trouxe, e na ausência de uma decisão de adequação da Comissão Europeia, passaram a adotar medidas idênticas de forma a alcançar a desejada *compliance*, que permitisse a continuidade e o crescimento dos seus negócios.

Assim, após a entrada em vigor do RGPD, têm vindo a surgir diversas leis e regulamentos de privacidade pelo mundo fora. Por exemplo, o Brasil adotou a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, a qual apresenta semelhanças evidentes ao RGPD, tendo entrado em vigor a 18 de setembro de 2020[65]. Outro exemplo a considerar, trata-se da primeira lei do Quénia relativa à proteção de dados pessoais, o *Data Protection Act*, com entrada em vigor em novembro de 2019, o qual, uma vez mais, vai ao encontro dos requisitos do RGPD, no que concerne à recolha, partilha e armazenamento de dados pessoais[66]. Outro exemplo a destacar, prende-se com o *California Consumer Privacy Act* (CCPA) de 2018, o qual, também à semelhança do RGPD, veio atribuir aos consumidores um maior controlo sobre as suas informações pessoais, conferindo-lhes o direito de conhecer os dados recolhidos e processados, o direito ao apagamento e à não-discriminação e, ainda, o direito de *opt-out*, sendo atualmente uma referência do direito à privacidade no estado da Califórnia[67]. Esta compatibilidade de regimes acaba por facilitar a troca de dados e, por consequência, facilita o comércio transfronteiriço, fortalecendo a economia digital global e favorecendo a cooperação entre as autoridades policiais e judiciárias, as quais têm como objetivo comum o combate à cibercriminalidade[68].

Na tentativa de uniformizar o nível de proteção dos direitos fundamentais dos cidadãos europeus, na transferência dos seus dados pessoais para países terceiros, isto é, países fora do Espaço Económico Europeu (EEE), a Comissão Europeia recorreu ao estabelecimento de decisões de adequação com os países que, no seu entender, apresentam um nível de proteção adequado. Estas decisões de adequação procuram garantir a conformidade com os requisitos de proteção de dados pessoais da UE, aquando da sua transferência além-fronteiras, cujo efeito prático é permitir o fluxo de dados para esse país terceiro, sem que seja necessária qualquer salvaguarda adicional, sendo este fluxo encarado como se de uma transferência interna se tratasse. Atualmente, existem decisões de adequação com Andorra, Argentina, Canadá, Ilhas Faroé, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, Coreia do Sul, Suíça, Reino Unido e Uruguai[69]. Nas situações em que não existe uma decisão de adequação, a alternativa mais adotada para regular a transferência de dados pessoais para um país terceiro assenta no estabelecimento entre as partes de cláusulas-tipo, ou S*tandard Contratual Clauses (*SCC*)*, as quais garantam contratualmente um nível de proteção equivalente dos dados transferidos, cabendo às autoridades de controlo a competência desta verificação[70]. Esta opção tomou

[64] Jesus, 2018: 72.
[65] Governo do Brasil - Ministério da Defesa, 2020.
[66] Republic of Kenya - National Council for Law Reporting Library, 2019.
[67] Bonta, s.d.
[68] Jesus, 2018: 75.
[69] Comissão Europeia, s.d.
[70] Pinheiro, 2020.

um maior destaque aquando da decisão do Tribunal de Justiça da UE (Acórdão C-311/18), de 16 de julho de 2020, conhecida como *Schrems* II, que veio invalidar a Decisão 2016/1250, relativa à adequação do *Privacy Shield* quanto ao nível de proteção por este assegurado, relativamente aos dados pessoais de cidadãos europeus transferidos para os EUA, tendo, consequentemente, sido emitida pelo *European Data Protection Board* (EDPB)[71] a Recomendação 1/2020[72], relativamente às medidas adicionais para complementar as ferramentas de transferência de dados pessoais[73].

2.3.1. Regulamento Geral de Proteção de Dados

A globalização, em conjunto com a rápida evolução tecnológica, facilitou a livre circulação de dados pessoais e permitiu a sua utilização numa escala sem precedente pelas organizações, o que gerou novos desafios em matéria de proteção de dados pessoais. Esta evolução tecnológica exige um quadro sólido de proteção de dados, apoiado pela aplicação rigorosa de regras, através do qual os titulares dos dados devem poder controlar a utilização dos seus dados pessoais. Neste sentido, foi criado o Regulamento (UE) n.º 2016/679, de 27 de abril de 2016, relativo à proteção das pessoas singulares, no que diz respeito ao tratamento dos seus dados pessoais e à livre circulação desses dados, o qual veio reforçar os direitos fundamentais dos cidadãos da UE na era digital e, de certa forma, minimizar a fragmentação que existia. O Regulamento Geral de Proteção de Dados aplica-se ao tratamento de dados pessoais, efetuado no âmbito das atividades de empresas ou entidades com sucursais estabelecidas na UE, independentemente do local onde os dados são efetivamente processados, bem como ao tratamento de dados pessoais de titulares residentes na UE, efetuado por empresas constituídas fora da UE que ofereçam bens ou serviços a esses titulares ou qualquer tratamento relacionado com o controlo do comportamento destes[74].

O RGPD veio revolucionar a cultura das organizações, uma vez que veio reforçar a orientação pelos mesmos princípios e o respeito pelas mesmas regras, por parte de todos os intervenientes, assim como permitir a criação de produtos e serviços mais éticos ao colocar a temática do direito à proteção dos dados pessoais em cima da mesa[75]. Assim, a entrada em vigor deste Regulamento trouxe consigo a obrigação de todas as organizações, independentemente do local onde estejam estabelecidas, cumprirem com os requisitos de proteção de dados do Regulamento, sempre que processem dados pessoais de cidadãos residentes na UE[76].

O RGPD encontra-se dividido em onze capítulos, os quais por sua vez se dividem em noventa e nove artigos, dos quais irei salientar os mais pertinentes relativamente à temática em estudo. O capítulo I, "Disposições gerais", está dividido em quatro artigos, onde se encontram o objetivo do

[71] Trata-se de um órgão europeu independente cuja missão objetivo é garantir a aplicação consistente do Regulamento Geral de Proteção de Dados bem como promover a cooperação entre as autoridades de proteção de dados da União Europeia. O EDPB foi estabelecido pelo RGPD, o qual veio substituir o Grupo de Trabalho do Artigo 29.º.
[72] Tribunal de Justiça da União Europeia, 2020: 1.
[73] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
[74] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 32-33.
[75] Alves, 2021: 125.
[76] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 32-33.

Regulamento, nomeadamente o de estabelecer regras relativas à proteção dos titulares dos dados, no que diz respeito ao tratamento dos seus dados pessoais; o âmbito de aplicação material, isto é, o tratamento de dados pessoais independentemente de estes serem processados de forma total ou parcialmente automatizada ou não automatizada; o âmbito de aplicação territorial do mesmo, de acordo com o mencionado acima; bem como algumas definições importantes para a leitura de todo o documento[77].

O capítulo II, intitulado de "Princípios", esclarece-nos quanto aos princípios relativos ao tratamento de dados pessoais, ou seja, que os dados devem ser objeto de um tratamento lícito e transparente; ser recolhidos para finalidades explícitas e legítimas; ser adequados e limitados ao propósito pelo qual foram recolhidos; ser exatos e atualizados; e ainda processados de forma segura. Relativamente à licitude do tratamento, são apresentadas as situações em que o tratamento é considerado lícito, nomeadamente após ser dado o consentimento do titular para o tratamento dos seus dados pessoais, na execução de um contrato ou diligências pré-contratuais a pedido do titular, caso o tratamento seja necessário para o cumprimento de uma obrigação jurídica, para a defesa de interesses vitais ou para o exercício de funções de interesse público, bem como para efeito de interesses legítimos prosseguidos pelo responsável do tratamento. As condições aplicáveis ao consentimento são também introduzidas neste ponto, as quais incluem o dever do *Controller* demonstrar que o titular dos dados deu efetivamente o seu consentimento, bem como o direito do titular dos dados retirar o seu consentimento a qualquer momento, devendo estar informado disso mesmo. Para além disto, o pedido de consentimento deve ser apresentado de forma claramente distinta de outros assuntos, ser de fácil acesso e transmitido através de uma linguagem clara e simples. O tratamento de categorias especiais de dados pessoais, isto é, dados sensíveis, é proibido a não ser que sejam reunidas determinadas condições para que esse tratamento seja lícito, como no caso de existir consentimento explícito do titular para o tratamento desses dados, no caso de ser necessário para efeitos do cumprimento de obrigações do *Controller* ou do titular dos dados em matéria de legislação laboral, entre outras situações[78].

O capítulo III é inteiramente dedicado aos direitos dos titulares de dados, sendo, em primeiro lugar, introduzidas as regras para o exercício desses mesmos direitos, nomeadamente a responsabilidade do *Controller* de tomar as medidas adequadas para que o titular dos dados tenha conhecimento dos seus direitos e possa exercer os mesmos, bem como o período estabelecido de um mês para o *Controller* dar seguimento ao pedido de exercício de direito apresentado por parte de um titular. No que diz respeito às informações a facultar ao titular dos dados, é estabelecida uma listagem de informação para as situações em que os dados pessoais são recolhidos junto do titular e para as situações em que a recolha não é efetuada junto do mesmo, tais como a identidade e o contacto do DPO, o propósito e a base legal para o tratamento, os destinatários dos dados pessoais, o período de retenção, entre outros. Quanto aos direitos dos titulares propriamente ditos, estes são os seguintes: o direito de acesso, ou seja, o direito de obter do *Controller* a confirmação de que os seus dados pessoais são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e

[77] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 32-33.
[78] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 35-39.

a informações relativas aos mesmos; o direito de retificação dos dados pessoais caso estes não sejam exatos; o direito ao apagamento, ou o direito a ser esquecido, isto é, obter o apagamento dos seus dados pessoais, sem demora injustificada; o direito à limitação do tratamento por parte do *Controller*; o direito à portabilidade dos dados, ou seja, o direito de receber os dados pessoais previamente fornecidos a um *Controller* e de os transmitir a outro *Controller*; o direito de oposição ao tratamento dos seus dados pessoais; e, por último, o direito de não sujeição a quaisquer decisões individuais automatizadas, incluindo a definição de perfis[79].

O capítulo IV inclui os requisitos relativos às responsabilidades do *Controller* e do *Processor*. Assim, o *Controller*, tendo em consideração o âmbito e as finalidades do tratamento dos dados, deve aplicar as medidas técnicas e organizativas adequadas para garantir e comprovar que o tratamento é realizado em conformidade com o RGPD. Quanto ao *Processor*, este deve apresentar garantias suficientes da implementação das medidas técnicas e organizativas adequadas, de forma a cumprir os requisitos do RGPD, para que o *Controller* possa recorrer a esta entidade para efetuar o tratamento de dados por sua conta. O tratamento de dados pessoais, com recurso a um *Processor*, deve ser regulado por um contrato que vincule esta entidade ao *Controller* e estabeleça a finalidade e a duração do tratamento, as categorias de dados pessoais e dos titulares envolvidas, assim como as obrigações e direitos do *Controller* e as responsabilidades do *Processor,* nomeadamente tratar os dados pessoais apenas mediante instruções documentadas do *Controller* e não subcontratar outro *Processor* sem a sua autorização prévia. Também estão previstas as situações em que existem dois ou mais *Controllers,* a trabalhar de forma conjunta na determinação das finalidades do tratamento, sendo encarados perante o RGPD como responsáveis conjuntos, ou *joint-controllers*, cuja relação deve ser também regulada por um contrato[80].

Neste capítulo é também introduzido o princípio da proteção de dados desde a conceção e por defeito, ou *privacy by design and by default*, o qual estabelece que o *Controller* deve implementar as medidas necessárias para assegurar que, por defeito, apenas são tratados os dados pessoais que forem necessários para cada finalidade específica de tratamento. Estas medidas devem ser selecionadas e implementadas, tendo em consideração as técnicas mais avançadas e os custos da sua aplicação, como por exemplo a pseudonimização ou a encriptação dos dados pessoais, as quais têm o intuito de reforçar a proteção dos dados pessoais na organização, ao aplicar eficazmente os princípios da proteção de dados estabelecidos no RGPD[81].

Ainda sobre o capítulo IV, é importante referir que o *Controller* tem o requisito de manter um registo de todas as atividades de tratamento de dados pessoais levadas a cabo pela organização, o qual deve incluir o nome e os contactos do *Controller*, do DPO e, quando for caso disso, do *joint-controller*; as finalidades do tratamento; as categorias dos titulares e dos dados pessoais; as categorias dos destinatários a quem os dados são divulgados; as transferências de dados para países terceiros ou organizações internacionais; o período de retenção dos dados pessoais; e a descrição das medidas de segurança *in place* para proteger os dados pessoais. O *Processor* tem também a responsabilidade

[79] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 39-46.
[80] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 47-49.
[81] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 48.

de manter um registo idêntico, relativamente às atividades de tratamento de dados pessoais que realiza sob a responsabilidade de um *Controller*[82].

A secção 2 do capítulo IV dedica-se à segurança dos dados pessoais. Nesta secção, há a destacar o requisito de o *Controller* e o *Processor* aplicarem as medidas técnicas e organizativas adequadas, as quais garantam um nível de segurança apropriado ao risco identificado, incluindo, consoante o que for adequado, a pseudonimização e a encriptação dos dados pessoais, a capacidade de assegurar a confidencialidade, a integridade, a disponibilidade e a resiliência permanentes dos sistemas onde os dados são processados, assim como a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais, no caso de ocorrência de um incidente de segurança e privacidade. Outro ponto relevante, prende-se com a notificação em caso de violação de dados pessoais, que deve ser feita pelo *Controller* à autoridade de controlo, no prazo de 72 horas após ter tido conhecimento da mesma. Esta notificação deve incluir a descrição da violação dos dados pessoais, incluindo as categorias e o número de titulares afetados, assim como as categorias dos dados pessoais e seu número aproximado, as potenciais consequências da mesma e as medidas adotadas ou propostas para reparar os danos causados, e o nome e os contactos do DPO. O *Controller* é também responsável por documentar todas as violações de dados pessoais que ocorrem na sua organização, bem como por comunicar a violação dos dados ao titular, sempre que o incidente seja suscetível de implicar um risco elevado para os seus direitos e liberdades[83].

Relativamente à secção 3, há a destacar o requisito de efetuar avaliações de impacto sobre a proteção de dados, nas situações em que o tratamento de dados pessoais utilize novas tecnologias ou que seja suscetível de representar um risco elevado para os titulares. Nas situações previstas neste Regulamento, e de acordo com as listagens divulgadas pelas autoridades de controlo[84], esta avaliação de impacto deve ser levada a cabo pelo *Controller*, antes de se iniciar o tratamento dos dados pessoais, devendo também ser solicitado o parecer do DPO[85].

A secção 4 é dedicada ao DPO, em português Encarregado de Proteção de Dados (EPD), o qual deve estar envolvido em todas as questões relacionadas com a proteção de dados pessoais na organização sendo que, para tal, deve ser apoiado pelo *Controller* e pelo *Processor*, de forma a obter os recursos necessários para o desempenho das suas funções e o acesso às atividades de processamento de dados efetuadas. O DPO reporta diretamente ao *top management* e serve como ponto de contacto para os titulares dos dados esclarecerem todas as questões, relacionadas com o tratamento dos seus dados pessoais e com o exercício dos seus direitos. As funções do DPO incluem informar e aconselhar, relativamente aos requisitos do RGPD e outras disposições de proteção de dados da EU; monitorizar e controlar a conformidade com o RGPD e com as políticas de proteção de dados da organização; sensibilizar e dar formação aos colaboradores da organização; prestar aconselhamento no que diz respeito à avaliação de impacto sobre a proteção de dados; bem como cooperar e ser ponto de contacto para a autoridade de controlo[86].

[82] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 50-51.
[83] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 51-52.
[84] Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados: 1-2.
[85] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 53-54.
[86] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 55-56.

Por último, neste capítulo, encontra-se estabelecido que a criação de procedimentos de certificação em matéria de proteção de dados é promovida, em especial ao nível da UE, para efeitos de comprovação da conformidade das atividades de processamento de dados pessoais, realizadas por *Controllers* e *Processors,* com o RGPD. Estes procedimentos de certificação podem ser também estabelecidos para efeitos de comprovação da existência de garantias adequadas, por parte de *Controllers* e *Processors,* que não estejam sujeitos ao cumprimento do RGPD[87]. Contudo, conforme referido anteriormente, ainda não clarificada qual a certificação a implementar para cumprimento dos artigos 42.º e 43.º do RGPD[88].

Para terminar a apreciação sumária do RGPD, resta mencionar o capítulo V, no qual podemos encontrar as disposições relativas à transferência de dados pessoais para países terceiros ou organizações internacionais, que devem ser respeitadas pelo *Controller* e pelo *Processor*, inclusivamente no que diz respeito às transferências ulteriores do país terceiro para outro país terceiro ou organização internacional. Estas disposições incluem, em primeiro lugar, a possibilidade de transferir dados pessoais com base numa decisão de adequação da Comissão Europeia, ou seja, para um país terceiro considerado seguro (por possuir um nível de proteção equivalente ao da UE), no que diz respeito à proteção de dados pessoais e seus titulares, sem que seja exigida nenhuma autorização específica adicional. Nos casos em que não existe uma decisão de adequação, apenas podem ser transferidos dados pessoais para um país terceiro, caso este apresente garantias adequadas e no qual os titulares dos dados possuam direitos oponíveis e medidas jurídicas corretivas eficazes. Para tal, o *Controller* pode recorrer, por exemplo, ao estabelecimento de cláusulas-tipo de proteção de dados adotadas pela Comissão Europeia ou por uma autoridade de controlo e aprovadas pela Comissão, mas também pode realizar tal transferência por meio de um código de conduta que vincule as partes no país terceiro a aplicarem as medidas de proteção adequadas, ou até mesmo através de um procedimento de certificação, entre outros exemplos[89].

2.3.2. Nova Estratégia da União Europeia para a Cibersegurança

A Comissão Europeia publicou a 16 de dezembro de 2020 a nova estratégia da UE para a Cibersegurança e novas regras para aumentar a resiliência das entidades críticas físicas e digitais. Esta estratégia tem como objetivo reforçar a resiliência coletiva da Europa contra as ciberameaças e contribuir para a garantia de que todos os cidadãos e todas as empresas beneficiem de serviços e ferramentas digitais seguros e fiáveis. Os cidadãos europeus devem poder utilizar dispositivos conectados à *internet*, bem como outros serviços como bancos e hospitais, com a garantia de estarem protegidos contra as ciberameaças, nomeadamente aquelas que possam colocar em causa o seu direito à privacidade[90]. A nova estratégia da UE para a Cibersegurança contempla um reforço no seu papel de liderança, no que diz respeito a regras e normas internacionais no domínio do ciberespaço,

[87] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 58-59.
[88] IPAC – Instituto Português de Acreditação, 2021; IPAC – Instituto Português de Acreditação, s.d.
[89] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 60-65.
[90] Comissão Europeia. Comunicado de Imprensa – Nova Estratégia da EU para a Cibersegurança e novas regras para aumentar a resiliência das entidades críticas físicas e digitais: 1.

permitindo estreitar a cooperação com parceiros de todo o mundo para promover um ciberespaço à escala mundial aberto, estável e seguro, assente no Estado de direito, nos direitos humanos, nas liberdades fundamentais e nos valores democráticos[91].

Na época em que vivemos, "A cibersegurança é uma das principais prioridades da Comissão Europeia e uma pedra angular da Europa digital e conectada. O aumento dos ciberataques durante a crise do coronavírus demonstrou a importância de proteger os hospitais, os centros de investigação e outras infraestruturas. Para preparar a economia e a sociedade europeias para o futuro, são necessárias medidas enérgicas neste domínio", pelo que a nova estratégia apresentada pretende integrar a cibersegurança de forma transversal, agrupando de forma eficaz as atividades e os recursos da UE no mercado interno, aplicação da lei, diplomacia e defesa[92].

[91] Comissão Europeia. Comunicado de Imprensa – Nova Estratégia da EU para a Cibersegurança e novas regras para aumentar a resiliência das entidades críticas físicas e digitais: 1-2.
[92] Comissão Europeia. Comunicado de Imprensa – Nova Estratégia da EU para a Cibersegurança e novas regras para aumentar a resiliência das entidades críticas físicas e digitais: 4.

3. A Gestão da Privacidade nas Organizações

3.1. Papel do standard ISO/IEC 27701 na garantia de conformidade com o RGPD

A Segurança da Informação, apesar de ser essencial para garantir um nível adequado de proteção de dados pessoais, por si só não é suficiente. A prevenção da divulgação e alteração indesejadas, perda ou corrupção dos dados pessoais apenas é verdadeiramente eficaz se existir uma abordagem multidisciplinar capaz de, por um lado, garantir a implementação dos controlos de segurança em todo o ciclo do processamento de dados pessoais e, por outro lado, também compreender os requisitos da legislação de privacidade aplicável e tomar as diligências necessárias para garantir a *compliance* na organização[93]. A implementação de um SGP, em conformidade com a ISO/IEC 27701, tem um impacto significativo na forma como as organizações abordam os requisitos de privacidade do RGPD, uma vez que, à semelhança de várias legislações de privacidade em todo o mundo, também o RGPD fornece informação pouco detalhada sobre como implementar os processos que garantam a conformidade com o mesmo[94].

Neste ponto, a ISO 27701 fornece uma grande ajuda ao detalhar os requisitos para a implementação e melhoria contínua do SGP, os quais, por representarem o estado da arte em termos de privacidade, espelham uma abordagem proativa para a proteção dos dados pessoais na organização[95]. A *Commission Nationale de l'Informatique et des Libertés* (CNIL), isto é, a autoridade de controlo para a proteção de dados francesa, cujos especialistas contribuíram para a elaboração da ISO/IEC 27701, emitiu um comunicado a enfatizar a importância da norma para a proteção dos dados pessoais nas organizações e a destacar que, apesar de não ter sido desenvolvida especificamente para ir ao encontro do RGPD, este foi, de facto, tido em conta na sua elaboração, pelo que a implementação de um SGP alinhado com esta ISO pode ser a chave para o cumprimento das disposições gerais do Regulamento[96].

Por se tratar de um standard relativamente recente, não existe muito *guidance* disponível sobre como e em que medida a ISO 27701 pode apoiar as organizações no cumprimento do RGPD, sendo precisamente este o objetivo de estudo do presente trabalho. Sabendo que a ISO 27701 não foi desenvolvida especificamente para ir ao encontro do RGPD, é necessária a devida adaptação do SGP às suas exigências. Para perceber qual o nível de adaptação necessário, no próximo subcapítulo é apresentada a análise comparativa entre as exigências regulamentares e os requisitos normativos, identificando os pontos de convergência e divergência, de forma a aferir em que medida esta ISO pode, então, garantir a conformidade com o RGPD nas organizações.

[93] Soenen, 2019: 2.
[94] NQA – Global Certification Body, s.d.
[95] NQA – Global Certification Body, s.d.
[96] Commission Nationale Informatique & Libertés, 2020.

3.2. ISO/IEC 27701:2019 e os requisitos do RGPD: Análise comparativa

Conforme referido anteriormente, neste ponto é apresentada a análise comparativa entre as cláusulas 5, 6, 7 e 8 da ISO/IEC 27701:2019, assim como os seus Anexos A e B, e os requisitos do RGPD, com o objetivo de clarificar em que medida a certificação do SGP neste standard fornece as ferramentas necessárias às organizações, para estarem em conformidade com os requisitos do Regulamento e poderem demonstrá-lo através de evidências documentadas.

Na tabela abaixo, com o intuito de facilitar a compreensão, são apresentados alguns termos chave relacionados com a proteção de dados, na medida em que existe uma diferença na terminologia usada na ISO/IEC 27701 e no RGPD.

Tabela 3 - Glossário de termos relacionados na ISO/IEC 27701 e no RGPD.

ISO/IEC 27701	**RGPD**
Personally Identifiable Information (PII)	Dados Pessoais
PII Controller	*Controller* ou Responsável pelo Tratamento
PII Processor	*Processor* ou Subcontratante
Joint PII Controller	*Joint-controller* ou Responsável conjunto pelo Tratamento
PII Principle	Titular dos Dados
Privacy by Design and by Default	Proteção de Dados desde a Conceção e por Defeito

3.2.1. Cláusulas 5, 6, 7 e 8 da ISO/IEC 27701 *vs*. RGPD

Conforme referido anteriormente, a ISO/IEC 27701:2019 trata-se de uma extensão da ISO/IEC 27001:2013, tendo sido já previamente indicados no Capítulo 2.2 os requisitos adicionais previstos no standard para a gestão da Privacidade, os quais devem ser implementados em conjunto com os requisitos para a gestão da Segurança da Informação. Por este motivo, na análise comparativa abaixo, foram tidos também em consideração os requisitos da ISO/IEC 27001 referidos na ISO/IEC 27701.

Tabela 4 - Análise comparativa dos requisitos do RGPD com os da ISO/IEC 27701.

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
Cláusula 5 – Requisitos de privacidade específicos relacionados com a ISO/IEC 27001		
5.2 *Context of the organization*	Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 26.º - Responsáveis conjuntos pelo tratamento Artigo 28.º - Subcontratante Artigo 31.º - Cooperação com a autoridade de controlo	A determinação do papel da organização enquanto *Controller, joint-Controller* ou *Processor* é uma necessidade apresentada tanto na norma como no Regulamento, bem como a preocupação de incluir as autoridades de controlo, *Processors* e outros *Controllers* como parte interessada no processamento de dados pessoais. Na ISO é referido que podem existir requisitos regulamentares relevantes para o processamento de dados pessoais, onde se enquadra o RGPD. Ao contrário da ISO, o RGPD não exige a implementação de um SGP.
5.3 *Leadership*	Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 32.º - Segurança do tratamento Artigo 39.º - Funções do encarregado da proteção de dados Artigo 25.º - Proteção de dados desde a conceção e por defeito	Não existe menção a liderança no RGPD. No entanto, algumas das responsabilidades definidas na ISO para a liderança assemelham-se às responsabilidades do *Controller* e DPO, previstas no RGPD. Pode-se fazer um paralelismo entre os requisitos para o SGP e as medidas técnicas e organizativas exigidas no RGPD, ambas com o objetivo de garantir a proteção dos dados pessoais. No que diz respeito aos objetivos e à política do SGP, estes devem ter em conta os requisitos do RGPD.

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
		O conceito de melhoria contínua está bastante presente na ISO, no entanto, o RGPD ao prever a atualização das medidas técnicas e organizativas, consoante as necessidades, acaba por ter este conceito subentendido ao longo dos seus artigos.
5.4 *Planning*	Artigo 25.º - Proteção de dados desde a conceção e por defeito Artigo 32.º - Segurança do tratamento Artigo 35.º - Avaliação de impacto sobre a proteção de dados Artigo 36.º - Consulta prévia	A avaliação dos riscos de privacidade é requisito comum à ISO e ao RGPD, assim como as regras para a sua *performance*. Apenas na ISO é exigida a elaboração de um SoA, no qual se faz referência aos controlos aplicáveis e não aplicáveis na organização, bem como as respetivas justificações para a inclusão/exclusão (conceito que não existe no RGPD).
5.5 *Support*	Artigo 7.º - Condições aplicáveis ao consentimento Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 26.º - Responsáveis conjuntos pelo tratamento Artigo 28.º - Subcontratante Artigo 30.º - Registos das atividades de tratamento Artigo 33.º - Notificação de uma violação de dados pessoais à autoridade de controlo Artigo 34.º - Comunicação de uma violação de dados pessoais ao titular dos dados	Segundo a ISO, a organização deve providenciar os recursos necessários para o bom funcionamento do SGP, o que vai ao encontro do dever do *Controller/Processor* de fornecer os recursos para o bom desempenho das funções do DPO e manutenção do seu conhecimento, conforme dita o RGPD. A ISO exige que sejam determinadas as competências das pessoas que desempenham funções no SGP, tal como no RGPD é exigido determinado *know-how* para o DPO, assim como para todas as pessoas que tenham acesso a dados pessoais na organização. A formação sobre o SGP é exigida na ISO para todas as pessoas da organização, do mesmo modo que no RGPD se encontra definido que todos os colaboradores com acesso a dados pessoais devem assistir a formações sobre proteção de dados. A ISO requer que sejam definidas as necessidades de comunicação interna e externa relevantes para o SGP, o que vai ao encontro das necessidades de notificação de violações de dados pessoais à autoridade de controlo e ao titular dos dados (externa),

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
	Artigo 37.º - Designação do encarregado da proteção de dados Artigo 38.º - Posição do encarregado da proteção de dados Artigo 39.º - Funções do encarregado da proteção de dados Artigo 47.º - Regras vinculativas aplicáveis às empresas	ou ao *Controller,* caso a organização tenha o papel de *Processor,* e de *awareness* sobre proteção de dados na organização (interna). No que diz respeito à informação documentada, a ISO exige que a organização documente toda a informação que considere necessária para garantir a eficácia do SGP, o que, sem dúvida, inclui a documentação exigida pelo RGPD, como por exemplo os registos das atividades de processamento de dados pessoais.
5.6 *Operation*	Artigo 35.º - Avaliação de impacto sobre a proteção de dados Artigo 36.º - Consulta prévia	Tanto a ISO como o RGPD têm exigências a respeito da avaliação dos riscos de privacidade, as quais, com a devida adaptação, se complementam.
5.7 *Performance Evaluation*	Artigo 28.º - Subcontratante Artigo 40.º - Códigos de conduta Artigo 41.º - Supervisão dos códigos de conduta aprovados Artigo 42.º - Certificação	A ISO tem parâmetros definidos para a monitorização, análise e avaliação da *performance* do SGP, incluindo momentos de revisão pela gestão e auditorias internas, que são obrigatórios para obtenção e manutenção da certificação do SGP. A este respeito, o RGPD não prevê a obrigatoriedade de auditorias internas nem momentos de revisão pela gestão, mas estabelece o direito do *Controller* auditar as práticas do *Processor,* para verificar se este cumpre com o estipulado em contrato ou outro ato normativo, e ainda a certificação voluntária das organizações (a qual, conforme referido anteriormente, não se encontra ainda operacionalizada).
5.8 *Improvement*	Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 25.º - Proteção de dados desde a conceção e por defeito	Apenas na ISO existe a obrigatoriedade de corrigir as não conformidades identificadas no SGP, no seguimento das auditorias internas e externas. Quanto à melhoria contínua, também o RGPD prevê a atualização das medidas técnicas e organizativas, consoante as necessidades, a atualização dos dados pessoais armazenados, entre outros aspetos que acabam por incorporar este conceito no Regulamento.

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
Cláusula 6 – Requisitos de privacidade específicos relacionados com a ISO/IEC 27002		
6.2 *Information security policies*	Artigo 5.º - Princípios relativos ao tratamento de dados pessoais Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 28.º - Subcontratante	A ISO refere a necessidade de existirem políticas de privacidade na organização, que a suportem no compromisso de estar em conformidade com a legislação de proteção de dados aplicável, bem como com os termos contratuais acordados. Apesar de no RGPD não ser exigida a elaboração de políticas, é exigido o cumprimento integral das disposições do Regulamento, o que é precisamente um dos pontos que as Políticas procuram vincular. A conformidade com a legislação e regulamentos aplicáveis é também uma exigência da própria ISO.
6.3 *Organization of information security*	Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 25.º - Proteção de dados desde a conceção e por defeito Artigo 26.º - Responsáveis conjuntos pelo tratamento Artigo 28.º - Subcontratante Artigo 30.º - Registos das atividades de tratamento Artigo 33.º - Notificação de uma violação de dados pessoais à autoridade de controlo Artigo 34.º - Comunicação de uma violação de dados pessoais ao titular dos dados	Na ISO encontra-se definido que a organização deve nomear um ponto de contacto, relativamente ao processamento de dados pessoais para uso dos clientes e dos titulares dos dados. A este respeito, o RGPD define que o DPO deve ser o contacto para os titulares dos dados poderem esclarecer todas as questões relacionadas com o processamento dos seus dados pessoais e com o exercício dos seus direitos, havendo aqui mais um requisito em comum, sustentado pelas regras para a nomeação da tal entidade, semelhantes no standard e no Regulamento. A ISO refere também que devem existir procedimentos para o contacto com as autoridades e para a notificação de incidentes de privacidade, o que vai ao encontro do estipulado no RGPD (responsabilidade do DPO de cooperar com a autoridade de controlo e de ser o seu ponto de contacto na organização; responsabilidade do *Controller* de notificar a autoridade de controlo caso ocorra uma violação de dados pessoais), mesmo que não seja especificamente referido que deve existir um procedimento documentado.

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
	Artigo 35.º - Avaliação de impacto sobre a proteção de dados Artigo 37.º - Designação do encarregado da proteção de dados Artigo 38.º - Posição do encarregado da proteção de dados Artigo 39.º - Funções do encarregado da proteção de dados Artigo 44.º - Princípio geral das transferências Artigo 45.º - Transferências com base numa decisão de adequação Artigo 46.º - Transferências sujeitas a garantias adequadas	A ISO estabelece que os objetivos da privacidade devem ser incluídos nos métodos da organização para a gestão de projetos, de forma a garantir que os objetivos dos projetos incluam os da privacidade, e que seja levada a cabo uma avaliação de risco na fase inicial dos projetos para identificar os controlos necessários. De novo, a ISO dá maior detalhe sobre como implementar o que no fundo é requisito do RGPD – a organização deve conhecer e registar todas as atividades de processamento de dados pessoais efetuadas (incluindo as atividades realizadas em sede de projeto), realizar avaliações de risco nas situações previstas e aplicar controlos para mitigar eventuais riscos inaceitáveis para a organização. No que diz respeito ao *teleworking*, a ISO impõe regras específicas para as organizações que adotem esta forma de trabalhar, enquanto o RGPD não faz qualquer distinção, aplicando-se os mesmos requisitos (responsabilidade do *Controller* aplicar as medidas técnicas e organizativas necessárias para assegurar e comprovar a conformidade com o RGPD) independentemente de o trabalho ser realizado *on-site* ou *off-site*. No RGPD, apenas existem requisitos específicos quando o local de trabalho se encontra fora do EEE, estando estabelecidas regras para a transferência transfronteiriça de dados pessoais, que apenas é permitida sem quaisquer medidas adicionais para os países terceiros que tenham uma decisão de adequação reconhecida pela CE.
6.4 *Human resource security*	Artigo 5.º - Princípios relativos ao tratamento de dados pessoais Artigo 37.º - Designação do encarregado da proteção de dados Artigo 38.º - Posição do encarregado da proteção de dados	Nesta subcláusula, a ISO faz uma série de exigências para os colaboradores em três fases distintas: antes do emprego (*screening* e requisitos contratuais), durante o emprego (responsabilidades, formação e processo disciplinar) e após o emprego (cessação ou mudança das responsabilidades no trabalho). No RGPD não existe esta separação, no entanto, existem requisitos de formação sobre proteção de dados para todos os colaboradores que processem dados pessoais, requisitos quanto à limitação

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
	Artigo 39.º - Funções do encarregado da proteção de dados	do acesso aos mesmos, bem como a necessidade de ter em consideração os requisitos relativos aos direitos dos titulares dos dados e aos princípios para o tratamento dos dados pessoais, aquando da realização das atividades previstas na ISO.
6.5 *Asset management*	Artigo 6.º - Licitude do tratamento Artigo 17.º - Direito ao apagamento dos dados («direito a ser esquecido») Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 25.º - Proteção de dados desde a conceção e por defeito Artigo 30.º - Registos das atividades de tratamento Artigo 32.º - Segurança do tratamento	No que diz respeito aos ativos onde é processada a informação, a ISO exige que estes sejam inventariados, indicando os seus responsáveis. A este respeito, o RGPD exige que nos registos das atividades de tratamento de dados pessoais sejam elencadas as medidas técnicas e organizativas, as quais são implementadas nos locais onde são armazenados e processados dados pessoais, acabando por estar subentendida neste ponto a identificação dos ativos. Relativamente aos ativos de informação, a ISO apresenta ainda uma série de requisitos relativos às regras de uso aceitável, classificação e etiquetagem de informação (de acordo com as categorias de dados pessoais previstas no RGPD) e manuseamento dos ativos que ultrapassam o nível de pormenor existente no Regulamento, o qual refere repetidamente o termo genérico "medidas técnicas e organizativas" que assegurem um nível de proteção adequado, deixando a sua interpretação a cargo das organizações. A ISO refere ainda que os ativos devem ser eliminados de forma segura, através de procedimentos formais, de forma a minimizar o risco de fuga de informação confidencial. Esta medida vai ao encontro do RGPD, na medida em que é exigido o apagamento dos dados pessoais, quando termina o período de retenção ou quando já não existem motivos lícitos para a manutenção dessa informação ou ainda a pedido dos titulares no âmbito do direito ao esquecimento. Quanto à transferência de informação, a ISO exige que esta seja protegida contra o acesso não autorizado ou corrupção durante o seu transporte, nomeadamente através de encriptação, uma medida importante para evitar *data breaches*.

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
6.6 *Access control*	Artigo 6.º - Licitude do tratamento Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 25.º - Proteção de dados desde a conceção e por defeito Artigo 32.º - Segurança do tratamento	Segundo a ISO, deve existir uma política de controlo de acessos através da qual os responsáveis pelos ativos determinem as regras e as permissões/restrições de acesso, tendo como base os requisitos de segurança e privacidade. Apesar do RGPD não exigir uma política, esta é uma medida extremamente importante para garantir que apenas é concedido o acesso a dados pessoais aos *users* que de facto necessitam de aceder para a execução do seu trabalho, e de acordo com as suas necessidades específicas, protegendo os dados contra tratamento não autorizado ou ilícito ao restringir o seu acesso. A ISO também exige que seja mantido um registo dos *users* com acesso aos sistemas de informação que processam dados pessoais, assim como a gestão de acessos privilegiados, a revisão periódica dos acessos, a gestão de *passwords*, entre outras medidas, as quais mais uma vez extravasam o detalhe descrito no Regulamento, apesar de se encaixarem perfeitamente nas "medidas técnicas e organizativas" a implementar na organização, para garantir o processamento seguro e adequado dos dados pessoais.
6.7 *Cryptography*	Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 25.º - Proteção de dados desde a conceção e por defeito Artigo 32.º - Segurança do tratamento	A ISO requer uma política sobre a utilização de controlos criptográficos para a proteção da informação e refere que, em algumas jurisdições, é exigido o recurso à encriptação para proteger certas categorias de dados pessoais. No RGPD encontra-se estabelecido que tendo em conta a natureza e o âmbito das atividades de tratamento, assim como os riscos associados, devem ser aplicadas medidas para garantir a segurança do tratamento, dando como exemplo a pseudonimização e a encriptação de dados pessoais. A ISO vai para além do detalhe do RGPD ao incluir, por exemplo, requisitos para a gestão das chaves criptográficas.

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
6.8 *Physical and environmental security*	Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 25.º - Proteção de dados desde a conceção e por defeito Artigo 32.º - Segurança do tratamento	No que diz respeito à segurança física, o RGPD não faz qualquer distinção das restantes medidas de segurança incluídas nas "medicas técnicas e organizativas", pelo que a ISO vem, uma vez mais, acrescentar maior *guidance* para a implementação das medidas necessárias para assegurar um nível de proteção adequado. Por exemplo um requisito, relacionado com a reutilização de equipamentos, refere que deve ser assegurado que os dados pessoais anteriormente lá armazenados não podem estar acessíveis, indo ao encontro dos requisitos do RGPD relacionados com a limitação do acesso.
6.9 *Operations security*	Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 25.º - Proteção de dados desde a conceção e por defeito Artigo 32.º - Segurança do tratamento	A ISO requer que sejam documentados procedimentos que suportem as atividades operacionais relacionadas com o processamento de informação, incluindo a instalação e configuração de sistemas, *backup*, gestão de *audit trail*, etc. Relativamente ao *backup*, deve haver particular atenção quando existem dados pessoais no conteúdo da informação a recuperar, os quais podem ter de ser anonimizados/eliminados por se encontrarem desatualizados. A monitorização de *event logs* no acesso a dados pessoais é recomendada na ISO como uma medida para registar o acesso aos dados (quem, quando, a que dados acedeu e quais as alterações efetuadas). Estas medidas não se encontram explícitas no RGPD, mas são importantes para atingir o seu grande objetivo de assegurar um nível de proteção adequada dos dados pessoais e seus titulares, bem como a capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas.
6.10 *Communications security*	Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 25.º - Proteção de dados desde a conceção e por defeito Artigo 28.º - Subcontratante	A ISO vai ao detalhe da segurança da informação na rede, pelo que exige a implementação de controlos neste sentido, o que, de novo, vai além do exigido no RGPD, apesar de serem medidas subentendidas no âmbito das "medidas técnicas e organizativas" e com um objetivo em comum. No que diz respeito aos acordos de confidencialidade/não-divulgação, a ISO estabelece que os colaboradores que têm

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
	Artigo 32.º - Segurança do tratamento	acesso a dados pessoais devem estar sujeitos a um acordo que refira as suas obrigações, o que vai ao encontro do requisito do RGPD relativamente aos subcontratantes.
6.11 *Systems acquisition, development and maintenance*	Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 25.º - Proteção de dados desde a conceção e por defeito Artigo 32.º - Segurança do tratamento	A ISO estabelece que os requisitos de segurança da informação e privacidade devem ser considerados nos requisitos para os novos sistemas de informação onde sejam processados dados pessoais, bem como para melhoria dos sistemas já existentes. Neste ponto são também exigidas políticas que contribuam para a conformidade com o conceito de *privacy by design and by default*, as quais devem incluir *guidance* para a implementação dos princípios de privacidade, de acordo com a legislação aplicável, o que vai ao encontro do requisito do RGPD relativo à proteção de dados desde a conceção e por defeito. Mais acrescenta que, os sistemas relacionados com o tratamento de dados pessoais devem ser concebidos segundo os princípios de *privacy by design and by default*, facilitando a implementação dos controlos relevantes que limitem a recolha e o processamento de dados pessoais ao estritamente necessário, tal como previsto no RGPD.
6.12 *Supplier relationships*	Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 25.º - Proteção de dados desde a conceção e por defeito Artigo 28.º - Subcontratante Artigo 32.º - Segurança do tratamento	A respeito da gestão de fornecedores, a ISO exige a mitigação dos riscos associados ao acesso dos fornecedores aos ativos da organização, incluindo dados pessoais. Aqui é possível fazer um paralelismo entre os fornecedores (ISO) e os subcontratantes (RGPD), uma vez que ambos os termos se referem a uma terceira parte que processa dados pessoais da organização (*Controller*) em regime de prestação de serviços. Tanto no standard como no Regulamento, é requisito existir um contrato entre as partes onde estejam estabelecidos os requisitos de segurança da informação e privacidade e as responsabilidades de ambas as partes, bem como a finalidade e a duração do

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
		tratamento, as categorias de dados pessoais e de titulares dos dados envolvidos, entre outros requisitos.
6.13 *Information security incident management*	Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 33.º - Notificação de uma violação de dados pessoais à autoridade de controlo Artigo 34.º - Comunicação de uma violação de dados pessoais ao titular dos dados Artigo 39.º - Funções do encarregado da proteção de dados	Segundo a ISO, como parte do processo de gestão de incidentes de segurança da informação, a organização deve estabelecer responsabilidades e procedimentos para a identificação, registo e notificação de violações de dados pessoais. Neste ponto, ao referir que as organizações devem ter em conta os regulamentos aplicáveis, a ISO acaba por estar alinhada com o RGPD, o qual define um prazo de 72 horas para o *Controller* notificar a autoridade de controlo competente, bem como a informação a incluir na notificação, semelhante no standard e no Regulamento.
6.14 *Information security aspects of business continuity management*	Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 28.º - Subcontratante Artigo 25.º - Proteção de dados desde a conceção e por defeito Artigo 32.º - Segurança do tratamento	A ISO estabelece que a organização deve determinar os seus requisitos de segurança da informação e privacidade no âmbito da continuidade do negócio, nomeadamente na ocorrência de uma crise ou uma catástrofe. O RGPD não vai ao detalhe dos requisitos para os *Controllers* e *Processors* relativos à continuidade do negócio, mas estes podem ser enquadrados nos requisitos previstos para a segurança do tratamento, de forma a proteger os dados pessoais contra o acesso indesejado e respetiva divulgação, como consequência de um desastre que afete a informação da organização, devendo ser implementados planos de resposta a incidentes e planos de recuperação, bem como redundâncias das unidades de processamento de informação.
6.15 *Compliance*	Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 28.º - Subcontratante	A ISO dedica esta subcláusula aos requisitos para evitar violações de obrigações legais, regulamentares ou contratuais relacionadas com a segurança da informação e privacidade. A organização deve identificar e documentar todos os requisitos

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
	Artigo 5.º - Princípios relativos ao tratamento de dados pessoais	regulamentares e contratuais relevantes, assim como a sua abordagem para os cumprir. O RGPD é de cumprimento obrigatório pelas organizações que processam dados pessoais de titulares residentes na UE, pelo que as suas exigências e a abordagem para o seu cumprimento deve ser incluída neste ponto, de forma a evitar a aplicação das sanções previstas. Caso a organização tenha negócios noutros países fora da UE, a legislação desses mesmos países também deve ser considerada. Nesta subcláusula existem também requisitos relativos à propriedade intelectual, os quais não são objeto do Regulamento.
Cláusula 7 – Orientações adicionais para *Controllers*		
7.2 *Conditions for collection and processing*	Artigo 5.º - Princípios relativos ao tratamento de dados pessoais Artigo 6.º - Licitude do tratamento Artigo 7.º - Condições aplicáveis ao consentimento Artigo 9.º - Tratamento de categorias especiais de dados pessoais Artigo 11.º - Tratamento que não exige identificação Artigo 12.º - Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados	Neste ponto, a ISO estabelece os requisitos para um processamento de dados pessoais legal e com propósito bem definido, incluindo condições para a recolha e processamento dos dados, a identificação do propósito e da base legal para o tratamento, assim como as formas adequadas para obter e registar o consentimento dos titulares dos dados. Para além disto, são referidas ainda instruções para a realização *de privacy impact assessments*, para o estabelecimento de contratos com *Processors* e para a elaboração dos registos das atividades de tratamento. Nesta subcláusula, a ISO está totalmente alinhada com os requisitos do RGPD relacionados com os tópicos acima, descrevendo o "*implementation guidance*" em conformidade.

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
	Artigo 15.º - Direito de acesso do titular dos dados Artigo 16.º - Direito de retificação Artigo 17.º - Direito ao apagamento dos dados («direito a ser esquecido») Artigo 18.º - Direito à limitação do tratamento Artigo 19.º - Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento Artigo 20.º - Direito de portabilidade dos dados Artigo 21.º - Direito de oposição Artigo 22.º - Decisões individuais automatizadas, incluindo definição de perfis Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 25.º - Proteção de dados desde a conceção e por defeito Artigo 26.º - Responsáveis conjuntos pelo tratamento Artigo 28.º - Subcontratante	

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
	Artigo 30.º - Registos das atividades de tratamento Artigo 32.º - Segurança do tratamento Artigo 35.º - Avaliação de impacto sobre a proteção de dados	
7.3 *Obligations to PII principals*	Artigo 5.º - Princípios relativos ao tratamento de dados pessoais Artigo 6.º - Licitude do tratamento Artigo 7.º - Condições aplicáveis ao consentimento Artigo 12.º - Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados Artigo 13.º - Informações a facultar quando os dados pessoais são recolhidos junto do titular Artigo 14.º - Informações a facultar quando os dados pessoais não são recolhidos junto do titular Artigo 15.º - Direito de acesso do titular dos dados Artigo 16.º - Direito de retificação	Esta subcláusula estabelece as obrigações perante os titulares dos dados, relativamente ao processamento dos seus dados pessoais, assim como as informações que lhes devem ser fornecidas. Estas obrigações devem estar alinhadas com os requisitos legais, onde se inclui o RGPD. De acordo com a ISO, devem ser determinadas e documentadas as obrigações que a organização tem para com os titulares dos dados, bem como definidos os meios para as cumprir. Estes requisitos estão muito alinhados com o RGPD, inclusive nas informações a facultar aos titulares (por exemplo, os contactos do *Controller*, a finalidade e o propósito do tratamento, etc.), apenas com a diferença de que no Regulamento existem listagens diferentes para as situações em que os dados pessoais são recolhidos junto do titular e nas situações em que não são. Na ISO são também definidos os meios para providenciar esta informação aos titulares, sendo referido que deve ser feito de forma completa e transparente, utilizando linguagem clara e simples, apropriada à audiência, e ser de fácil acesso, o que também vai totalmente ao encontro do definido no RGPD. No que diz respeito ao direito dos titulares modificarem ou retirarem o consentimento, objetarem ao tratamento, acederem aos dados pessoais que lhes dizem respeito e solicitar a retificação ou o apagamento dos mesmos, todos são vinculados pelo RGPD e referidos nesta subcláusula da ISO acompanhados com "*implementation guidance*", para facilitar o seu cumprimento por parte das organizações. Para além destes direitos, o RGPD estabelece ainda o direito

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
	Artigo 17.º - Direito ao apagamento dos dados («direito a ser esquecido») Artigo 18.º - Direito à limitação do tratamento Artigo 20.º - Direito de portabilidade dos dados Artigo 21.º - Direito de oposição Artigo 22.º - Decisões individuais automatizadas, incluindo definição de perfis Artigo 24.º - Responsabilidade do responsável pelo tratamento	à limitação do tratamento e à portabilidade dos dados. Tanto no RGPD como na ISO, se encontra definido que o responsável pelo tratamento tem a obrigação de comunicar as alterações solicitadas ao tratamento de dados pessoais a todas as terceiras partes envolvidas no processamento, assim como a obrigação de providenciar uma cópia dos dados pessoais que são alvo de processamento, quando solicitado pelo titular dos dados. A ISO estabelece que devem ser definidas políticas e procedimentos para gerir e responder aos pedidos de exercício de direito dos titulares, devendo ser definido um período de resposta por parte da organização, de acordo com a legislação aplicável. Relativamente a este ponto, o RGPD estabelece um período máximo de um mês a contar da data de receção do pedido. Por último, no que concerne às decisões automatizadas, a ISO refere que a organização deve identificar as obrigações para com os titulares dos dados resultantes de decisões exclusivamente automatizadas que lhes digam respeito, as quais devem ser definidas em consonância com as obrigações legais, o que inclui, mais uma vez, as exigências do RGPD – o titular dos dados tem o direito de não ser sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis.
7.4 *Privacy by design and privacy by default*	Artigo 5.º - Princípios relativos ao tratamento de dados pessoais Artigo 6.º - Licitude do tratamento Artigo 24.º - Responsabilidade do responsável pelo tratamento Artigo 25.º - Proteção de dados desde a conceção e por defeito Artigo 32.º - Segurança do tratamento	Esta subcláusula tem o objetivo de assegurar que os processos e sistemas são concebidos de forma que a recolha e o processamento de dados pessoais sejam limitados ao necessário, sendo fornecidas linhas guia para limitar a recolha e o processamento de dados pessoais, para garantir a pertinência e a qualidade dos dados e cumprir com o objetivo de minimização dos mesmos, assim como para a sua anonimização e apagamento quando já não são necessários para o propósito inicialmente definido e ainda para definir o período de retenção. O *guidance* fornecido pela ISO neste ponto ajuda no cumprimento dos princípios relativos ao tratamento de

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
	Artigo 44.º - Princípio geral das transferências Artigo 45.º - Transferências com base numa decisão de adequação Artigo 46.º - Transferências sujeitas a garantias adequadas Artigo 47.º - Regras vinculativas aplicáveis às empresas Artigo 48.º - Transferências ou divulgações não autorizadas pelo direito da União	dados pessoais exigidos no RGPD. Ainda neste ponto, a ISO refere que a organização deve proteger os dados pessoais com controlos de segurança apropriados, quando existe necessidade de os transmitir para uma terceira parte, de forma que estes cheguem ao destino sem qualquer incidente. Este requisito vai ao encontro das exigências do RGPD relativas à transferência de dados pessoais, as quais são mais detalhadas na subcláusula seguinte da ISO.
7.5 *PII sharing, transfer, and disclosure*	Artigo 30.º - Registos das atividades de tratamento Artigo 32.º - Segurança do tratamento Artigo 36.º - Consulta prévia Artigo 44.º - Princípio geral das transferências Artigo 45.º - Transferências com base numa decisão de adequação Artigo 46.º - Transferências sujeitas a garantias adequadas Artigo 47.º - Regras vinculativas aplicáveis às empresas	O objetivo desta subcláusula da ISO é garantir que a partilha de dados pessoais, bem como a sua transferência para países terceiros é realizada em conformidade com as obrigações aplicáveis, pelo que os requisitos do RGPD relativos à transferência de dados pessoais são tidos em consideração. Por exemplo, é requisito do standard e do Regulamento identificar a base legal para a transferência de dados pessoais entre países ou organizações internacionais; registar as transferências de dados pessoais bem como a sua partilha com terceiras partes (no RGPD é requisito do registo das atividades de tratamento). No que diz respeito às transferências de dados pessoais, o RGPD estabelece requisitos para dois tipos de transferências, nomeadamente transferências com base numa decisão de adequação, isto é, para países considerados seguros pela CE por terem medidas de proteção oponíveis às garantidas na UE, e transferências sujeitas a garantias adequadas, ou seja, quando não existe decisão de adequação, sendo necessário salvaguardar que o país em causa providencia um nível

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
	Artigo 48.º - Transferências ou divulgações não autorizadas pelo direito da União Artigo 49.º - Derrogações para situações específicas	de proteção equivalente aos titulares dos dados, previamente à transferência. No entanto, estando explícito na ISO que as organizações devem ter em consideração a legislação aplicável, com a devida interpretação da norma, estes requisitos estão alinhados.
Cláusula 8 – Orientações adicionais para *Processors*		
8.2 *Conditions for collection and processing*	Artigo 28.º - Subcontratante Artigo 32.º - Segurança do tratamento Artigo 33.º - Notificação de uma violação de dados pessoais à autoridade de controlo Artigo 35.º - Avaliação de impacto sobre a proteção de dados	Esta subcláusula da ISO, à semelhança das subcláusulas abaixo, repete-se em relação à cláusula 7, mas na perspetiva de uma organização que atua enquanto *Processor*. Assim, na ISO é exigido o estabelecimento de um contrato para o processamento de dados pessoais que esclareça as suas obrigações para com o *Controller*, tais como a notificação de incidentes que envolvam dados pessoais, a realização de *privacy impact assessments*, a implementação de medidas que assegurem a segurança do processamento, etc. Para além disto, o contrato entre as partes deve também estabelecer que os dados são processados estritamente de acordo com as instruções do *Controller* e durante o tempo estipulado. Estes requisitos estão muito alinhados com as exigências do RGPD relativas aos subcontratantes, cujo tratamento em subcontratação deve ser regulado por contrato, ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o *Processor* ao *Controller*, estabeleça o objeto, a finalidade e a duração do tratamento, as categorias de dados pessoais e de titulares dos dados, bem como as obrigações e os direitos de ambas as partes, com destaque para o facto do *Processor* apenas tratar os dados pessoais de acordo com instruções documentadas do *Controller*.
8.3 *Obligations to PII principals*	Artigo 5.º - Princípios relativos ao tratamento de dados pessoais	Esta subcláusula estabelece as obrigações dos *Processors* perante os titulares dos dados. Enquanto *Processors*, as organizações devem garantir que são providenciadas

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
	Artigo 15.º - Direito de acesso do titular dos dados Artigo 16.º - Direito de retificação Artigo 17.º - Direito ao apagamento dos dados («direito a ser esquecido») Artigo 18.º - Direito à limitação do tratamento Artigo 28.º - Subcontratante Artigo 29.º - Tratamento sob a autoridade do responsável pelo tratamento ou do subcontratante Artigo 32.º - Segurança do tratamento	as informações adequadas, relativamente ao processamento de dados pessoais, indo ao encontro dos direitos estipulados no RGPD para os titulares. Tratando-se de um *Processor*, as suas obrigações devem ser estabelecidas no contrato com o *Controller*, como por exemplo a obrigação de corrigir dados pessoais incorretos/desatualizados nos seus sistemas, bem como assegurar a sua eliminação nos períodos previstos.
8.4 *Privacy by design and privacy by default*	Artigo 25.º - Proteção de dados desde a conceção e por defeito Artigo 28.º - Subcontratante Artigo 32.º - Segurança do tratamento	O objetivo desta subcláusula prende-se com a garantia que os processos e sistemas são concebidos de forma a que a recolha e o processamento de dados pessoais seja limitado ao estritamente necessário, de acordo com o princípio de *privacy by design and by default*, estabelecendo requisitos específicos para a eliminação dos ficheiros temporários que contenham dados pessoais; para devolver, transferir ou eliminar dados pessoais de forma segura, de acordo com o definido no contrato entre o *Controller* e o *Processor*; e para as redes utilizadas para transmitir dados pessoais, as quais devem ser seguras, permitindo a transmissão dos dados sem o seu comprometimento. O princípio de *privacy by design and by default* é estabelecido no RGPD como responsabilidade do *Controller*, no entanto, cabe ao *Processor* prestar-lhe assistência através da implementação de medidas técnicas e organizativas adequadas, tendo também o dever de garantir a segurança do tratamento. Assim, esta subcláusula vai

Subcláusulas da ISO/IEC 27701	Artigos do RGPD	Observações
		também ao encontro do definido no RGPD e providencia algum *guidance* para o seu cumprimento.
8.5 *PII sharing, transfer, and disclosure*	Artigo 28.º - Subcontratante Artigo 30.º - Registos das atividades de tratamento Artigo 32.º - Segurança do tratamento Artigo 44.º - Princípio geral das transferências Artigo 45.º - Transferências com base numa decisão de adequação Artigo 46.º - Transferências sujeitas a garantias adequadas Artigo 47.º - Regras vinculativas aplicáveis às empresas Artigo 48.º - Transferências ou divulgações não autorizadas pelo direito da União Artigo 49.º - Derrogações para situações específicas	Aqui o objetivo é garantir que a partilha de dados pessoais e a sua transferência para países fora da UE é realizada em conformidade com as obrigações aplicáveis, as quais incluem os requisitos do RGPD relativos à transferência de dados pessoais. Enquanto *Processor*, a organização apenas deve transferir dados pessoais de acordo com as instruções do *Controller* e deve informá-lo se existirem transferências e sempre que existam alterações para que possa tomar uma decisão sobre as mesmas. De acordo com o RGPD, caso as transferências sejam para países terceiros, tal só é possível caso existam decisões de adequação estabelecidas ou, eventualmente, acordos entre o remetente e o destinatário dos dados, nomeadamente *standard contractual clauses.* Segundo a ISO, quando ocorre transferência, estes países devem ser registados. Tanto na ISO como no RGPD é exigido que a partilha de dados pessoais com terceiras partes seja registada, incluindo a indicação dos dados pessoais que são partilhados. Enquanto *Processor*, se a organização for notificada por uma autoridade para partilhar dados pessoais deve notificar o *Controller* de tal pedido dentro dos prazos acordados, no entanto, tem o dever de cooperar com a autoridade de controlo a pedido desta. Se se tratar de um pedido que não seja juridicamente vinculativo, o *Controller* deve ser consultado antes de qualquer partilha. Tanto no standard como no Regulamento, é exigido que o *Processor* informe o *Controller* caso recorra a subcontratantes, devendo ser autorizado pelo *Controller* e estar estabelecido em contrato, assim como quando exista uma alteração nos subcontratantes utilizados.

3.2.2. Anexo A da ISO/IEC 27701 *vs*. RGPD

Este anexo é uma extensão ao Anexo A da ISO/IEC 27001:2013 que complementa os requisitos da cláusula 7 da ISO/IEC 27701:2019, o qual deve ser utilizado pelas organizações que atuam como *Controllers*, independentemente de recorrerem ou não a *Processors*. Neste anexo, repetem-se as subcláusulas 7.1, 7.2, 7.3, 7.4 e 7.5, analisadas acima, que definem o objetivo do controlo, bem como as respetivas indentações, que têm um controlo associado que descreve exatamente o que as organizações devem implementar para estar em cumprimento com o requisito da norma e, consequentemente, com a legislação que lhes é aplicável. Por exemplo, o controlo A.7.2.1, *Identify and document purpose*, estabelece que a organização deve identificar e documentar os propósitos específicos para o processamento de dados pessoais e o controlo A.7.4.1, *Limit collection*, define que a organização deve limitar a recolha de dados pessoais ao mínimo possível e de forma proporcional ao propósito identificado para o tratamento[97]. Todos os controlos presentes neste anexo são equivalentes aos requisitos da cláusula 7, apenas simplificados e descritos de um ponto de vista mais operacional, isto é, indicando uma ação específica para a organização levar a cabo, cuja comparação com as exigências do RGPD foi realizada na Tabela 4.

Os controlos do Anexo A estão muito alinhados com o RGPD, nomeadamente com os requisitos relativos aos princípios do tratamento de dados pessoais, tais como o facto dos dados pessoais serem recolhidos para finalidades determinadas, explícitas e legítimas e serem adequados, pertinentes e limitados ao que é necessário, bem como objeto de um tratamento lícito e transparente[98]. Para além dos controlos estarem alinhados com os princípios do tratamento, estão também com as condições aplicáveis ao consentimento, devendo a organização ser capaz de demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais; com os requisitos para o recurso a *Processors*, nomeadamente com a necessidade de existir um contrato entre as partes que estabeleça o objeto e a duração do tratamento, as categorias de dados pessoais e dos titulares, bem como as responsabilidades perante o *Controller* e as condições específicas para o tratamento; e com as imposições relativas ao registo das atividades de tratamento que estabelecem que o *Controller* deve registar todas as atividades de processamento de dados pessoais que são realizadas sob a sua responsabilidade, as quais devem incluir o nome e o contacto do responsável pelo tratamento, a finalidade do tratamento, as categorias dos dados e dos titulares, a identificação dos destinatários a quem os dados são divulgados, identificação se existe transferência de dados pessoais para países terceiros, o período de retenção dos dados e ainda a descrição das medidas técnicas e organizativas que asseguram a segurança do tratamento[99]. Ainda encontramos paralelismo com os requisitos do RGPD relativos à avaliação de impacto sobre a proteção de dados, ou seja, para a realização de PIAs, em particular quando o tratamento utiliza novas tecnologias e nas situações definidas pela autoridade de controlo competente[100].

[97] International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 49-51.
[98] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 35-36.
[99] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 37; 49-51.
[100] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 53-54.

3.2.3. Anexo B da ISO/IEC 27701 *vs*. RGPD

Este anexo é uma extensão ao Anexo A da ISO/IEC 27001:2013 que complementa os requisitos da cláusula 8 da ISO/IEC 27701:2019, o qual deve ser utilizado pelas organizações que atuam como *Processors*, independentemente de recorrerem ou não a outros *Processors*. Neste anexo, repetem-se as subcláusulas 8.1, 8.2, 8.3, 8.4 e 8.5, anteriormente analisadas, que definem o objetivo do controlo, bem como as respetivas indentações, as quais têm um controlo associado que descreve o que as organizações devem implementar para assegurar o cumprimento dos requisitos da norma, assim como com a legislação aplicável. Por exemplo, o controlo B.8.2.1, *Customer agreement*, define que a organização deve assegurar que o contrato estabelecido para o tratamento de dados pessoais determina o seu papel na prestação de assistência ao *Controller*, de forma que este consiga cumprir com as suas obrigações perante os titulares dos dados, e o controlo B.8.5.3, *Records of PII disclosure to third parties*, define que a organização deve registar sempre que partilhe dados pessoais com terceiras partes, incluindo nesse registo quais os dados pessoais partilhados, com quem e quando foram partilhados[101]. Á semelhança do que acontece com o Anexo A, todos os controlos presentes no Anexo B são equivalentes aos requisitos da cláusula 8, estando apenas descritos de forma diferente, nomeadamente no formato de uma ação que a organização deve tomar, cuja comparação com as exigências do RGPD foi também realizada na Tabela 4.

Os controlos do Anexo B estão em linha com o RGPD, em particular com os requisitos para a contratação de *Processors*, cujo tratamento em regime de subcontratação deve ser regulado por contrato, ou outro ato normativo ao abrigo do direito da UE, que vincule o *Processor* ao *Controller*, estabeleça o objeto, a duração e a finalidade do tratamento e ainda garanta que o processamento de dados pessoais é efetuado exclusivamente de acordo com as instruções documentadas do *Controller* e que o *Processor* só contrata outro subcontratante com a devida autorização do *Controller*. Para além dos requisitos para a contratação, também é exigido no standard e no Regulamento que o *Processor* informe prontamente o responsável pelo tratamento caso, no seu entender, alguma instrução viole o RGPD ou outra legislação aplicável em matéria de proteção de dados, devendo ainda prestar auxílio e disponibilizar a informação necessária para que o *Controller* consiga demonstrar o cumprimento das suas obrigações. Existe também alinhamento no que diz respeito ao dever do *Processor* de apagar ou devolver os dados pessoais, consoante a escolha do *Controller*, quando a prestação de serviços relacionada com o tratamento estiver concluída[102]. A transferência de dados pessoais pelo *Processor* deve respeitar as instruções documentadas do *Controller* para tal, bem como o princípio geral das transferências para países terceiros previsto no RGPD e, no que diz respeito aos registos, devem ser documentados os destinatários dos dados pessoais incluindo o país de destino[103]. Por último, também existe concordância relativamente ao dever de informar o *Controller* quando existem pedidos de divulgação de dados pessoais, salvo se estiver proibido de o fazer por motivos de interesse público[104].

[101] International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 53-54.
[102] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 49-50.
[103] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 50-51; 60-61.
[104] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 50-51; 60-61.

3.3. Pontos de convergência

Após análise cuidada das cláusulas 5, 6, 7 e 8 da ISO/IEC 27701:2019 e dos requisitos para a proteção de dados exigidos no RGPD, procedemos ao estudo dos pontos de convergência entre o standard para a gestão da privacidade e o Regulamento, os quais, como vimos, têm um papel preponderante na demonstração da conformidade das organizações com os requisitos regulatórios aplicáveis.

De acordo com o Anexo D da ISO/IEC 27701:2019, a norma cobre os artigos 5.º ao 49.º do RGPD, com exceção do artigo 43.º (Organismos de certificação), sendo que os restantes artigos, do 50.º ao 99.º, não se dirigem diretamente às organizações mas sim às autoridades de controlo, ao Comité Europeu para a Proteção de Dados e aos Estados-Membros, tratando-se de requisitos que, na sua maioria, extravasam as responsabilidades das organizações enquanto *Controllers* e/ou *Processors*, sendo esta a razão principal para não estarem incluídos na ISO. Assim, é possível afirmar que a norma e o RGPD têm uma ampla convergência, nomeadamente na determinação do papel e das responsabilidades da organização enquanto *Controller, joint-Controller* ou *Processor*; na definição de medidas técnicas e organizativas que garantam a segurança do tratamento de dados pessoais (apesar de na norma serem mais detalhadas); na aplicação do conceito de melhoria contínua quer nas medidas técnicas e organizativas utilizadas, quer nos dados pessoais processados (os quais devem estar sempre atualizados); na avaliação dos riscos de privacidade; na disponibilização dos recursos necessários para o bom desempenho e funcionamento da organização, no que diz respeito às exigências de proteção de dados; na exigência de formação adequada das pessoas que têm acesso a dados pessoais; na definição de necessidades de comunicação interna e externa, como por exemplo para a notificação de *personal data breaches,* internamente para as equipas dedicadas ou externamente para a autoridade de controlo competente; na necessidade de existir *awareness* sobre a temática de proteção de dados em toda a organização; no registo de todas as atividades de processamento de dados pessoais levadas a cabo, incluindo a identificação dos ativos onde se encontram os dados pessoais; na exigência de conformidade com a legislação e regulamentos aplicáveis (onde se inclui obviamente o RGPD); na definição de um ponto de contacto para questões relacionadas com o processamento de dados pessoais, quer para os titulares dos dados quer para as autoridades competentes, cujo papel é compatível com o do DPO definido no RGPD; na garantia de que apenas quem necessita de aceder a dados pessoais tem acesso aos mesmos; na utilização de controlos criptográficos para a proteção de certas categorias de dados pessoais; na capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas onde são processados dados pessoais; no estabelecimento de contrato entre o *Controller* e o *Processor* onde estejam estabelecidos os requisitos de proteção de dados, bem como na necessidade dos colaboradores, que acedem a dados pessoais, assumirem um compromisso de confidencialidade; na necessidade de seguir os princípios de *privacy by design and by default* nos sistemas relacionados com o tratamento de dados pessoais; e nas regras para a notificação de *privacy breaches* às autoridades de controlo e tratamento dos mesmos.

De salientar ainda que os requisitos das cláusulas 7 e 8, para os *Controllers* e *Processors*, respetivamente, estão muito em linha com os artigos 5.º (Princípios relativos ao tratamento de dados pessoais) e 6.º (Licitude do tratamento) do RGPD, ao estabelecer requisitos para a obtenção de consentimento e para o processamento lícito de dados pessoais, bem como ao impor condições para a recolha dos dados. Para além disto, também existem requisitos similares com os dos artigos 24.º (Responsabilidade do responsável pelo tratamento) e 28.º (Subcontratante) do RGPD, nomeadamente na necessidade de aplicar medidas adequadas que garantam a proteção dos dados pessoais na organização e na necessidade de existir um contrato que vincule o *Processor* ao *Controller*, o qual diga explicitamente que o *Processor* apenas processa dados pessoais de acordo com as instruções documentadas do *Controller*. Também existe *guidance* na ISO equivalente às instruções para a elaboração do registo das atividades de processamento de dados pessoais, previstas no artigo 30.º (Registos das atividades de tratamento) do RGPD, cujos pontos de registo obrigatório se sobrepõem, como por exemplo o propósito do processamento, as categorias dos titulares dos dados e dos dados pessoais. No que concerne à realização de *privacy impact assessments* também existe um alinhamento com o artigo 35.º (Avaliação de impacto sobre a proteção de dados) do RGPD, uma vez que são dadas instruções semelhantes para a realização desta avaliação*,* tais como a indicação de que a avaliação deve ser feita quando existem decisões automatizadas ou processamento de dados pessoais em larga escala. Também é referido na ISO que em determinadas jurisdições são definidas as situações em que devem ser realizadas estas avaliações de impacto, como é o caso de Portugal, em que a Comissão Nacional de Proteção de Dados definiu as seguintes: quando se introduz uma nova tecnologia de tratamento de dados pessoais; quando existe um controlo sistemático de zonas acessíveis publicamente em larga escala, nomeadamente com recurso a videovigilância e quando é realizado *profiling*[105] e, subsequentemente, tomadas decisões automatizadas que possam afetar os titulares dos dados[106].

O Capítulo III (Direitos do titular dos dados) do RGPD está presente nas subcláusulas 7.3 e 8.3 (*Obligations to PII principals*) da ISO, nas quais são estabelecidas as obrigações que a organização tem para com os titulares dos dados e as informações a fornecer aos mesmos em consonância com o Regulamento. Os direitos dos titulares previstos nos artigos 15.º, 16.º, 17.º, 18.º, 20.º, 21.º e 22.º (Direito de acesso, retificação, apagamento dos dados, limitação do tratamento, portabilidade dos dados, oposição e não sujeição a decisões individuais automatizadas, incluindo definição de perfis, respetivamente) do RGPD, encontram-se tratados na ISO sob a forma de *guidance* para as organizações conseguirem assegurar o seu cumprimento. Também a obrigação do *Controller* comunicar as alterações, solicitadas pelo titular ao tratamento dos seus dados, ao *Processor* e outras entidades envolvidas no processamento se encontra acautelada na ISO.

O alinhamento com o artigo 25.º (Proteção de dados desde a conceção e por defeito) do RGPD é de extrema importância para as organizações, uma vez que na ISO é fornecido um complemento ao

[105] *Profiling*, de acordo com o RGPD, trata-se de qualquer forma de processamento automático de dados pessoais que avalie aspetos pessoais relativos a um titular, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente. Este processamento inclui a definição de perfis.

[106] CNPD – Comissão Nacional de Proteção de Dados, 2021.

princípio de *privacy by design and by default* para assegurar que os processos e sistemas são concebidos de forma a limitar a recolha e o processamento de dados pessoais ao estritamente necessário, conforme dita o princípio preconizado pelo RGPD. Para tal, são estabelecidas linhas guia para limitar a recolha e o processamento de dados pessoais na organização, definir o período de retenção, garantir a qualidade dos dados e cumprir o objetivo de minimização dos mesmos, bem como para a anonimização e apagamento dos dados pessoais quando já não são necessários, de acordo com o propósito definido.

A temática da transferência de dados pessoais, tratada no Capítulo V (Transferências de dados pessoais para países terceiros ou organizações internacionais) do RGPD, também está presente na ISO, mais precisamente nas suas subcláusulas 7.5 e 8.5 (*PII sharing, transfer, and disclosure*). O grande objetivo é garantir que sempre que haja necessidade de transferir dados pessoais para países terceiros, que tal não comprometa a proteção dos dados pessoais e seus titulares, sendo que a ISO dá *guidance* para as organizações cumprirem com este requisito, referindo que as transferências de dados pessoais devem seguir os requisitos regulamentares aplicáveis. No caso do RGPD, conforme indicado anteriormente, encontram-se previstas duas formas para a transferência de dados pessoais para países fora da UE – transferência com base numa decisão de adequação ou transferência sujeita a garantias adequadas (cláusulas-tipo de proteção de dados) - as quais devem ser obrigatoriamente acauteladas pelas organizações que processam dados pessoais de cidadãos europeus.

Com a análise da ISO/IEC 27701:2019 é fácil perceber a analogia existente com os princípios que regem o RGPD, nomeadamente a licitude, a lealdade e a transparência no tratamento de dados pessoais, a limitação do propósito para o tratamento, a exatidão e a minimização dos dados pessoais, a limitação da recolha e conservação de dados, a integridade e confidencialidade dos dados armazenados e, por último, a responsabilização das organizações que realizam as atividades de processamento por eventuais danos causados, pelo acesso indevido ou pela incorreta utilização dos dados pessoais[107].

De um ponto de vista mais geral, tanto a ISO/IEC 27701:2019 como o RGPD visam reforçar a privacidade dos dados, focando-se no processo de obtenção, gestão e proteção dos mesmos, sendo que o RGPD se concentra na definição dos princípios básicos para a recolha e processamento de dados pessoais enquanto que a ISO procura auxiliar as organizações a implementar os procedimentos necessários para assegurar a conformidade com a legislação aplicável e o seu compromisso de garantir a confidencialidade e integridade dos dados pessoais. Para além disto, ambos têm uma abordagem baseada no risco para a segurança do tratamento, sendo obrigatório avaliar os riscos associados ao tratamento de dados pessoais, de forma a identificar quaisquer ameaças que possam comprometer a segurança e atuar na sua minimização, antes do início do processamento dos mesmos. A norma e o Regulamento responsabilizam as organizações pelas potenciais violações de dados pessoais e exigem prontidão na notificação das autoridades competentes, sendo que a diferença reside no facto de o RGPD exigir 72 horas para a notificação e a ISO não exigir um tempo específico, aconselhando as organizações a reportar e tomar medidas corretivas, apesar de referir que devem ser respeitadas as imposições legais aplicáveis, as quais claramente incluem o RGPD. Ambos reforçam a importância de

[107] SGS Portugal, 2021.

proteger os dados pessoais em todas as fases em que são processados, especificando que devem existir medidas implementadas também na fase de conceção de sistemas, de acordo com o princípio de *privacy by design and by default* que, como já vimos, é preconizado na norma e no Regulamento. Por último, de salientar a pertinência de manter os registos de todas as atividades de tratamento de dados pessoais atualizados e completos, incluindo todos os pontos exigidos no RGPD (a categoria dos dados pessoais, a finalidade do tratamento, as medidas de segurança aplicáveis ao tratamento, as categorias dos destinatários dos dados, etc.) e, consequentemente, na ISO[108].

Uma organização, cujo tratamento de dados pessoais esteja em conformidade com os requisitos do RGPD, trata os dados pessoais que tem na sua posse com o devido cuidado, sendo-lhe exigido que os proteja contra divulgação ou acesso indesejado que possa resultar na exfiltração de dados pessoais, os quais podem ser apropriados e cujo tratamento ilícito pode causar dano na esfera jurídica dos titulares. A ISO/IEC 27701 vem expandir este âmbito ao estabelecer controlos que visam assegurar que os dados pessoais são alvo de processamento seguro, estando devidamente protegidos. Portanto, o cumprimento do RGPD pode ser encarado como a base para a proteção de dados pessoais, enquanto a implementação de um SGP alinhado com a norma ISO/IEC 27701, como extensão ao SGSI alinhado com a ISO/IEC 27001, deve ser visto como um reforço das políticas internas e boas práticas na organização, revelando-se uma mais-valia na garantia de conformidade com o RGPD, entre outras legislações relevantes, ao complementar o Regulamento com uma abordagem mais prática do tema e direcionada para a implementação concreta de medidas, que visem assegurar o processamento seguro de dados pessoais[109].

3.4. Pontos de divergência

As divergências entre o RGPD e a ISO são, essencialmente, a nível conceptual, na medida em que as abordagens sugeridas para a proteção de dados divergem entre a centralização no direito à proteção dos dados pessoais por parte dos titulares e à livre circulação dos mesmos dentro do EEE, em que a segurança da informação é apenas uma componente na garantia de uma proteção adequada (RGPD), e a dependência total da segurança da informação para tal (ISO)[110]. Além disto, a natureza distinta destes documentos - um regulamento de aplicação obrigatória pelas organizações que processam dados pessoais de cidadãos europeus e um standard de aplicação voluntária por parte de organizações interessadas em melhorar as suas práticas de segurança da informação e privacidade - vem reforçar algumas diferenças de fundo, nomeadamente relacionadas com o âmbito de aplicação material, em que o RGPD se aplica ao tratamento de dados pessoais de forma não automatizada, parcial ou totalmente automatizada, e o âmbito de aplicação territorial, sendo que o RGPD se aplica ao tratamento de dados pessoais de titulares residentes na UE, o qual é efetuado por um *Controller* ou *Processor* estabelecido ou não em território da UE, ou seja, independentemente do tratamento ocorrer dentro ou fora da UE. No caso da ISO, o âmbito não é restrito ao território da UE nem aos titulares nele

[108] NQA – Global Certification Body, 2021.
[109] Ernst & Young Global, 2020.
[110] Anwar e Gill, 2020: 5-6; Lachaud, 2020: 5.

residentes, sendo aplicável a todas as organizações que sejam *Controllers* e/ou *Processors*, as quais têm responsabilidade pelo processamento de dados pessoais que efetuam[111].

Outra divergência prende-se com o facto da ISO/IEC 27701 exigir a implementação de um sistema de gestão alinhado com outros standards ISO, nomeadamente a ISO 27001 e a ISO 27002, enquanto o RGPD não faz qualquer exigência neste sentido, estabelecendo um regime legal com princípios e requisitos próprios, os quais não têm como objetivo ser diretamente auditáveis[112]. De referir ainda que apenas a ISO propõe requisitos para a proteção da propriedade intelectual das organizações, o que está fora do âmbito de aplicação do RGPD.

No que diz respeito à certificação, no RGPD encontra-se prevista a criação de procedimentos de certificação, em matéria de proteção de dados, que comprovem a conformidade das operações de tratamento com o Regulamento ou, por outro lado, para efeitos de comprovação de que existem garantias adequadas por parte de *Controllers* ou *Processors* que não estejam sujeitos ao cumprimento do RGPD, de acordo com o âmbito de aplicação supracitado. A certificação prevista é voluntária e emitida por organismos de certificação com nível de competência adequado em matéria de proteção de dados, pela autoridade de controlo competente ou o Comité Europeu para a Proteção de Dados, sendo válida durante um período máximo de três anos e possivelmente renovada nas mesmas condições[113]. Contudo, como vimos anteriormente, este procedimento de certificação nunca chegou a ser implementado desde a entrada em vigor do RGPD, não existindo uma certificação oficial acreditada ainda nos dias de hoje[114], apesar da EDPB ter definido os critérios de certificação[115] e da CNPD já ter publicado, em Diário da República, os requisitos adicionais de acreditação que compete às autoridades de controlo estabelecer[116]. Ao comparar com o esquema de certificação ISO, o qual foi concebido para certificar sistemas de gestão, é possível concluir que os mesmos não são equivalentes, por um lado, devido ao facto das normas ISO serem privadas e protegidas por direitos de autor, pelo que não poderiam ser aprovadas pelas entidades públicas com autoridade de supervisão nem os requisitos para a certificação tornados públicos e facilmente acessíveis, conforme previsto no RGPD, e, por outro lado, porque o processo de auditoria exigido na ISO para a certificação das organizações, realizado por auditores certificados e oficializado pelas entidades acreditadoras competentes, também não compactua com o estabelecido no Artigo 42.º (Certificação) do RGPD[117]. No entanto, sendo a ISO/IEC 27701 uma norma amplamente aplicável e uma *framework* internacionalmente reconhecida, existem vários autores que defendem que a certificação do SGP nesta norma poderia servir de base para um potencial mecanismo de certificação do RGPD[118].

---

[111] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 32-33; International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines: 1.
[112] Lachaud, 2020: 10-12.
[113] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 58-59.
[114] IPAC – Instituto Português de Acreditação, 2021; IPAC – Instituto Português de Acreditação, s.d.
[115] Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento, de 4 de junho de 2019.
[116] Regulamento n.º 834/2021, 6 de setembro de 2021- Requisitos adicionais de acreditação para os organismos de certificação.
[117] Anwar e Gill, 2020: 5-6.
[118] Lachaud, 2020: 4;18-19; Anwar e Gill, 2020: 3; CNIL, 2020; Siganto, 2020.

Sabendo que o não cumprimento do RGPD pode suscitar danos na esfera jurídica dos titulares, ao violar o seu direito fundamental à proteção de dados pessoais, está previsto no Regulamento o direito de o titular apresentar reclamação à autoridade de controlo, caso considere que os seus dados tenham sido alvo de tratamento indevido, bem como o direito à ação judicial contra a autoridade de controlo, o *Controller* ou o *Processor*, tendo o direito a receber uma indemnização pelos danos sofridos. Para além disto, a aplicação de coimas por parte da autoridade de controlo também está prevista, sempre que se verifique uma violação ao RGPD, dependendo da natureza, gravidade e duração da infração, entre outros fatores, sendo o valor máximo vinte milhões de euros ou quatro porcento do volume de negócios anual a nível mundial da organização, aplicando-se o montante mais elevado[119]. Nos standards ISO não se encontram previstas quaisquer penalizações para as organizações, havendo apenas identificação das situações não conformes, aquando das auditorias, as quais, dependendo da gravidade, têm prazos estipulados para a correção, podendo a certificação ficar suspensa enquanto as situações não forem mitigadas[120]. Ainda a referir que se encontra previsto na norma a possibilidade de as organizações identificarem controlos não aplicáveis, de acordo com o seu contexto de atuação, desde que esta exclusão seja devidamente justificada no SoA, o que não se encontra previsto no RGPD, onde os *Controllers* e *Processors* são responsáveis por cumprir todos os princípios de proteção de dados que lhes digam respeito[121].

Após esta análise, é possível concluir que a convergência e a complementaridade destes dois documentos são superiores às divergências encontradas, pelo que as organizações interessadas podem beneficiar de um maior alinhamento com a legislação em vigor e uma maior maturidade face aos requisitos de proteção de dados, com a adoção de um SGP em conformidade com a ISO 27701. Como fica patente neste capítulo, a ISO pode auxiliar no cumprimento da legislação aplicável de proteção de dados, com a devida interpretação da norma, de forma a ultrapassar os pontos de divergência referidos, facilitando a operacionalização das medidas necessárias que garantam um processamento seguro de dados pessoais.

[119] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: 80-83.
[120] APCER, s.d.: 12-16.
[121] Lachaud, 2020:13.

4. *Case-study*: A perceção de melhoria na conformidade com o RGPD na Celfocus, S.A. com recurso a um Sistema de Gestão da Privacidade alinhado com o standard ISO/IEC 27701

O presente *case-study*, realizado na empresa Celfocus, S.A., tem como objetivo analisar em que medida o alinhamento do seu Sistema de Gestão da Privacidade com a ISO/IEC 27701:2019 proporcionou uma melhoria no cumprimento dos requisitos do RGPD. Este estudo teve como base a análise comparativa entre os requisitos do RGPD e os da ISO 27701, apresentada no capítulo anterior, os quais foram então confrontados com as práticas implementadas na organização e respetiva informação documentada.

4.1. Celfocus, S.A.

A Celfocus foi fundada no ano 2000, tendo sido inicialmente uma *joint venture* entre a Novabase e a Vodafone Portugal. Atualmente, pertence apenas à Novabase - a maior empresa portuguesa de Tecnologias de Informação cotada na *Euronext Lisbon Stock Exchange* – e presta serviço a clientes em mais de vinte e cinco países, ajudando a transformar os seus negócios no sentido de melhorar o seu desempenho e posicionamento competitivo. A Celfocus combina um profundo conhecimento empresarial com a compreensão de diferentes tecnologias, com destaque para o domínio digital e cognitivo, sendo constituída por equipas com vasta experiência em sistemas de informação, motivo pelo qual tem vindo a construir uma reputação no mercado global. A empresa conta com sete escritórios próprios, em Portugal (Lisboa e Porto), Inglaterra (*Newbury)*, Emirados Árabes Unidos (Dubai) e Holanda (*Eindhoven*, Amesterdão e *Maastricht*), onde as suas equipas se dedicam ao estudo das necessidades do complexo mercado das telecomunicações e financeiro, apresentando aos clientes soluções de elevada qualidade. A Celfocus trabalha com uma rede de parceiros reconhecidos mundialmente, nomeadamente fornecedores de *software*, *hardware* e outras organizações altamente especializadas em determinadas tecnologias, o que acrescenta valor à oferta e possibilita o fornecimento de soluções de ponta[122].

Com o intuito de aumentar a sua competitividade no mercado global e a qualidade dos seus entregáveis, a Celfocus aposta na certificação como meio de atingir a excelência e, consequentemente, a confiança dos vários *stakeholders*. Deste modo, a empresa é certificada na ISO 9001 (Sistema de Gestão da Qualidade), ISO 14001 (Sistema de Gestão Ambiental), ISO 45001 (Sistema de Gestão de Saúde e Segurança no Trabalho) e, mais recentemente, na ISO 27001 (Sistema de Gestão da Segurança da Informação) e ISO 27701 (Sistema de Gestão da Privacidade)[123]. Estas certificações atuam como elemento diferenciador, demonstrando um compromisso da gestão de topo e de todos os colaboradores em alinhar a visão e os valores da empresa com as necessidades do mercado e com as

[122] Celfocus, s.d.
[123] Novabase, s.d.

melhores práticas, estabelecendo processos dinâmicos, capazes de assegurar a coerência e a integridade organizacionais e também a melhoria contínua.

Independentemente do seu papel enquanto *Controller* ou *Processor*, a Celfocus tem patente a importância e a necessidade de proteger a informação pessoal que processa, reconhecendo os requisitos exigidos para a sua proteção desde a recolha à eliminação dos dados. Para tal, são feitos os esforços necessários para assegurar o cumprimento integral do RGPD e dos requisitos contratuais no que diz respeito à proteção de dados pessoais; garantir a integração dos requisitos de privacidade nos processos de negócio; e estabelecer um SGP de acordo com a dimensão e relevância da organização, o qual proporcione um processamento adequado e seguro dos dados pessoais.

4.2. Sistema de Gestão da Privacidade da Celfocus, S.A.

A implementação do SGP da Celfocus teve início em 2017, tendo inicialmente sido construído de acordo com a ISO/IEC 29151:2017[124] e em paralelo com o SGSI, por sua vez alinhado com a ISO/IEC 27001:2013. Com a entrada em vigor do RGPD, e mais tarde com a publicação da ISO/IEC 27701:2019, surgiu a necessidade de rever o SGP para o adaptar aos novos requisitos regulamentares e normativos, com o intuito também de o aproximar ao SGSI numa ótica de gestão mais integrada da Segurança da Informação e da Privacidade na Celfocus. Neste processo, foi essencial o estabelecimento de uma equipa de Privacidade dedicada, responsável pela operacionalização do SGP, a qual colocou em prática as medidas essenciais para melhorar continuamente a eficácia do sistema, bem como dos serviços e processos que o suportam. Atualmente, o SGP é um sistema de gestão coeso e robusto, o qual obteve recentemente a certificação ISO/IEC 27701, mais precisamente em julho de 2022, em simultâneo com a certificação ISO/IEC 27001 do SGSI, tornando a Celfocus numa das primeiras empresas em Portugal a ser certificada na extensão da norma para a gestão da Privacidade.

Em conjunto, o SGSI e o SGP da Celfocus têm como objetivo principal garantir a fiabilidade da informação e dos sistemas, garantindo a continuidade das atividades do negócio, bem como garantir que a informação de caráter pessoal é processada de acordo com os requisitos legais e contratuais aplicáveis.

4.2.1. Alinhamento com o Sistema de Gestão da Segurança da Informação

Na Celfocus existe uma relação de sinergia entre as equipas de Segurança da Informação e de Privacidade, as quais se dedicam à operacionalização e melhoria contínua do SGP e do SGSI. Sendo a ISO/IEC 27701 uma extensão da ISO/IEC 27001, no que diz respeito à gestão da Privacidade,

[124] A ISO/IEC 29151:2017 estabelece objetivos de controlo, controlos e orientações para a sua implementação, a fim de cumprir os requisitos identificados na avaliação de risco e impacto relacionada com a proteção de dados pessoais. Esta norma é aplicável a todas as organizações que atuam como *Controllers*, a qual especifica orientações baseadas na ISO/IEC 27002, tendo em consideração os requisitos para o processamento de dados pessoais que possam ser aplicáveis no contexto dos riscos de segurança da informação de uma organização.

é natural e está previsto na norma que existam práticas comuns e até mesmo documentação partilhada entre os sistemas, pelo que a interação e o trabalho conjunto de ambas as equipas é crucial para a adequada manutenção destes sistemas de gestão. Na Celfocus não se optou por um sistema de gestão único da Segurança da Informação e Privacidade (o designado PIMS na ISO 27701), no entanto o SGP e o SGSI estão perfeitamente alinhados e orientados para um objetivo comum – assegurar o cumprimento dos requisitos contratuais e regulamentares, com destaque para o RGPD; assegurar a confidencialidade, integridade e disponibilidade da informação, incluindo dados pessoais; e estabelecer um padrão de qualidade consistente com a dimensão e importância da organização - o que significa que muitas das práticas da Privacidade são sustentadas em processos, procedimentos e metodologias da Segurança da Informação. A título de exemplo, o procedimento de gestão de incidentes e a metodologia de risco são partilhados por ambos os sistemas de gestão e a Revisão pela Gestão é realizada em conjunto. Abaixo, na Figura 3, encontra-se uma representação da relação dos sistemas de gestão da Segurança da Informação e da Privacidade da Celfocus.

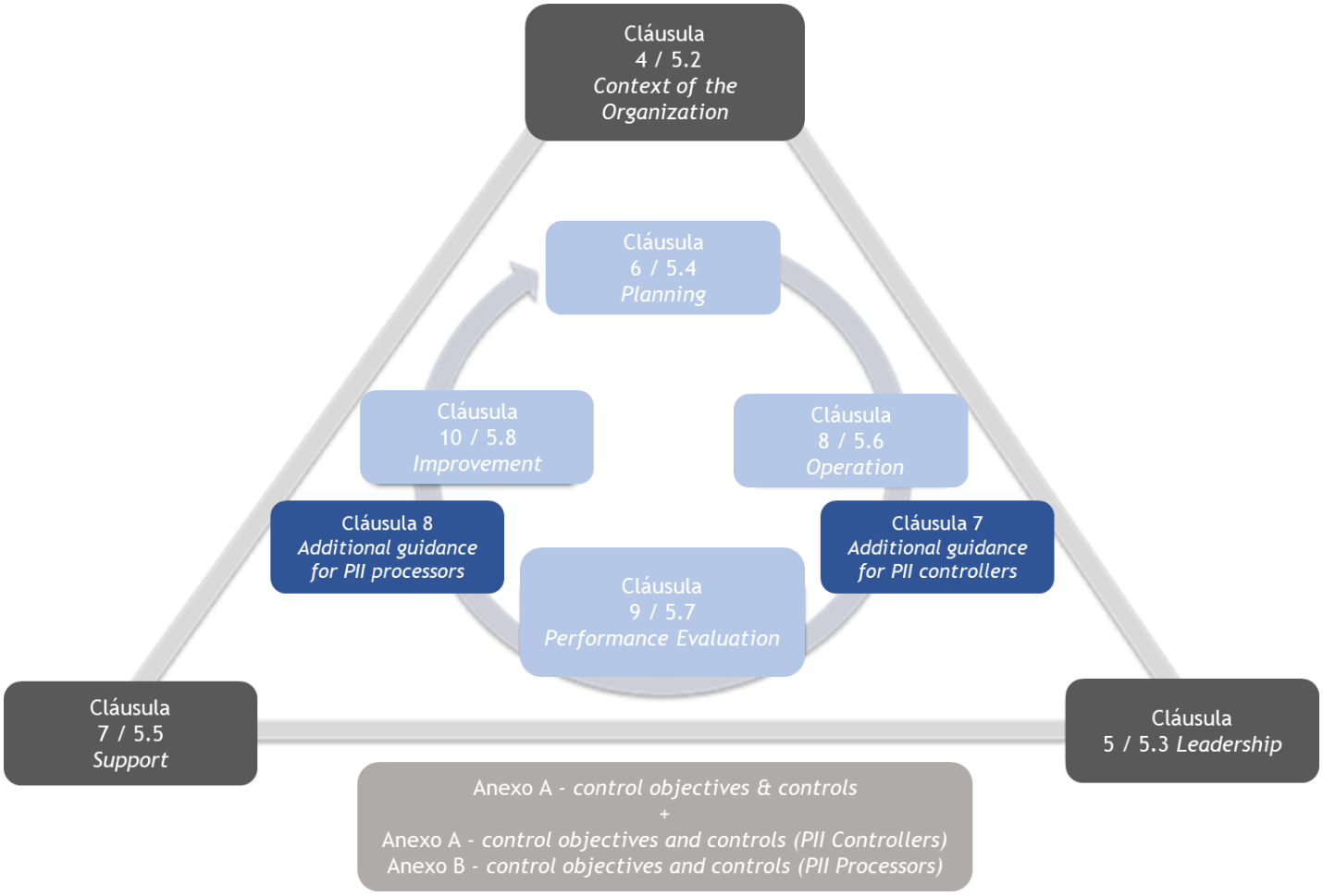

Figura 3 - Representação da relação entre o SGSI e o SGP da Celfocus (alinhados com os standards ISO/IEC 27001 e ISO/IEC 27701, respetivamente).

4.2.2. Alinhamento com a ISO/IEC 27701

O alinhamento do SGP com a ISO/IEC 27701 foi efetuado a par com o alinhamento do SGSI com a ISO/IEC 27001, pois, como já vimos, a base dos controlos e objetivos de controlo é comum, assim como as cláusulas respetivas ao contexto da organização, liderança, suporte, planeamento, operação, avaliação do desempenho e melhoria, aos quais a ISO 27701 acrescenta pontualmente requisitos relacionados com a proteção de dados, a incorporar no sistema de gestão e ainda todos os requisitos das cláusulas 7 e 8, suportados pelos Anexos A e B, com indicações específicas sobre a atuação da organização enquanto *Controller* e *Processor*, respetivamente.

4.2.2.1. Cláusula 5

Na Celfocus, para responder aos requisitos adicionais relacionados com a proteção de dados da cláusula 5.2 *Context of the Organization*, foi criado um Manual do SGP, no qual se encontram indicadas as partes interessadas e os seus requisitos, incluindo as autoridades de controlo, bem como estabelecido o objetivo do SGP, o seu contexto interno e externo, o modelo operacional e os mecanismos de controlo e melhoria.

Em resposta à cláusula 5.3 *Leadership*, no Modelo Organizacional da Privacidade, encontra-se determinado o papel da organização enquanto *Controller* e enquanto *Processor* (não sendo aplicável na Celfocus o papel de *joint-Controller*), assim como as responsabilidades de todas as funções no SGP, nomeadamente a equipa de Privacidade, o *Manager* da área, o *Head of* do SGP, o membro da gestão de topo responsável, os *Single Point of Contact* (SPOC) de Privacidade, o DPO e ainda de todos os colaboradores. O SPOC de Privacidade, apesar de não ser propriamente uma exigência da norma nem do RGPD, na Celfocus tem o papel de ponto de contacto para todas as questões relacionadas com a proteção de dados em cada unidade de negócio ou área de suporte, recebendo para tal formação específica. Ainda como resposta aos requisitos adicionais relacionados com a liderança, foi definida uma Política de Privacidade em consonância com as melhores práticas internacionais, aprovada pelo responsável máximo da Privacidade na organização, onde se encontra estabelecido o compromisso da Celfocus em assegurar um processamento seguro dos dados pessoais, em cumprimento com o RGPD e outra legislação relevante aplicável, bem como os princípios e diretrizes para uma gestão eficaz da privacidade em todas as geografias em que opera. Nesta Política, encontra-se patente a necessidade do envolvimento de todos os colaboradores para a adequada gestão da Privacidade e ainda os objetivos anuais para a sua monitorização e gestão.

Em alinhamento com os requisitos adicionais da cláusula 5.4 *Planning*, foi definida uma Metodologia de Gestão de Risco, comum ao SGSI e ao SGP, a qual tem instruções para a avaliação dos riscos relacionados com o processamento de dados pessoais na organização. Estas avaliações de risco são efetuadas semestralmente pela equipa de Privacidade, em conjunto com o SPOC de cada unidade de negócio/área, mas também sempre que sejam identificados riscos e oportunidades relacionados com a proteção de dados ao nível da organização; sempre que haja uma alteração nos serviços prestados ou nas suas componentes; sempre que sejam revistas políticas e objetivos de

Privacidade, os quais possam influenciar o processamento de dados pessoais; sempre que sejam detetadas vulnerabilidades não consideradas anteriormente; e sempre que os pressupostos da Metodologia de Gestão de Risco sejam alterados. Ainda a propósito da cláusula 5.4, foi estabelecido o *Privacy* SoA com os controlos da ISO 27701 e a respetiva justificação de inclusão e exclusão, assim como a visão geral da implementação dos controlos na Celfocus. No *Privacy* SoA da Celfocus, apenas se encontram excluídos os controlos 7.2.7 *Joint PII controller* e 7.3.10 *Automated decision making*, uma vez que não foram identificados *joint-Controllers* nem são efetuadas decisões automatizadas relativamente a dados pessoais. Em paralelo, existe o *Information Security* SoA que engloba todos os controlos da ISO 27001.

Para estar em conformidade com os requisitos adicionais da cláusula 5.5 *Support*, foram definidas na Celfocus as competências necessárias para as pessoas que integram funções no SGP, mais precisamente para o *Head of* SGP, *Privacy Manager*, *Privacy Team*, DPO e ainda para Auditor Coordenador e Auditor de Privacidade, existindo requisitos quanto à formação académica, qualificações profissionais, experiência profissional e aptidões técnicas. Também foi criada uma sessão de formação específica para a temática da proteção de dados, em formato *e-Learning,* que inclui, por um lado, informação sobre os requisitos do RGPD e, por outro, informação sobre as políticas, processos e procedimentos que integram o SGP da Celfocus. Esta sessão faz parte do programa de formação "*Plugin*", isto é, o *kit* de formação inicial obrigatório para todas as novas admissões na empresa. Para além desta sessão, existe ainda uma formação de Privacidade de recorrência anual, também obrigatória para todos os colaboradores, a qual aborda temas distintos todos os anos. Existe ainda uma formação inicial para os SPOCs, ministrada em modo *classroom* pela equipa de Privacidade, quando esta função lhes é atribuída, na qual são abordados os requisitos de proteção de dados do RGPD com mais afinco, dado a conhecer o SGP com maior detalhe e explicadas as responsabilidades pretendidas desta função. Periodicamente, os SPOCs frequentam outras sessões com a equipa de Privacidade, nomeadamente quando existem alterações relevantes com impacto no SGP.

No Manual do SGP, encontram-se definidas as necessidades de comunicação interna e externa, bem como os respetivos requisitos e interlocutores, tais como a necessidade de garantir a conformidade com os requisitos do SGP e de notificar a autoridade de controlo, caso ocorra uma *privacy breach*. No que diz respeito à comunicação interna, também foi desenvolvido um plano de atividades anual onde são estabelecidas as campanhas de sensibilização a desenvolver pela equipa de Privacidade, as quais geralmente são definidas em sintonia com datas importantes a assinalar, como por exemplo o Dia da Proteção de Dados e o aniversário do RGPD. Nestas campanhas são lançadas comunicações a toda a organização, nos diversos canais disponíveis, quer seja através do envio de *e-mail*, publicação no *Teams* ou até mesmo colocação de cartazes nos escritórios.

No que diz respeito à informação documentada, o SGP é composto por várias Políticas, Processos, Procedimentos, Metodologias e *Guidelines* que, em conjunto, reúnem a informação necessária para garantir a eficácia do SGP. Para além da Política de Privacidade referida anteriormente, a Celfocus possui dez Políticas operacionais cujos princípios estão alinhados com a ISO 27701, a saber: *Consent and Choice Policy; Purpose Legitimacy and Specification Policy; Collection Limitation Policy; Data Minimization Policy; Use, Retention and Disclosure Limitation Policy; Accuracy*

and Quality Policy; Openness, Transparency and Notice Policy; Personal Data Subject Participation and Access Policy; Accountability Policy; e a *Privacy Compliance Policy.* Os Processos do SGP são comuns com o SGSI, nomeadamente o Processo de Gestão da Segurança da Informação e da Privacidade; o Processo de Gestão de Incidentes de Segurança da Informação e da Privacidade; e o Processo de Auditoria Interna. Também foram documentados os procedimentos de Privacidade mais operacionais, com destaque para o *Personal Data Processing Procedure,* um procedimento personalizado a cada unidade de negócio/área da Celfocus, documentado em conjunto com o respetivo SPOC, o qual tem o objetivo de dar a conhecer as principais preocupações relacionadas com o processamento de dados pessoais na unidade/área, as respetivas atividades de processamento efetuadas e os dados pessoais envolvidos. Quanto às Metodologias, além da Metodologia de Gestão de Risco partilhada com o SGSI, existe a Metodologia PIA que define as situações em que se deve realizar esta avaliação de impacto e as instruções para tal. Existem também algumas *Guidelines* relativas a vários temas como o conceito de *privacy by design and by default* e sobre como atuar em caso de suspeita de incidente de privacidade, entre outros, as quais se encontram partilhadas com toda a organização, à semelhança da restante documentação do SGP mencionada acima. Ainda sobre a informação documentada, todos os documentos do SGP estão alinhados com a ISO 27701 e também com o RGPD, sendo que existem, por exemplo, vários registos de atividades de processamento de dados pessoais, um por cada unidade de negócio, sendo estes registos efetuados com o auxílio do respetivo SPOC e atualizados sempre que existam alterações.

Em resposta aos requisitos adicionais da cláusula 5.6 *Operation*, além da avaliação e tratamento de risco já mencionado anteriormente, dentro do planeamento operacional e controlo, foram ainda definidos objetivos anuais para o SGP, os quais são monitorizados trimestralmente pela equipa de Privacidade e revistos anualmente no âmbito da Revisão pela Gestão. Este ponto relaciona-se com a cláusula 5.7 *Performance evaluation*, em resposta à qual é criado anualmente um programa de auditorias internas de Privacidade, que abrangem todas as áreas onde existe processamento de dados pessoais na Celfocus, existindo ainda o momento de Revisão pela Gestão onde é efetuada a revisão e a apreciação global do sistema de gestão, definido o programa de auditorias para o ano e ainda o conjunto de ações a desenvolver.

Relativamente à cláusula 5.8 *Improvement*, é realizado o acompanhamento das constatações identificadas nas auditorias de Privacidade, quer internas quer externas, assim como das respetivas ações corretivas, sendo a melhoria contínua do SGP uma preocupação constante.

4.2.2.2. Cláusula 6

Avançando para o capítulo 6 da norma, relativamente à cláusula 6.2 *Information security policies*, conforme mencionado anteriormente, foram documentadas onze políticas de Privacidade, alinhadas com os princípios da ISO 27701, sendo que a *Privacy Policy* inclui a declaração de compromisso do cumprimento da legislação e regulamentação aplicável, em matéria de proteção de dados, bem como dos termos contratuais acordados entre a Celfocus e terceiras partes, que é aprovada

pela gestão de topo. Para garantir o cumprimento da legislação aplicável, a *Privacy Team* mantém uma relação próxima com o departamento jurídico e com a área responsável pela gestão contratual.

Para endereçar os requisitos adicionais à cláusula 6.3 *Organization of information security, a* Celfocus nomeou um DPO que reporta diretamente à gestão de topo e cujas funções e responsabilidades estão discriminadas no *Privacy Organisational Model*, as quais incluem informar e aconselhar a empresa e os seus colaboradores, relativamente às suas obrigações perante a legislação de proteção de dados aplicável; ser o ponto de contacto para as reclamações e pedidos dos titulares dos dados e garantir que estes são tratados atempadamente; monitorizar a conformidade da organização com a legislação de proteção de dados aplicável, através de auditorias, sessões de sensibilização e de formação; dar o seu parecer relativamente à elaboração de PIAs; cooperar e ser o ponto de contacto das autoridades de controlo competentes; conhecer os riscos associados às atividades de tratamento de dados pessoais, entre outras.

No que diz respeito à gestão de projetos, na Celfocus há a salientar a preocupação com a não utilização de dados pessoais, no âmbito dos testes realizados às soluções informáticas; a utilização de canais seguros de comunicação; a partilha de dados pessoais das equipas de projeto com o cliente, que sejam estritamente necessários, nomeadamente para a criação de acessos aos seus sistemas e/ou instalações; a utilização exclusiva dos dados pessoais dos clientes, de acordo com o âmbito definido em contrato; e a necessidade de providenciar aos colaboradores formação adequada para as suas funções. Em resposta às exigências relativas ao *teleworking*, existe em vigor na Celfocus uma Política de trabalho híbrido, e foi criada uma *guideline* com instruções específicas para a alocação de pessoas fora da UE em projetos, as quais não podem ter acesso a dados pessoais de clientes, a não ser que seja expressamente autorizado por estes.

Quanto à cláusula 6.4 *Human resource security*, mais precisamente quanto aos requisitos pré-contratuais, foi implementado na Celfocus um processo de *screening* a todas as novas admissões, de acordo com a legislação em vigor, no qual é solicitado, por exemplo, o registo criminal. Os contratos de trabalho também foram revistos para incluir novas cláusulas de Privacidade, em linha com as exigências para o tratamento de dados pessoais do RGPD, sendo que todos os colaboradores que iniciaram funções na empresa antes desta alteração assinaram uma declaração de compromisso, cujas alíneas são dedicadas à temática da proteção de dados pessoais e à segurança da informação, incluindo preocupações com a informação confidencial da Celfocus e cláusulas de não-revelação. Durante a relação contratual é exigido que todos os colaboradores internos e externos cumpram com os princípios estabelecidos nas Políticas e Procedimentos de Privacidade estabelecidos na organização, os quais se encontram partilhados na página de *Sharepoint*, sendo-lhes dada formação sobre os mesmos e comunicado sempre que exista alguma atualização. O departamento jurídico trata as questões relacionadas com procedimentos disciplinares, referentes a eventuais casos de *privacy breach*, nas situações em que se prove que os mesmos tenham sido gerados de forma intencional por um colaborador.

Não existem propriamente requisitos adicionais na ISO 27701 para a cessação do emprego ou mudança de funções, seguindo-se a boa prática, já implementada, de revisão e remoção dos acessos dos colaboradores. Nestas situações é garantido que, quando um colaborador sai da empresa, os seus

acessos são removidos e quando existe mudança de funções os colaboradores não têm acesso a mais informação, além da estritamente necessária na nova posição.

A maioria do trabalho, para estar em conformidade com as cláusulas seguintes (6.5 a 6.15) foi realizado no âmbito do SGSI, obviamente com a devida adaptação ao SGP. Relativamente à cláusula 6.5 *Asset management*, todos os requisitos do SGSI foram também aplicados aos ativos onde são processados dados pessoais, pelo que existe um inventário destes ativos com a respetiva identificação do responsável. Não existem regras específicas na ISO 27701 para o uso aceitável dos ativos, sendo, portanto, seguidas as regras já definidas no SGSI. Quanto à classificação e etiquetagem dos mesmos, de acordo com a Política de Classificação da Informação da Celfocus, quando existem dados pessoais é atribuída a classificação mais elevada - confidencial. No que diz respeito aos dispositivos amovíveis, de acordo com as Políticas da Celfocus, o seu uso não é permitido para armazenar dados pessoais. A eliminação dos ativos onde são processados dados pessoais segue, mais uma vez, os procedimentos definidos no SGSI, que garantem que os ativos são eliminados de forma segura quando já não são necessários.

Passando para a cláusula 6.6 *Access control*, são seguidos os princípios da *Access Control Policy* do SGSI, havendo um cuidado especial com o registo, a eliminação e a revisão dos *users* com acesso a dados pessoais nas ferramentas corporativas. É ainda mantido um registo, no *Personal Data Processing Procedure* da respetiva unidade de negócio/área, dos perfis de acesso às ferramentas corporativas onde são processados dados pessoais. Na Celfocus não existe processamento de dados sensíveis, de acordo com a definição do RGPD, pelo que não existem requisitos legais relativamente à encriptação dos mesmos. Em função das exigências das soluções existentes ou a desenvolver são seguidos os princípios da *Cryptography Policy* do SGSI, aplicando-se controlos criptográficos nos sistemas, dados e serviços que exijam proteção por *password.* Segundo esta política, são também aplicados controlos criptográficos para a proteção de informação de caráter sensível para o negócio, incluindo durante a sua transmissão e, ainda, para a proteção de dados pessoais como resultado de um PIA.

No que diz respeito à segurança física, tratada na cláusula 6.8 *Physical and environmental security*, apenas existem requisitos adicionais na ISO 27701 sobre eliminação ou reutilização segura dos equipamentos, tendo sido acrescentado um princípio à *Physical and Environmental Security Policy* do SGSI sobre o tema, o qual estabelece que os equipamentos, que contenham dados pessoais armazenados, devem ser eliminados ou reatribuídos de forma segura, seguindo os procedimentos definidos, de forma a que a informação anterior não seja recuperável. Ainda existe outro requisito adicional relativo ao princípio de *clear desk,* pelo que foi acrescentado um princípio na política dedicada ao tema que estabelece que a criação de material impresso, que contenha dados pessoais, deve ser reduzida ao mínimo necessário.

Seguindo para a análise da cláusula 6.9 *Operations security*, continuamos com o alinhamento total com as práticas e Políticas definidas no SGSI que foram complementadas com os requisitos para o *backup*, recuperação e restabelecimento de informação que contenha dados pessoais, de forma a garantir que sempre que ocorra a sua recuperação, a informação é restaurada a um estado em que a sua fiabilidade seja assegurada ou então que seja possível detetar e corrigir as imprecisões, por

exemplo com recurso aos titulares dos dados pessoais. As exigências dos clientes relativas ao *backup* de informação são definidas contratualmente caso a caso, sendo criados os procedimentos necessários para o seu cumprimento no âmbito dos projetos. Ainda no âmbito das operações, está implementado *event logging* nas ferramentas corporativas. A monitorização destes *logs* é realizada de acordo com os princípios da *Operations Security Policy* e permite identificar quem acedeu aos dados pessoais, quando ocorreu esse acesso, quais os dados acedidos e alterações efetuadas. De acordo com esta Política, quando é permitido que os clientes acedam ao registo dos *logs* controlados pela Celfocus, existem controlos para assegurar que o cliente apenas acede aos *logs* relacionados com as suas atividades e que não os pode alterar de forma alguma.

A cláusula 6.10 *Communications security*, pouco acrescenta aos requisitos aplicáveis ao SGSI, tendo apenas sido reforçados os procedimentos de transferência de informação, quando esta contém dados pessoais, os quais têm de garantir que as regras estabelecidas para o processamento de dados pessoais são também aplicadas aquando da sua transferência, de acordo com a *Communications Security Policy*. Para além disto, conforme referido anteriormente, todos os colaboradores internos e externos da Celfocus assinam um acordo de confidencialidade.

Quanto à cláusula 6.11, foram acrescentados princípios à *System Acquisition Development and Maintenance Policy* do SGSI que referem que os dados e comunicações são protegidos por *firewalls* ou outros sistemas e que para melhorar a segurança e a privacidade das comunicações são utilizados protocolos de comunicação seguros, tais como SSL (*Secure Sockets Layer*) e TLS (*Transport Security Layer*) e ainda que os dados críticos para a organização, incluindo os dados pessoais, que passam através de redes públicas, são encriptados.

Relativamente às práticas de desenvolvimento seguro, foi incorporado o conceito de *privacy by design and by default* pela ação da *Application Security Team*, uma equipa dedicada ao tema, tendo em consideração os seguintes aspetos, conforme definido na Política do SGSI: implementar os princípios de proteção de dados ao longo de todo o ciclo de vida do desenvolvimento de *software*; basear a definição de requisitos de proteção de dados para a fase de *design* nos resultados dos PIAs; definir pontos de controlo de proteção de dados pessoais, de acordo com as *milestones* dos projetos; e, por defeito, minimizar o processamento de dados pessoais ao estritamente necessário. Para tal, a *Application Security Team* desenvolveu um documento intitulado *Rule Book*, o qual inclui instruções técnicas e procedimentos para o desenvolvimento de código seguro, que se encontra partilhado no *Sharepoint* para utilização das equipas dedicadas ao desenvolvimento de *software*. Neste âmbito, foi também desenhada uma *guideline* sobre o conceito de *privacy by design and by default*, a qual resume os elementos-chave a ter em consideração na aplicação deste princípio, nomeadamente a transparência, legalidade, justiça, limitação do propósito, minimização dos dados, precisão dos dados, limitação do armazenamento, integridade, confidencialidade e responsabilização. Na Celfocus o desenvolvimento de sistemas onde irá ocorrer processamento de dados pessoais segue este princípio, pois além de ser algo exigido nas Políticas internas da organização, também o é por parte dos clientes. De referir ainda que os projetos não utilizam dados pessoais reais em testes.

Relativamente à cláusula 6.12 *Supplier relationships*, também teve de haver a devida adaptação para cumprir com os seus requisitos adicionais, nomeadamente a adição, nos contratos com

os fornecedores, de cláusulas com indicação das medidas técnicas e organizativas mínimas que o fornecedor tem de cumprir para garantir um processamento seguro de dados pessoais. Neste sentido, foram reformulados os acordos com os fornecedores que processam informação pessoal em nome da Celfocus, bem como desenvolvido um *Data Processing Agreement* (DPA) que deve ser assinado por todos os fornecedores. O DPA inclui a definição clara da responsabilidade de cada uma das partes; vincula o fornecedor a respeitar as instruções da Celfocus, no que diz respeito ao processamento de dados pessoais, assim como a atuar em conformidade com a legislação de privacidade aplicável; prevê o direito da Celfocus auditar as práticas do fornecedor; vincula os fornecedores à obrigatoriedade de cooperar com a Celfocus, de forma a que esta esteja em cumprimento das suas obrigações perante a legislação de Privacidade aplicável; impede o fornecedor de processar dados pessoais fora da UE, a não ser que formalmente autorizado; impede a subcontratação sem autorização; vincula o fornecedor a eliminar de forma segura ou a devolver toda a informação pessoal, aquando do término do contrato; refere a obrigatoriedade de notificar a Celfocus no prazo de 24 horas caso ocorra um incidente que envolva dados pessoais; entre outros requisitos.

Quanto á cláusula 6.13 *Information security incident management*, conforme já mencionado, foi criado um processo conjunto do SGSI e do SGP para a gestão dos incidentes de Segurança da Informação e de Privacidade, o qual procura garantir o cumprimento dos requisitos de ambas as normas (ISO 27001 e ISO 27701). Neste processo são estabelecidas as responsabilidades e o procedimento para a identificação, registo, análise e tratamento de *privacy breaches*, bem como a necessidade de notificar a autoridade de controlo competente no prazo de 72 horas e, no caso de processamento de dados pessoais em nome do cliente, a necessidade de o notificar dentro do período estabelecido contratualmente (geralmente até 24 horas após conhecimento do incidente).

Na Celfocus, caso ocorra um incidente de Segurança da Informação ou de Privacidade, será realizado um relatório pela equipa responsável, que inclui a descrição detalhada do incidente; a identificação da pessoa que notificou a equipa competente; a categorização do incidente; a identificação dos ativos afetados; a identificação se houve ou não dados pessoais envolvidos no incidente e, se sim, qual a categoria dos mesmos e o número de registos afetados; a análise do impacto do incidente para a organização e para os eventuais titulares envolvidos; as potenciais consequências do incidente; as medidas preventivas existentes antes do incidente; a data de resolução do incidente; a identificação das entidades internas e externas que foram notificadas; a descrição das ações levadas a cabo no imediato para mitigar o incidente; e, por último, as ações a desenvolver para mitigar o incidente e prevenir situações futuras semelhantes.

A cláusula 6.14 *Information security aspects of business continuity management* não tem requisitos específicos adicionais de Privacidade, pelo que, para endereçar este tópico na Celfocus, houve apenas o trabalho de incluir as preocupações relacionadas com a proteção de dados na Política e Plano de Continuidade de Negócio, concretamente a colocação dos sistemas em que os dados pessoais são processados no radar, de forma a garantir que, em caso de desastre, seja possível restabelecer de forma eficaz as operações críticas para o negócio, no período de tempo mais curto possível com o mínimo de perda de dados. Previamente à elaboração do Plano, foi levado a cabo um *Business Impact Analysis* para identificar os serviços, processos, áreas e projetos considerados

essenciais para manter a continuidade do negócio na Celfocus, de forma a determinar o tempo e o nível de serviço necessários para restabelecer os mesmos, incluindo a definição dos respetivos *Recovery Point Objectives* (RPO) e *Recovery Time Objectives* (RTO), bem como os recursos necessários para esse restabelecimento.

Com o Plano de Continuidade de Negócio pretendeu-se estabelecer uma linha de ação clara para atingir os seguintes objetivos: garantir a segurança e a proteção das pessoas e dos ativos; responder prontamente a eventos disruptivos, reduzindo o tempo de inatividade dos serviços e operações de negócio críticas; minimizar as perdas financeiras; mitigar os efeitos negativos causados pelos eventos disruptivos no planeamento estratégico, reputação, capacidade de entrega e a capacidade de manter a conformidade com a legislação e regulamentação aplicável, incluindo o RGPD; permitir que a organização regresse às operações normais e controladas; e ainda sensibilizar os colaboradores a agirem adequadamente perante uma situação de crise. A par com a elaboração deste plano, foi também desenvolvido o *Disaster Recovery Plan*, o qual se foca na recuperação das plataformas e infraestruturas tecnológicas da Celfocus, após um eventual desastre, com o objetivo de limitar as perdas e o tempo de inatividade e recuperar os dados e informações críticas para o negócio, de forma organizada e eficaz. Este plano contempla todas as ferramentas onde são processados dados pessoais na organização e as equipas responsáveis pela recuperação. Quanto às redundâncias, de acordo com a *Organisation Security Policy*, a Celfocus garante a redundância necessária dos recursos de processamento de informação e outros relacionados, de acordo com os requisitos de disponibilidade impostos. De referir ainda que toda a documentação relacionada com a Continuidade de Negócio está alinhada com a ISO 22031[125].

Por último, relativamente à cláusula 6.15 *Compliance*, na Celfocus são considerados os requisitos legais, regulamentares e contratuais de proteção de dados pessoais, os quais se encontram identificados na listagem de legislação aplicável mantida pela equipa de Privacidade com auxílio do departamento jurídico, assim como nos contratos assinados com terceiras partes, nomeadamente fornecedores e clientes. Na Celfocus, todos os contratos estabelecidos com fornecedores que tenham acesso a dados pessoais são sujeitos à assinatura de DPA, os quais vinculam ambas as partes ao cumprimento dos requisitos do RGPD ou outra legislação aplicável. Naturalmente, sempre que a Celfocus processa dados pessoais no âmbito de um serviço prestado a um cliente, também está sujeita às suas imposições contratuais que incluem cláusulas relacionadas com o processamento de dados pessoais e, pela tipologia dos clientes da Celfocus, estão muito em linha com as exigências do RGPD.

No que concerne às revisões independentes, no caso de Segurança da Informação e Privacidade, de forma a cumprir com este requisito normativo, a Celfocus tem auditorias internas levadas a cabo por auditores externos à organização, as quais também serviram para atestar a capacidade tanto do SGSI como do SGP para avançar para a Auditoria de Concessão das certificações ISO/IEC 27001 e ISO/IEC 27701. Por último, estão incluídas no programa anual de auditorias internas, a elaboração de *technical compliance reviews*, que incluem as ferramentas corporativas onde são processados dados pessoais, nomeadamente através de *vulnerability assessments* realizados por equipas especializadas.

[125] ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements.

4.2.2.3. Cláusula 7

Para ir ao encontro dos requisitos do sétimo capítulo da ISO/IEC 27701, começando pela cláusula 7.2 *Conditions for collection and processing*, encontra-se no *website* da Celfocus a *Privacy Notice*[126] que faz referência às regras para recolha e utilização da informação de caráter pessoal, com destaque não só para o processamento de dados de candidatos a oportunidades de emprego, mas também para uso do negócio em si; à utilização de dados pelo *website* ou outras plataformas *online;* aos *cookies* utilizados nas plataformas *online;* à proteção da informação; a algumas notas sobre a transferência e retenção de dados pessoais; aos direitos dos titulares de dados e seu exercício; e, por último, aos contactos da equipa de Privacidade e do DPO. De salientar que, qualquer candidato, antes de partilhar os seus dados na plataforma de recrutamento em uso na Celfocus, tem obrigatoriamente de aceitar as condições relativas ao processamento dos seus dados pessoais, conforme descrito na *Privacy Notice* e dar o seu consentimento para tal. Nesta fase, o candidato toma conhecimento do propósito do tratamento dos seus dados pessoais e de todas as outras informações relevantes sobre o mesmo, de forma a dar um consentimento livre, explícito e informado, o qual fica registado na plataforma de recrutamento. Aquando da contratação, no contrato de trabalho, os colaboradores dão o seu consentimento quanto ao tratamento dos seus dados, no âmbito da sua relação com a empresa.

Para além disto, foi criado um documento intitulado *Record of Processing Activities*, no qual cada SPOC, em conjunto com a equipa de Privacidade, regista todas as atividades de processamento de dados pessoais levadas a cabo pela respetiva área, no qual se encontra mencionado o propósito do tratamento de dados pessoais e a base legal para o tratamento, entre outras informações relevantes, tais como: a categoria dos titulares e dos dados pessoais processados; se existe ou não transferência de dados para fora da UE (e se existe, a identificação dos países destinatários); se existe ou não partilha de informação com terceiras partes (e se existe, a identificação das entidades e do motivo pelo qual os dados são partilhados); o papel da Celfocus no processamento (*Controller* ou *Processor*); o repositório dos dados; o período de retenção dos dados; os controlos de segurança implementados para proteger os dados pessoais, entre outros. A título de exemplo, no *Record of Processing Activities* da equipa de recrutamento encontra-se registada a atividade de processamento de dados dos candidatos, com recurso à plataforma de recrutamento, conforme explanado acima.

Sempre que a Celfocus recorre a uma terceira parte, com a qual exista partilha de dados pessoais, são assinados DPAs que definem as responsabilidades de ambas as partes e estabelecem os requisitos mínimos de segurança, que devem ser implementados pelo *Processor*, de forma a garantir um processamento seguro. Ainda sobre a cláusula 7.2, foi desenhada a já mencionada metodologia para elaboração de PIAs, a qual é utilizada sempre que necessário, de acordo com o exigido pela CNPD.

Sobre o ponto 7.3 *Obligations to PII principals*, a Celfocus tem documentado na *Privacy Notice* as suas obrigações para com os titulares dos dados e informações a facultar aos mesmos, bem como esclarecimentos relativos ao processamento dos seus dados pessoais. Para além disto, foi

[126] A *Privacy Notice* da Celfocus pode ser consultada em: https://www.celfocus.com/home/privacy-notice.

desenvolvido um procedimento interno, intitulado *Request for Consent and Data Subject's Exercise of Rights Procedure*, que estabelece os meios para o exercício de direitos dos titulares dos dados e explica como o tratamento desses pedidos é realizado pela equipa de Privacidade e restantes áreas envolvidas, definindo também as regras para o pedido de consentimento. Este procedimento encontra-se partilhado com toda a organização e refere o prazo legal de um mês para resposta aos pedidos e reclamações dos titulares dos dados, conforme estabelecido no RGPD, e abrange os direitos de acesso, retificação, apagamento, portabilidade, objeção e retirada de consentimento. De referir ainda que, meros pedidos de alteração ou atualização dos dados (por exemplo, alteração do estado civil, apelido, morada, etc.), conforme descrito neste procedimento, podem ser tratados diretamente na página da *intranet*, através da qual são efetuados pedidos e esclarecimento de dúvidas aos Recursos Humanos da Celfocus. No que diz respeito aos mecanismos para modificar ou retirar o consentimento, os mesmos estão descritos no *Request for Consent and Data Subject's Exercise of Rights Procedure*, onde são mencionadas as condições em que os titulares podem fazer este pedido e o procedimento para tal, assim como a identificação das equipas responsáveis por endereçar internamente estes pedidos. Neste procedimento também se encontra documentada a necessidade de informar as terceiras partes, com as quais são partilhados dados pessoais, sempre que algum pedido de exercício de direito possa afetar o tratamento de dados efetuado e ainda a capacidade de fornecer uma cópia dos dados pessoais tratados, quando solicitado pelo titular. Por último, conforme referido anteriormente, não existem decisões automatizadas implementadas na Celfocus, pelo que os requisitos relacionados com esta temática não são aplicáveis.

Para cumprimento dos requisitos relacionados com a cláusula 7.4 *Privacy by design and privacy by default*, a Celfocus segue a boa prática de apenas solicitar os dados pessoais estritamente necessários para o propósito do tratamento, em particular aos seus colaboradores, tendo a preocupação de manter os seus dados pessoais atualizados nos sistemas, implementando mecanismos para tal; definir períodos de retenção para os dados pessoais que processa, eliminando-os quando este período termina; e garantir linhas de transmissão segura, sempre que existe a necessidade de transferir dados para uma terceira parte. Nos registos de tratamento de dados pessoais encontra-se definido o período de retenção para cada atividade de processamento, assim como os *security controls* associados que garantem um tratamento seguro.

No que diz respeito ao tratamento de dados pessoais de clientes, a Celfocus cumpre as imposições contratuais, as quais, conforme referência anterior, estão geralmente muito em linha com as exigências do RGPD. No âmbito desta cláusula, foi ainda desenvolvida a já referida *Data Protection by Design and by Default guideline*, a qual lista os elementos-chave a ter em consideração no desenho de soluções informáticas que irão processar informação de caráter pessoal.

Relativamente à cláusula 7.5 *PII sharing, transfer, and disclosure*, nos registos de tratamento de dados pessoais da Celfocus encontram-se identificadas as transferências de dados pessoais efetuadas, incluindo a identificação do país de destino, caso seja fora da UE; a identificação da entidade de destino; os contactos do DPO; e a base legal para esta transferência. Sempre que existe transferência de dados pessoais, existe um contrato que estabelece as regras relativas à partilha e

processamento de dados pessoais, o qual estipula os requisitos mínimos de segurança associados, tanto nas situações em que a Celfocus tem o papel de *Controller* como de *Processor*.

Conforme exigido no RGPD e instanciado neste ponto da ISO, não pode existir transferência de dados pessoais para países não confiáveis, isto é, países sem decisão de adequação reconhecida pela CE, sem serem estabelecidas salvaguardas prévias entre as partes, as quais vinculem o *Processor* ao cumprimento de medidas que garantam uma proteção dos dados e seus titulares equivalente à existente na UE. A Celfocus cumpre com este requisito, tendo criado mecanismos para as situações em que possa ser necessário transferir dados pessoais para fora do EEE. Assim, na Celfocus surgiu a necessidade de criar uma *guideline* sobre a contratação de pessoas fora do EEE, especialmente na sequência da pandemia COVID-19, em que o trabalho em regime remoto cresceu consideravelmente. Esta *guideline* estabelece claramente que não é permitido contratar pessoas fora da UE e dos países com decisão de adequação, para trabalhar em projetos de clientes europeus, sempre que haja acesso a dados pessoais. Nesta *guideline* também é referido que, não sendo um cliente com sede na UE, ou seja, onde o RGPD pode não ser aplicado diretamente, a legislação de proteção de dados desse mesmo país deve ser tida em consideração.

4.2.2.4. Cláusula 8

O oitavo capítulo da ISO/IEC 27701 versa os requisitos para o desempenho de papel de *Processor* e nessa perspetiva a Celfocus, para se alinhar com as cláusulas 8.2 *Conditions for collection and processing* e 8.3 *Obligations to PII principals*, tem acordos relativos ao tratamento de dados pessoais estabelecidos pelos seus clientes (os já mencionados DPAs), os quais vinculam o *Processor* (neste caso, a Celfocus) a atuar de acordo com as instruções do *Controller* (o cliente), incluindo requisitos sobre o princípio *privacy by design and by default*; requisitos de segurança mínimos associados ao processamento de dados pessoais; responsabilidades na notificação de incidentes; instruções relativas à realização de PIAs; garantia de assistência por parte do *Processor* para que o cliente seja capaz de cumprir com as suas obrigações para com os titulares; entre outras exigências necessárias para garantir um processamento seguro à luz da legislação aplicável. Relativamente aos registos de processamento de dados pessoais exigidos, como já referido, na Celfocus este ponto encontra-se coberto pelos *Record of Processing Activities* de cada área.

Relativamente à cláusula 8.4 *Privacy by design and privacy by default*, a Celfocus recebe instruções por parte dos clientes sobre a necessidade de devolver ou apagar os dados pessoais no fim de um dado projeto, no entanto, é de salientar que na maioria dos casos as equipas de projeto apenas processam dados pessoais nos sistemas informáticos do cliente, não existindo transferência para fora da sua organização, estando protegidos pelos seus controlos de segurança.

Por último, sobre a cláusula 8.5 *PII sharing, transfer, and disclosure*, todas as disposições relativas à partilha e transferência de dados pessoais de clientes, e eventuais modificações a estas operações, encontram-se estabelecidas nos contratos entre as partes e, para além disto, na Celfocus também foi criada a *guideline* anteriormente referida, alusiva à contratação de pessoas fora da UE, a qual coloca a imposição de solicitar uma autorização formal ao cliente, que ateste a possibilidade de

contratar alguém extracomunitário e tomar as devidas diligências, nomeadamente o estabelecimento de SCCs para a transferência internacional de dados. O registo destas transferências encontra-se no *Record of Processing Activities* da respetiva área de projeto.

Caso a Celfocus receba um pedido de partilha de dados pessoais, por exemplo por parte de uma autoridade de controlo, deve seguir o *Clients' Personal Data Disclosure to Third Parties Procedure* para avaliar a legalidade do pedido e notificar o cliente em conformidade.

De referir ainda que, toda a documentação do SGP da Celfocus é divulgada na página do *Sharepoint* acessível a todos os colaboradores, existindo a prática de comunicar a toda a empresa sempre que existe nova documentação a considerar ou quando existem alterações significativas à existente. A documentação que suporta o SGP é apresentada na sessão de *privacy awareness* disponibilizada no *onboarding* de novos colaboradores. Tanto na sessão de Privacidade no *onboarding* como nas sessões anuais seguintes são transmitidas as boas práticas e os princípios relacionados com o processamento de dados pessoais, cujo cumprimento é dever de todos os colaboradores da Celfocus, para a boa manutenção e melhoria contínua do SGP.

4.2.3. Perceção de melhoria na conformidade com o RGPD

Tendo por base o alinhamento do SGP da Celfocus com a ISO/IEC 27701:2019, é possível afirmar que a perceção de melhoria da conformidade com o RGPD aumentou significativamente, pois apesar das divergências existentes entre a norma e o Regulamento, sem dúvida que a certificação na norma em estudo tornou o SGP mais coeso, com processos, procedimentos e responsabilidades melhor definidos e com um maior envolvimento, sensibilização e sentido de responsabilização por parte de todos os colaboradores, incluindo a gestão de topo, e terceiras partes com influência na gestão da Privacidade.

O SGP da Celfocus, depois de submetido à certificação na ISO/IEC 27701:2019, passou a sofrer um maior escrutínio nas práticas de proteção de dados por parte de uma entidade externa independente, uma vez que as auditorias anuais de acompanhamento e de recertificação a cada triénio passam a ser obrigatórias para a manutenção do certificado. A monitorização mais sistemática e regular, por parte da equipa de Privacidade, resulta num conhecimento mais profundo das atividades de processamento de dados pessoais levadas a cabo pela organização, bem como dos procedimentos a seguir para o tratamento dos dados e ainda num maior compromisso de todos para com os requisitos de Privacidade. Na verdade, a necessidade de documentar as práticas de proteção de dados *in place* e respetiva divulgação a toda a organização, faz com que os colaboradores, no geral, estejam mais cientes dos seus deveres para com o sistema de gestão e dos seus direitos enquanto titulares dos dados, o que é fundamental na garantia de conformidade da empresa com os requisitos normativos e regulamentares impostos.

A existência de uma cultura de Privacidade na organização, sustentada na evolução e crescimento dos processos do SGP, numa ótica de melhoria contínua, potencia a compreensão das exigências do RGPD e a capacidade dos colaboradores agirem naturalmente em conformidade. Outra mais-valia para a melhoria da conformidade com o RGPD prende-se com o maior conhecimento e

consciência dos riscos relacionados com a proteção de dados, nas várias áreas que integram o SGP, cuja avaliação e controlo pode evitar eventuais situações de incumprimento. De destacar ainda que não ocorreram quaisquer *privacy breaches* na Celfocus comunicadas à CNPD, ou outra autoridade de controlo, nem foram aplicadas quaisquer multas por incumprimento dos deveres de proteção de dados impostos pelo RGPD, o que prova que, de facto, as boas práticas implementadas no SGP, baseadas na ISO 27701 como complemento aos requisitos da ISO 27001 implementados no SGSI, garantem um tratamento seguro de dados pessoais também de acordo com as exigências do Regulamento.

No caso da Celfocus, ao alinhar o SGP com a ISO/IEC 27701 foi possível complementar o trabalho já efetuado anteriormente em torno dos requisitos do RGPD e consolidar algumas práticas, tendo-se conseguido definir medidas técnicas e organizativas que sustentem um tratamento de dados pessoais seguro; determinar o papel da organização enquanto *Controller* e *Processor;* nomear um DPO; registar as atividades de processamento de dados pessoais efetuadas; identificar os ativos onde se encontram os dados pessoais; realizar avaliações de risco de privacidade periódicas; disponibilizar formação sobre proteção de dados pessoais a todos os colaboradores; implementar o princípio de *privacy by design and by default* nos sistemas; definir as necessidades de comunicação interna e externa; garantir a adequada gestão de incidentes de segurança que envolvam dados pessoais e respetiva notificação às autoridades de controlo; rever os contratos quer com colaboradores quer com fornecedores ou outras terceiras partes, para inclusão de cláusulas alusivas à proteção de dados; e aumentar a garantia de confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas onde são processados dados pessoais. Também os requisitos para a recolha de dados pessoais, obtenção de consentimento, exercício de direitos dos titulares e garantia de um tratamento lícito e transparente foram implementados na Celfocus, em conformidade com a norma e com o RGPD. As práticas para a transferência segura de dados pessoais, garantindo a proteção dos dados e seus titulares, foram também definidas em total consonância com ambos os documentos.

A Celfocus está consciente que a certificação na norma em estudo veio impulsionar a conformidade das suas práticas com as exigências do RGPD, no entanto, continua a ser da responsabilidade da equipa de Privacidade conhecer e incorporar os requisitos legais e regulatórios emergentes e aplicáveis ao contexto e objetivos da organização, para que o alinhamento do SGP seja o mais completo, atualizado e abrangente possível. No fundo, todo o percurso percorrido para alinhar o SGP com a ISO 27701 serviu em simultâneo para implementar políticas, processos, procedimentos e práticas em conformidade com o RGPD. Contudo, durante este percurso houve a necessidade de ajustar o SGP nos pontos em que a abordagem da norma e do Regulamento não é análoga, de forma a não comprometer, por um lado, o alinhamento do SGP com a ISO, conforme atestado pela certificação recentemente obtida e, por outro lado, garantindo o cumprimento dos requisitos do RGPD, os quais, por imposição legal, são de implementação obrigatória.

Depois de todo o trabalho de preparação, efetuado em torno da certificação ISO/IEC 27701:2019, demonstrou-se que o alinhamento do SGP da Celfocus com esta norma veio garantir a integração de todos os requisitos do RGPD aplicáveis à organização no seu sistema, o que vem provar que a implementação deste standard tem um papel preponderante na garantia do cumprimento do RGPD, sendo uma ferramenta útil e eficaz para uma gestão rigorosa e transparente da Privacidade.

5. Considerações finais

A gestão da Segurança da Informação tem um papel fundamental na garantia de um tratamento seguro de dados pessoais, contudo é manifestamente insuficiente se, em paralelo, não existir um compromisso de cumprimento da legislação de privacidade aplicável. Na verdade, a proteção de dados pessoais tornou-se uma questão fulcral para as organizações aquando da entrada em vigor do RGPD, o que veio causar alterações profundas no *modus operandi* das empresas, com o objetivo de demonstrar conformidade com este Regulamento, garantindo um tratamento seguro de dados pessoais. Nesta perspetiva, a norma em estudo, ISO/IEC 27701:2019, é, sem dúvida, uma ferramenta importante para as empresas, na medida em que fornece linhas guia para o estabelecimento de um SGP em consonância com a legislação aplicável.

O alinhamento do SGP com a norma ISO/IEC 27701:2019 traz benefícios acrescidos para as organizações através de uma abordagem assente na gestão integrada da Privacidade e da Segurança da Informação, duas áreas indissociáveis, onde a implementação dos controlos procura assegurar a adequada proteção de toda a informação organizacional, incluindo os dados pessoais. Assim, é consensual que esta norma mune as organizações, que atuam enquanto *Controllers* e/ou *Processors,* com as diretrizes que possibilitam agilizar a implementação de práticas que garantam um tratamento seguro e transparente de dados pessoais, contribuindo para a difusão da conformidade com os requisitos do RGPD.

A análise comparativa entre a norma e o Regulamento, documentos com cariz e finalidades diferentes, denota que os regimes estabelecidos por ambos não são totalmente equivalentes. No entanto, é possível concluir que os pontos de convergência suplantam largamente as divergências encontradas, sendo claro o benefício associado ao alinhamento do SGP com a ISO/IEC 27701:2019, espelhado no auxílio do cumprimento da legislação aplicável em matéria de proteção de dados, com foco no RGPD, desde que exista a devida adaptação aos seus requisitos nas situações em que as abordagens não são equivalentes. De destacar que os requisitos presentes nas cláusulas 5, 6, 7 e 8 da ISO/IEC 27701:2019 estão alinhados com os pontos chave do RGPD, nomeadamente os princípios relativos ao tratamento de dados pessoais, a licitude do tratamento, o registo de todas as atividades de processamento de dados pessoais, as responsabilidades das organizações enquanto *Controllers* e *Processors*, o papel do *Data Protection Officer*, a notificação de incidentes de privacidade, a avaliação dos riscos relacionados com o tratamento de dados pessoais, os requisitos para as transferências *cross-border* de dados pessoais, assim como a integração do conceito de *privacy by design and by default* nos sistemas, abrangendo, na sua essência, os artigos 5.º ao 49.º do RGPD, com exceção do artigo 43.º referente aos organismos de certificação, cujas abordagens, como vimos, não são equivalentes.

O RGPD, ao definir os princípios fundamentais para a recolha e processamento de dados pessoais, pode ser considerado como o alicerce para a garantia da proteção dos dados e seus titulares, sendo de certa forma complementado pela norma ISO/IEC 27701:2019, que define de forma clara e objetiva os procedimentos que as organizações devem seguir para assegurar, por um lado, a conformidade com a legislação aplicável e, por outro, a implementação e melhoria contínua de um SGP

que garanta a confidencialidade e integridade dos dados pessoais processados, trabalhando em consonância para um objetivo comum – assegurar o respeito do direito fundamental dos titulares à proteção dos seus dados pessoais.

O *case-study* realizado na empresa Celfocus, S.A. vem corroborar a importância do papel da ISO/IEC 27701:2019 na garantia de conformidade com o RGPD nas organizações, uma vez que a certificação, bem como todo o trabalho preparatório realizado demonstraram uma eficaz integração quer dos requisitos normativos quer das exigências do RGPD, aplicáveis ao sistema de gestão, tornando a organização idónea e com práticas de proteção de dados comprovadamente consolidadas. A certificação do SGP da Celfocus, S.A. na norma ISO/IEC 27701:2019 propiciou não só um conhecimento rigoroso dos requisitos para o tratamento de dados pessoais e das atividades de processamento levadas a cabo, como também um maior sentido de responsabilização por parte de todos os colaboradores, no que diz respeito às Políticas e práticas de Privacidade implementadas, resultando no estabelecimento de uma cultura de Privacidade sustentada neste sistema de gestão, agora mais robusto e capaz de fazer face às exigências do Regulamento.

De notar que a certificação dota a Celfocus, S.A. de uma validação, independente e internacionalmente reconhecida, de que as suas práticas de proteção de dados pessoais estão em conformidade com a ISO/IEC 27701:2019 e, consequentemente, com o RGPD, dada a comprovada convergência dos seus requisitos. Contudo, é de referir que este certificado não torna as empresas à prova de bala, pois no mundo digital, indubitavelmente, as ameaças e vulnerabilidades encontram-se em constante evolução, pelo que a exposição ao risco, mesmo que controlada, nunca é inexistente.

Nesta medida, a ideia de um cumprimento integral do RGPD pode ser considerada algo utópica, mesmo numa empresa com certificação ISO/IEC 27701:2019, pois existem uma série de fatores, quer internos quer externos, que podem condicionar a garantia de um tratamento completamente seguro de dados pessoais. Não obstante, o alinhamento do SGP com a norma em análise tem um papel determinante nas organizações que pretendem elevar as suas práticas de proteção de dados, visto que o standard pode ser a chave para o cumprimento das disposições gerais do RGPD, ao exigir a monitorização constante e sistemática das práticas de proteção de dados em vigor, numa ótica de melhoria contínua, bem como um estudo permanente da evolução da legislação aplicável, de modo a garantir o cumprimento rigoroso das imposições legais de proteção de dados e seus titulares.

Bibliografia

ACCENTURE SECURITY,
"The cost of cybercrime", 2019. [Online] Disponível em: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf [Consultado a 15/12/2021].

AGARWAL, Sushant,
"Towards dealing with GDPR uncertainty", Institute for Management Information Systems, Vienna University of Economics and Business, 2016. [Online] Disponível em: https://docplayer.net/124763164-Towards-dealing-with-gdpr-uncertainty.html [Consultado a 30/07/2022].

ALHOGAIL, Areej,
"Design and validation of information security culture framework. Computers in Human Behavior", 2015. [Online]. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0747563215002447?via%3Dihub [Consultado a 14/12/2021].

ALMEIDA, Luís Miguel Sousa Trindade,
"Decision Support for Selecting Information Security Controls", 2018. [Online]. Disponível em: https://repositorio.ul.pt/bitstream/10451/33934/1/ulfc124363_tm_Lu%c3%ads_Almeida.pdf [Consultado a 11/12/2021].

ALMEIDA TEIXEIRA, Gonçalo Villa de Freitas de,
"The Critical Success Factors of GDPR Implementation", Thesis to obtain the Master of Science Degree in Information Systems and Computer Engineering, Instituto Superior Técnico da Universidade de Lisboa, 2019. [Online]. Disponível em: https://fenix.tecnico.ulisboa.pt/downloadFile/1689244997260442/82070-goncalo-teixeira_dissertacao.pdf [Consultado a 25/07/2022].

ALVES, Diogo Lopes,
"O papel da Cibersegurança na Proteção de Dados Pessoais", Anuário da Proteção de Dados, 2021, pp. 121-154. [Online]. Disponível em: https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2021/08/Anuario-da-Protecao-de-Dados-2021_Eletronico-1.pdf [Consultado a 05/01/2022].

ANWAR, Memoona Javeria; GILL, Asif Qumer,
"Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model", Australasian Conference on Information Systems, 2020. [Online]. Disponível em: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1055&context=acis2020 [Consultado a 04/12/2021].

APCER,
“Regulamento Geral de Certificação de Produtos, Processos e Serviços”, s.d. [Online]. Disponível em: https://apcergroup.com/images/site/downloads/Regulamentos/APCER_REG002_RGC-PPS_PT.pdf [Consultado a 05/04/2022].

BONTA, Rob,
“California Consumer Privacy Act (CCPA)”, State of California Department of Justice, s.d. [Online]. Disponível em: https://oag.ca.gov/privacy/ccpa#sectionb [Consultado a 04/01/2022].

BSI - British Standards Institution,
“ISO/IEC 27701 Privacy Information Management - Your implementation guide”, 2019, pp. 4-6 [Online]. Disponível em: https://www.bsigroup.com/globalassets/localfiles/en-gb/isoiec-27701-privacy-information-management/resources/iso-27701-implementation-guide.pdf [Consultado a 25/11/2021].

CANO, Jeimy,
“Privacy and Information Security: The Territorial Challenges”, 2014. [Online] Disponível em: https://iapp.org/news/a/privacy-and-information-security-the-territorial-challenges1/ [Consultado a 04/12/2021].

Carta dos Direitos Fundamentais da União Europeia, Jornal Oficial da União Europeia, 2016. [Online] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR [Consultado a 06/12/2021].

Celfocus,
“Who We Are. High Technology. Handmade”, s.d. [Online] Disponível em: https://celfocus.com/home/who-we-are [Consultado a 25/05/2022].

Comissão Europeia,
“Adequacy decisions - How the EU determines if a non-EU country has an adequate level of data protection”, s.d. [Online]. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [Consultado a 04/01/2022].

Comissão Europeia,
“Comunicado de Imprensa – Nova Estratégia da EU para a Cibersegurança e novas regras para aumentar a resiliência das entidades críticas físicas e digitais”, 2020. [Online]. Disponível em: https://ec.europa.eu/commission/presscorner/detail/pt/ip_20_2391 [Consultado a 14/01/2022].

Comissão Nacional de Proteção de Dados (CNPD),
“Obrigações – Avaliação de Impacto sobre a Proteção de Dados”, 2021. [Online] Disponível em: https://www.cnpd.pt/organizacoes/obrigacoes/avaliacao-de-impacto/ [Consultado a 25/03/2022].

Comissão Nacional de Proteção de Dados (CNPD),
“Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados”, Parte B. 2018. [Online]. Disponível em: https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121818. [Consultado a 22/04/2022].

Commission Nationale Informatique & Libertés (CNIL),
“ISO 27701, an international standard addressing personal data protection”, 2020. [Online] Disponível em: https://www.cnil.fr/en/iso-27701-international-standard-addressing-personal-data-protection [Consultado a 24/01/2022].
CROCETTI, Paul; PETERSON, Stacey; HEFNER, Kim,
“What is data protection and why is it important?”, 2021. [Online] Disponível em: https://www.techtarget.com/searchdatabackup/definition/data-protection [Consultado a 01/08/2022].

Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=EN [Consultado a 19/02/2022].

Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento, 2019. [Online] Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_pt [Consultado a 07/04/2022].

Ernst & Young Global,
“How ISO 27701 could be a new framework for sustained GDPR compliance”, 2020. [Online]. Disponível em: https://www.ey.com/en_gl/consulting/how-iso-27701-could-be-a-new-framework-for-sustained-gdpr-compliance [Consultado a 30/03/2022].

European Data Protection Board,
“Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data”, adopted on 10 November 2020. [Online]. Disponível em: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementary measurestransferstools_en.pdf [Consultado a 05/01/2022].

Governo do Brasil - Ministério da Defesa,
“Lei Geral de Proteção de Dados – LGPD”, 2020. [Online] Disponível em: https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd [Consultado a 03/01/2022].

Governo do Reino Unido,
“Data Protection Act – UK’s implementation of the General Data Protection Regulation (GDPR)”, s.d. [Online] Disponível em: https://www.gov.uk/data-protection/print [Consultado a 05/01/2022].

IPAC – Instituto Português de Acreditação,
“Notícias – Portugal pioneiro na certificação da Maturidade Digital”, 2021. [Online]. Disponível em: http://www.ipac.pt/ [Consultado a 07/04/2022].

IPAC – Instituto Português de Acreditação,
“Questões Frequentes – Q3”, s.d. [Online]. Disponível em: http://www.ipac.pt/faqs/faqs.asp [Consultado a 07/04/2022].

IRWIN, Luke,
“How ISO 27001 can help you achive GDPR compliance”, 2018. IT Governance. [Online]. Disponível em: https://www.itgovernance.co.uk/blog/how-iso-27001-can-help-you-achieve-gdpr-compliance [Consultado a 16/12/2021].

ISO/IEC 27001:2013, International Standard ISO / IEC Information technology — Security techniques — Information security management systems — Requirements, 2013.

ISO/IEC 29151.2017, Information technology — Security techniques — Code of practice for personally identifiable information protection, 2017.

International Standard, ISO/IEC 27701 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines. 1ª edição de agosto de 2019.

ISO - International Organization for Standardization,
“ISO/IEC 27701:2019 Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines”. 2019. [Online] Disponível em: https://www.iso.org/standard/71670.html [Consultado a 25/10/2021].

ISO - International Organization for Standardization,
“Certification & Conformity”. 2020. [Online]. Disponível em: https://www.iso.org/certification.html [Consultado a 10/12/2020].

IT Governance,
“How you will benefit from ISO 27001 certification”, 2020. [Online]. Disponível em: https://www.itgovernance.co.uk/iso27001-benefits [Consultado a 16/12/2020].

JESUS, Inês Oliveira Andrade,
"O direito à proteção de dados pessoais e o regime jurídico das transferências internacionais de dados: a proteção viaja com as informações que nos dizem respeito?", Anuário da Proteção de Dados. 2018, pp.71-90. [Online]. Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf [Consultado a 29/12/2021].

KNUUTI, Olli; TUUMI, Antti-Jussi; EVESTI, Antti,
"ISO 27701 Privacy Certification". KPMG Webinar Presentation. 2020, pp. 16-24. [Online] Disponível em: https://assets.kpmg/content/dam/kpmg/ru/pdf/2020/06/ru-en-iso-iec-27701-2019-certification.pdf [Consultado a 11/12/2020].

LACHAUD, Eric,
"ISO/IEC 27701: Threats and Opportunities for GDPR Certification". 2020, pp. 2-14. [Online] Disponível em:
https://www.researchgate.net/publication/338676835_ISOIEC_27701_Threats_and_Opportunities_for_GDPR_Certification [Consultado a 17/12/2021].

LAMEIRAS, André,
"5 reasons why GDPR was a milestone for data protection", 2022. [Online]. Disponível em: https://www.welivesecurity.com/2022/05/25/5-reasons-why-gdpr-milestone-data-protection/
[Consultado a 01/08/2022].

LOPES, Joaquim de Seabra,
"O Artigo 35.º da Constituição: da génese à atualidade e ao futuro previsível", *in* Forum de Proteção de Dados – em foco 40 anos da constituição e do direito à proteção de dados, n.º 02, 2016. [Online]. Disponível em: https://www.cnpd.pt/media/kjspegob/forum_2_af_web_low.pdf [Consultado a 30/03/2022].

LOPES, Isabel Maria; OLIVEIRA, Pedro; GUARDA, Teresa,
"Implementation of ISO 27001 Standards as GDPR Compliance Facilitator". 2019, pp.1-8. [Online]. Disponível em:
https://www.researchgate.net/publication/335358551_Implementation_of_ISO_27001_Standards_as_GDPR_Compliance_Facilitator [Consultado a 10/12/2021].

MATTES, Icaro Valente; PETRI, Sérgio Murilo,
"Accounting Information Security: Procedures for the Preparation of the Security Policy based on ISO 27001 and ISO 27002", 2015. 10th International Conference on Information Systems and Technology Management. [Online]. Disponível em:
http://www.contecsi.tecsi.org/index.php/contecsi/10contecsi/paper/download/205/6 [Consultado a 14/12/2021].

MILLER, Bryon; MILLER, Katelin; ZHANG, Xihui; TERWILLIGER, Mark G,
“Prevention of Phishing Attacks: A Three-pillared Approach”, Issues in Information Systems, Volume 21, Issue 2, 2020. [Online]. Disponível em: http://www.iacis.org/iis/2020/2_iis_2020_1-8.pdf [Consultado a 06/12/2021].

Novabase,
“Certificações – Porque somos responsáveis…”, s.d. [Online]. Disponível em: https://www.novabase.com/pt/sobre-nos/certificacoes/ [Consultado a 25/05/2022].

NQA – Global Certification Body,
“ISO/IEC 27701 Implementation Guide”, s.d. [Online]. Disponível em: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-27701-Mini-Implementation-Guide.pdf [Consultado a 23/01/2022].

NQA – Global Certification Body,
“ISO 27701 and GDPR”, 2021. [Online]. Disponível em: https://www.nqa.com/en-us/resources/blog/june-2021/iso-27701-gdpr [Consultado a 29/03/2022].

Observatório de Cibersegurança,
“Relatório Riscos & Conflitos 2021”, Cibersegurança em Portugal, 2021. [Online]. Disponível em: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf [Consultado a 29/12/2021].

Observatório de Cibersegurança,
“Relatório Riscos & Conflitos 2022”, Cibersegurança em Portugal, 2022. [Online]. Disponível em: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf [Consultado a 14/08/2022].

PINHEIRO, Alexandre Sousa,
“Consequências do Acordão Schrems II”, 2020. [Online]. Disponível em: https://asousapinheiro.com/2020/08/21/consequencias-do-acordao-schrems-ii/ [Consultado a 05/01/2022].

Regulamento n.º 834/2021 de 6 de setembro de 2021. Diário da República, n.º 173 Parte B, pp. 15-23. Requisitos adicionais de acreditação para os organismos de certificação. [Online]. Disponível em: https://files.dre.pt/2s/2021/09/173000000/0001500023.pdf [Consultado a 07/04/2022].

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de

Dados). [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN [Consultado a 25/01/2022].

Republic of Kenya - National Council for Law Reporting Library,
"The Data Protection Act, No. 24 of 2019", 2019. [Online]. Disponível em: https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/109333/135597/F752512879/KEN109333.pdf [Consultado a 02/01/2022].

SANTOS, Ana Felícia Canilho,
"O Cibercrime: desafios e respostas do Direito", Dissertação para obtenção do grau de Mestre em Direito, Universidade Autónoma de Lisboa, 2015. [Online]. Disponível em: https://repositorio.ual.pt/bitstream/11144/2640/1/TESE%20COMPLETA2.pdf [Consultado a 06/12/2021].

SGS Portugal,
"RGPD – 7 princípios fundamentais", 2021. [Online]. Disponível em: https://www.sgs.pt/pt-pt/news/2021/11/rgpd-7-principios-fundamentais [Consultado a 30/03/2022].

SIGANTO, Jodie,
"ISO 27701 Privacy Management System: How useful is it?", Privacy 108 – We Protect Privacy, 2020. [Online]. Disponível em: https://privacy108.com.au/insights/iso-27701/ [Consultado a 04/04/2022].

SOENEN, Patrick,
"Privacy Information Management with ISO 27701", Qualified Audit Academy, 2019. [Online]. Disponível em: https://www.audit-academy.be/images/downloads/IS-ISO27701-2019V1.pdf [Consultado a 23/01/2022].

TEIXEIRA, Angelina,
"RGPD nas organizações: a ecografia (possível) dos 6 meses", *in* O RGPD e o impacto nas organizações: 6 meses depois – congresso Internacional de Ciências Jurídico-Empresariais, 2019, pp. 7-18. [Online]. Disponível em: https://cicje.ipleiria.pt/files/2020/01/Atas.pdf [Consultado a 10/01/2022].

Tribunal de Justiça da União Europeia,
"Comunicado de Imprensa nº91/20 de 16 julho 2020 relativo ao Acórdão no processo C-311/18", 2020. [Online]. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091pt.pdf [Consultado a 05/01/2022].

VEIGA, Adélcia Solange Pereira Gonçalves,

“Proteção de Dados: O Direito à Privacidade na Era Digital”, Dissertação para obtenção do grau de Mestre em Direito, Universidade Autónoma de Lisboa, 2020. [Online]. Disponível em: https://repositorio.ual.pt/bitstream/11144/5046/1/Disserta%C3%A7%C3%A3o%20de%20Mestrado%20-%20Final%20-%20Revista%206.7.202o_%20AV.pdf [Consultado a 22/01/2022].