Mestrado em Gestão de Sistemas e Tecnologias de Informação

Solução para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD

Luís Miguel Ribeiro Pedroso

Número

201929286

Nome da Orientadora

Professora Doutora Virgínia Araújo

Junho de 2021

Agradecimentos

À Atlântica – Instituto Universitário e à minha orientadora em particular, professora Doutora Virgínia Araújo, pela oportunidade e apoio na concretização deste trabalho de investigação.

À Associação Nacional das Pequenas e Médias Empresas pela colaboração, e a todas as PME que tornaram possível este trabalho.

A todos os amigos e familiares que me apoiaram e ajudaram a construir este documento.

E, em especial, aos meus grandes amores: Vanessa, Henrique, Simão e Benjamim.

Resumo

A União Europeia criou, em 2016, o Regulamento Geral sobre a Proteção de Dados – RGPD – com aplicação obrigatória em toda a União Europeia a partir de 25 de maio de 2018.

Uma das principais obrigações de todas as empresas, no RGPD, incluindo PME – Pequenas e Médias Empresas, que atuam como responsáveis pelo tratamento ou subcontratantes, é a segurança dos dados pessoais.

Se as grandes empresas têm a possibilidade de responder adequadamente a estes desafios, com as devidas iniciativas, as PME nem sempre têm a experiência e/ou os recursos necessários para o fazer.

A aplicação de multas e coimas, neste cenário imprevisível de violação de dados, sem existir capacidade de demonstração do nível de conformidade das organizações, pode condicionar a continuidade do seu negócio.

Este trabalho teve como objetivo principal criar uma solução para conformidade, proteção e privacidade dos dados pessoais, que permita que as pequenas e médias empresas se prepararem para o cumprimento das regras relativas às obrigações legais do RGPD, incluindo critérios de apoio à decisão, tendo em conta as sanções jurídicas existentes no contexto europeu.

Palavras-Chave: RGPD, PME, Dados Pessoais, Privacidade, Proteção de Dados, Gestão da Segurança da Informação, Sanções jurídicas, Conformidade.

Abstract

The General Data Protection Regulation – GDPR – was created by the European Union in 2016, with mandatory application throughout the European Union from 25 May 2018.

One of the main obligations of all companies, in the GDPR, including SMEs - Small and Medium Enterprises, acting as controllers or subcontractors, is the security of personal data.

While large companies can implement and respond appropriately to these challenges, SMEs do not always have the expertise and/or resources to do so.

The application of fines and penalties, in this unpredictable scenario of data breach, without the ability to demonstrate the adequate level of compliance, may jeopardize the continuity of their business.

The main goal of this research is to propose a solution for the compliance, protection and privacy of personal data, which allows small and medium-sized enterprises to prepare for compliance with the rules regarding the legal obligations of the GDPR, including decision support criteria, considering the existing legal sanctions in the European context.

Keywords: GDPR, SMEs, Personal Data, Privacy, Data Protection, Information Security Management, Regulatory Sanctions, Compliance.

Índice

Índice de Tabelas

Índice de Figuras

Lista de Siglas e Abreviaturas

ANPME - Associação Nacional das Pequenas e Médias Empresas

CIA - Confidentiality, Integrity and Availability

CISTI - Conferência Ibérica de Sistemas e Tecnologias de Informação

CISO - Chief Information Security Officer

CNCS - Centro Nacional de Cibersegurança

CNIL - Commission Nationale de l'Informatique et des Libertés

CNPD - Comissão Nacional de Proteção de Dados

Diretiva SRI - Diretiva relativa à Segurança das Redes e dos Sistemas de Informação

DPC - Data Protection Commission

DPIA / AIPD - Avaliação de impacto sobre a proteção de dados

DPO / EPD - Encarregado/a de Proteção de Dados

DSR - Design Science Research

EDPB - European Data Protection Board

ENISA - Agência da União Europeia para a Segurança de Redes e Informações

ICO - Information Commissioner's Office

INE - Instituto Nacional de Estatística

IoT - Internet das coisas

ISO - Organização Internacional de Normalização

NIST - National Institute of Standards and Technology

NUT - Nomenclatura das Unidades Territoriais para Fins Estatísticos

PME - Pequenas e Médias Empresas

PoC - Prova de Conceito

PrOnto - Privacy Ontology for Legal Reasoning

RGPD - Regulamento Geral sobre a Proteção de Dados

RH - Recursos Humanos

SDLC - ciclo de vida de desenvolvimento de software

SI - Sistemas de Informação

SLR - Systematic literature review

TFUE - Tratado sobre o Funcionamento da União Europeia

TI - Tecnologias de Informação

TIC - Tecnologias da Informação e Comunicação

UE - União Europeia

Capítulo 1 - Introdução

A União Europeia criou, em 2016, o Regulamento Geral sobre a Proteção de Dados – RGPD – com aplicação obrigatória em toda a União Europeia a partir de 25 de maio de 2018.

O RGPD está no cerne do quadro da União Europeia que garante o direito fundamental à proteção de dados, tal como consagrado na Carta dos Direitos Fundamentais da União Europeia (artigo 8º) e nos Tratados (artigo 16º do Tratado sobre o Funcionamento da União Europeia, «TFUE») (Comissão Europeia, 2020).

A mudança de paradigma, por força da aplicação deste documento legal, face ao seu documento anterior, Diretiva 95/46/CE, de 24 de outubro de 1995, releva a necessidade de autorregulação dos agentes económicos, aplicável em todos os Estados-Membros.

Uma das principais obrigações de todas as empresas, no RGPD, incluindo Pequenas e Médias Empresas (PME), que atuam como responsáveis pelo tratamento ou subcontratantes, é a segurança dos dados pessoais. Em particular, de acordo com o RGPD, a segurança dos dados abrange a confidencialidade, integridade e disponibilidade e deve ser considerada seguindo uma abordagem baseada no risco: quanto maior o risco, mais rigorosas são as medidas que o responsável pelo tratamento ou o subcontratante precisa tomar, a fim de gerir o risco (ENISA, 2017, pág. 6).

A segurança, no sentido da integridade e confidencialidade, é estabelecida como um dos princípios relativos ao tratamento de dados pessoais: alínea f) do número 1 do artigo 5º do RGPD. Isto coloca a segurança no centro da proteção de dados, juntamente com os outros princípios da proteção de dados, designadamente, licitude, lealdade e transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação e responsabilidade.

Sobre a abordagem baseada em risco, destacam-se, no RGPD, três artigos fundamentais:

> Artigo 25º - Proteção de dados desde a conceção e por defeito, "(…) bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável (…) aplica (…) medidas técnicas e organizativas adequadas";
>
> Artigo 32º - Segurança do tratamento, "um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas" e "ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento";
>
> Artigo 35º - Avaliação de impacto sobre a proteção de dados, "uma avaliação dos riscos para os direitos e liberdades dos titulares".

Contudo, não obstante o quadro sancionatório ser bastante elevado, podendo atingir montantes na ordem dos 20 milhões de Euros ou até 4% do volume de negócios anual de uma empresa, "apenas 2,5% dos decisores em Portugal acha que a sua organização está preparada para lidar com o RGPD" (Microsoft, 2018). Freitas e Mira da Silva (2018) referem, no seu estudo, que as PME têm falta de conhecimento sobre as suas obrigações e deveres em relação à proteção

de dados pessoais, enquanto Carvalho Silva (2019) conclui que apenas uma minoria das PME (25,85%) realizou uma auditoria aos dados que detêm.

Verifica-se, portanto, uma fraca preparação do tecido empresarial português para esta mudança.

Neste contexto, e como parte do seu apoio contínuo à implementação da política da União Europeia, a ENISA – Agência da União Europeia para a Segurança de Redes e Informações, publicou em 2016 (ENISA, 2016), e atualizou em 2017 (ENISA, 2017), um conjunto de orientações para as PME, atuando como responsáveis pelo tratamento ou subcontratantes, que visam ajudá-las a avaliar os riscos de segurança e, consequentemente, adotar medidas de segurança para a proteção de dados pessoais, e garantir a conformidade com o RGPD.

Em particular, o objetivo do estudo é facilitar às PME a compreensão do contexto da operação de tratamento de dados pessoais e, subsequentemente, avaliar os riscos de segurança associados (ENISA, 2017, pág. 9).

Numa tentativa de facilitar ainda mais este procedimento, também está incluído na ferramenta de avaliação do nível de risco um mapeamento do conjunto de medidas proposto com os controlos de segurança da ISO/IEC 27001:2013 relativo à segurança da informação (ENISA, 2016, pág.33). Adicionalmente, e tendo em conta a extensão da ISO/IEC 27001 para a gestão de informações de privacidade – ISO/IEC 27701:2019, o mapeamento integral ao RGPD permite às PME a utilização das orientações da ENISA para o cumprimento total do regulamento.

O âmbito e a aplicação do RGPD trazem, efetivamente, desafios para as PME por meio de um único conjunto de regras na UE. Espera-se que as PME saibam gerir os seus fluxos de dados e processos de dados pessoais da mesma forma que as grandes organizações, que possuem melhores recursos (ENISA, 2016, pág.16).

1.1.Motivação e Objetivos

Brodin (2019), na sua análise do estado da arte, indica que o número de artigos científicos sobre o RGPD é limitado. No entanto, a maioria dos problemas de conformidade é encontrada nas Pequenas e Médias Empresas, pois possuem recursos mais limitados com exceção das empresas com um foco em termos de segurança.

Chatzipoulidis et al (2019) também apresentam uma ferramenta de avaliação de conformidade com o RGPD, mantendo o enfoque nas Pequenas e Médias Empresas que ambicionam estar em conformidade.

Freitas e Mira da Silva (2018), no contexto português, reforçam a necessidade de definir uma metodologia para poder cumprir as obrigações do RGPD, considerando a análise realizada a dez PME nos distritos de Lisboa, Aveiro e Leiria, onde se identificou a falta de conhecimento dessas empresas sobre as suas obrigações e deveres em relação à proteção de dados pessoais.

Brodin (2019) afirma também que grande parte dos investigadores trabalham temas específicos do RGPD, como a portabilidade dos dados, certificação, ou numa área de atividade concreta.

De facto, quando se tenta pesquisar o envolvimento de algoritmos e a identificação de tendências na construção de modelos de referência para o RGPD, as únicas respostas obtidas são específicas para as questões das decisões individuais automatizadas, incluindo a definição de perfis (Castets-Renard, 2019; Henderson, 2017).

Neste sentido, verifica-se que a utilização de algoritmos como parte integrante de ferramentas de avaliação da conformidade com o RGPD ainda está longe de ser uma realidade, como verificado nos estudos de Brodin (2019) e de Chatzipoulidis et al (2019).

Considerando, assim, que não existem ferramentas "chave na mão" disponíveis para aplicação direta por parte das empresas, uma grande parcela do tecido empresarial – PME – não tem capacidade de implementação efetiva das obrigações do RGPD, principalmente pelas exigências técnicas e organizativas por força das mudanças tecnológicas que os negócios impõem com os seus Sistemas de Informação, deixando, deste modo, vulneráveis as informações dos seus clientes e também dos seus negócios.

Não obstante várias autoridades de controlo de alguns Estados-Membros publicarem, com alguma regularidade, documentos orientadores para o cumprimento das regras relativas à privacidade de dados pessoais, os documentos são de leitura técnica, restringindo-os a um grupo de especialistas.

A aplicação de multas e coimas, neste cenário imprevisível de violação de dados, sem existir capacidade de demonstração do nível de conformidade do regulamento, pode condicionar a continuidade do negócio das organizações, nomeadamente das PME.

Desta forma, como referido nos pontos anteriores, verifica-se que os modelos de referência também deveriam incorporar as tendências das autoridades como critério de tomada de decisão e de priorização, nomeadamente ao nível das Pequenas e Médias Empresas.

Assim sendo, observa-se a pertinência deste projeto, que diz respeito à construção de uma solução para conformidade, proteção e privacidade dos dados pessoais, considerando as sanções jurídicas do RGPD na União Europeia como fator de suporte à tomada de decisão, com vista à obtenção da conformidade com o Regulamento.

1.2.Objetivos de Investigação

Pretende-se construir uma solução para proteção da privacidade e dos dados pessoais, que permita garantir a conformidade legal, priorizando os requisitos de privacidade e dados pessoais que possam ter maior impacto financeiro nas organizações, nomeadamente em Pequenas e Médias Empresas, baseada em sanções jurídicas do RGPD, tendo como referência um conjunto de orientações da Agência da União Europeia para a Segurança de Redes e Informações – ENISA, e a aplicação dos requisitos existentes na família ISO/IEC 27000, nomeadamente as normas ISO/IEC 27001:2013 e ISO/IEC 27701:2019, relativas à segurança da informação e à privacidade.

Adicionalmente, enquanto ponto de partida, para reforçar a pertinência do objetivo principal, pretende-se analisar o impacto do RGPD nas Pequenas e Médias Empresas, em Portugal.

Em síntese, com base nas informações apresentadas acima, este trabalho apresenta os seguintes objetivos e atividades:

O1 – verificar qual o impacto do RGPD nas Organizações - PME

O2 – desenvolver uma solução para proteção da privacidade e dos dados pessoais baseada em sanções jurídicas do RGPD

A1 – definir um processo de gestão do risco – proposta inicial da solução

A2 – desenvolver uma Prova de Conceito

A3 – avaliar os resultados da Prova de Conceito

A4 – apresentar uma solução para conformidade e proteção da privacidade e dos dados pessoais

1.3.Estrutura do Trabalho

O trabalho apresentado consiste em 7 capítulos estruturados da seguinte forma. O capítulo 1 apresenta a introdução ao tema, motivações e objetivos da pesquisa. O capítulo 2 apresenta a revisão da literatura sobre soluções e modelos de referência para a conformidade com o RGPD, nomeadamente para Pequenas e Médias Empresas. Apresenta também o enquadramento das PME no contexto nacional, o RGPD, a evolução da aplicação do RGPD em toda a União Europeia, aspetos teóricos da segurança e gestão dos riscos na área dos dados pessoais. No capítulo 3 é apresentada a Metodologia de Investigação aplicada neste trabalho. O capítulo 4 descreve todo o processo de desenho e desenvolvimento das atividades necessárias para a implementação da solução proposta, aplicando o método de investigação apresentado no capítulo 3. No capítulo 5 são apresentados os dados recolhidos, enquanto que no capítulo 6 apresentam-se a análise, discussão e demonstração dos resultados da prova de conceito. Por último, no capítulo 7, são apresentadas as conclusões do trabalho realizado, limitações sentidas ao longo da dissertação e possíveis trabalhos futuros.

Capítulo 2 – Revisão da Literatura

2.1.Modelos de referência para a conformidade com o RGPD

O Regulamento Geral Europeu de Proteção de Dados (UE) 2016/679 entrou em vigor em 25 de maio de 2016 e foi considerado válido na União Europeia, após um período transitório de dois anos, desde 25 de maio de 2018. O RGPD estabelece regras sobre a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e protege os direitos e liberdades fundamentais das pessoas singulares, em particular o seu direito à proteção de dados pessoais (UAG, 2020).

Três anos após a sua entrada em vigor, o RGPD ainda apresenta vários desafios. Na medida em que o quadro sancionatório é bastante elevado, sendo que as coimas podem atingir montantes até 4% do volume de negócios ou até vinte milhões de euros (RGPD, 2016), consoante o montante que for mais elevado, de acordo com o artigo 83º do Regulamento, é relevante a criação de mecanismos de conformidade sob pena da atividade económica de uma organização poder ser posta em causa.

Não obstante o RGPD ser de aplicação em toda a União Europeia, querendo-se um nível de proteção equivalente em todos os Estados-Membros, conforme referido no considerando 10 do regulamento, a nível nacional poderá haver disposições concretas para especificar a aplicação das regras do regulamento. Neste caso, em Portugal, acresce a Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento 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, aplicando-se todas as exclusões previstas no artigo 2º do RGPD, sem haver mudanças ao paradigma do regulamento.

De acordo com o comunicado de imprensa da Comissão Europeia sobre a avaliação dos dois anos de aplicação do RGPD (Comissão Europeia, 2020), as empresas, incluindo as PME, agora têm apenas um conjunto de regras para aderir. Ao estabelecer um quadro harmonizado para a proteção de dados pessoais, o RGPD garante que todas as empresas no mercado interno estão sujeitas às mesmas regras e beneficiam das mesmas oportunidades, independentemente de estarem estabelecidas e do local onde o tratamento ocorre.

Uma das principais obrigações de todas as empresas, em todos os Estados-Membros, no RGPD, é a segurança da informação e em particular a segurança dos dados pessoais. De acordo com o RGPD, a segurança dos dados abrange a confidencialidade, integridade e disponibilidade da informação (ENISA, 2017, pág. 6).

Segurança da Informação visa a proteção dos sistemas de informação contra o acesso ou a modificação não autorizados da informação, durante o seu armazenamento, processamento ou transmissão, e contra a negação de serviço a utilizadores autorizados ou o fornecimento de serviço a utilizadores não autorizados, incluindo as medidas necessárias para detetar, documentar e contrariar tais ameaças (CNCS, 2021).

Segundo Laudon e Laudon, Sistema de Informação é definido por componentes interligados que trabalham em conjunto para recolher, processar, armazenar e divulgar informação para apoiar a tomada de decisão, coordenação, controlo, análise e visualização numa organização (Laudon e Laudon, 2018).

De acordo com a Organização Internacional de Normalização (ISO), mais propriamente através da norma ISO 27001:2013, os profissionais de segurança da informação devem proteger os ativos da organização, incluindo a proteção de dados pessoais, e devem garantir o nível de proteção exigido, conforme definido nas leis e regulamentos relevantes (ISO, 2013).

A norma ISO 27001:2013 foi preparada para proporcionar os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão da segurança da informação, preservando a confidencialidade, integridade e disponibilidade da informação através da aplicação de um processo de gestão do risco, dando desta forma, a confiança às partes interessadas de que os riscos associados à segurança da informação são geridos adequadamente (ISO, 2013).

Enquanto extensão à ISO/IEC 27001:2013 para a gestão de privacidade da informação, o Comité Técnico Conjunto ISO/IEC JTC 1, Tecnologia da Informação, Subcomité SC27, Técnicas de Segurança, projetou um conjunto adicional de requisitos específicos do setor, que podem ser implementados em conjunto com os requisitos e controlos da ISO/IEC 27001:2013, de acordo com o documento ISO/IEC 27701:2019 (ISO, 2019). Este documento inclui um mapeamento da sua estrutura de privacidade para outras iniciativas, nomeadamente para o RGPD, visando a definição, implementação e a melhoria contínua de um sistema de gestão de privacidade da informação.

Em suma, embora as grandes empresas tenham a possibilidade de responder e implementar adequadamente estas estruturas, as PME nem sempre têm a experiência e/ou os recursos necessários para o fazer. Na verdade, é em muitos casos difícil para as PME compreender as especificidades dos riscos associados ao tratamento de dados pessoais, bem como avaliar e gerir esses riscos de acordo com um método formal. Isso pode prejudicar os dados pessoais tratados pelas PME, dificultando, ao mesmo tempo, o cumprimento das obrigações legais do GDPR por parte das mesmas (ENISA, 2016, pág. 8).

Com o intuito de apoiar as Pequenas e Médias Empresas (PME), como referido no Capítulo 1 – Introdução, a Agência da União Europeia para a Segurança de Redes e Informações – ENISA, publicou em 2016 (ENISA, 2016), e atualizou em 2017 (ENISA, 2017), um conjunto de orientações para as PME, que visam ajudá-las a avaliar os riscos de segurança e, consequentemente, adotar medidas de segurança para a proteção de dados pessoais, garantindo a conformidade com o RGPD.

Neste contexto, Brodin (2019) apresenta um modelo de referência para a conformidade com o RGPD para Pequenas e Médias Empresas. Brodin (2019) refere que estas organizações não dispõem de recursos ou conhecimentos para gerir este processo sozinhos. Refere também que a solução deve ser abrangente, não consumir muitos recursos e deve funcionar para as empresas desde o primeiro dia.

O modelo de referência de Brodin (2019) consiste numa lista de verificação das medidas que uma organização precisa de executar para estar em conformidade com o RGPD,

designadamente análises que precisam ser feitas, documentos e rotinas que precisam ser criadas ou atualizadas. O modelo está organizado em três grandes componentes (Brodin, 2019):

- Análise, para determinar o estado atual da organização (análise de informações; análise do fluxo de informações; classificação das informações; base legal para o tratamento dos dados pessoais; e segurança e informação das Tecnologias de Informação);

- Desenho, em termos de rotinas, políticas e modelos. Rotinas em termos dos direitos do titular dos dados ou responsabilidades dos responsáveis pelo tratamento; Políticas em termos de referência principal dentro da organização; Modelos relacionais entre as políticas e as rotinas para garantir coesão dentro da estrutura e evitar soluções individuais;

- Implementação, onde o foco está na criação de condições de compatibilidade contínua com o RGPD, introduzindo novas rotinas e criação de um sistema de relatórios para incidentes; Designação de pessoas para os novos papéis e condições para a execução das novas tarefas; e revisão regular da organização com vista à atualização dos seus processos, como a eliminação de dados pessoais desnecessários ou a remoção das várias atividades de tratamento de dados pessoais que não sejam compatíveis com o RGPD.

Se o modelo de Brodin (2019) apresenta como foco principal a análise e o design, deixando a parte da implementação para projetos futuros, onde necessita de ser examinada com maior detalhe, em termos conceptuais refere que um aspeto importante da demonstração da conformidade com os requisitos do RGPD é garantir a segurança por medidas técnicas e organizativas. Para tal, inclui os standards ISO/IEC 27000 na sua fundamentação teórica para uma gestão estratégica.

Efetivamente, quando a Segurança da Informação é referida, para além da ISO 27001:2013, é pertinente considerar toda a família ISO/IEC 27000. Destaca-se, por exemplo, a publicação realizada em agosto de 2019 da ISO/IEC 27701:2019, documento que especifica os requisitos e fornece orientações para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Privacidade da Informação (SGPI), na forma de uma extensão à ISO/IEC 27001:2013 e ISO/IEC 27002:2013 (ISO, 2019).

Chatzipoulidis et al (2019) também apresentam uma ferramenta de avaliação de conformidade com o RGPD, mantendo o enfoque nas Pequenas e Médias Empresas que ambicionam estar em conformidade, como meio auxiliar dos mecanismos de auditoria, interna e externa, e como instrumento de avaliação do estado atual da proteção de dados num ambiente empresarial e num contexto de sistemas de informação, através de quatro fatores:

- Contexto de negócio, que inclui uma lista de regulamentos e requisitos de gestão que devem corresponder aos padrões de cada setor;

- Suporte às autoridades, aos encarregados de proteção de dados, quando aplicável, ou, na sua ausência, ao representante da empresa para as questões de privacidade;

- Controlo de processos, ao nível da avaliação de impacto sobre a proteção de dados como meio de gestão de riscos à privacidade, e ao nível da segurança da informação, incluindo a seleção e aplicação de controlos;

- Melhoria de processos, através de processos de certificações como a gestão da qualidade (ISO 9001:2015), a gestão de segurança da informação (ISO 27001:2013) e a gestão da continuidade

de negócio (ISO 22301:2012), e através de processos de consciencialização e formação à medida.

Ao contrário de Brodin (2019), Chatzipoulidis et al (2019) apresentam no seu modelo uma escala de pontuação onde, para cada item de evidência listada, é avaliado o nível de conformidade e são atribuídas classificações. Esta ferramenta de avaliação permite destacar as áreas de melhoria e, ao mesmo tempo, avaliar, em tempo real, o nível de conformidade da organização com o RGPD, bem como os respetivos processos dos sistemas de informação.

Chatzipoulidis et al (2019) referem que o tratamento de dados está constantemente ameaçado devido a vários desafios, como a mudança acelerada de tecnologia, redes abertas, dependências de terceiros, envolvimento das partes interessadas e requisitos governamentais para regulamentação mais rigorosa através de conformidade e políticas.

Neste ponto de vista, os modelos de referência também poderiam considerar as tendências das autoridades como critério de tomada de decisão e de priorização, nomeadamente ao nível das Pequenas e Médias Empresas, estruturas que, citando Brodin (2019), não dispõem de recursos ou conhecimentos para gerir este processo sozinhas. Poderiam, portanto, ser aconselhadas a priorizar determinados requisitos em detrimento de outros, numa lógica de suporte à tomada de decisão.

Teixeira et al (2019), no seu trabalho de revisão sistemática da literatura, identificaram oito fatores críticos de sucesso para a implementação do RGPD, a saber: extensão do Regulamento, complexidade, subjetividade, falta de conhecimento e experiência em privacidade, falta de orçamento, falta de recursos humanos, falta de tecnologia necessária e falta de orientações práticas ou de normas / standards de aplicação.

Costa et al (2018) propõem um modelo conceptual inovador para fornecer a mudança necessária que atenda às preocupações do RGPD, com base no conceito de facilitadores, incluindo a perceção das partes interessadas, para além da eficácia organizacional, que é definida pela aplicação dos requisitos legais e pela demonstração da conformidade do Regulamento.

Em suma, a perceção do que constitui o sucesso de um projeto não pode ser avaliado apenas pela restrição convencional de tempo, orçamento e âmbito, mas também pela concretização dos objetivos e dos benefícios organizacionais que todo o projeto de implementação do RGPD traz a todas as partes interessadas, em diferentes escalas do tempo (Costa et al, 2018).

Também de modo inovador, com o objetivo de apoiar as organizações ao entendimento do RGPD e dos seus requisitos, Geko e Tjoa (2018) apresentam a interdependência entre o RGPD e a Segurança da Informação através da criação de uma ontologia, pretendendo ajudar as organizações a entender os requisitos do texto jurídico em relação às principais exigências relevantes para a segurança da informação.

As ontologias são projetadas para expressar conceitos relacionados entre domínios, e fornecem uma solução bem estabelecida para gestão de informação e partilha de conhecimento (Slimani, 2014). A ontologia proposta por Geko e Tjoa (2018) consiste em cinco áreas: Dados; Organização; Princípios de proteção de dados; Direitos dos titulares dos dados; e Obrigações. Cada área identifica uma pessoa que é responsável pela mesma (Titular dos dados, Responsável pelo Tratamento, Subcontratante), bem como as relações entre os objetos na ontologia.

Geko e Tjoa (2018) referiram também que a sua ontologia não considerava as especificidades de proteção de dados em cada Estado-Membro, concentrando-se apenas nos aspetos relevantes, deixando de fora muitos aspetos legais do regulamento e dos requisitos de segurança da informação, não obstante os autores referirem que o desenvolvimento de ontologias pode ser visto como um processo iterativo e que novos desenvolvimentos podem ser considerados.

Palmirani et al (2018) também apresentam uma ontologia para modelar conceitos e normas do RGPD. Contudo, com critérios ligeiramente diferentes dos apresentados por Geko e Tjoa (2018). Palmirani et al (2018) apresentam o PrOnto (*Privacy Ontology for Legal Reasoning*), a ontologia que tem como objetivo fornecer uma modelação de conhecimento jurídico dos agentes de privacidade, tipos de dados, tipos de operações de tratamento, direitos e obrigações. A metodologia usada aqui é baseada na análise da teoria jurídica, associada a padrões ontológicos.

O modelo PrOnto ainda se encontra em fase de testes, em contexto escolar, e carece de integração dos três níveis de representação semântica: 1) modelação de dados; 2) modelação de fluxo de tratamentos de dados; e 3) abordagens centradas no ser humano, em diferentes contextos. Para além disso, Palmirani et al (2018) reconhecem a importância de uma discussão alargada com vista ao consenso, sem esquecer, no entanto, as necessárias adaptações às leis nacionais.

Ambos os projetos ainda carecem de aceitação alargada. Se a ontologia PrOnto ainda está em fase de testes, a ontologia proposta por Geko e Tjoa (2018) ainda não foi avaliada. Contudo, como referido, é possível realizar algumas consultas básicas no software Protege que ajudam a responder a questões relativas a princípios de tratamento, direitos do titular dos dados, as principais obrigações de um responsável pelo tratamento e as funções de um dado subcontratante.

Em suma, é neste contexto que o trabalho realizado tem como suporte a utilização das orientações da ENISA para as PME, estando alinhado, por exemplo, ao modelo de Brodin (2019) que, em termos concetuais, utiliza a família ISO/IEC 27000 na sua fundamentação teórica para a gestão estratégica enquanto fator de demonstração da conformidade com os requisitos do RGPD.

As orientações da ENISA estão, noutro ponto de vista, alinhados ao modelo de Chatzipoulidis et al (2019) pela utilização de uma escala de pontuação onde, para cada item de evidência listada, é avaliado o nível de conformidade e são atribuídas classificações.

Como referido acima, Chatzipoulidis et al (2019) afirmam que o tratamento de dados está constantemente ameaçado devido a vários desafios, como a mudança acelerada de tecnologia, redes abertas, dependências de terceiros, envolvimento das partes interessadas e requisitos governamentais para regulamentação mais rigorosa por meio de conformidade e políticas.

Acrescenta-se a esta afirmação que os entendimentos das sanções jurídicas das autoridades de controlo e dos tribunais também podem variar ao longo do tempo, podendo apresentar tendências ao nível do âmbito de aplicação do RGPD.

É nesta perspetiva que o modelo preconizado neste trabalho incorpora as sanções jurídicas do RGPD.

2.2.As PME no contexto nacional

Pequenas e Médias Empresas, de acordo com a recomendação da União Europeia 2003/361, de 6 de maio, podem ser definidas como empresas que têm menos de 250 assalariados e um volume de negócios anual inferior a 50 milhões de euros ou balanço inferior a 43 milhões de euros, no caso de média empresa; menos de 50 assalariados e um volume de negócios anual ou balanço inferior a 10 milhões de euros, no caso de pequena empresa; e menos de 10 assalariados e um volume de negócios anual ou balanço inferior a 2 milhões de euros, no caso de microempresa. As pequenas e médias empresas (PME) representam 99% de todas as empresas na UE (Comissão Europeia, 2003).

Em Portugal, os dados mais recentes encontrados no portal da Pordata, referentes a 2018, indicam que existem 1.294.037 empresas consideradas como PME num total de 1.295.299 empresas. Ou seja, as PME correspondem a 99,9% do total das empresas nacionais, contrapondo com as 1.262 empresas classificadas na dimensão "Grandes" (Pordata, 2021).

No universo das PME, 1.244.495 são microempresas (96,2%), 42.581 são pequenas empresas (3,3%) e apenas 6.961 são consideradas médias empresas (0,5%) (Pordata, 2021).

As PME nacionais refletem 78,5% de toda a capacidade empregadora nacional, representando, nominalmente, 3.230.077 trabalhadores (Pordata, 2020).

Em termos de distribuição geográfica, dados de 2019, 32,9% do total de empresas localizam-se na Área Metropolitana de Lisboa, seguindo-se a Área Metropolitana do Porto com um total de 17,6% de empresas (Banco de Portugal, 2020).

Dentro das PME, os três setores de atividade económica mais relevantes são o Comércio por grosso e a retalho (16,82%), Agricultura, produção animal, caça, silvicultura e pesca (10,27%) e Alojamento, restauração e similares (8,74%) (Pordata, 2020).

Relativamente à sociedade da informação e do conhecimento, o Instituto Nacional de Estatística (INE), procedeu a um inquérito relativo à utilização de tecnologias da informação e da comunicação nas empresas, tendo chegado a várias conclusões, destacando-se as seguintes (INE, 2020):

- Cerca de 97% das empresas com 10 ou mais pessoas ao serviço e 42,8% das pessoas ao serviço utilizam computador com ligação à internet para fins profissionais;

- Cerca de dois terços das empresas referem ter website próprio ou do grupo económico a que pertencem;

- As vendas de bens e serviços realizadas através do comércio eletrónico, pelas empresas com 10 ou mais pessoas ao serviço, representam cerca de 20% do total do volume de negócios em 2019;

- Em 2020, 29% das empresas compram serviços de computação em nuvem na internet, com destaque para a compra do serviço de correio eletrónico e armazenamento de ficheiros;

- Em 2019, mais de metade das empresas não analisaram *big data*[1] por insuficiência de recursos humanos, conhecimentos ou competências nestas áreas. Ainda assim, 10,2% das empresas com 10 ou mais pessoas ao serviço analisaram *big data*, com destaque para o método de análise *machine learning*[2] (33,7% destas empresas);

- Em 2020, 22,9% das empresas têm pessoal ao serviço especialista em Tecnologias da Informação e Comunicação (TIC). Em 2019, 6,5% das empresas com 10 ou mais pessoas ao serviço recrutaram ou tentaram recrutar especialistas em TIC, sendo que destas 44,5% tiveram dificuldade no preenchimento destes postos de trabalho;

- Em 2020, 13% das empresas com 10 ou mais pessoas ao serviço utilizam dispositivos ou sistemas interconectados que podem ser monitorizados ou controlados remotamente através da Internet (IoT) e 9,1% utilizam robôs industriais e/ou de serviço.

2.3.As PME portuguesas e o RGPD

Uma das principais obrigações de todas as empresas no Regulamento Geral sobre a Proteção de Dados (RGPD), incluindo as PME, é a segurança dos dados pessoais (ENISA, 2017, pág. 6).

De acordo com um inquérito endereçado às PME portuguesas (Carvalho Silva, 2019), com o objetivo de avaliar como é que as empresas portuguesas lidam com os dados pessoais, que conhecimento têm do RGPD, e como se adaptaram à novas regras, obtiveram-se os seguintes resultados e análises:

- A maioria das PME portuguesas (96,3%) têm conhecimento do que é o RGPD. Sendo que 52,7% só tiveram conhecimento em 2018, ano da entrada em vigor do regulamento;

- As microempresas foram as empresas que tiveram o conhecimento mais tardio sobre o RGPD;

- Mais de metade dos inquiridos consideram ter um bom ou muito bom nível de conhecimento sobre o regulamento;

- Das 762 PME que participaram no inquérito, 47% identificam apenas uma categoria de dados pessoais como alvo de tratamento, sendo a categoria de "identificação" a principal, o que poderá sugerir que estão apenas a considerar os dados de clientes, ignorando dados pessoais de colaboradores e fornecedores, por exemplo;

- Apenas uma minoria das PME (25,85%) realizou uma auditoria aos dados que detém: a análise destes dados sugere que poderá existir uma dificuldade das empresas em identificar o que são dados pessoais;

- Quando questionadas quais as principais dificuldades que tiveram na implementação do RGPD nas empresas, 46,06% indicaram a falta de conhecimento sobre o RGPD, 23,23% a falta

[1] *Big Data* é o conjunto das tecnologias, ferramentas, dados e análises utilizadas no tratamento de grande quantidade de dados (ENISA, 2015).
[2] *Machine Learning* é o estudo de como os programas computacionais podem melhorar o seu desempenho sem haver uma programação explícita, utilizando, por exemplo, o reconhecimento de padrões, experiência ou conhecimentos passados (Laudon e Laudon, 2018).

de Recursos Humanos e 22,31% a incapacidade em identificar se os dados são alvo de um tratamento lícito. 29,53% não identificaram nenhuma dificuldade.

Noutro estudo realizado no contexto português, Freitas e Mira da Silva (2018) reforçam a necessidade de definir uma metodologia para poder cumprir as obrigações do RGPD, considerando a análise realizada a dez PME nos distritos de Lisboa, Aveiro e Leiria, onde se identificou a falta de conhecimento dessas empresas sobre as suas obrigações e deveres em relação à proteção de dados pessoais. Destacam-se as seguintes conclusões:

- A maioria dos entrevistados não tinha conhecimento relativo ao novo regulamento nem das suas obrigações enquanto empresa em termos de consentimento, princípios de tratamento e registo das atividades de tratamento;

- Todas as empresas responderam que desconheciam os direitos dos titulares dos dados, razão pela qual não implementaram procedimentos para garantir esses mesmos direitos;

- Todas as empresas que contratam prestadores de serviços desconheciam a necessidade de ter esses contratos em conformidade com o RGPD, caso os mesmos prestadores necessitem de armazenar, aceder ou tratar dados pessoais no âmbito do contrato;

- Nenhuma empresa transfere dados para países fora da União Europeia / Espaço Económico Europeu;

- Todas as empresas responderam que os funcionários com acesso a dados pessoais não são informados dos seus deveres e obrigações, e dos deveres e obrigações da empresa; apenas uma empresa mencionou ter um plano de formação sobre este assunto;

- Todas as empresas desconhecem a responsabilidade do responsável pelo tratamento. Nenhuma das empresas regularmente, ou de tempos em tempos, avalia a conformidade com os regulamentos e leis sobre proteção de dados pessoais;

- Todas as empresas responderam que desconheciam a obrigação de notificação de uma violação de dados pessoais à Autoridade de Controlo.

Adicionalmente, num estudo desenvolvido pela IDC para a Microsoft Portugal, que se dispôs a fazer um raio-X às organizações portuguesas e às perspetivas de evolução em relação ao Regulamento Geral de Proteção de Dados (RGPD), em geral, PME e não PME, onde a maioria das respostas obtidas foram de empresas com mais de 250 colaboradores, apenas 2,5% dos decisores considera que a sua organização está preparada (Microsoft, 2018). Destacam-se também os seguintes pontos deste estudo:

- Os principais desafios apontados pelas organizações em relação à conformidade com o RGPD são a "definição dos processos" (320 empresas), "a identificação, classificação e gestão dos dados" (319), a "formação dos colaboradores" (253), o "estabelecimento de medidas de segurança" (219) e "lidar com a gestão do consentimento" (183);

- Já sobre os principais benefícios do RGPD para a sua organização 350 das empresas inquiridas reconhece que será a "melhoria da segurança e privacidade da informação", 278 a "melhoria da gestão da informação", 219 "garantir a confiança dos clientes", 199 "redução de risco sancionatório", e 150 "melhorar a imagem pública e reputação da organização".

Para reforçar a importância deste trabalho junto das PME, verifica-se, portanto, ser pertinente atualizar os estudos do impacto do RGPD nas organizações, realizados pelos autores supramencionados.

2.4.A evolução da aplicação do RGPD na União Europeia

O RGPD, aplicável desde 25 de maio de 2018, está no cerne do quadro da União Europeia que garante o direito fundamental à proteção de dados, tal como consagrado na Carta dos Direitos Fundamentais da União Europeia (artigo 8º) e nos Tratados (artigo 1º do Tratado sobre o Funcionamento da União Europeia, «TFUE») (Comissão Europeia, 2020).

De acordo com a mesma fonte de informação - Comunicação da Comissão ao Parlamento Europeu e ao Conselho relativa aos dois anos de aplicação do Regulamento Geral sobre a Proteção de Dados – relatório "A proteção de dados enquanto pilar da capacitação dos cidadãos e a abordagem da UE para a transição digital" (Comissão Europeia, 2020), a opinião geral é que, dois anos após a sua entrada em vigor, o RGPD cumpriu os seus objetivos de reforçar a proteção do direito dos cidadãos em matéria de proteção de dados pessoais e de garantir a livre circulação de dados pessoais na União Europeia. No entanto, foram também identificados alguns domínios que carecem de melhorias no futuro. Apresentam-se as principais conclusões:

- O desenvolvimento de uma verdadeira cultura europeia comum em matéria de proteção de dados entre as autoridades responsáveis pela sua proteção continua a ser um processo ainda não concluído;

- De um modo geral, as partes interessadas congratulam-se com as orientações e diretrizes do Comité e solicitam outras sobre conceitos-chave do RGPD, mas apontam também para algumas incoerências entre as orientações nacionais e as orientações do Comité;

- Sublinham a necessidade de um aconselhamento mais prático, nomeadamente de exemplos mais concretos, e a necessidade de as autoridades de proteção de dados serem dotadas dos recursos humanos, técnicos e financeiros necessários para desempenhar eficazmente as suas funções;

- De acordo com um inquérito sobre os direitos fundamentais, 69% da população da UE com mais de 16 anos ouviu falar do RGPD e 71 % das pessoas na UE sabem da existência da sua autoridade nacional responsável pela proteção dos dados;

- A Comissão observa que as autoridades recorreram a coimas administrativas oscilando entre alguns milhares de euros e vários milhões, em função da gravidade das infrações. Outras sanções, como a proibição de tratamento de dados, podem ter também um efeito dissuasor igual, se não superior, ao das coimas.

A Comissão Europeia refere em comunicado de imprensa, no entanto, que o sucesso do RGPD não deve ser medido pelo número de multas aplicadas, uma vez que o regulamento prevê um leque mais amplo de poderes corretivos concedido às autoridades de controlo nacionais de proteção de dados que não se esgotam nas multas administrativas, tais como advertências e repreensões, ou ordens para cumprir os pedidos do titular dos dados, como por exemplo, para retificar, apagar ou restringir o tratamento (Comissão Europeia, 2020).

Relativamente a multas administrativas, entre 25 de maio de 2018 e 30 de novembro de 2019, 22 autoridades de proteção de dados da União Europeia / Espaço Económico Europeu emitiram aproximadamente 785 multas. Apenas algumas autoridades ainda não impuseram multas administrativas, embora processos em andamento possam levar a essas multas. A maior parte das multas refere-se a infrações contra: o princípio da legalidade; consentimento válido; proteção de dados sensíveis; a obrigação de transparência, os direitos dos titulares dos dados; e violações de dados (Comissão Europeia, 2020).

Como referido acima, Chatzipoulidis et al (2019) afirmam que o tratamento de dados está constantemente ameaçado devido a vários desafios, como requisitos governamentais para regulamentação mais rigorosa por meio de conformidade e políticas.

Acrescenta-se, assim, a esta afirmação que os entendimentos das sanções jurídicas das autoridades de controlo e dos tribunais também podem variar ao longo do tempo, podendo apresentar tendências ao nível do âmbito de aplicação do RGPD.

É nesta perspetiva que o modelo preconizado neste trabalho incorpora as sanções jurídicas do RGPD, porque a aplicação de multas e coimas pode condicionar a continuidade do negócio das PME.

Por isto tudo, apresenta-se neste trabalho de investigação uma solução para conformidade, proteção e privacidade dos dados pessoais, utilizando as orientações da ENISA para as PME, alinhada às ISO/IEC 27001:2013 e 27701:2019, que permita que as Pequenas e Médias Empresas se preparem para o cumprimento das regras relativas às obrigações legais do RGPD, incluindo critérios de apoio à decisão, tendo em conta as sanções jurídicas existentes no contexto europeu.

2.5.Segurança e Gestão dos Riscos na área dos dados pessoais

De acordo com o documento "Guidelines for SMEs on the security of personal data processing", publicado pela ENISA, a avaliação dos riscos é o primeiro passo para a adoção de medidas de segurança adequadas para a proteção de dados pessoais (ENISA, 2016, pág. 17).

Segurança da informação engloba medidas tomadas para defender as informações tratadas num sistema, por exemplo eletrónico ou físico, de acesso não autorizado, uso, divulgação, perturbação, modificação, leitura, inspeção, registo ou destruição (ENISA, 2016, pág. 10).

Como também já referido, pela definição do Centro Nacional de Cibersegurança (CNCS, 2021), Segurança da Informação também pode ser entendida como a proteção dos sistemas de informação contra o acesso ou a modificação não autorizados da informação, durante o seu armazenamento, processamento ou transmissão, e contra a negação de serviço a utilizadores autorizados ou o fornecimento de serviço a utilizadores não autorizados, incluindo as medidas necessárias para detetar, documentar e contrariar tais ameaças.

O modelo mais utilizado para orientar o desenvolvimento e implementação de uma estrutura para gerir a segurança da informação dentro de uma organização é representado pela chamada

tríade CIA, do inglês, *confidentiality, integrity and availability* – confidencialidade, integridade e disponibilidade da informação (ENISA, 2016, pág. 10).

De acordo com o Quadro Nacional de Referência para a Cibersegurança, do Centro Nacional de Cibersegurança (CNCS, 2019, pág.17), tendo como referência a ISO/IEC 27000, Confidencialidade é definida como "A propriedade de a informação não ser divulgada a pessoas ou entidades não autorizadas, ou segundo processos não autorizados"; Integridade como "A propriedade de salvaguardar o caráter exato e completo da informação e dos ativos"; e Disponibilidade como "Propriedade de estar acessível e de poder ser utilizada a pedido de uma entidade autorizada".

Ao incorporar medidas de segurança num sistema de tratamento de informação, onde os dados pessoais se incluem, é crucial garantir que a tríade CIA é aplicada conforme as condições acordadas entre as partes interessadas. Embora todos os três elementos sejam importantes, diferentes aspetos da tríade poderão ter prioridades distintas, dependendo do setor e da organização (ENISA, 2016, pág. 11). É reforçada, nesta perspetiva, a necessidade de haver um processo de gestão do risco de segurança dos dados.

A gestão dos riscos de segurança da informação é, de acordo com a ENISA (2016, pág. 11), portanto, o processo de identificação, quantificação e gestão dos riscos de segurança da informação que uma organização enfrenta; um processo que visa a obtenção de um equilíbrio eficiente entre perceber oportunidades de ganhos e minimizar vulnerabilidades e perdas.

De acordo com a ENISA, um processo de gestão do risco compreende quatro fases principais (Figura 1):

- **Avaliação do risco.** Pode ser entendido como a criação de um retrato de um momento atual do risco. Um risco é frequentemente definido como uma função de probabilidade de ocorrência de um evento adverso (ameaça), multiplicado pela magnitude do mesmo evento, caso ele venha efetivamente a ocorrer (impacto). A avaliação do risco começa com a identificação de ameaças, seguida da determinação da probabilidade e do impacto de cada risco. Para avaliar adequadamente o risco, deve-se igualmente ter em consideração a probabilidade e o impacto (ENISA, 2016, pág. 11). A análise quantitativa do risco poderá ficar facilitada com o conhecimento do valor das multas aplicadas.

- **Tratamento do risco**. Com base nos resultados da avaliação do risco, a organização seleciona e implementa medidas de segurança para tratar os riscos. As medidas podem ter efeitos diferentes, como: mitigação, transferência, prevenção ou retenção dos riscos (ENISA, 2016, pág. 11).

- **Aceitação do risco**. Mesmo quando os riscos são tratados, podem persistir outros riscos: os mesmos com magnitude inferior, ou seja, riscos residuais; ou outros riscos, ou seja, riscos secundários. Neste sentido, deverá haver um processo de aceitação do risco que permita a gestão e a tomada de decisão quanto à permanência dos riscos após a fase de tratamento. Este processo de gestão de aceitação deve ocorrer num momento de tomada de decisão (ENISA, 2016, pág. 11).

- **Comunicação do risco**. Todas as partes interessadas devem ser informadas sobre as decisões tomadas; e que controlos foram adotados e que riscos foram aceites (ENISA, 2016, pág. 11).

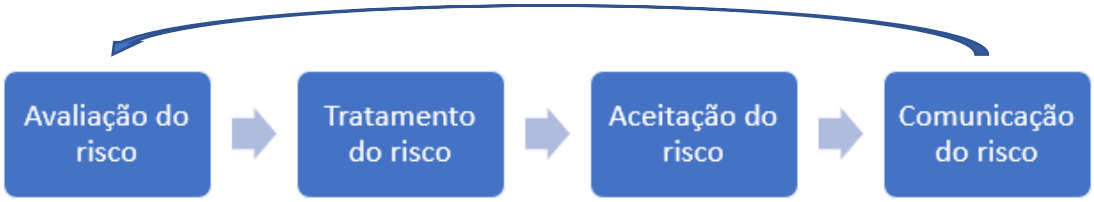


Figura 1 - As quatro fases principais de um processo de gestão do risco. Adaptado de ENISA, 2016.

Importa enfatizar que a segurança do tratamento de dados pessoais não é uma obrigação isolada no RGPD, pelo contrário, deve ser considerada dentro da estrutura geral de responsabilidade da organização no que à implementação do RGPD diz respeito, numa lógica cíclica de gestão do risco (ENISA, 2016, pág. 13).

Na gestão dos riscos de segurança de dados pessoais, é antes de tudo importante definir o contexto do tratamento (por exemplo, tipos de dados pessoais tratados, finalidades do tratamento, quais os destinatários, prazos de conservação, etc.), que então apoiará a definição de possíveis ameaças e riscos com base no impacto para os indivíduos / titular dos dados. As medidas técnicas e organizativas apropriadas serão finalmente adotadas para gerir os riscos, levando em consideração as especificidades do tratamento de dados pessoais (ENISA, 2016, pág. 15). Outras abordagens mais detalhadas podem ser encontradas na ISO/IEC 27005 e ISO 31000.

Capítulo 3 – Metodologia de Investigação

Neste trabalho de investigação é aplicada a metodologia *Design Science Research* (DSR) para sistemas de informação, apresentada por Henver et al (2004), onde este trabalho de investigação se enquadra – sistema de gestão de informação – categoria específica dos SI que fornecem relatórios sobre o desempenho organizacional para ajudar a gestão a monitorizar e controlar os seus negócios (Laudon e Laudon, 2018).

Os SI são implementados dentro de uma organização com o objetivo de melhorar a eficácia e eficiência dessa mesma organização, sendo que a concretização deste objetivo está dependente das capacidades do próprio SI e das características da organização (Hevner et al, 2004). Ou seja, deverá haver uma construção que tenha em consideração, por um lado, as organizações e pessoas e, por outro lado, a tecnologia. Dito por outras palavras, a implementação de um SI deverá incluir, em complemento, as chamadas ciências do *design* e ciências *comportamentais* (Hevner et al, 2004):

O design science tem como foco a criação de artefactos de Tecnologias de Informação (TI) que impactam pessoas e organizações, ao nível da criação, implantação, avaliação e seu aprimoramento. Estes artefactos são, essencialmente, um paradigma de resolução de problemas definidos genericamente como construções, designadamente vocabulários e símbolos; modelos, tais como abstrações e representações; métodos, como algoritmos; e instanciações, como são os sistemas implementados ou os protótipos.

A ciência *comportamental*, passiva quanto à tecnologia, tem como principal objetivo descrever as implicações da tecnologia – a intenção do uso, isto é, o seu impacto sobre indivíduos, grupos e organizações. Inclui regularmente estudos que examinam como as pessoas empregam uma tecnologia, relatam os benefícios e as dificuldades encontradas quando uma tecnologia é implementada dentro de uma organização.

A criação do processo tecnológico deverá, portanto, ser combinada com as teorias comportamentais e organizacionais para desenvolver uma compreensão dos problemas de negócios, sua contextualização, soluções e abordagens adequadas (Hevner et al, 2004).

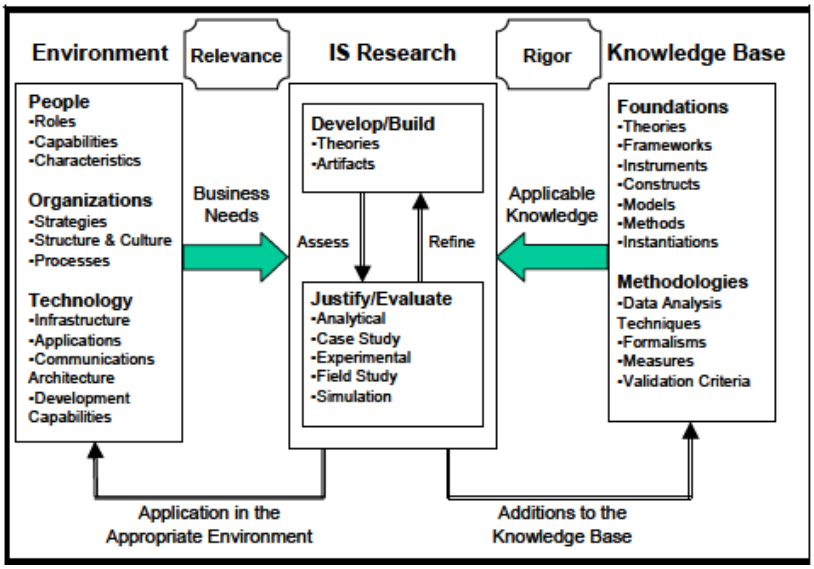


Figura 2 - Estrutura de pesquisa para Sistemas de Informação

A Figura 2 (Hevner et al, 2004), apresenta uma estrutura concetual para entender, executar e avaliar a pesquisa em SI, combinando o design science e a ciência *comportamental*.

Henver et al (2004), neste contexto, define que a metodologia DSR é um processo de resolução de problemas, que pode ser desenvolvido em sete passos sequenciais. A Tabela 1 apresenta as atividades desenvolvidas neste trabalho, alinhadas com os passos sequenciais da metodologia DSR propostos por Henver et al (2004).

Passos sequenciais da metodologia DSR (Hevner et al, 2004, pág. 89)	Descrição da metodologia DSR (Hevner et al, 2004, pág. 89)	Desenvolvimento do trabalho proposto
1 – *Design* como um artefacto	A pesquisa do design science deve produzir um artefacto viável na forma de um constructo, um modelo, um método ou uma instanciação.	O trabalho de investigação apresenta no seu ponto 4.2 a solução para a proteção da privacidade e dos dados pessoais baseada em sanções jurídicas do RGPD.
2 – Relevância do problema	O objetivo da pesquisa do design science é desenvolver soluções baseadas em tecnologia para problemas importantes e relevantes do negócio.	A motivação e os objetivos do trabalho estão apresentados no ponto 1.1 do Capítulo 1 – Introdução, onde se verifica a pertinência deste trabalho de investigação.
3 – Avaliação do *Design*	A utilidade, qualidade e eficácia de um artefacto de *design* devem ser rigorosamente demonstradas por meio de métodos de avaliação bem executados.	O ponto 4.2.3 do Capítulo 4 apresenta o mecanismo de avaliação do artefacto junto das PME sob a forma de Prova de Conceito, concretizado no 5.2 do Capítulo 5.
4 – Contribuições da pesquisa	A pesquisa eficaz do design science deve fornecer contribuições claras e verificáveis nas áreas do *design* do artefacto, fundamentos de *design* e / ou metodologias de *design*.	De acordo com a revisão da literatura – Capítulo 2 – verificou-se que os atuais modelos de referência para a conformidade com o RGPD para Pequenas e Médias Empresas não consideram as sanções jurídicas do RGPD enquanto critérios de apoio à decisão, tema de estudo e contribuição deste trabalho de investigação – Capítulos 5 e 6.
5 – Rigor da Pesquisa	A pesquisa do design science baseia-se na aplicação de métodos rigorosos tanto na construção quanto na avaliação do artefacto de *design*.	A construção do modelo assenta em propostas desenvolvidas por entidades oficiais como a ENISA - Agência da União Europeia para a Segurança de Redes e Informações, a ISO - Organização Internacional de Normalização, ou a Autoridade de Controlo nacional, CNPD - Comissão Nacional de Proteção de Dados, através de metodologias apropriadas. A

		avaliação do trabalho resulta, nomeadamente, no preconizado nos pontos 4.1 e 4.2.3 do Capítulo 4.
6 – *Design* como um processo de pesquisa	A busca por um artefacto eficaz requer a utilização dos meios disponíveis para alcançar os fins desejados e, ao mesmo tempo, satisfazer as necessidades do seu contexto.	O trabalho desenvolvido tem em consideração as necessidades do seu contexto através da construção do modelo, sua aplicação, avaliação e decisão da versão final ajustada à realidade das PME, pela aplicação da Prova de Conceito, nomeadamente através do ponto 4.2 do Capítulo 4 e 5.2 do Capítulo 5.
7 – Comunicação da pesquisa	A pesquisa do design science deve ser apresentada tanto numa orientação tecnológica como numa orientação para a gestão, que permita a sua utilização dentro de uma organização.	O modelo proposto apresenta no processo de gestão do risco o ponto 4.2.1.4 – Comunicação do risco, a todas as partes interessadas. O desenvolvimento da Prova de Conceito ocorre com os intervenientes chave das organizações, conforme o ponto 4.2.2 do Capítulo 4, sendo-lhes também comunicado os resultados obtidos. O desenvolvimento do trabalho de investigação é, por si só, uma forma de comunicação da pesquisa – Capítulos 6 e 7.

Tabela 1 - Aplicação da metodologia DSR no âmbito do trabalho proposto

Em síntese, apresenta-se na Figura 3 a relação entre as orientações do modelo DSR e as atividades deste trabalho.

Relativamente à revisão sistemática da Literatura (SLR, do inglês *systematic literature review*), tem como critério de pesquisa os estudos realizados nos últimos 5 anos que relacionassem o Regulamento Geral sobre a Proteção de Dados e as Pequenas e Médias Empresas, e seus modelos de referência para a conformidade com o regulamento. As fontes de pesquisa utilizadas (Datasets) são Google Académico e a EBSCO da Atlântica – Instituto Universitário e entidades oficiais como a ENISA - Agência da União Europeia para a Segurança de Redes e Informações, a ISO - Organização Internacional de Normalização, e a Autoridade de Controlo nacional, CNPD - Comissão Nacional de Proteção de Dados.

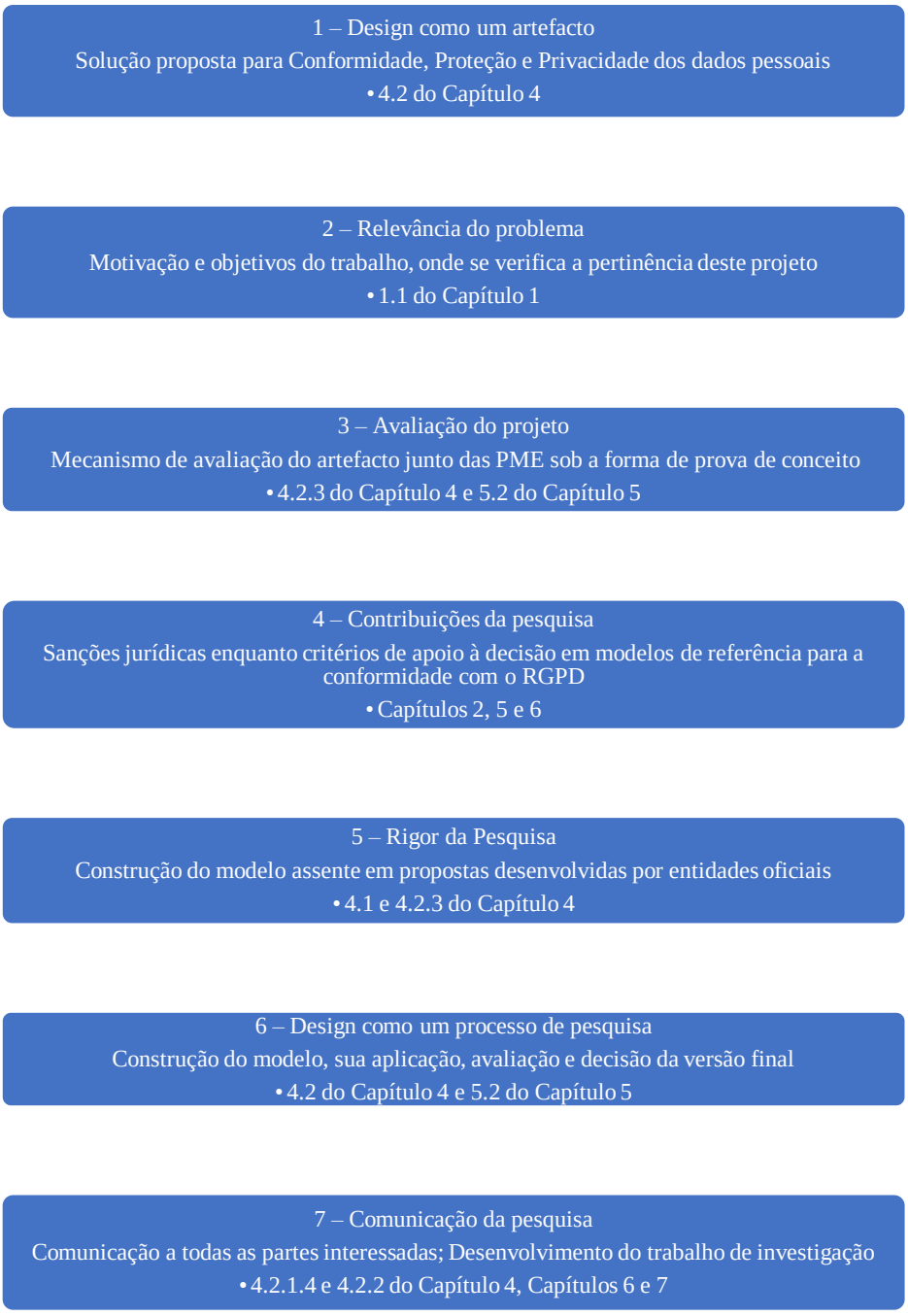


Figura 3 - Síntese da relação entre as orientações do modelo DSR e as atividades deste trabalho de investigação

A metodologia aplicada neste trabalho de investigação está adequada ao objeto de estudo, orientando a identificação, avaliação e interpretação de todas as pesquisas disponíveis e relevantes para a concretização deste trabalho.

Para a realização de revisão sistemática da literatura, o método utilizado baseia-se no documento "Procedures for Performing Systematic Reviews" (Kitchenham, 2004), através da concretização das seguintes etapas:

- Planeamento, onde se identificam as necessidades da revisão e o desenvolvimento de um protocolo de revisão (Kitchenham, 2004, pág.3);

- Realização, onde se identifica a pesquisa, selecionam-se os estudos, avalia-se a qualidade dos estudos, recolhem-se as informações e realizam-se as respetivas sínteses (Kitchenham, 2004, pág.7);

- Relato, onde se resume e sintetizam as ideias e dados extraídos dos estudos selecionados, incorporando-os no próprio trabalho de investigação (Kitchenham, 2004, pág.22), neste caso, no Capítulo 2.

Sobre os questionários realizados, estes foram elaborados tendo como referência o livro "Research Methods for Business Students", de Saunders et al (2009), enquanto método de recolha de informação às PME durante a Fase I, e de avaliação da Prova de Conceito, de acordo com o ponto 4.2.3 da Fase II, através da utilização de formulários online (Saunders et al, 2009, pág. 440).

Em termos de atividades, o trabalho assenta em duas fases distintas, como referido no ponto 1.2 Objetivos de Investigação.

Para reforçar a pertinência do objetivo principal, pretende-se, em primeiro lugar, analisar o impacto do RGPD nas pequenas e médias empresas, em Portugal – Fase I.

Posteriormente – Fase II, pretende-se construir uma solução para conformidade, proteção e privacidade dos dados pessoais, que permita garantir a conformidade legal das PME com o RGPD.

Capítulo 4 – Desenho e Desenvolvimento

Descrevem-se a seguir as fases identificadas como necessárias para conceber o artefacto resultante deste trabalho.

4.1 Fase I – Impacto do RGPD nas Organizações – PME

O trabalho de investigação sobre o impacto do RGPD nas PME nacionais tem como ponto de partida a revisão de literatura efetuada, e em particular os estudos de Freitas e Mira da Silva (2018), de Teixeira et al (2019), de Carvalho Silva (2019), o estudo desenvolvido pela IDC para a Microsoft Portugal (2018) e o Inquérito que o INE realizou relativo à utilização de tecnologias da informação e da comunicação nas empresas (INE, 2020). A ideia é de reciclar algumas questões e conclusões obtidas à data, capitalizando-as para este trabalho, quase três anos depois da entrada em vigor do RGPD. É este o contexto de construção do inquérito "Impacto do RGPD nas Pequenas e Médias Empresas, em Portugal" (ver Anexo 1).

O inquérito permite conhecer as principais dificuldades das PME na implementação do regulamento, os principais desafios que as PME percecionam em relação à conformidade com o RGPD e quais os principais benefícios do RGPD para as empresas, aspetos importantes para a criação da solução para Conformidade, Proteção e Privacidade dos Dados Pessoais.

Adicionalmente, o inquérito apresenta questões de continuidade do trabalho de investigação – Fase II, nomeadamente ao nível do interesse em realizar uma Prova de Conceito à solução proposta e sobre o seu propósito, por exemplo, qual o entendimento ao nível de abordagens baseadas em risco ou qual o conhecimento existente ao nível das instituições de referência como a ISO ou a ENISA.

O inquérito "Impacto do RGPD nas Pequenas e Médias Empresas, em Portugal" foi realizado em formulário online, através da conta académica Office 365 – formulários da Microsoft, garantido a confidencialidade das respostas por via das suas características técnicas.

O público-alvo do inquérito é todo o universo de PME. Neste sentido, foi realizada uma pesquisa na internet de modo a conseguir alcançar uma amostra de organizações em todo o território nacional, tendo sido selecionada e concretizada, deste modo, uma parceria com a ANPME – Associação Nacional das Pequenas e Médias Empresas, entidade que tem âmbito de atuação em todo o território nacional, sendo uma das principais associações empresariais do país (ANPME, 2021), mediante a qual se despoletou a divulgação do inquérito a todas as PME nacionais, através de newsletter da ANPME – ver Anexo 2).

O inquérito foi disseminado também em redes sociais através da divulgação inicial da ANPME. O inquérito foi divulgado no dia 18 de fevereiro de 2021 e esteve disponível até ao dia 31 de março de 2021. Foram obtidas respostas de 34 organizações.

Os dados recolhidos foram analisados sob o ponto de vista estatístico, através da aplicação Excel, cujos resultados estão apresentados no Capítulo 5 – Resultados obtidos.

4.2 Fase II – Solução para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD

A Fase 2, Solução para proteção da privacidade e dos dados pessoais baseada em sanções jurídicas no RGPD, está organizada em 4 pontos:

4.2.1 - Definição do Processo de gestão do Risco – proposta inicial de solução

4.2.2 - Fase de testes - desenvolvimento da Prova de Conceito junto das PME

4.2.3 - Avaliação da Prova de Conceito com as PME

4.2.4 - Apresentação da solução para Conformidade, Proteção e Privacidade dos dados pessoais

4.2.1 – Definição do Processo de gestão do Risco – proposta inicial da solução

De acordo com o documento "Guidelines for SMEs on the security of personal data processing", publicado pela ENISA (2016), as PME não estão totalmente familiarizadas com a perceção de risco do ponto de vista dos dados pessoais e poderiam beneficiar de uma abordagem mais orientada que preencheria a lacuna entre as disposições legais e a sua compreensão e perceção de risco.

Ao longo da última década, várias metodologias e estruturas de avaliação de risco de segurança foram propostas por diferentes órgãos, com o objetivo de apoiar as organizações na avaliação de riscos de segurança associadas às suas operações de negócios. A título de exemplo, a ENISA - Agência da União Europeia para a Segurança de Redes e Informações, publicou um inventário de metodologias e ferramentas de avaliação do risco (ENISA, 2021).

Embora as grandes empresas tenham a possibilidade de responder e implementar adequadamente estas estruturas, as PME nem sempre têm a experiência e os recursos necessários para fazê-lo (ENISA, 2016, pág. 8).

No intuito de apoiar as PME, a ENISA, como já referido no âmbito deste trabalho, publicou em 2016 (ENISA, 2016), e atualizou em 2017 (ENISA, 2017), um conjunto de orientações para as PME, atuando como responsáveis pelo tratamento ou subcontratantes, que visam ajudá-las a avaliar os riscos de segurança e, consequentemente, a adotar medidas de segurança para a proteção de dados pessoais, e garantir a conformidade com o RGPD.

Numa tentativa de facilitar ainda mais este procedimento, também está incluído na ferramenta de avaliação do nível de risco um mapeamento do conjunto de medidas proposto com os controlos de segurança da ISO/IEC 27001:2013 relativo à segurança da informação (ENISA, 2016, pág.33). Adicionalmente, e tendo em conta a extensão da ISO/IEC 27001 para a gestão de informações de privacidade – ISO/IEC 27701:2019, o mapeamento integral ao RGPD permite às PME a utilização das orientações da ENISA, para o cumprimento total do regulamento.

Como tal, e para uma maior facilidade de implementação prática por parte das PME, a abordagem proposta não apresenta uma nova metodologia de avaliação do risco, mas, sim,

baseia-se no trabalho existente para fornecer orientações às PME (ENISA, 2016, pág. 17), de acordo com o ponto 2.5 Segurança e Gestão dos Riscos na área dos dados pessoais, concretizada nas suas quatro fases principais:

4.2.1.1 Avaliação do risco;

4.2.1.2 Tratamento do risco;

4.2.1.3 Aceitação do risco; e

4.2.1.4 Comunicação do risco.

Para além da base do processo de gestão do risco corresponder às orientações da ENISA, alguns pontos da metodologia foram densificados com outros inputs, nomeadamente:

- Esclarecimentos da Comissão Nacional de Proteção de Dados (CNPD), nomeadamente os respeitantes à caracterização geral da organização, classificação das categorias de dados, fundamento de licitude e classificação dos destinatários para que, tanto quanto possível, as PME portuguesas possam estar alinhadas ao modelo de registo das atividades de tratamento disponibilizado pela CNPD em especial para as Micro, Pequenas e Médias empresas (CNPD, 2019);

- Documentação da Organização Internacional de Normalização (ISO), mais propriamente através dos documentos ISO/IEC 27001:2013, ISO/IEC 27002:2013 e ISO/IEC 27701:2019;

- RGPD, Regulamento Geral sobre a Proteção de Dados, e orientações oficiais do EDPB – European Data Protection Board, e do anterior Grupo de Trabalho do artigo 29;

- Documentação das várias Autoridades de Controlo, tais como Autoridade Francesa (CNIL), Inglesa (ICO), Irlandesa (DPC), nomeadamente para a definição de propostas de resolução para as não conformidades;

- Notificações das sanções jurídicas do RGPD nos sítios de internet das Autoridades de Controlo dos vários Estados-Membros da União Europeia e Espaço Económico Europeu;

- Outros documentos relevantes tais como a Resolução do Conselho de Ministros nº 41/2018, relativa aos requisitos técnicos mínimos das redes e sistemas de informação ou o boletim do National Institute of Standards and Technology (NIST) relativo à integração da segurança no ciclo de vida de desenvolvimento de software (SDLC).

4.2.1.1 – Avaliação do risco

As diretrizes da ENISA para as PME propõem uma abordagem de avaliação do risco, que se baseia em quatro etapas, como se apresenta de seguida (ENISA, 2017, pág. 10):

Etapa 0: Caracterização geral

Etapa 1: Definição da operação de tratamento e seu contexto

Etapa 2: Compreender e avaliar o impacto

Etapa 3: Definição de possíveis ameaças e avaliação da sua probabilidade

Etapa 4: Avaliação do risco

A avaliação do risco começa com a identificação de ameaças, seguida da determinação da probabilidade e do impacto de cada risco. Para avaliar adequadamente o risco, deve-se igualmente levar em consideração a probabilidade e o impacto (ENISA, 2016, pág. 11).

Etapa 0: Caracterização geral

Esta etapa - ver Anexo 3 - diz respeito à codificação do tratamento alvo de avaliação do risco, à caracterização geral da organização alvo da avaliação, e respetivo enquadramento em termos de tratamento de dados, por exemplo, se subcontratante, responsável pelo tratamento ou responsável conjunto, tendo como referência os modelos de registo das atividades de tratamento (CNPD, 2019):
- # tratamento (código interno do tratamento alvo de avaliação do risco);
- Enquadramento da Organização no tratamento de dados, com as respostas possíveis: subcontratante; responsável pelo tratamento; responsável conjunto;
- Dados da Organização, com os seguintes campos de preenchimento obrigatório: Nome; Morada; E-mail; Telefone; Nome Pessoa de Contacto; Área/Departamento;
- Dados do Encarregado de Proteção de Dados (se existir), com os seguintes campos de preenchimento obrigatório: Nome; Morada; E-mail; Telefone;
- Dados do(s) Responsável(eis) Conjunto(s) (se existir(em)), com os seguintes campos de preenchimento obrigatório: Nome; Morada; E-mail; Telefone; Nome Pessoa de Contacto; Referência para o(s) acordo(s) conjunto(s).

Etapa 1: Definição da operação de tratamento e seu contexto

A etapa 1 – ver Anexo 4 - é o ponto de partida da avaliação do risco e é fundamental para a organização definir os limites do sistema de tratamento de dados (em avaliação) e o seu contexto. Para apoiar as PME na definição da atividade de tratamento, é fornecido um conjunto de perguntas (ENISA, 2017, pág.10):

1. Qual é a operação de tratamento de dados pessoais?
2. Quais são os tipos de dados pessoais tratados?
3. Qual é a finalidade do tratamento?
4. Quais são os meios utilizados para o tratamento dos dados pessoais?
5. Onde ocorre o tratamento de dados pessoais?
6. Quais são as categorias dos titulares dos dados?
7. Quais são os destinatários dos dados?
8. Qual a licitude do tratamento?

Ao responder a essas perguntas, uma PME precisa considerar as várias fases do tratamento de dados (recolha, conservação, utilização, transferência, eliminação, etc.) e seus parâmetros subsequentes (ENISA, 2017, pág.10).

Etapa 2: Compreender e avaliar o impacto

Com base na análise da Etapa 1, a organização, nesta fase, deve avaliar o impacto sobre os direitos e liberdades fundamentais dos titulares dos dados, resultante da possível perda de

segurança dos dados pessoais. Quatro níveis de impacto são considerados (baixo, médio, alto, muito alto) (ENISA, 2017, pág.11).

A avaliação do impacto é um processo qualitativo e uma série de fatores precisam de ser considerados pelo responsável pelo tratamento, como os tipos de dados pessoais, criticidade da operação de tratamento, volume de dados pessoais, características especiais do responsável pelo tratamento, também como categorias especiais de titulares dos dados (ENISA, 2017, pág.11).

Além dos parâmetros mencionados, outro aspeto importante que pode ser considerado pela organização é a identificabilidade dos titulares dos dados, ou seja, o quão fácil é para uma parte que tem acesso ao conjunto dos dados relacioná-los univocamente a uma determinada pessoa (ENISA, 2016, pág.22). É importante notar que, ao avaliar o impacto, também devem ser considerados possíveis efeitos secundários (para os direitos e liberdades dos indivíduos).

O impacto, deste modo, é avaliado separadamente quanto à perda de confidencialidade, integridade e disponibilidade, através das seguintes perguntas (ENISA, 2016, pág.22):

1. Por favor, reflita sobre o impacto que uma divulgação não autorizada (perda de confidencialidade) de dados pessoais - no contexto em que a sua atividade comercial ocorre - poderia ter sobre a pessoa / titular dos dados e expresse uma classificação em conformidade.
2. Por favor, reflita sobre o impacto que uma alteração não autorizada (perda de integridade) de dados pessoais - no contexto em que a sua atividade comercial ocorre - poderia ter sobre a pessoa / titular dos dados e expresse uma classificação em conformidade.
3. Por favor, reflita sobre o impacto que uma destruição ou perda não autorizada (perda de disponibilidade) de dados pessoais - no contexto em que a sua atividade comercial ocorre - poderia ter sobre a pessoa / titular dos dados e expresse uma classificação em conformidade.

No Anexo 5 encontram-se desenvolvimentos sobre esta etapa.

Etapa 3: Definição de possíveis ameaças e avaliação da sua probabilidade

Na etapa 3, o objetivo da organização é entender as ameaças relacionadas com o ambiente geral do tratamento de dados pessoais (externos ou internos) e avaliar a sua probabilidade (probabilidade de ocorrência de ameaças) (ENISA, 2017, pág.12).

Neste contexto, uma ameaça é qualquer circunstância ou evento que tenha o potencial de afetar adversamente a segurança dos dados pessoais. Diferentes níveis e tipos de ameaças à confidencialidade, integridade e disponibilidade de dados pessoais podem ser considerados a este respeito (ENISA, 2016, pág.24).

Para simplificar esta etapa para as PME, a ENISA definiu uma série de questões de avaliação que podem ajudar uma organização. As questões estão agrupadas em quatro dimensões, a saber (ENISA, 2016, pág.24):

A - Rede e recursos técnicos (hardware e software)

1. Alguma parte do tratamento de dados pessoais é realizada pela internet?

2. É possível fornecer acesso a um sistema interno de tratamento de dados pessoais através da Internet (por exemplo, para determinados utilizadores ou grupos de utilizadores)?
3. O sistema de tratamento de dados pessoais está interconectado a outro sistema ou serviço de TI externo ou interno (à sua organização)?
4. Pessoas não autorizadas podem aceder facilmente ao ambiente de tratamento de dados?
5. O sistema de tratamento de dados pessoais é projetado, implementado ou mantido sem seguir as melhores práticas relevantes?

B - Processos / procedimentos relacionados com o tratamento de dados pessoais

6. As funções e responsabilidades em relação ao tratamento de dados pessoais são vagas ou não estão claramente definidas?
7. O uso aceitável da rede, do sistema e dos recursos físicos dentro da organização é ambíguo ou não está claramente definido?
8. Os funcionários podem trazer e usar os seus próprios dispositivos para se ligarem ao sistema de tratamento de dados pessoais?
9. Os funcionários estão autorizados a transferir, armazenar ou tratar dados pessoais fora das instalações da organização?
10. As atividades de tratamento de dados pessoais podem ser realizadas sem a criação de arquivos de log/registos?

C - Diferentes partes e pessoas envolvidas no tratamento de dados pessoais

11. O tratamento de dados pessoais é realizado por um número indefinido de funcionários?
12. Alguma parte da operação de tratamento de dados é realizada por um prestador de serviços / terceiro (subcontratante)?
13. As obrigações das partes / pessoas envolvidas no tratamento de dados pessoais são ambíguas ou não estão claramente definidas?
14. O pessoal envolvido no tratamento de dados pessoais não está familiarizado com as questões de segurança da informação?
15. As pessoas / partes envolvidas na operação de tratamento de dados negligenciam o armazenamento seguro e / ou destruição de dados pessoais?

D - Setor empresarial e dimensão do tratamento

16. Considera que este setor empresarial está sujeito a ciber ataques?
17. A organização sofreu algum ciber ataque ou outro tipo de violação de segurança nos últimos dois anos?
18. Recebeu alguma notificação e / ou reclamação relativa à segurança do sistema informático (utilizado para o tratamento de dados pessoais) no último ano?
19. Uma operação de tratamento diz respeito a um grande volume de pessoas individuais e / ou dados pessoais?
20. Existem práticas recomendadas de segurança, específicas para este setor empresarial, que não foram seguidas de forma adequada?

Como no caso da avaliação de impacto, a avaliação da probabilidade de ocorrência de um risco pode ser qualitativa ou quantitativa, e está muito relacionada com o ambiente específico de tratamento de dados pessoais.

No contexto desta abordagem, estão definidos três níveis de probabilidade de ocorrência de uma ameaça (ENISA, 2016, pág.29):

1 - Baixo - é improvável que a ameaça se materialize;

2 - Médio - há uma possibilidade razoável de que a ameaça se materialize;

3 - Alto - a ameaça provavelmente se materializará.

Se todas as respostas, numa área de avaliação, forem positivas, a organização deve considerar a probabilidade de ameaça para essa área como alta, enquanto se todas forem negativas, a probabilidade de ameaça deve ser considerada baixa. Para casos com duas a três respostas positivas, a organização deve atribuir a probabilidade de ameaça média (ENISA, 2016, pág.29).

Em cada uma das perguntas, uma resposta positiva (SIM) indica uma alta probabilidade de ameaça, enquanto uma resposta negativa (NÃO), uma menor probabilidade de ameaça. Com base neste entendimento, a avaliação da probabilidade de ocorrência de uma ameaça é realizada (ENISA, 2016, pág.29).

A probabilidade final de ocorrência de uma ameaça é calculada após a soma das pontuações obtidas nas quatro dimensões já mencionadas, associando o resultado à seguinte escala (ENISA, 2017, pág.15):

– Nível de probabilidade de ocorrência de ameaça BAIXO, se a soma geral da probabilidade estiver compreendida entre os valores 4 e 5;

– Nível de probabilidade de ocorrência de ameaça MÉDIO, se a soma geral da probabilidade estiver compreendida entre os valores 6 e 8; e

– Nível de probabilidade de ocorrência de ameaça ALTO, se a soma geral da probabilidade estiver compreendida entre os valores 9 e 12.

No Anexo 6 encontram-se os desenvolvimentos sobre esta etapa.

Etapa 4: Avaliação do risco

Depois de avaliar o impacto da operação de tratamento de dados pessoais e a probabilidade de ocorrência de ameaças relevantes, é possível calcular a avaliação final do risco, de acordo com a seguinte fórmula de cálculo (ENISA, 2016, pág.31):

Nível do risco = Impacto x Probabilidade de ocorrência de uma ameaça

As opções indicadas na matriz do risco abaixo – Figura 4, onde se identificam os seus vários níveis, foi realizada no pressuposto do pior cenário possível (maior impacto no titular dos dados). Consequentemente, o nível de impacto teve mais peso do que a probabilidade de

ocorrência de ameaças, sendo que apenas dois níveis de risco baixo e três níveis de risco médio foram identificados. Os níveis de impacto alto e muito alto são identificados como riscos de nível elevado e agrupados (ENISA, 2016, pág.31).

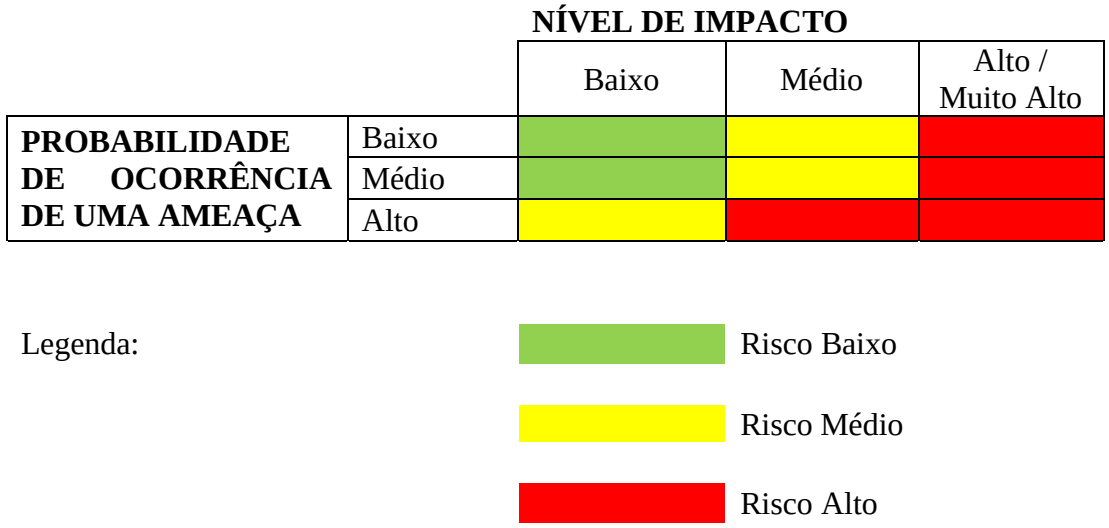


Figura 4 - Matriz do risco

Independentemente do resultado final deste exercício, a organização deve sentir-se livre para ajustar o nível de risco obtido, tendo em consideração as características específicas da operação de tratamento de dados (que foram perdidas durante o processo de avaliação) e fornecendo a justificação adequada para esse ajuste (ENISA, 2017, pág.16).

Após a avaliação do nível de risco, a organização pode prosseguir com a seleção de medidas de segurança adequadas para a proteção de dados pessoais (ENISA, 2017, pág.16), incluídas no ponto seguinte, tratamento do risco.

Reforça-se que esta componente de avaliação do risco no contexto solução proposta para a conformidade, proteção e privacidade dos dados pessoais baseada em sanções jurídicas do RGPD, é focada exclusivamente na avaliação dos riscos de segurança e não deve ser confundida com avaliação de impacto sobre a proteção de dados (DPIA - artigo 35º do RGPD). Na verdade, embora a primeira seja uma parte crítica deste último, um DPIA leva em consideração outros parâmetros que estão relacionados com o tratamento de dados pessoais e vão para além da segurança. Ainda assim, a abordagem proposta também pode ser útil no contexto de um DPIA e / ou pode ser estendido no contexto de uma organização para cobrir também a condução de uma avaliação de impacto (ENISA, 2016, pág. 17).

4.2.1.2 – Tratamento do risco

Nesta etapa, duas categorias principais de medidas são discutidas: as medidas técnicas e as medidas organizativas. Estas categorias foram divididas em subcategorias com uma breve

descrição, explicando como cada subcategoria se relaciona com as disposições específicas do RGPD (ENISA, 2016, pág.33).

Em cada subcategoria, as medidas são apresentadas por nível de risco, seguindo o mesmo esquema de cores usado nas etapas anteriores (baixo: verde, médio: amarelo, alto: vermelho). Para alcançar escalabilidade, presume-se que todas as medidas descritas no nível inferior (verde) são aplicáveis a todos os níveis. Da mesma forma, as medidas apresentadas no nível médio (amarelo) são aplicáveis também no nível de risco alto. As medidas apresentadas no nível alto (vermelho) não são aplicáveis em nenhum outro nível de risco (ENISA, 2016, pág.33).

Deve-se notar que a correspondência das medidas com níveis de risco específicos não deve ser percebida como absoluta. E, dependendo do contexto do tratamento de dados pessoais, a organização pode considerar a adoção de medidas adicionais, mesmo que sejam atribuídas a um nível de risco mais elevado. Além disso, a lista de medidas proposta não tem em conta outros requisitos adicionais de segurança específicos do setor, bem como obrigações regulamentares específicas, decorrentes, por exemplo, da Diretiva *ePrivacy* ou da Diretiva SRI (ENISA, 2016, pág.33).

Numa tentativa de facilitar ainda mais este procedimento, também está incluído um mapeamento do conjunto de medidas proposto com os controlos de segurança da ISO/IEC 27001:2013, relativo à segurança da informação (ENISA, 2016, pág.33). O mapeamento foi verificado e analisado de modo mais capilar, introduzindo relações ao nível dos controlos.

Adicionalmente, e tendo em conta a extensão da ISO/IEC 27001:2013 (e ISO/IEC 27002:2013) para a gestão de informações de privacidade – ISO/IEC 27701:2019, analisaram-se as relações entre ambos e também com os requisitos do RGPD.

Deste modo, verifica-se, por um lado, relações diretas entre as medidas preconizadas pela ENISA e o cumprimento do RGPD, mas, por outro, verificam-se lacunas no cumprimento integral do regulamento. Para garantir a completude do regulamento, foram desenvolvidos novos controlos [3], iniciativa alinhada com as recomendações da ENISA previamente enunciadas (Anexo 7). Por estar em causa a completude do regulamento, o nível de risco das novas medidas é sempre o mais baixo, para permitir a conformidade legal em todos os níveis de risco.

Esta fase do processo de gestão do risco concretiza-se numa só etapa: o início da construção do plano de tratamento do risco, que inclui a lista completa de medidas propostas por nível de risco, e sua relação com o RGPD, com vista ao cumprimento total das obrigações do mesmo.

As medidas deverão ser respondidas com base nas possibilidades "Conforme", "Não Conforme" e/ou "Sem aplicação". Sempre que possível, deverá ser incluído um racional e

[3] Os artigos não mapeados não implicam as organizações (responsáveis pelo tratamento e/ou subcontratantes) no cumprimento do RGPD, dizendo respeito a especificações da Comissão Europeia (n.º8 do Artigo 12º e n.º7 do Artigo 28º), especificações das Autoridades de Controlo (n.º8 do Artigo 28º, n.º6 do Artigo 35º, n.º4 do Artigo 36º, Artigo 51º e seguintes), especificações da Comissão Europeia e das Autoridades de Controlo (Artigo 50º), especificações de Organismos de Certificação (Artigo 43º) e limitações por medidas legislativas (Artigo 23º).

respetivas evidências que permita cumprir o princípio da responsabilidade, de acordo com o nº 2 do artigo 5º do RGPD.

Adicionalmente, e de modo a preparar a fase seguinte do processo de gestão do risco – Aceitação do risco – deverá ser incluído também:

- O tipo de tratamento do risco: mitigação, transferência, prevenção ou retenção dos riscos (ENISA, 2016, pág. 11);

- A indicação se há riscos secundários associados ao tipo de tratamento considerado; e

- Propostas de resolução para as não conformidades.

As propostas para as não conformidades (Anexo 8) foram desenvolvidas com base na informação disponível das Autoridades de Controlo dos vários Estados-Membros da União Europeia e Espaço Económico Europeu, orientações oficiais do EDPB – European Data Protection Board, e do anterior Grupo de Trabalho do artigo 29, documentação da Organização Internacional de Normalização (ISO), mais propriamente através dos documentos ISO/IEC 27001:2013, ISO/IEC 27002:2013 e ISO/IEC 27701:2019, e outros documentos relevantes tais como a Resolução do Conselho de Ministros nº 41/2018, relativa aos requisitos técnicos mínimos das redes e sistemas de informação ou o boletim do National Institute of Standards and Technology (NIST) relativo à integração da segurança no ciclo de vida de desenvolvimento de software (SDLC).

4.2.1.3 – Aceitação do risco

Mesmo quando os riscos são tratados, podem persistir outros riscos: os mesmos com magnitude inferior, ou seja, riscos residuais; ou outros riscos, ou seja, riscos secundários. Neste sentido, deverá haver um processo de aceitação do risco que permita a gestão e a tomada de decisão quanto à permanência de riscos após a fase de tratamento (ENISA, 2016, pág. 11).

Deverá ocorrer, deste modo, a "Aceitação" ou a "Não Aceitação" do risco, dando sequência ao ponto anterior 3.2.1.2 Tratamento do risco, através do plano de tratamento do risco.

No caso de não aceitação do risco, deverão ser enunciadas as medidas de tratamento; as preconizadas na etapa anterior (Anexo 8) ou outras, de modo a concretizar o plano de tratamento.

A decisão deverá estar datada. As exigências de revisão ou monitorização e a suas calendarizações, deverão estar também definidas.

Neste momento, as decisões podem ter em consideração as sanções jurídicas do RGPD, enquanto fator de priorização das várias tarefas incluídas no plano de tratamento, no processo de tomada de decisão.

A solução baseada em sanções jurídicas identifica, e prioriza, as medidas preconizadas em 4.2.1.2 em termos de multas RGPD, tanto pela incidência do valor monetário das multas como pela frequência da sua ocorrência, através da verificação dos artigos do RGPD que originaram as multas, pelo facto das medidas de 4.2.1.2 estarem alinhadas aos mesmos artigos do RGPD – ver Anexo 9.

Foram consideradas, deste modo, as seguintes fases na construção do fator de priorização:

1 - Identificação de todos os artigos do RGPD, com o detalhe ao nível das suas alíneas, conforme consta no Anexo 7.

2 - Análise de todas as multas do RGPD aplicadas pelas autoridades de controlo dos Estados-Membros da União Europeia e do Espaço Económico Europeu, ou seja, membros do EDPB – European Data Protection Board (EDPB, 2021), através de pesquisa nos seus respetivos sítios da internet, incluindo a Autoridade de Controlo do Reino Unido, membro até 2020, inclusive;

- O período temporal de análise de multas, para a construção do fator de priorização, esteve compreendido entre 25 de maio de 2018 e 31 de março de 2021, através da pesquisa da informação disponível nos sítios da internet das várias autoridades de controlo;

- Foram desconsideradas todas as multas que tiveram origem em legislação nacional ou outro instrumento legal que não o RGPD, como acontece com a Diretiva das Comunicações Eletrónicas (ePrivacy) e multas relativas a cookies, bem como aquelas decisões que não foram tornadas públicas;

- Sempre que as deliberações indicavam o montante da multa pelo respetivo artigo, a classificação foi desagregada para incluir esta especificação. Nos casos em que era referido o valor global para um conjunto de artigos, foi considerada, para este exercício, uma distribuição proporcional para cada um deles;

- A informação relativa à análise das multas incluiu, sempre que divulgada pela Autoridade de Controlo, os seguintes atributos: nome do país, nome da Autoridade de Controlo, website direto da multa, data da multa, valor monetário da multa, artigo(s) RGPD que deram origem à multa, nome da entidade multada, âmbito do RGPD (responsável pelo tratamento / subcontratante), classificação da entidade multada (entidade pública, entidade privada, pessoa individual e tipo de organização (entidade pública, entidade privada – grande empresa, entidade privada – PME, pessoa individual) (Anexo 10).

3 – Após construção do *dataset* relativo às multas RGPD no Espaço Económico Europeu, foram considerados dois cenários para a construção do fator de priorização:

- Cenário 1, com valor monetário das multas

- Cenário 2, sem valor monetário das multas, ou seja, através da frequência da sua ocorrência

Se no cenário 1, foi imputado o valor monetário correspondente a cada artigo para o estabelecimento do somatório de todas as multas existentes, no cenário 2 o cálculo ocorreu através da soma do número de ocorrências.

Tendo em conta que há uma relação entre os artigos do RGPD e as medidas da solução para a proteção da privacidade e dos dados pessoais (ver Anexo 7), o passo seguinte foi a imputação dos valores apurados às medidas correspondentes, quer para o cenário 1, quer para o cenário 2.

4 – A concretização do fator de priorização, para a solução proposta para a conformidade, proteção e privacidade dos dados pessoais baseada em sanções jurídicas do RGPD, teve em consideração apenas as multas classificadas para entidades privadas – PME, através da média ponderada dos dois cenários considerados; com valores monetários e com frequência absoluta das ocorrências das multas no Espaço Económico Europeu.

4.2.1.4 – Comunicação do risco

Todas as partes interessadas devem ser informadas sobre as decisões tomadas; que controlos foram adotados e que riscos foram aceites (ENISA, 2016, pág. 11), bem como quais os próximos passos, por exemplo, quais os critérios para o estabelecimento da revisão e sua monitorização – concretização do plano de tratamento do risco. A comunicação às partes interessadas deverá ficar evidenciada.

4.2.2 – Fase de testes – desenvolvimento da Prova de Conceito junto das PME

Uma Prova de Conceito (PoC) é a entrega de um sistema funcional para provar que a tecnologia funciona e funciona conforme pretendido. Geralmente, é um processo pequeno e pode incluir todas as funções ou apenas parte das mesmas. Em simultâneo, é um processo que envolve um número relativamente pequeno de utilizadores. No fim do processo, o PoC deve ser dado como concluído, desmontado, caso se aplique, e considerado completo após os resultados terem sido documentados (Government of Newfoundland and Labrador, 2021).

Conforme Government of Newfoundland and Labrador (2021), um exemplo de PoC poderá ser a instalação de uma rede sem fios. Este PoC resulta na instalação de uma infraestrutura sem fios em três salas de reuniões dentro de um determinado prédio, com um pequeno número de utilizadores que tiveram acesso a esta rede para teste. Por fim, cria-se um documento com as lições aprendidas, juntamente com outras recomendações sobre como proceder numa implementação completa de uma mesma rede.

Relativamente ao objeto do trabalho de investigação, pretendeu-se realizar um PoC junto das PME portuguesas, de modo a testar a solução proposta para conformidade, proteção e privacidade dos dados pessoais baseada em sanções jurídicas do RGPD.

As organizações foram definidas através do inquérito "Impacto do RGPD nas Organizações" – Fase 1 da metodologia deste trabalho (Anexo 1), através da resposta afirmativa à pergunta número 25. Após identificação das PME, o PoC resulta na concretização das seguintes fases (Government of Newfoundland and Labrador, 2021):

- Iniciação: o caso de estudo do PoC, neste caso a solução proposta para conformidade, proteção e privacidade dos dados pessoais, é apresentada à PME, ao seu responsável, conforme Fase I do Anexo 11 "Prova de Conceito junto das PME". A proposta inclui prazos estimados para a concretização da iniciativa, bem como outros recursos necessários, como a necessidade de participação de atores relevantes, como são os responsáveis de informática, juristas, encarregado de proteção de dados, se aplicável, ou membros da direção. Tratando-se de um exercício académico, não são considerados custos com a iniciativa.

- Planeamento e Análise: a organização deve determinar um gestor de projeto e deverá ser definido um plano detalhado para a concretização do PoC, que deverá incluir um plano de projeto, um plano de recursos e uma análise das partes interessadas. Deverá existir, também, um termo de abertura do projeto, onde consta o âmbito do trabalho acordado, lista de entregas e prazos (Fase 2 do Anexo 11). As estimativas de custo, como referido acima, não são consideradas. A solução proposta para conformidade, proteção e privacidade dos dados

pessoais baseada em sanções jurídicas do RGPD (conjunto das quatro etapas do ponto 4.1.1, a saber: avaliação do risco, tratamento do risco, aceitação do risco e comunicação do risco) foi apresentada a cada PME em reunião de início de projeto, e disponibilizada em ficheiro próprio, em formato Excel (Anexo 12 – modelo desenvolvido para a concretização do PoC).

- Fecho do Projeto – Na fase de conclusão do PoC, o gestor de projeto, consultando a equipa de projeto, finaliza as entregas (Fase 3 do Anexo 11).

Relativamente à duração da iniciativa, esta não deverá ser superior a 100 dias úteis. A duração da instalação, configuração e uso do produto, no que é aplicável, não deve ser superior a 90 dias úteis, e a avaliação escrita do produto, incluindo toda a documentação, não deve demorar mais de 10 dias úteis (Government of Newfoundland and Labrador, 2021). O PoC foi iniciado no dia 14 de abril de 2021 através de envio, por email, de convite à participação – início da Fase 1 – com vista ao agendamento de uma reunião de início de projeto, de apresentação e planeamento – Fase 2. O PoC teve todas as fases concluídas até ao fim do mês de maio de 2021.

É apresentado no Anexo 12 o modelo desenvolvido para a concretização do PoC, enquanto sistema funcional para provar junto das PME que a solução proposta para conformidade, proteção e privacidade dos dados pessoais baseada em sanções jurídicas do RGPD funciona como pretendido.

4.2.3 – Avaliação da Prova de Conceito com as PME

A avaliação do PoC deverá ser escrita, e deve incluir toda a documentação necessária. A sua concretização não deverá demorar mais de 10 dias úteis após a concretização do mesmo (Government of Newfoundland and Labrador, 2021).

A avaliação, para além de incluir as lições aprendidas, enquanto componente essencial de feedback das PME, e outras recomendações sobre como proceder numa implementação completa, incorpora pontos concretos relativos ao trabalho de investigação em questão, alinhado ao inquérito "Impacto do RGPD nas organizações", da Fase I da metodologia (Anexo 1) e, principalmente, enquadrado na solução proposta para conformidade, proteção e privacidade dos dados pessoais baseada em sanções jurídicas do RGPD.

A avaliação é parte integrante do Anexo 11, Fase 3 – Fecho do Projeto.

4.2.4 – Apresentação da solução para Conformidade, Proteção e Privacidade dos dados pessoais

Após o desenvolvimento da solução para Conformidade, Proteção e Privacidade dos dados pessoais baseada em sanções jurídicas do RGPD, o desenvolvimento da Prova de Conceito e sua avaliação, é apresentada a solução para proteção da privacidade e dos dados pessoais, e comunicada às partes interessadas.

Capítulo 5 – Resultados obtidos

5.1 Fase I – Impacto do RGPD nas Organizações – PME

O inquérito foi divulgado no dia 18 de fevereiro de 2021 e esteve disponível até ao dia 31 de março de 2021.

A estratégia de divulgação contou com a participação da ANPME – Associação Nacional das Pequenas e Médias Empresas, conforme referido em 3.1. O inquérito foi divulgado também em redes sociais, através da divulgação inicial realizada pela ANPME.

No total foram obtidas respostas de 34 organizações. No Anexo 13 encontra-se o conjunto de respostas obtidas, excluindo os dados de identificação pessoal existentes.

5.1.1 – Caracterização da PME

As organizações foram caracterizadas através das primeiras quatro questões do inquérito:

1. Dimensão da PME;
2. Antiguidade da PME;
3. Localização geográfica (NUT II); e
4. Setor de atividade.

Relativamente à dimensão das organizações que participaram neste trabalho de investigação, mais de metade (65%) responderam que são microempresas.

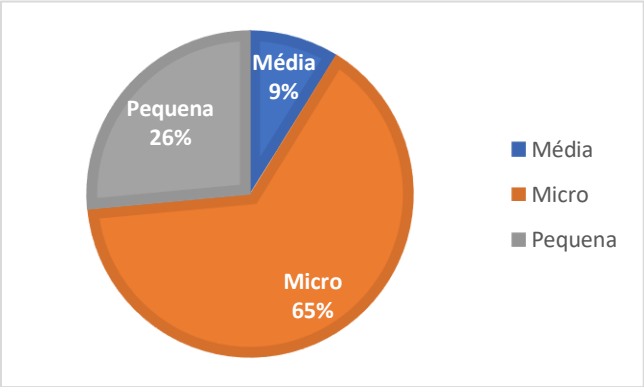


Figura 5 - Dimensão da PME

Em termos de antiguidade, verifica-se alguma semelhança na distribuição das respostas dadas; 38% das PME dizem ter menos de 5 anos. O mesmo número de organizações tem entre 6 a 19 anos, enquanto que 24% (8 PME) responderam que têm mais de 20 anos de presença no mercado.

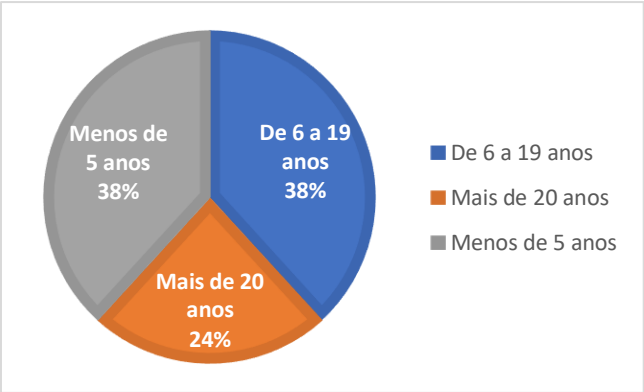


Figura 6 - Antiguidade da PME

Relativamente à localização geográfica das organizações inquiridas, metade encontram-se na Área Metropolita de Lisboa (17). A segunda região que apresenta mais organizações que participaram neste inquérito é a região Norte, com 10 PME (cerca de 30%). Das regiões do Algarve e Região Autónoma dos Açores não foram obtidas quaisquer respostas.

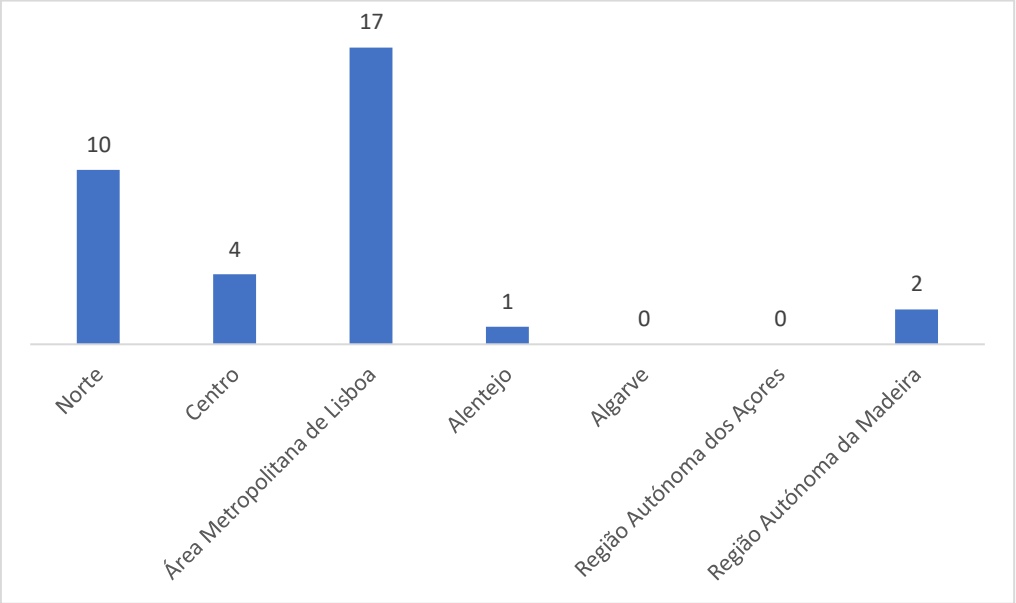


Figura 7 - Localização geográfica (NUT II)

Em termos do setor de atividade a resposta dominante, 21 respostas, correspondendo a 62% do total foi “outros setores”. Comércio por grosso e a retalho foi a segunda resposta mais obtida (4 respostas).

Figura 8 - Setor de atividade

5.1.2 – Caracterização do inquirido na Organização e face ao RGPD

O inquirido, nas questões 5 a 7, foi questionado quanto à sua função na PME, incluindo responsabilidades ao nível da implementação do RGPD.

As duas maiores respostas quanto ao papel do inquirido na organização dizem respeito às funções de gestor/a e proprietário/a, cerca de 30%, cada.

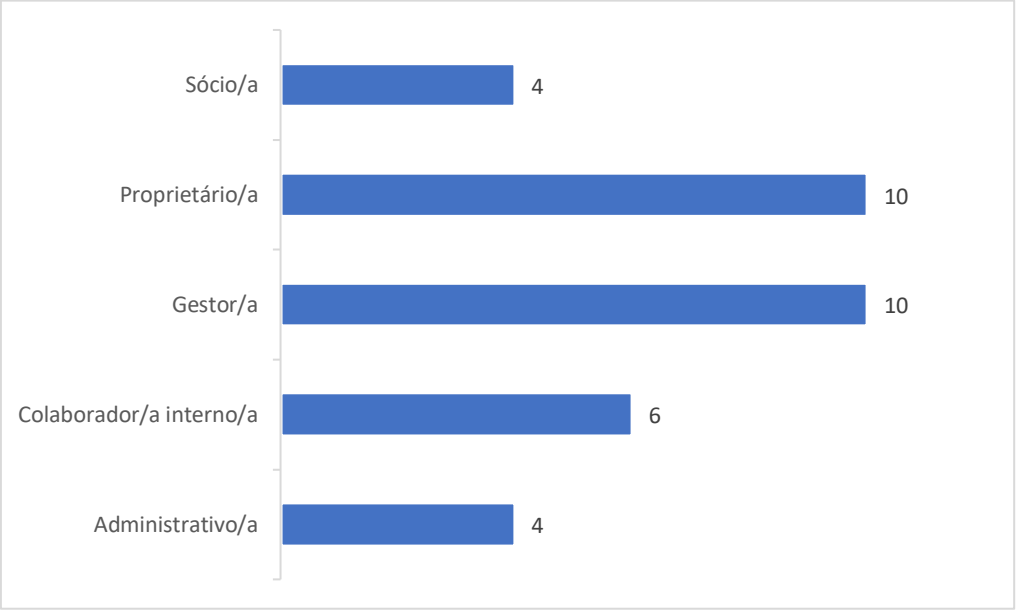


Figura 9 - Função do/a inquirido/a na PME

62% respondeu afirmativamente quanto à responsabilidade na implementação do RGPD (21 respostas).

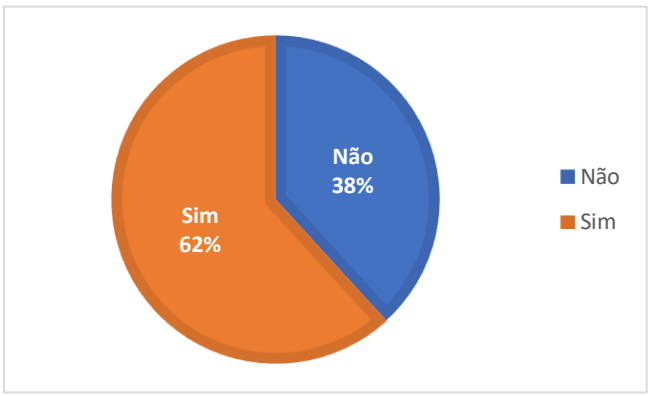


Figura 10 - Responsabilidades do/a inquirido/a na implementação do RGPD

Destes, um terço das organizações inquiridas indicou que ocupa o cargo equivalente ao de Encarregado de Proteção de dados (7 respostas em 21 possíveis). A resposta "outro" foi a segunda mais respondida, com 6 observações, onde se inclui informação como diretor/gerente/responsável da organização e também a informação administrativa/receção.

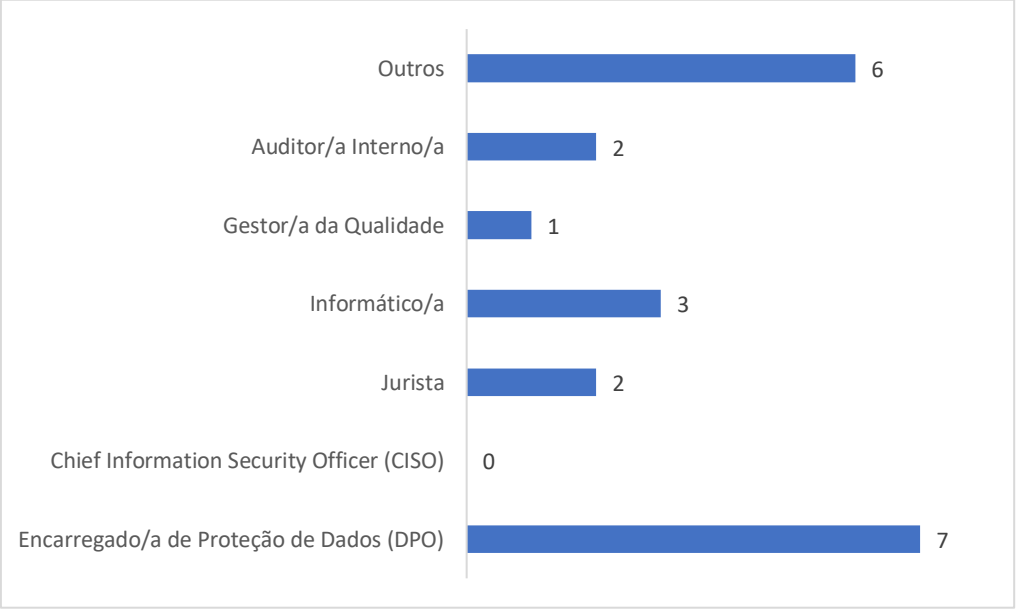


Figura 11 - Cargo do/a inquirido/a na implementação do RGPD

5.1.3 – Utilização de tecnologias da informação e comunicação

Tendo como ponto de partida o Inquérito que o INE realizou (INE, 2020), conforme mencionado em 3.1 Fase I – Impacto do RGPD nas Organizações – PME, o grupo de empresas que participou neste inquérito referiu que:

- 76% das empresas tem website próprio ou do grupo económico a que pertence (26 respostas);

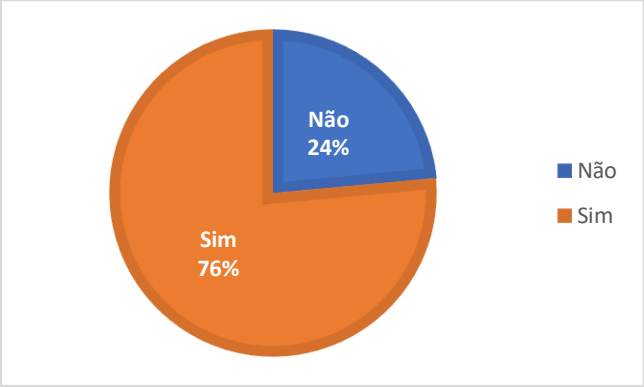


Figura 12 - Empresas com website próprio ou do grupo económico a que pertence

- Apenas 9% das empresas inquiridas (3 empresas) realizam vendas de bens ou serviços através do comércio eletrónico, representando 100% do volume total de vendas de duas PME e 24% na outra PME inquirida;

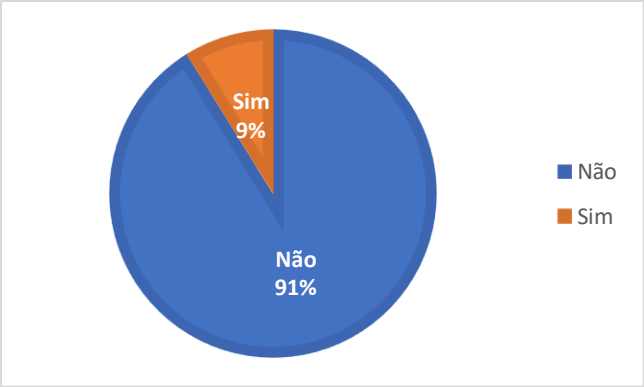


Figura 13 - Empresas que realizam vendas de bens ou serviços através do comércio eletrónico

- 82% das PME responderam que têm serviços de computação em nuvem na internet, como é o caso de serviços de correio eletrónico ou armazenamento de ficheiros;

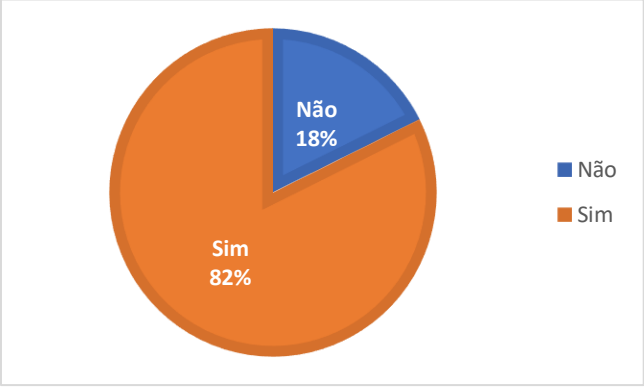


Figura 14 - Empresas que têm serviços de computação em nuvem na internet

- Relativamente à utilização de serviços de big data, apenas 12% respondeu afirmativamente. 56% respondeu que não utiliza e 32% respondeu que não sabe;

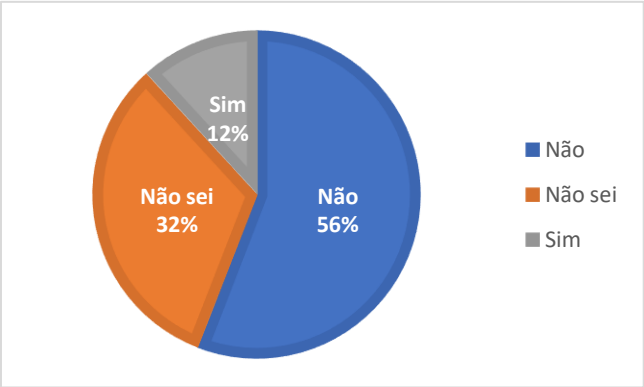


Figura 15 - Empresas que utilizam serviços de big data

- 50% das empresas inquiridas referiu que tem pessoal especialista em TIC (Tecnologias de Informação e Comunicações);

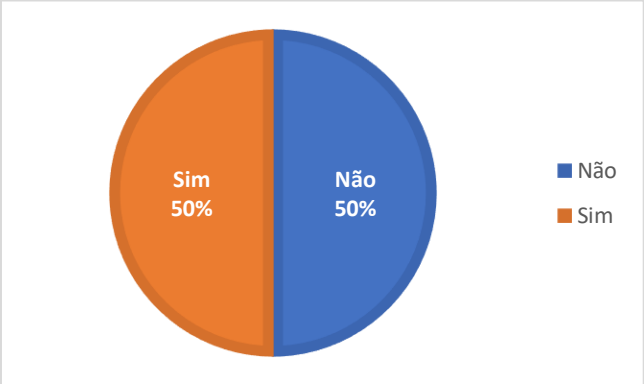


Figura 16 - Empresas que têm pessoal especialista em TIC

- 47% respondeu "sim" quanto à utilização de dispositivos ou sistemas interconectados que podem ser monitorizados ou controlados remotamente através da Internet (IoT).

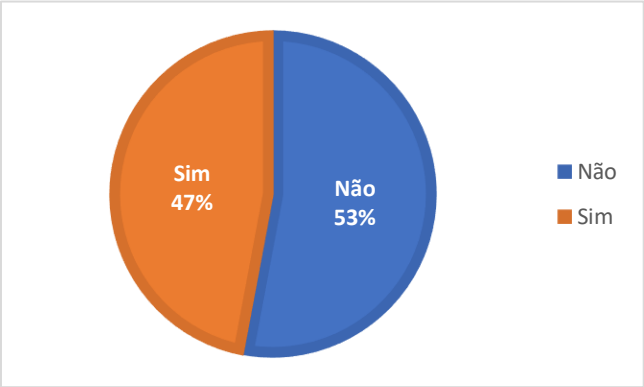


Figura 17 - Empresas que utilizam dispositivos ou sistemas interconectados que podem ser monitorizados ou controlados remotamente através da internet

5.1.4 – Conhecimento sobre o RGPD por parte das PME

Nesta secção do inquérito – perguntas 15 a 21 – pretendeu-se conhecer o nível de conhecimento que as PME têm na matéria em análise.

De modo geral, 94% das organizações inquiridas responderam que têm conhecimento do que é o RGPD (32 respostas num total de 34 respostas possíveis).

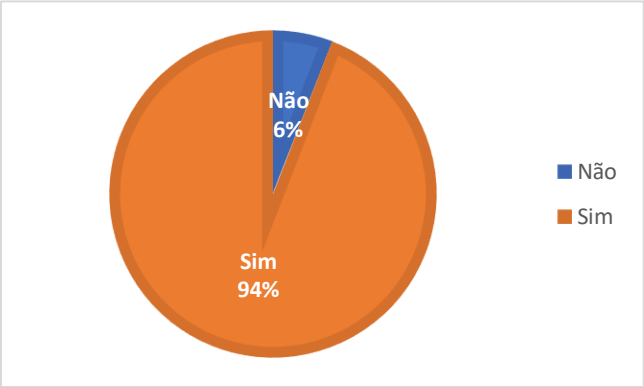


Figura 18 - Empresas que têm conhecimento do que é o RGPD

38% das organizações que responderam afirmativamente à questão anterior indicou que teve conhecimento antes de 2018, ou seja, antes da entrada em vigor do regulamento. 72% do total das PME responderam que tiveram conhecimento antes ou durante o ano de 2018.

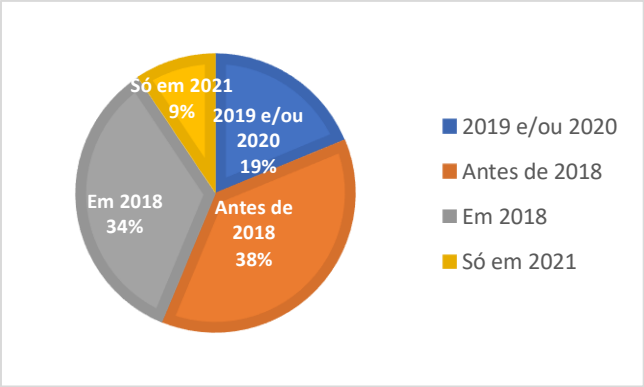


Figura 19 - Momento em que as empresas tiveram conhecimento do RGPD

Relativamente à perceção que as organizações e os/as seus/suas representantes têm quanto ao nível de conhecimento que os/as seus/suas colaboradores/as têm sobre o regulamento, 56% respondeu que o nível é suficiente; 21 % respondeu que o nível de conhecimento é bom/muito bom e 24% respondeu que o nível de conhecimento é limitado/muito limitado.

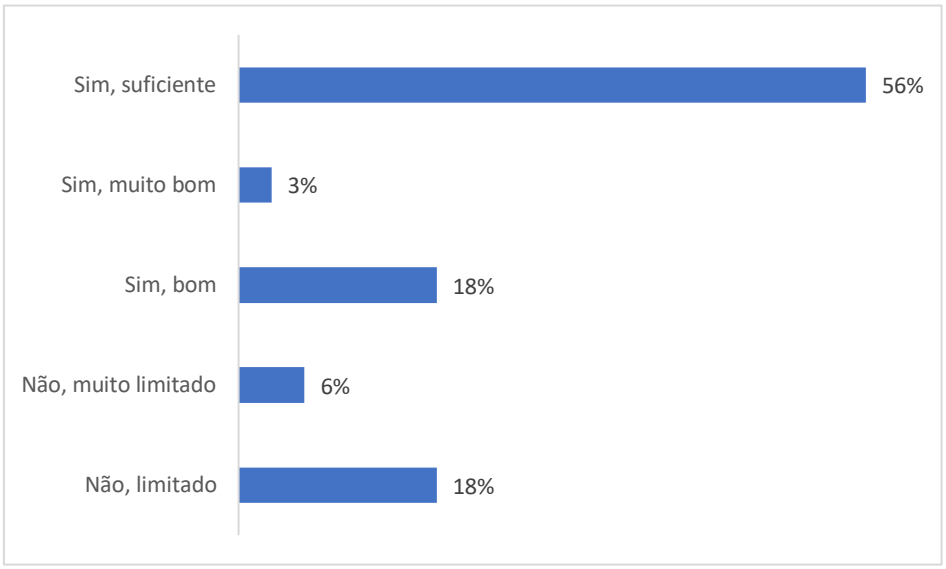


Figura 20 - Perceção das empresas quanto ao nível de conhecimento sobre o regulamento dos/as seus/suas colaboradores/as

Em termos de implementação, 50% das organizações respondeu afirmativamente quanto ao bom nível de implementação do regulamento em contrabalanço com 26% das inquiridas que respondeu negativamente. 24% das organizações não conhece o seu nível de implementação.

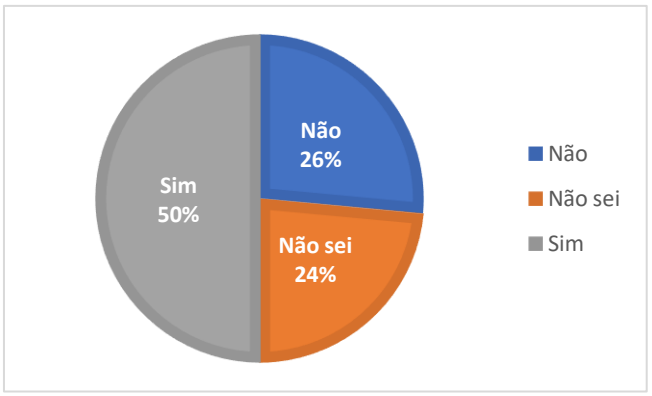


Figura 21 - Perceção das empresas quanto ao nível de implementação do regulamento

Quando apresentado às organizações uma bateria das principais dificuldades na implementação do regulamento com base nos estudos de Carvalho Silva (2019) e de Freitas e Mira da Silva (2018), foi indicada como principal dificuldade das PME a falta de formação (contínua) sobre o tema (RGPD) – 17% do total de dificuldades e, em segundo lugar, a falta de orientações práticas ou de normas de aplicação – 13% do total de dificuldades identificadas.

Seis inquiridos (18% das PME) responderam que não apresentam dificuldades na implementação do regulamento.

Figura 22 - Principais dificuldades das PME na implementação do regulamento

Relativamente aos principais desafios que as empresas percecionam em relação à conformidade com o RGPD, estes são "definição de processos" e "gestão do consentimento" (25% e 21%, respetivamente). A opção "Outro" não obteve nenhuma resposta.

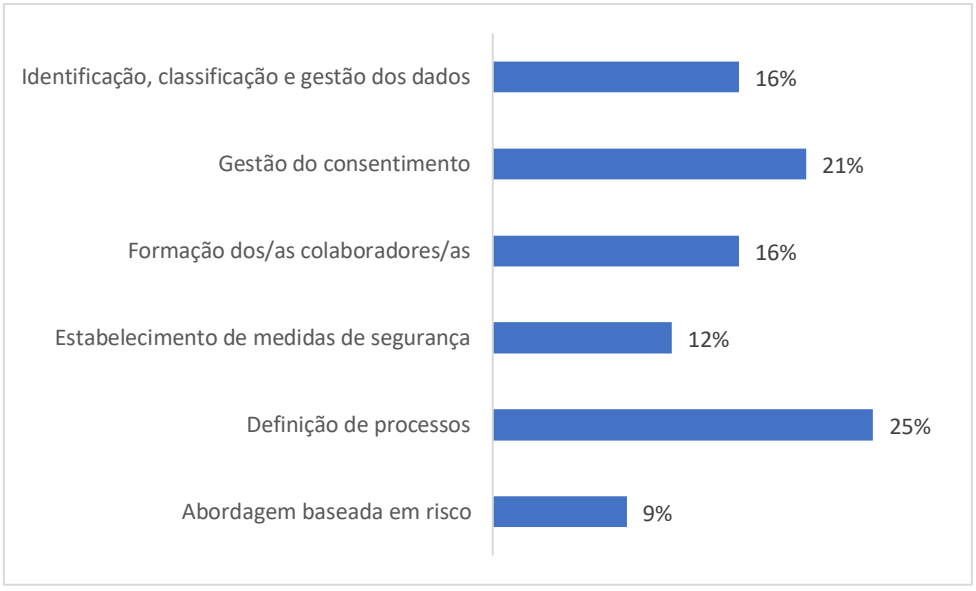


Figura 23 - Principais desafios que as PME percecionam em relação à conformidade com o RGPD

A concluir esta secção, relativamente aos principais benefícios do RGPD, foi indicado que a "garantia da confiança dos clientes" era o mais importante, tendo sido referido por 74% das organizações inquiridas (25 PME), correspondendo a 40% da totalidade das respostas. "Redução do risco sancionatório" foi a segunda opção mais observada, com 13 respostas (38% das organizações que participaram no inquérito), ou seja, 21% da totalidade das respostas obtidas.

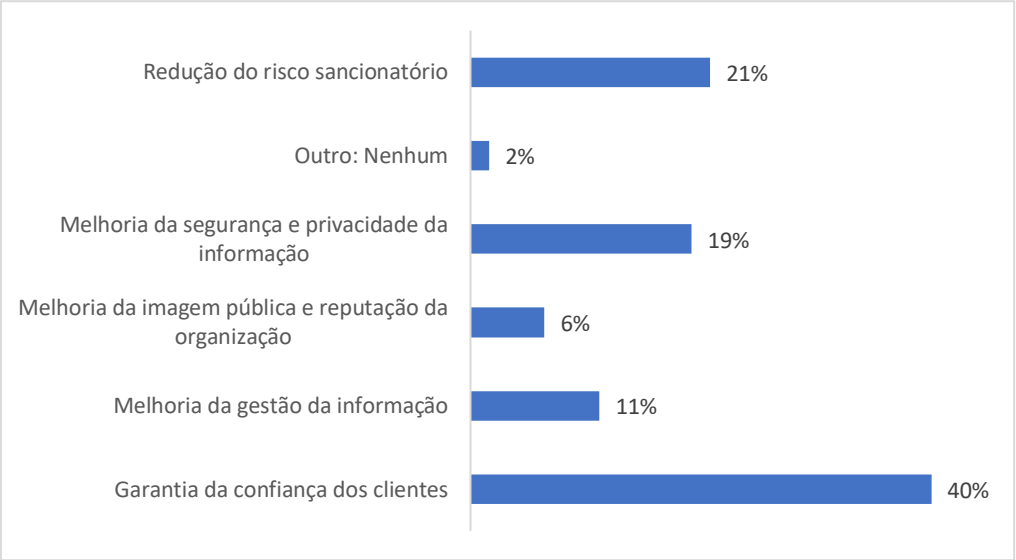


Figura 24 - Principais benefícios do RGPD para as empresas

5.1.5 – Implementação do RGPD em PME

Nesta secção questionaram-se os inquiridos quanto ao conhecimento sobre a ENISA – Agência da União Europeia para a Segurança de Redes e Informações, e as suas orientações para as PME. Apenas 21% dos inquiridos (7 organizações) responderam afirmativamente.

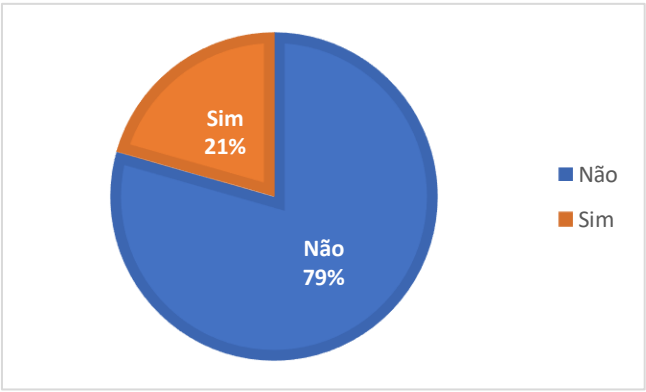


Figura 25 - Conhecimento da ENISA por parte das PME

No que diz respeito aos controlos de segurança da ISO/IEC 27001:2013 e à sua extensão ISO/IEC 27701:2019, relativa à gestão de informações de privacidade, sete (7) foi também o

número de organizações que responderam afirmativamente quando ao seu conhecimento, correspondendo a 21% do total de respostas.

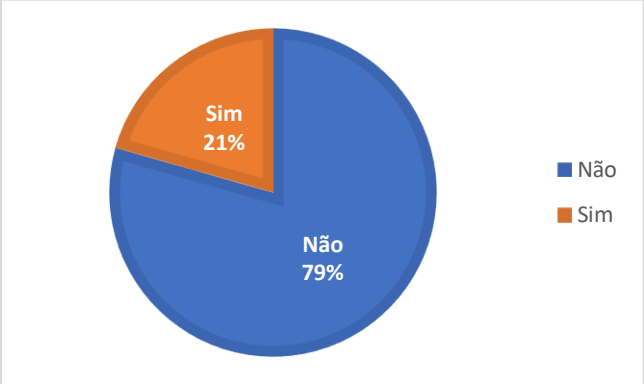


Figura 26 - Conhecimento das ISO 27001:2013 e 27701:2019 por parte das PME

5.1.6 – Próximos passos – PROVA DE CONCEITO

O inquérito às organizações terminou com as perguntas relativas ao início da fase II desta investigação, ou seja, direcionadas à intenção de realizar uma prova de conceito à solução proposta para conformidade, proteção e privacidade dos dados pessoais baseada em sanções jurídicas do RGPD.

Oito das inquiridas respondeu afirmativamente quanto à intenção de realizar um PoC, correspondendo a 24% das respostas.

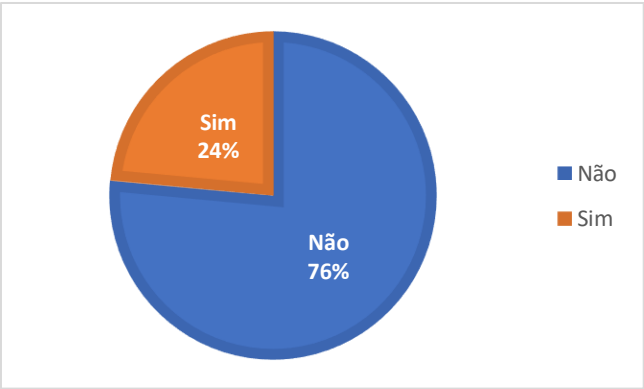


Figura 27 - PME que desejam realizar uma Prova de Conceito da solução proposta para conformidade, proteção e privacidade dos dados pessoais

Contudo, destas oito organizações apenas seis PME disponibilizam os seus dados de identificação que permitiu o seu contacto.

O universo da fase II desenrola-se, portanto, com estas 6 organizações.

5.2 Fase II – Solução para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD

Na fase II, conforme enunciado no Capítulo 3, nomeadamente na tabela 1 – aplicação da metodologia DSR e na figura 3 – Síntese da relação entre as orientações do modelo DSR e as atividades deste trabalho de investigação, pretende-se construir uma solução proposta para conformidade, proteção e privacidade dos dados pessoais, que permita garantir a conformidade legal das PME com o RGPD.

A Fase II, conforme descrito no Capítulo 4, em 4.2, concretizou-se em 4 momentos destintos.

5.2.1 – Proposta inicial de solução

Em primeiro lugar desenvolveu-se uma proposta inicial da solução, de acordo com 4.2.1 do desenho e desenvolvimento, tendo como ponto de partida o documento da ENISA (2016) "Guidelines for SMEs on the security of personal data processing" (Anexo 12), constituída por 4 fases: Avaliação do risco; Tratamento do risco; Aceitação do risco; e Comunicação do risco.

A Avaliação do risco teve como referência a abordagem preconizada pela ENISA para as PME (Anexos 3, 4, 5 e 6). Esta abordagem foi densificada pelos esclarecimentos da Comissão Nacional de Proteção de Dados (CNPD), nomeadamente os respeitantes à caracterização geral da organização, classificação das categorias de dados, fundamento de licitude e classificação dos destinatários para que, tanto quanto possível, as PME portuguesas possam estar alinhadas ao modelo de registo das atividades de tratamento disponibilizado pela CNPD em especial para as Micro, Pequenas e Médias empresas (CNPD, 2019) – Etapa 0: Caracterização geral do 4.2.1.1 – Avaliação do risco (Anexo 3).

Esta proposta inicial, no contexto da fase Tratamento do risco (4.2.1.2 do Capítulo 4) inclui um mapeamento do conjunto de medidas proposto pela ENISA com os controlos de segurança da ISO/IEC 27001:2013, relativo à segurança da informação (ENISA, 2016, pág.33). Adicionalmente, e tendo em conta a extensão da ISO/IEC 27001:2013 (e ISO/IEC 27002:2013) para a gestão de informações de privacidade – ISO/IEC 27701:2019, analisaram-se as relações entre ambos e também com os requisitos do RGPD.

Para garantir a completude do regulamento, foram desenvolvidos novos controlos, iniciativa alinhada com as recomendações da ENISA previamente enunciadas (ver Anexo 7).

Num total de 184 medidas de segurança, 118 são controlos da abordagem da ENISA e 66 controlos foram criados no âmbito deste trabalho, para garantir a completude do regulamento.

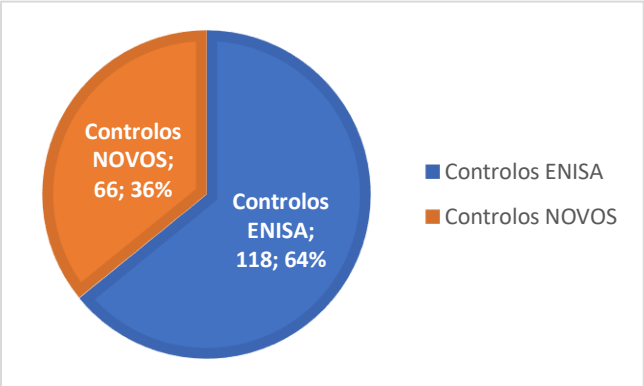


Figura 28 - Medidas de segurança da solução proposta para conformidade, proteção e privacidade dos dados pessoais

Também na fase de Tratamento do risco foram desenvolvidas propostas para as não conformidades das medidas de segurança, de acordo com 4.2.1.2 do Capítulo 4 – ver Anexo 8.

Na fase de Aceitação do risco (4.2.1.3 do desenho e desenvolvimento) foi desenvolvido um fator de priorização das várias tarefas incluídas no plano de tratamento, tendo em consideração as sanções jurídicas do RGPD, enquanto critério de tomada de decisão – ver Anexo 9.

Especificamente para as PME, os artigos do RGPD mais referenciados nas multas existentes no Espaço Económico Europeu (Anexo 10), são:

- ✓ Artigo 5º - princípios relativos ao tratamento de dados pessoais (105 vezes, representando o total de 30%);
- ✓ Artigo 6º - licitude do tratamento (64 vezes, representando o total de 18%);
- ✓ Artigo 32º - segurança do tratamento (37 vezes, representando o total de 11%);
- ✓ Artigo 13º - informações a facultar quando os dados pessoais são recolhidos junto do titular (35 vezes, representando o total de 10%);
- ✓ Artigo 58º - poderes das autoridades de controlo (20 vezes, representando o total de 6%).

Estes 5 artigos representam 75% do total.

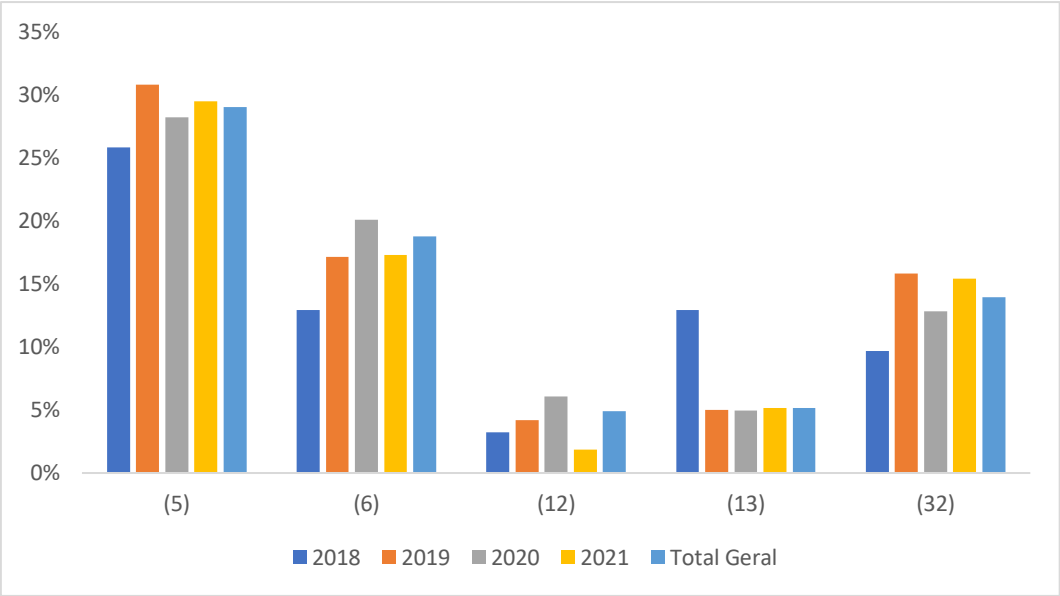


Figura 29 - Artigos RGPD mais identificados nas multas a PME

Deste modo, as 10 medidas mais críticas, tendo em consideração a relação dos artigos do RGPD e as medidas de segurança e o fator de priorização com base nas sanções jurídicas, são:

ID.C	ID Medida	Descrição da Medida	Nível de Risco	Obs:
4.1	F.2	Ao identificar uma violação de dados pessoais, o subcontratante deve notificar o responsável pelo tratamento sem demora injustificada.	Baixo	ENISA
4.1	F.3	Os requisitos e as obrigações devem ser formalmente acordadas entre o responsável pelo tratamento e o subcontratante. O subcontratante deve fornecer evidências de conformidade suficientemente documentadas.	Baixo	ENISA
4.1	F.5	Os funcionários do subcontratante, que tratam dados pessoais, devem estar sujeitos a acordos de confidencialidade /de não divulgação, específicos e devidamente documentados.	Alto	ENISA
4.1	U.1.1	Deve haver um processo atualizado de todos os requisitos legais e contratuais ajustado à natureza da organização e aos seus sistemas de TI.	Baixo	NOVO
4.1	V.1.2	A licitude do tratamento de dados pessoais deve ser identificada e documentada para que seja possível demonstrar que a legalidade do tratamento foi devidamente estabelecida antes do mesmo ocorrer.	Baixo	NOVO
4.1	V.2.2	Dependendo das obrigações legais e contratuais, a organização determina os requisitos que devem constar nas informações fornecidas aos titulares dos dados, tanto ao nível do seu conteúdo como ao nível da sua tempestividade.	Baixo	NOVO
4.1	V.3.1	A organização deve limitar a recolha de dados pessoais apenas ao que é necessário relativamente às finalidades identificadas.	Baixo	NOVO
4.1	V.3.4	A organização deve definir e documentar os objetivos de minimização de dados e como é que os dados pessoais são limitados às finalidades do tratamento, bem como quais os mecanismos utilizados para alcançar a minimização dos dados (ex: técnicas de desidentificação).	Baixo	NOVO
4.1	V.3.5	A organização deve eliminar ou apresentar os dados pessoais de uma forma que não permita a sua identificação ou reidentificação, assim que os mesmos não sejam mais necessários para a(s) finalidade(s) do tratamento.	Baixo	NOVO
4.1	W.1.2	A organização deve garantir que os dados pessoais tratados em nome de um cliente ocorrem apenas mediante instruções documentadas do responsável pelo tratamento, limitadas às finalidades previstas.	Baixo	NOVO

Tabela 2 - As 10 medidas de segurança principais, tendo em conta o fator de priorização com base nas sanções jurídicas

Relativamente à fase de Comunicação do risco (4.2.1.4 deste trabalho de investigação) foi desenvolvido na solução um espaço onde se pode gerir quais as partes interessadas que devem ser informadas sobre as decisões tomadas, que controlos foram adotados, que riscos foram aceites, bem como quais os próximos passos – ver Anexo 12.

5.2.2 – Fase de testes – desenvolvimento da Prova de Conceito junto das PME

A Prova de Conceito permitiu testar em contexto real a proposta inicial da solução. As organizações foram definidas através do inquérito "Impacto do RGPD nas Organizações" – Fase 1 da metodologia deste trabalho (Anexo 1), através da resposta afirmativa à pergunta número 25: PME que desejam realizar uma Prova de Conceito da solução proposta para a proteção da privacidade e dos dados pessoais (Figura 27). No total participaram 6 organizações.

O PoC concretizou-se em três fases: Iniciação; Planeamento e Análise; e Fecho do Projeto, e decorreu entre os dias 14 de abril e 10 de maio de 2021.Relativamente ao preenchimento da Fase 1 – Iniciação – Identificação da PME, obtiveram-se os seguintes resultados (Anexo 14):

- Das organizações que participaram, quatro têm morada em Lisboa e duas têm morada no Porto;

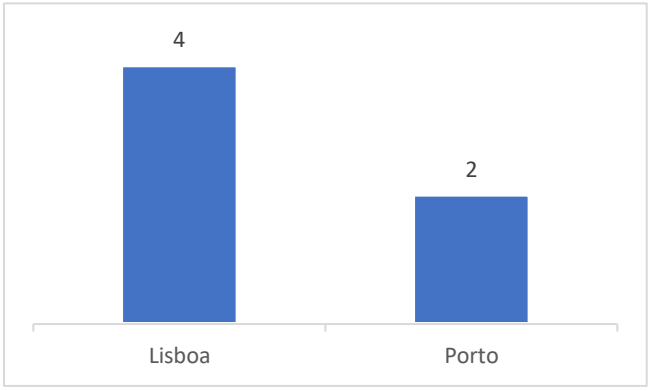


Figura 30 - Morada das organizações participantes no PoC

- Os inquiridos foram maioritariamente os proprietários das próprias organizações (5 respostas). Na outra PME a função dentro da empresa é de gestor/a;

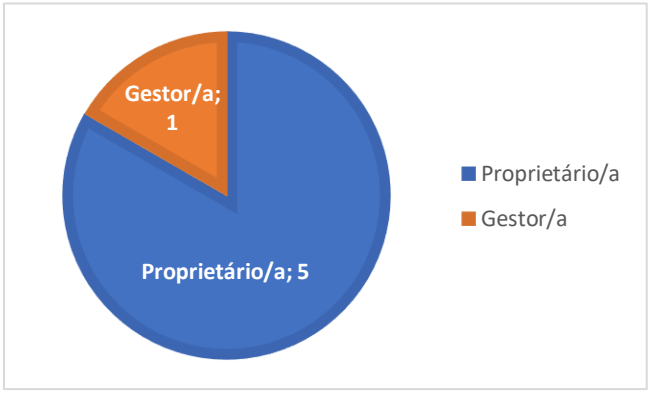


Figura 31 - Função do responsável da PME dentro da empresa

- Em todas as PME que participaram no PoC, o responsável da organização é também responsável pela implementação do RGPD;

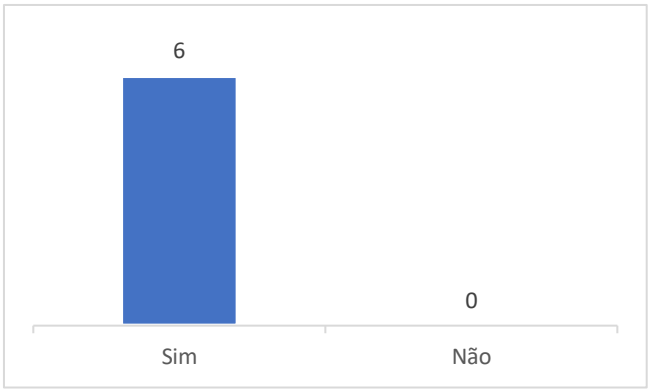


Figura 32 - Função de responsável pela implementação do RGPD pelo responsável da PME

De acordo com as respostas obtidas na Fase I (Anexo 13), as organizações que participaram no PoC são:

- Em termos de dimensão, quatro são microempresa e duas são pequenas empresas;

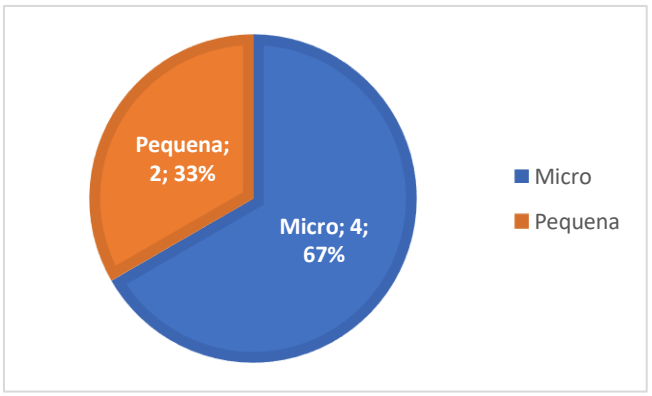


Figura 33 - Dimensão da PME participante no PoC

- Relativamente à antiguidade: 4 têm entre 6 e 19 anos, uma tem menos de 5 anos e outra empresa que participou tem mais de 20 anos;

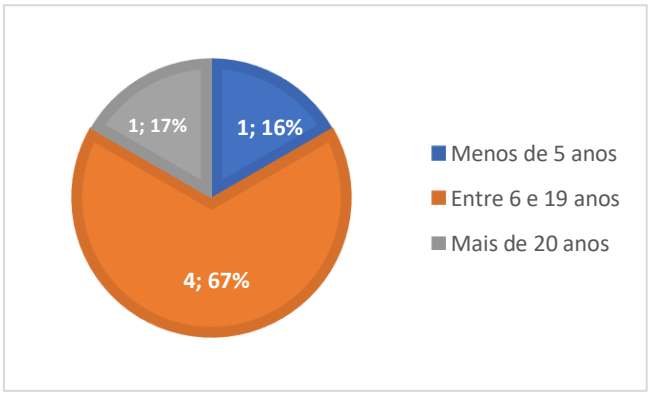


Figura 34 - Antiguidade da PME participante no PoC

- Em termos de setor de atividade, uma organização participante no PoC é do setor da construção enquanto que as restantes organizações são de "outros setores".

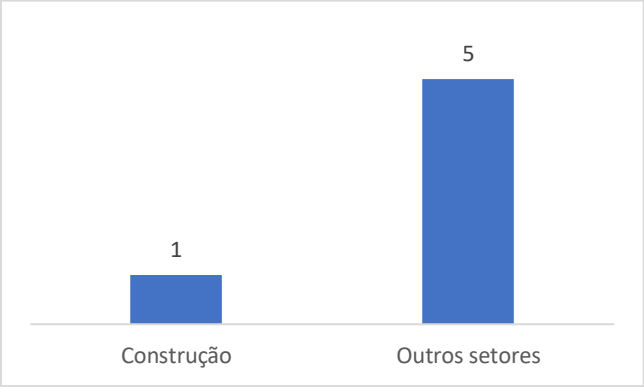


Figura 35 - Setor de atividade da PME participante no PoC

A Fase 2 – Planeamento e Análise, decorreu no período compreendido entre os dias 16 de abril e 5 de maio, conforme proposta de data da Fase 1, num total de 6 reuniões.

Enquanto concretização da Fase 2 – Planeamento e Análise, obtiveram-se os seguintes resultados (Anexo 14), organizados em plano de projeto e plano de recursos:

Sob o ponto de vista do plano de projeto, a definição do âmbito teve como resposta dominante tratamentos de dados pessoais relacionados com campanhas de marketing (3 respostas). Gestão de clientes e recrutamento e seleção de Recursos Humanos foram temas também considerados (Figura 36).

Duas respostas estão também ligadas à relação com clientes; por um lado, na relação de negócio / gestão de clientes individuais/singulares e, por outro lado, na relação com clientes corporativos, na componente de gestão de eventos que envolve a emissão de certificados de participação, produção de brindes personalizados e/ou reportagens fotográficas. Recrutamento e seleção de Recursos Humanos foi outro âmbito considerado no PoC.

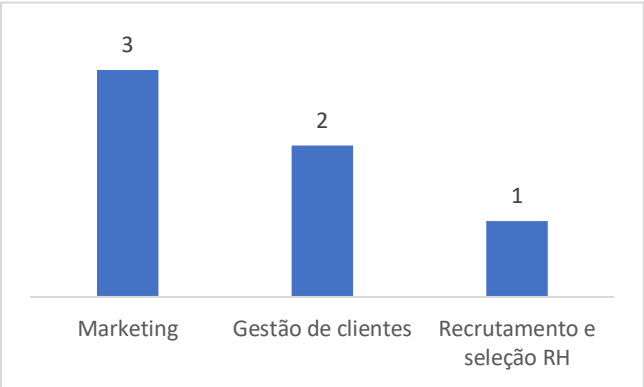


Figura 36 - Definição do âmbito do PoC

Relativamente às entregas previstas durante a realização do PoC, 5 PME indicaram como objetivo o preenchimento da solução proposta para os tratamentos definidos no âmbito,

enquanto que uma PME determinou o seu pré-preenchimento sob o ponto de vista de testar a funcionalidade da solução proposta para conformidade, proteção e privacidade dos dados pessoais.

Em termos do plano de recursos, o/a gestor/a do projeto foi maioritariamente o proprietário da organização (5 respostas). A resposta da outra PME indicou como gestor/a do PoC a pessoa que assume funções de gestão dentro da organização.

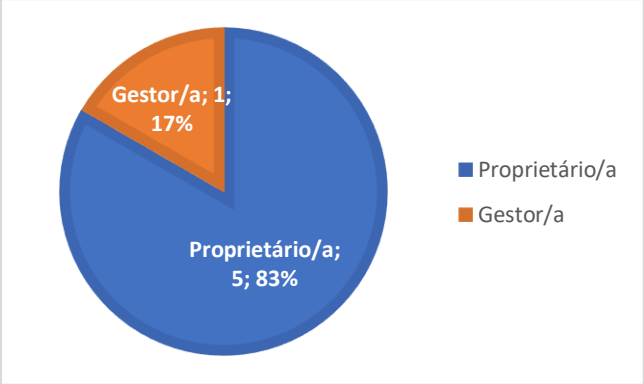


Figura 37 - Função dentro da organização do/a gestor/a do projeto do PoC

A definição da equipa de projeto foi constituída maioritariamente apenas pelo/a próprio/a gestor/a de projeto do PoC. Adicionalmente, duas das PME indicaram como equipa de projeto do PoC outros elementos da organização: responsáveis de Recursos Humanos, Responsável de Estratégia/Marketing e Responsável Financeiro/CFO.

Relativamente à indicação das partes interessadas no PoC, três tipos distintos foram considerados: clientes, parceiros de negócio e pessoas entrevistadas no contexto do recrutamento e seleção de Recursos Humanos.

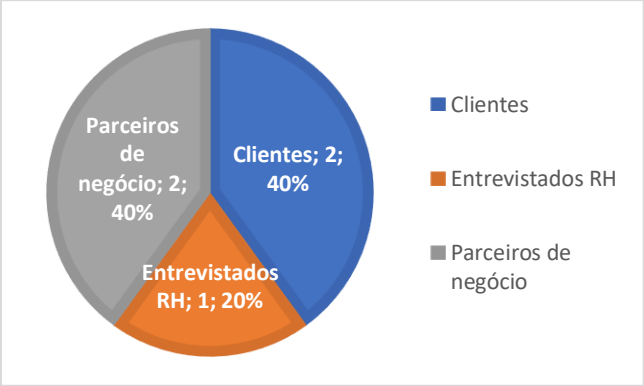


Figura 38 - Partes interessadas no PoC

5.2.3 – Avaliação da Prova de Conceito com as PME

Na fase de conclusão do PoC, o gestor do projeto, consultando a equipa de projeto, finaliza as entregas.

Foram obtidos os seguintes resultados (Fase III – Fecho do Projeto do Anexo 14):

- Todos os participantes consideraram que a apresentação do PoC foi satisfatória;

- Em termos de lições aprendidas com o PoC, as empresas participantes referiram que esta solução proposta para conformidade, proteção e privacidade dos dados pessoais deu condições para considerar o RGPD como uma forma de encarar o serviço. Foi referido também que se verifica a possibilidade de aplicar o RGPD de um modo faseado;

- Cinco das organizações considerou que a definição do âmbito foi ajustada ao PoC;

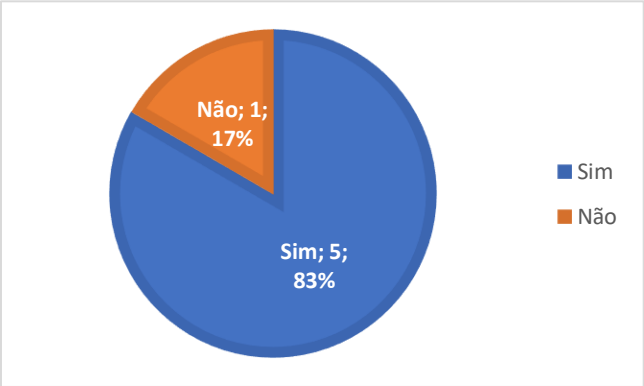


Figura 39 - Concretização do âmbito do PoC

- Alinhado com o tema anterior, uma organização referiu que os prazos definidos não foram cumpridos. As restantes 5 PME consideraram que os prazos foram cumpridos;

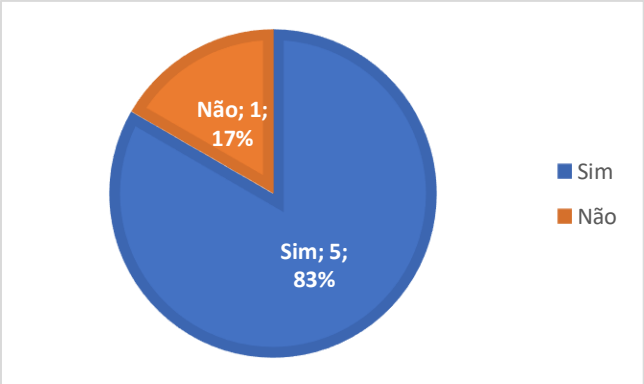


Figura 40 - Cumprimento dos prazos do PoC

- Todas as organizações participantes afirmaram que a duração do PoC foi satisfatória;

- Todas as organizações também afirmaram que a alocação de recursos foi ajustada às necessidades do PoC e à definição do âmbito;

- No que às entregas diz respeito, apenas uma organização considerou que estas não foram cumpridas;

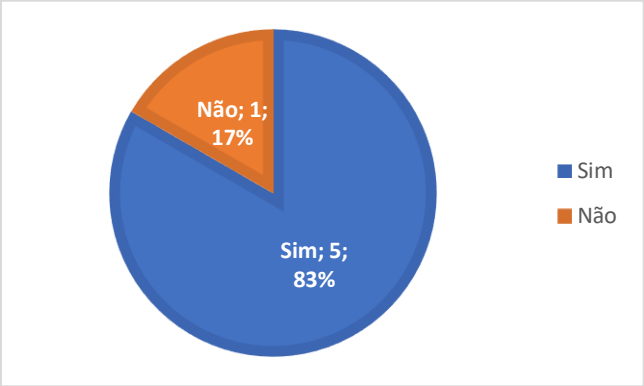


Figura 41 - Cumprimento das entregas do PoC

- De acordo com a pergunta anterior, a organização que indicou que as entregas previstas não foram cumpridas, também referiu que não gostava de ter esta solução implementada em toda a organização na medida em que a sua estrutura tem poucos dados pessoais. As outras 5 PME responderam afirmativamente, que gostavam de ter esta solução implementada em toda a organização.

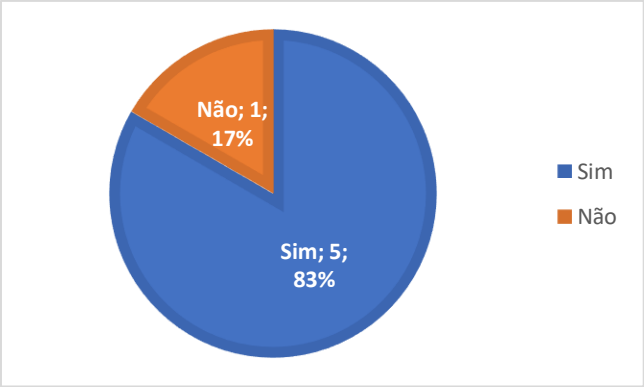


Figura 42 - PME que gostavam de ter esta solução implementada em toda a organização

No que diz respeito à própria solução alvo do PoC, as organizações apresentaram as seguintes propostas de melhoria / e comentários, para as suas quatro etapas:

- Etapa de Avaliação do risco:
  - *Há perguntas formuladas na negativa que tornam difícil o preenchimento;*
  - *Muito bem explicado.*

- Etapa de Tratamento do risco:
  - *A componente visual deveria estar mais simplificada. Tem muita informação. A informação deveria ser apresentada apenas quando é necessária;*

- *Está bem conseguido. Está simples e concreto. Relaciona-se diretamente com os artigos do RGPD;*
- *Muito bem explicado.*

- Etapa de Aceitação do risco:
  - *Muito bem explicado. O Ranking (fator de priorização, com base nas sanções jurídicas) faz sentido na medida em que ajuda a tomar decisões / começar a trabalhar;*
  - *Está bem conseguido. Ajuda a tomar decisões e apresenta propostas de solução. As medidas estão associadas ao RGPD, o que dá segurança / conforto a quem toma decisões perante as questões que surgem na organização. Esta etapa ajuda também a priorizar / tomar decisões de acordo com os diferentes níveis de risco;*
  - *A componente visual deveria estar mais simplificada. Tem muita informação. A informação deveria ser apresentada apenas quando é necessária;*
  - *A componente de aceitação poderia ter uma vertente financeira associada às opções de melhoria, para além do ranking das multas;*
  - *Impecável. Sem dúvidas de interpretação.*

- Etapa de Comunicação do risco:
  - *Tudo óbvio: ligado aos procedimentos a aplicar em caso de risco efetivo;*
  - *Muito bem explicado;*
  - *Também a componente visual, mas não tão relevante como nas etapas anteriores;*
  - *Sem comentários: numa PME, a comunicação é algo intrínseco visto haver poucos recursos e haver comunicação fluída.*

A nível global verifica-se uma aceitação da proposta, tendo sido obtido os resultados de "bom" e "muito bom" em termos de satisfação global do PoC.

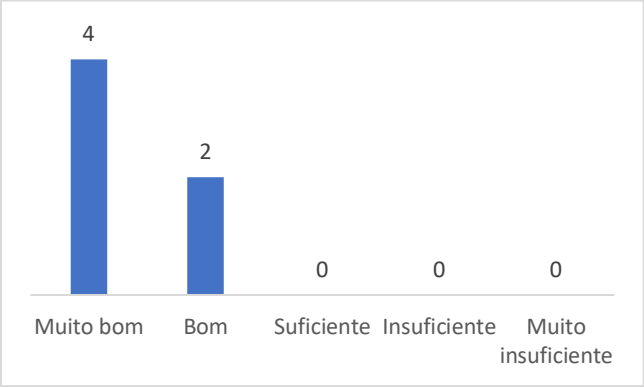


Figura 43 - Nível global de satisfação do PoC

A finalizar, relativamente a outras recomendações sobre como proceder numa implementação completa no contexto da organização e enquanto comentários finais, foi respondido que:

- *É importante envolver todos os decisores no processo global de implementação, ao contrário do PoC;*
- *Faz falta este tipo de iniciativas no contexto da organização;*
- *A ocorrer uma implementação completa, esta deverá ser faseada, para todos os tratamentos existentes;*
- *Pode ser pertinente implementar o PoC, de um modo global, transformado numa solução web-based, que facilita a sua aplicação a todos os utilizadores que tenham acesso ao mesmo;*
- *É um processo complexo, nomeadamente para as empresas que não estão por dentro deste tema;*
- *Foi enriquecedor participar neste estudo e perceber que mesmo para baixos riscos que as organizações enfrentam, é fundamental garantir a sua resolução e prevenção.*

5.2.4 – Apresentação da solução para Conformidade, Proteção e Privacidade dos dados pessoais

Após solução proposta para conformidade, proteção e privacidade dos dados pessoais baseada em sanções jurídicas do RGPD, desenvolvimento da Prova de Conceito e sua avaliação, é, de acordo com o ponto 4.2.4 deste trabalho de investigação, construída a proposta final de solução para conformidade, proteção e privacidade dos dados pessoais.

Os resultados do PoC evidenciam os seguintes aspetos de alteração, de acordo com a análise às quatro fases da proposta, de acordo com o ponto 5.2.3:

- Etapa de Avaliação do risco:
    - *Há perguntas formuladas na negativa que tornam difícil o preenchimento;*

      A formulação pela negativa é a forma como a ENISA considerou na sua ferramenta de gestão do risco. Não foi alvo deste trabalho alterar as orientações da ENISA. Contudo, para trabalhos futuros, sugere-se que se adapte a redação das questões existentes na etapa de avaliação do risco.

- Etapas de Tratamento do risco, de Aceitação do risco e de Comunicação do risco:
    - *A componente visual deveria estar mais simplificada. Tem muita informação. A informação deveria ser apresentada apenas quando é necessária;*

      Conforme desenvolvimento desta solução proposta, no ponto de outras recomendações e nos comentários finais, e na Etapa de Aceitação do risco, uma PME propôs a transformação desta proposta numa solução web-based. Neste sentido, propõe-se para trabalhos futuros o desenvolvimento da proposta alinhado a um ambiente gráfico mais amigável do utilizador final, que permita apresentar apenas a informação essencial, remetendo para segundo plano a componente de suporte e seu conteúdo explicativo.

- Etapa de Aceitação do risco:
    - *A componente de aceitação poderia ter uma vertente financeira associada às opções de melhoria, para além do ranking das multas;*

      Considera-se a observação relativa à vertente financeira associada às opções de melhoria, para além do ranking das multas, muito pertinente para a tomada de decisão das organizações. Ou seja, para além da componente do âmbito deste trabalho de investigação – as sanções jurídicas – verifica-se que a determinação do custo de aplicação/investimento pode também ajudar a tomar decisões. Neste sentido, e tendo em conta a necessidade de auscultar o mercado para todo um cenário de propostas de melhoria, propõe-se que para trabalhos futuros se possa desenvolver uma nova variável de tomada de decisão para a implementação do RGPD nas organizações, numa vertente financeira.

Relativamente a outras recomendações sobre como proceder numa implementação completa no contexto da organização e enquanto comentários finais, foi respondido que:

- *Pode ser pertinente implementar a proposta de um modo global transformando o PoC numa solução web-based que facilita a sua aplicação, aumentando a integridade dos processos e permitindo a escalabilidade da solução.*

De acordo com os pontos enunciados acima, relativos à fase de teste e avaliação da Prova de Conceito, verifica-se que as propostas de melhoria são materialmente significativas, carecendo de grandes desenvolvimentos, podendo ser, elas próprias, assunto para trabalhos futuros.

Atendeu-se, deste modo, que a solução proposta no âmbito deste trabalho, não deva sofrer alterações nem correções. Posto isto, solução final para a conformidade, proteção e privacidade dos dados pessoais é a solução proposta inicialmente (Anexo 12), remetendo-se, portanto, para trabalhos futuros os pontos referidos acima.

Capítulo 6 – Avaliação e Demonstração dos resultados

6.1 Fase I – Impacto do RGPD nas Organizações – PME

O inquérito "Impacto do RGPD nas Organizações – PME" (ver Anexo 1) teve como referência os estudos mencionados em 4.1, Capítulo 4 – Desenho e Desenvolvimento, nomeadamente os trabalhos de Freitas e Mira da Silva (2018), de Teixeira et al (2019) e de Carvalho Silva (2019).

Outros dois documentos foram considerados na construção do inquérito às PME, a saber: o estudo desenvolvido pela IDC para a Microsoft Portugal (2018) e o Inquérito que o INE – Instituto Nacional de Estatística, realizou relativo à utilização de tecnologias da informação e da comunicação nas empresas (INE, 2020).

Neste trabalho de investigação participaram 34 organizações. Os resultados encontram-se no Anexo 13. 65% das entidades que participaram correspondem a microempresas, 26% a pequenas empresas e 9% a médias empresas, de acordo com a Figura 5 – Dimensão da PME, do ponto 5.1.1 Caracterização da PME, do Capítulo 5 – Resultados obtidos.

Em termos de setor de atividade – Figura 8, a resposta dominante foi a opção "outros setores", correspondendo a 62% das observações. As tipologias de referência utilizadas foram as existentes em Pordata (2021), para a classificação das PME por setores de atividade. Verifica-se, pelas respostas obtidas, um não alinhamento ao pretendido, onde a opção "outros setores" deveria ser respondido apenas de modo residual. Admite-se que as organizações inquiridas não se identificaram com as tipologias apresentadas.

Os inquiridos foram maioritariamente gestor/a e proprietário/a, correspondendo a 60% das respostas obtidas – Figura 9. Verificaram-se, portanto, respostas dos responsáveis pelas organizações – os mesmos que indicaram que têm responsabilidades na implementação do RGPD – Figura 10. A figura 5 – Dimensão da PME – indica que 65% das entidades inquiridas são microempresas. Pode-se verificar uma semelhança na ordem de grandeza entre inquiridos responsáveis pelas organizações e pelo RGPD e o tamanho das organizações. Ou seja, quanto mais pequena é uma organização, mais concentradas se encontram as responsabilidades. Aquando da Prova de Conceito – Fase II, verificou-se que as microempresas participantes tinham como pessoa responsável pelo RGPD o/a próprio/a responsável pela organização.

Relativamente à utilização de tecnologias da informação e comunicação, tendo como ponto de partida o Inquérito que o INE realizou relativo à utilização de tecnologias da informação e da comunicação nas empresas (INE, 2020), o grupo de empresas que participou neste inquérito referiu que 76% das empresas tem website próprio ou do grupo económico a que pertence (Figura 12), alinhado com o estudo do INE que indica o valor de dois terços, conforme o ponto 2.2 As PME no contexto nacional, do Capítulo 2 – Revisão da Literatura.

82% das PME – Figura 14, responderam que têm serviços de computação em nuvem na internet, como é o caso de serviços de correio eletrónico ou armazenamento de ficheiros, demonstrando um grande desfasamento quanto às respostas obtidas no inquérito do INE (2020), onde a percentagem de empresas que compram serviços de computação em nuvem na internet foi de 29%.

Em termos de utilização de serviços de big data – Figura 15, apenas 12% (4 organizações) respondeu afirmativamente. 56% respondeu que não utiliza e 32% respondeu que não sabe. No estudo do INE (2020), 10,2% das empresas inquiridas, que têm 10 ou mais pessoas ao serviço, responderam afirmativamente quanto à utilização de serviços de big data.

50% das empresas inquiridas referiu que tem pessoal especialista em TIC (Tecnologias de Informação e Comunicações) – Figura 16. O estudo do INE (2020) indicou que apenas 22,9% de empresas tem pessoal ao serviço especialista em TIC. Admite-se que esta divergência, tendo em conta as entrevistas realizadas às organizações em momento de Fase II – Prova de Conceito, diz respeito ao entendimento da pergunta, onde algumas organizações consideraram pessoal especialista em TIC os prestadores de serviços TIC que possuem.

47% das respostas foram afirmativas quanto à utilização de dispositivos ou sistemas interconectados que podem ser monitorizados ou controlados remotamente através da Internet (IoT) – Figura 17. Para a mesma pergunta, o estudo do INE (2020) indicou o valor de 13% de empresas que beneficiam do IoT.

As PME inquiridas responderam massivamente que têm conhecimento do que é o RGPD – 94%, representando 32 entidades em 34 possíveis – ver Figura 18. Carvalho Silva (2019) referiu no seu estudo que a maioria das PME portuguesas (96,3%) têm conhecimento do que é o RGPD, sendo que 52,7% só tiveram conhecimento em 2018. Refere também que as microempresas foram aquelas que tiveram um conhecimento mais tardio sobre o RGPD. No inquérito realizado no âmbito deste trabalho, 72% do total das PME responderam que tiveram conhecimento antes ou durante o ano de 2018 – Figura 19.

Relativamente à perceção que as organizações e os/as seus/suas representantes têm quanto ao nível de conhecimento que os/as seus/suas colaboradores/as têm sobre o regulamento, 56% respondeu que o nível é suficiente; 21 % respondeu que o nível de conhecimento é bom/muito bom e 24% respondeu que o nível de conhecimento é limitado/muito limitado – Figura 20. O estudo de Carvalho Silva (2019) referiu que mais de metade dos inquiridos consideram ter um bom ou muito bom nível de conhecimento sobre o regulamento. Verifica-se uma divergência nas respostas, designadamente, 21% bom/muito bom neste inquérito em relação a um valor superior a 50% de Carvalho Silva (2019). A análise realizada, por observação das PME na Fase II deste trabalho – Prova de Conceito – conclui que as organizações estão mais prudentes e conscientes das muitas tarefas a que o RGPD obriga, refletindo-se na forma como responderam a esta pergunta, quase 3 anos depois da entrada em vigor do regulamento, alinhada à pergunta da Figura 22, onde se destaca a falta de formação sobre o tema RGPD como principal dificuldade das PME na implementação do regulamento (17%).

Em segundo lugar – ver Figura 22, encontra-se a falta de orientações e práticas ou de normas de aplicação, representando 13% do total de dificuldades identificadas. Carvalho Silva (2019), no seu estudo, indicou que as principais dificuldades das PME na implementação do RGPD foram, também, a falta de conhecimento sobre o regulamento e a falta de Recursos Humanos (46% e 22%, respetivamente). Noutro estudo realizado no contexto português, Freitas e Mira da Silva (2018) reforçam a necessidade de definir uma metodologia para poder cumprir as obrigações do RGPD, considerando a análise realizada a dez PME nos distritos de Lisboa,

Aveiro e Leiria, onde se identificou a falta de conhecimento dessas empresas sobre as suas obrigações e deveres em relação à proteção de dados pessoais.

A "formação a colaboradores" é também uma das conclusões do estudo desenvolvido pela IDC para a Microsoft Portugal (Microsoft, 2018). Ou seja, estes estudos independentes apresentam conclusões semelhantes quanto à necessidade de formação aos colaboradores das PME no que ao RGPD diz respeito.

Relativamente aos principais desafios que as empresas percecionam em relação à conformidade com o RGPD – Figura 23, estes são "definição de processos" e "gestão do consentimento" (25% e 21%, respetivamente). A opção "Outro" não obteve nenhuma resposta. Quando comparado com o estudo desenvolvido pela IDC para a Microsoft Portugal (Microsoft, 2018), de acordo com o ponto 2.3 - As PME portuguesas e o RGPD, verifica-se que "definição dos processos" é também o desafio mais referenciado.

Quanto aos principais benefícios do RGPD – Figura 24, foi indicado que a "garantia da confiança dos clientes" era o mais importante, tendo sido referido por 74% das organizações inquiridas (25 PME), correspondendo a 40% da totalidade das respostas. "Redução do risco sancionatório" foi a segunda opção mais observada, correspondendo a 13 respostas (38% das organizações que participaram no inquérito), refletindo 21% da totalidade das respostas obtidas. A opção "Outro" foi referida uma vez, tendo sido indicado que não há nenhum benefício do RGPD na organização. Relativamente ao estudo da IDC para a Microsoft Portugal (2018) tinha sido indicado como principal benefício a "melhoria da segurança e privacidade da informação".

Na secção 4.1.5 do inquérito – Implementação do RGPD em PME, quanto ao conhecimento sobre a ENISA – Agência da União Europeia para a Segurança de Redes e Informações, e as suas orientações para as PME, no sentido de ajudá-las a avaliar os riscos de segurança e, consequentemente, adotar medidas de segurança para a proteção de dados pessoais e garantir a conformidade com o RGPD, quanto ao conhecimento dos controlos de segurança da ISO/IEC 27001:2013 e sobre a extensão da ISO/IEC 27001 para a gestão de informações de privacidade – ISO/IEC 27701:2019, apenas 21% dos inquiridos (7 organizações) responderam afirmativamente – ver Figura 25.

Foram também 7 as organizações que responderam afirmativamente quanto ao seu conhecimento sobre os controlos de segurança das ISO 27001:2013 e 27701:2019 – Figura 26.

O inquérito terminou com um convite às organizações para a participação na FASE II – Prova de Conceito – Figura 27. Cerca de um quarto das organizações (24%) aceitou.

Não obstante a relevância e a pertinência em verificar o impacto do RGPD nas organizações quase 3 anos depois da sua entrada em vigor, designadamente nas PME portuguesas, o desenrolar deste exercício permitiu identificar um grupo de organizações interessadas em testar uma solução proposta para conformidade, proteção e privacidade dos dados pessoais baseada em sanções jurídicas do RGPD.

6.2 Fase II – Solução para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD

Como referido em 5.2 do Capítulo 5 – Resultados obtidos, pretende-se construir uma solução para a conformidade, proteção e privacidade dos dados pessoais que permita garantir a conformidade legal das PME com o RGPD, consubstanciado à metodologia DSR, de acordo com o Capítulo 3.

Esta solução deriva, por um lado, da verificação de que as Pequenas e Médias Empresas não dispõem de recursos ou conhecimentos para gerir modelos de referência para a conformidade com o RGPD, de acordo com Brodin (2019), e de que os modelos de referência também podem considerar as tendências das autoridades como critério para a tomada de decisão e de priorização, na medida em que o tratamento de dados está constantemente ameaçado devido a vários desafios, conforme Chatzipoulidis et al (2019), enunciados em 2.1 Modelos de referência para a conformidade com o RGPD, do Capítulo 2 – Revisão da Literatura.

Verifica-se também, de acordo com a mesma Revisão da Literatura que no contexto português há a necessidade de definir uma metodologia para poder cumprir as obrigações do RGPD, Freitas e Mira da Silva (2018).

Por outro lado, e de acordo com a importância da atualização dos estudos do impacto do RGPD nas organizações, realizados pelos autores referidos em 2.3 - As PME portuguesas e o RGPD, esta solução proposta deriva também dos resultados obtidos na Fase I – Impacto do RGPD nas Organizações, nomeadamente ao nível das principais dificuldades das PME na implementação do regulamento (Figura 22), os principais desafios que as PME percecionam em relação à conformidade com o RGPD (Figura 23), e principais benefícios do RGPD para as empresas (Figura 24) do Capítulo 5, e ponto 6.1 do Capítulo 6.

Ou seja, a solução proposta permite, ela própria, ser um mecanismo prático de aplicação do RGPD, orientado para o cumprimento do regulamento, possibilitando a identificação dos dados alvo de tratamento e, de acordo com a possibilidade de autopreenchimento por via dos diversos textos explicativos, permite também aumentar o nível de conhecimento dos/as colaboradores/as das PME. Neste sentido, a proposta concorre para a resposta às principais dificuldades sentidas pelas PME que participaram no trabalho de investigação da Fase I, na implementação do regulamento (Figura 22).

Relativamente aos principais desafios que as PME percecionaram (Figura 23), a definição de processos foi o mais referido. Tendo em conta que a etapa "Definição da operação de tratamento e seu contexto" é o ponto de partida da avaliação do risco (ENISA, 2017, pág.10) – Fase 1 da solução, considera-se que a utilização da ferramenta da ENISA, parte integrante da solução, permite apoiar as PME na definição dos seus processos e, consequentemente, na concretização dos passos seguintes que o regulamento exige.

Para além da base do processo de gestão do risco corresponder às orientações da ENISA, alguns pontos da metodologia foram densificados com outros inputs, nomeadamente com esclarecimentos da Comissão Nacional de Proteção de Dados (CNPD) e da Organização Internacional de Normalização (ISO), mais propriamente através dos documentos ISO/IEC 27001:2013, ISO/IEC 27002:2013 e ISO/IEC 27701:2019. Ou seja, esta integração aumenta a confiança do processo, melhora o nível de segurança e privacidade da informação e reduz o

risco sancionatório pelo facto da proposta incluir um fator de priorização com base nas sanções jurídicas do RGPD. Portanto, a solução permite às PME concretizarem os benefícios que o RGPD traz às empresas, de acordo com as respostas ao Inquérito da Fase I (Figura 24).

Abaixo, apresenta-se a discussão e análise dos resultados obtidos na Fase II.

6.2.1 – Discussão e análise dos resultados - Proposta inicial de solução

Esta proposta inicial, no contexto da fase Tratamento do risco (4.2.1.2 do Capítulo 4) inclui um mapeamento do conjunto de medidas proposto pela ENISA com os controlos de segurança da ISO/IEC 27001:2013, relativo à segurança da informação (ENISA, 2016, pág.33). Adicionalmente, e tendo em conta a extensão da ISO/IEC 27001:2013 (e ISO/IEC 27002:2013) para a gestão de informações de privacidade – ISO/IEC 27701:2019, analisaram-se as relações entre ambos e também com os requisitos do RGPD.

Deste modo, verificou-se, por um lado, relações diretas entre as medidas preconizadas pela ENISA e o cumprimento do RGPD, mas também se verificaram lacunas no cumprimento integral do regulamento.

Para garantir a completude do regulamento, foram desenvolvidos novos controlos (66) – Figura 28, iniciativa alinhada às recomendações da ENISA previamente enunciadas (ver Anexo 7). Por estar em causa a completude do regulamento, o nível de risco das novas medidas é sempre o mais baixo, para permitir a conformidade legal em todos os níveis de risco. Concretiza-se, também por esta via, o aumento do nível de confiança no processo, de acordo com a Figura 24 – Principais benefícios do RGPD para as empresas.

Também na fase de Tratamento do risco foram desenvolvidas propostas para as não conformidades das medidas de segurança. Estas propostas tiveram por base a informação disponível das Autoridades de Controlo dos vários Estados-Membros da União Europeia e Espaço Económico Europeu, orientações oficiais do EDPB – European Data Protection Board, e do anterior Grupo de Trabalho do artigo 29, documentação da Organização Internacional de Normalização (ISO), mais propriamente através dos documentos ISO/IEC 27001:2013, ISO/IEC 27002:2013 e ISO/IEC 27701:2019, e outros documentos relevantes tais como a Resolução do Conselho de Ministros nº 41/2018, relativa aos requisitos técnicos mínimos das redes e sistemas de informação ou o boletim do National Institute of Standards and Technology (NIST) relativo à integração da segurança no ciclo de vida de desenvolvimento de software (SDLC) – ver Anexo 8.

Na fase de Aceitação do risco (4.2.1.3 do trabalho de investigação) foi desenvolvido um fator de priorização das várias tarefas incluídas no plano de tratamento, tendo em consideração as sanções jurídicas do RGPD, enquanto critério de tomada de decisão.

A solução baseada em sanções jurídicas identifica e prioriza as medidas preconizadas em 4.2.1.2 em termos de multas RGPD, tanto pela incidência do valor monetário das multas como pela frequência da sua ocorrência, através da verificação dos artigos do RGPD que originaram as multas, pelo facto das medidas em 4.2.1.2 estarem alinhadas aos mesmos artigos do RGPD – ver Anexo 9.

O período temporal de análise de multas, para a construção do fator de priorização, esteve compreendido entre 25 de maio de 2018, desde a entrada em vigor do regulamento, e 31 de março de 2021, data máxima que permitiu acomodar todas as multas RGPD na construção da proposta e no desenvolvimento da Prova de Conceito, através da pesquisa da informação disponível nos sítios da internet das várias autoridades de controlo.

Neste intervalo de tempo, 75% das multas do RGPD relacionam-se apenas com 5 artigos do RGPD, de acordo com a análise da Figura 29 – Artigos RGPD mais identificados nas multas a PME, tendo em conta o dataset do Anexo 10 e o ponto 4 do 3.2.1.3 da metodologia: artigo 5º, artigo 6º, artigo 13º, artigo 32º e artigo 58º.

Consequentemente, as medidas de segurança mapeadas com os artigos do RGPD que foram mais vezes consideradas nas multas apresentam-se como as mais críticas, tendo em conta o fator de priorização (Tabela 2).

Das 10 medidas de segurança mais críticas, 7 são "novas" e 3 são das orientações da ENISA. Deste modo, verifica-se também a pertinência do desenvolvimento dos novos controlos (66) – Figura 28, sob pena de criar uma falsa sensação de segurança na utilização da ferramenta da ENISA, tal como ela se encontra. Considera-se que este *upgrade*, face às multas existentes, aumenta o nível de confiança no processo, uma das prioridades das PME, de acordo com os resultados obtidos na Figura 24 – Principais benefícios do RGPD para as empresas.

Considera-se também que o risco "alto" da medida de segurança F.5 da tabela 2 não permite que ela seja considerada em todos os processos das PME, quando, por exemplo, o risco dos processos é baixo ou médio. Sugere-se, portanto, a alteração da classificação definida pela ENISA.

Relativamente à fase de Comunicação do risco (3.2.1.4 do trabalho de investigação), foi desenvolvido na solução proposta para conformidade, proteção e privacidade dos dados pessoais um espaço onde se pode gerir quais as partes interessadas que devem ser informadas sobre as decisões tomadas, que controlos foram adotados, que riscos foram aceites, bem como quais os próximos passos, por exemplo, quais os critérios para o estabelecimento da revisão e sua monitorização – concretização do plano de tratamento do risco – ver Anexo 12.

Todas estas fases, que constituem a proposta inicial da solução, foram testadas por 6 PME, no âmbito da Prova de Conceito, de acordo com 4.2.2 do desenho e desenvolvimento.

6.2.2 – Discussão e análise dos resultados – Fase de testes – desenvolvimento da Prova de Conceito junto das PME

Após o desenvolvimento da proposta inicial da solução, de acordo com o ponto 4.2.1 deste trabalho de investigação – ver Anexo 12 – que permite garantir a conformidade legal das PME com o RGPD, a proposta foi testada em contexto real, por 6 PME.

Para tal, utilizou-se como metodologia a Prova de Conceito (PoC) que, por definição, é a entrega de um sistema funcional para provar que a tecnologia funciona e funciona conforme

pretendido (Government of Newfoundland and Labrador, 2021), de acordo com 4.2.2 do Capítulo 4.

O PoC foi realizado junto de PME portuguesas. As organizações foram definidas através do inquérito "Impacto do RGPD nas Organizações" – Fase 1 da metodologia deste trabalho (Anexo 1), através da resposta afirmativa à pergunta número 25: Figura 27 - PME que desejam realizar uma Prova de Conceito da solução proposta para conformidade, proteção e privacidade dos dados pessoais. Oito das inquiridas respondeu afirmativamente quanto à intenção de realizar um PoC, correspondendo a 24% das respostas. Contudo, destas oito organizações apenas seis PME disponibilizaram os seus dados de identificação, permitindo o seu contacto. O universo da fase II foi, portanto, estas 6 organizações.

O PoC concretizou-se em três fases: Iniciação; Planeamento e Análise; e Fecho do Projeto, decorrendo entre os dias 14 de abril e 10 de maio de 2021.

Relativamente à fase Iniciação, esta teve o seu arranque através do envio de um email às 6 organizações, com o convite à participação na Prova de Conceito sobre o impacto do RGPD nas PME. O convite permitiu o preenchimento da Fase 1 do Anexo 11 – Iniciação – Identificação da PME, bem como o agendamento de uma reunião de a concretização da Fase 2 – Planeamento e Análise.

A recolha da informação do PoC foi realizada com auxílio de formulário online, através da conta académica Office 365 – formulários da Microsoft, garantido a confidencialidade das respostas por via das suas características técnicas.

As PME que participaram no PoC têm a sua morada em Lisboa (4 PME) e Porto (2 PME) – Figura 30. De acordo com a Figura 7, trata-se das localizações geográficas mais representativas da Fase I: Área Metropolitana de Lisboa e Região Norte.

Os inquiridos do PoC foram gestor/a e proprietário/a (Figura 31), correspondendo a 60% das respostas obtidas da Fase I – Figura 9. Verificaram-se, portanto, respostas dos responsáveis pelas organizações – os mesmos que indicaram que têm responsabilidades na implementação do RGPD – Figura 32.

De acordo com as respostas obtidas na Fase I (Anexo 13), das 6 PME participantes no PoC, quatro são microempresas e duas são pequenas empresas (Figura 33). Relativamente à antiguidade: 4 têm entre 6 e 19 anos, uma tem menos de 5 anos e outra mais de 20 anos (Figura 34).

Em termos de setor de atividade, uma organização participante no PoC é do setor da construção enquanto as restantes organizações são de "outros setores" (Figura 35), alinhado com a Figura 8, onde a resposta dominante foi a opção "outros setores", correspondendo a 62% das observações. As tipologias de referência utilizadas foram as existentes em Pordata (2021), para a classificação das PME por setores de atividade. Verifica-se, pelas respostas obtidas, um não alinhamento ao pretendido, onde a opção "outros setores" deveria ser respondido apenas de modo residual. Admite-se que as organizações inquiridas não se identificaram com as tipologias apresentadas. De acordo com as reuniões da Fase 2 – Planeamento e Análise, verificou-se que as empresas "outros setores" desenvolvem a sua atividade na área dos serviços, marketing e publicidade, comércio, consultoria e desenvolvimento de software.

A Fase 2 – Planeamento e Análise, decorreu no período compreendido entre os dias 16 de abril e 5 de maio de 2021, conforme proposta de data da Fase 1, num total de 6 reuniões.

A duração das reuniões situou-se no intervalo entre uma e três horas. Todas as reuniões decorreram em modo remoto, através da ferramenta TEAMS, da conta académica Office 365.

Para além do preenchimento da Fase 2 do Anexo 11, a reunião permitiu fazer uma apresentação da solução proposta, incluindo a partilha das fontes de informação que podem acrescentar maior valor para a construção da proposta, nomeadamente documentação da ENISA, CNPD e, enquanto proposta de resolução para as não conformidades, a Resolução do Conselho de Ministros nº 41/2018, relativa aos requisitos técnicos mínimos das redes e sistemas de informação.

Sob o ponto de vista do plano de projeto – primeira parte da Fase 2, a definição do âmbito teve como resposta dominante tratamentos de dados pessoais relacionados com campanhas de marketing (3 respostas): Envio de marketing para clientes; Mailing para clientes – marketing / prospeção; e Campanha de marketing.

Duas respostas estão também ligadas à relação com clientes; por um lado na relação de negócio / gestão de clientes individuais/singulares e, por outro lado, na relação com clientes corporativos, na componente de gestão de eventos que envolve a emissão de certificados de participação, produção de brindes personalizados e/ou reportagens fotográficas. Recrutamento e seleção de Recursos Humanos foi outro âmbito considerado no PoC (Figura 36).

Ou seja, as organizações consideraram no âmbito do PoC atividades concretas e correntes do seu dia a dia, que, de acordo com as reuniões tidas, refletem processos de negócio que envolvem muitos dados pessoais. O PoC acabou por ser uma oportunidade para demonstrarem a preocupação quanto à conformidade com o RGPD.

Em termos do plano de recursos (Figura 37), o/a gestor/a do projeto foi maioritariamente o proprietário da organização (5 respostas), alinhado com as respostas determinadas na Fase 1 do PoC (Figura 9), onde quem participou no trabalho de investigação foi maioritariamente o/a proprietário/a da empresa, sendo ele próprio o responsável pela implementação do RGPD.

A definição da equipa de projeto foi constituída maioritariamente apenas pelo/a próprio/a gestor/a de projeto do PoC. Tal situação deveu-se ao facto de as organizações serem de tamanho reduzido e também pelo facto de se tratar de um teste, sendo suficiente a participação de um só elemento, nomeadamente de quem tem responsabilidades na implementação do RGPD.

Contudo, em duas das organizações, foi possível verificar que existiu sentido de oportunidade em alargar esta iniciativa aos/às colaboradores/as que exercem funções operacionais relacionadas com o regulamento geral sobre a proteção de dados, tendo sido indicados como equipa de projeto do PoC outros elementos da organização, tais como responsáveis de Recursos Humanos, responsável de Estratégia/Marketing e responsável financeiro/CFO.

Relativamente à indicação das partes interessadas no PoC – Figura 38 (ex: prestadores de serviços, fornecedores, instituições públicas, etc.), foram referidos parceiros de negócio, clientes e, no âmbito do recrutamento e seleção de Recursos Humanos, os entrevistados e os clientes finais / parceiros de negócio alvo do recrutamento.

6.2.3 – Discussão e análise dos resultados – Avaliação da Prova de Conceito com as PME

Para a concretização da Fase 3 – Fecho do Projeto, foram realizadas reuniões com cinco organizações. As reuniões permitiram auxiliar o preenchimento da solução proposta para conformidade, proteção e privacidade dos dados pessoais, alinhado com a apresentação realizada nas reuniões da Fase 2. Uma das organizações optou por fazer o exercício de forma autónoma.

A última resposta – Fecho do Projeto, foi enviada no dia 10 de maio de 2021, completando o PoC às seis organizações. Os resultados encontram-se no Anexo 14.

Todos os participantes consideraram que a apresentação do PoC foi satisfatória no sentido de os ajudar no cumprimento com o Regulamento. Foi indicado que todas as questões foram fundamentadas e com conteúdo. Em todo o momento foi mostrado onde se encontra a informação base e referido qual o fundamento para que seja solicitada a informação. Também foi referido que a apresentação foi assertiva, cumprindo-se o pretendido, tendo havido capacidade de transmissão de conhecimento.

Em termos de lições aprendidas com o PoC, as empresas participantes referiram que esta solução proposta para conformidade, proteção e privacidade dos dados deu condições para considerar o RGPD como uma forma de encarar o serviço, ou seja, compreendeu-se a lógica de aplicação do regulamento, podendo o RGPD ser incorporado nos processos de negócio. Foi referido também que se verifica a possibilidade de aplicar o RGPD de modo faseado e que este acrescenta valor na medida em que ajuda a tomar consciência sobre alguns pontos que, no dia-a-dia, ficam remetidos para segundo plano.

Adicionalmente, o PoC permitiu a duas organizações fazerem a sua auto-avaliação: uma organização concluiu que a sua empresa tem o processo de RGPD bastante bem organizado, enquanto que a outra organização percebeu que a sua estrutura terá de fazer várias melhorias para cumprir os requisitos do regulamento. Foi também referido por um participante que, tendo em conta a sua natureza, esta proposta pode ser útil para empresas que tenham mais dados pessoais.

Cinco das organizações consideraram que a definição do âmbito foi ajustada ao PoC (Figura 39). Uma organização reforçou a sua posição comentando que foi uma boa aposta definir o âmbito do PoC numa atividade / tratamento bastante importante da organização. Por outro lado, destaca-se uma resposta que não considerou a definição do âmbito como ajustada, tendo referido que foram bastante ambiciosos face ao nível de conhecimento de RGPD, para conseguir abarcar tanta informação em tão pouco tempo.

Alinhado com o tema anterior, uma organização referiu que os prazos definidos não foram cumpridos, tendo resvalado, visto terem aparecido várias questões de entendimento relativo ao pretendido. As restantes 5 PME consideraram que os prazos foram cumpridos, tendo uma organização partilhado que imprimiram uma tónica de urgência à melhoria da realidade da sua estrutura (Figura 40). Todas as organizações participantes afirmaram que a duração do PoC foi

satisfatória. Uma PME considerou que decorreu equilibradamente, durante o tempo que foi necessário.

Todas as organizações também afirmaram que a alocação de recursos foi ajustada às necessidades do PoC e à definição do âmbito, tendo sido referido que caso o PoC tivesse ocorrido com outros tratamentos, poderia ter sido útil considerar a participação de mais intervenientes. Foi também referido que num contexto mais alargado, para haver um exercício mais completo de conformidade, seria bom aumentar a equipa de projeto. Por outro lado, tendo em conta a natureza das organizações, foi indicado que o desafio teve mais a ver com a dimensão da empresa do que com a alocação de recursos, por ser uma PME com poucos/as colaboradores/as.

No que às entregas diz respeito, apenas uma organização considerou que estas não foram cumpridas (Figura 41), explicando que se deveu ao facto de se tratar de uma empresa com poucos dados pessoais. As restantes 5 organizações consideraram que as entregas previstas foram cumpridas.

Relativamente à implementação total da solução no contexto da organização, 5 PME responderam afirmativamente. Se por um lado foi referido que seria um processo complicado, com uma implementação trabalhosa, exigindo muito tempo e dedicação para a sua implementação por ser um processo bastante exigente e completo que requer bastante manutenção operacional, também foi referido que se trata de um processo que faz sentido, considerando que a organização tem outros aspetos que a preocupa em relação ao RGPD, nomeadamente os relacionados com ações de marketing. Adicionalmente, foi referido que a sua implementação total pode ser assumida como mais um dos fatores diferenciadores da organização.

No que diz respeito à própria solução alvo do PoC, as organizações apresentaram as seguintes propostas de melhoria / comentários, para as suas quatro etapas:

- Etapa de Avaliação do risco:
    - *Há perguntas formuladas na negativa que tornam difícil o preenchimento;*
    - *Muito bem explicado.*

  A formulação pela negativa é a forma como a ENISA considerou na sua ferramenta de gestão do risco. Não foi alvo deste trabalho alterar as orientações da ENISA. Contudo, para trabalhos futuros, sugere-se que se adapte a redação das questões existentes na etapa de avaliação do risco.

- Etapa de Tratamento do risco:
    - *A componente visual deveria estar mais simplificada. Tem muita informação. A informação deveria ser apresentada apenas quando é necessária;*
    - *Está bem conseguido. Está simples e concreto. Relaciona-se diretamente com os artigos do RGPD;*
    - *Muito bem explicado.*

  Conforme desenvolvimento desta solução proposta, no ponto de outras recomendações e nos comentários finais, e na Etapa de Aceitação do risco, uma PME propôs a

transformação desta proposta numa solução web-based. Neste sentido, propõe-se para trabalhos futuros o desenvolvimento da proposta alinhado a um ambiente gráfico mais amigável do utilizador final, que permita apresentar apenas a informação essencial, remetendo para segundo plano a componente de suporte e seu conteúdo explicativo.

- Etapa de Aceitação do risco:
    - *Muito bem explicado. O Ranking (fator de priorização, com base nas sanções jurídicas) faz sentido na medida em que ajuda a tomar decisões / começar a trabalhar;*
    - *Está bem conseguido. Ajuda a tomar decisões e apresenta propostas de solução. As medidas estão associadas ao RGPD, que dá segurança / conforto a quem toma decisões perante as questões que surgem na organização. Esta etapa ajuda também a priorizar / tomar decisões de acordo com os diferentes níveis de risco;*
    - *A componente visual deveria estar mais simplificada. Tem muita informação. A informação deveria ser apresentada apenas quando é necessária;*
    - *A componente de aceitação poderia ter uma vertente financeira associada às opções de melhoria, para além do ranking das multas;*
    - *Impecável. Sem dúvidas de interpretação.*

  Conforme desenvolvimento desta solução proposta, no ponto de outras recomendações e nos comentários finais, e na Etapa de Tratamento do risco, uma PME propôs a transformação desta proposta numa solução web-based. Neste sentido, propõe-se para trabalhos futuros o desenvolvimento da proposta alinhado a um ambiente gráfico mais amigável do utilizador final, que permita apresentar apenas a informação essencial, remetendo para segundo plano a componente de suporte e seu conteúdo explicativo.

  Considera-se a observação relativa à vertente financeira associada às opções de melhoria, para além do ranking das multas, muito pertinente para a tomada de decisão das organizações. Ou seja, para além da componente do âmbito deste trabalho de investigação – as sanções jurídicas – verifica-se que a determinação do custo de aplicação/investimento pode também ajudar a tomar decisões. Neste sentido, e tendo em conta a necessidade de auscultar o mercado para todo um cenário de propostas de melhoria, propõe-se que para trabalhos futuros se possa desenvolver uma nova variável de tomada de decisão para a implementação do RGPD nas organizações, numa vertente financeira.

- Etapa de Comunicação do risco:
    - *Tudo óbvio: ligado aos procedimentos a aplicar em caso de risco efetivo;*
    - *Muito bem explicado;*
    - *Também a componente visual, mas não tão relevante como nas etapas anteriores;*
    - *Sem comentários: numa PME, a comunicação é algo intrínseco visto haver poucos recursos e haver comunicação fluída.*

  A componente visual e a proposta de transformação do PoC numa solução web-based é a observação que se destaca na etapa de Comunicação do risco.

A nível global verificou-se uma aceitação muito positiva por parte das organizações. Adicionalmente aos objetivos concretos deste trabalho de investigação, as reuniões permitiram falar de assuntos técnicos relativos ao cumprimento do regulamento focado no negócio das PME, esclarecimento de dúvidas e partilha de informação acessória como o estado do RGPD no contexto europeu, o quadro sancionatório ou formação gratuita online. Relativamente aos resultados obtidos, verifica-se uma aceitação da proposta, tendo sido obtido os resultados de "bom" e "muito bom" em termos de satisfação global do PoC (Figura 43).

Em termos de recomendações sobre como proceder numa implementação completa, conforme descrito no último parágrafo do ponto 5.2.3, verifica-se uma aceitação geral por parte das PME que participaram no PoC, tendo sido destacada a importância de se envolverem todos os decisores da organização, que o processo possa ocorrer de modo faseado, e que, para aumentar a integridade e a escalabilidade dos processos, se possa aplicar esta proposta numa solução web-based, facilitando a validação da conformidade com o RGPD.

Capítulo 7 – Conclusões e Trabalhos Futuros

Este trabalho teve como objetivo principal criar uma solução proposta para conformidade, proteção e privacidade dos dados pessoais, que permita que as PME se preparem para o cumprimento das regras relativas às obrigações legais do RGPD, incluindo critérios de apoio à decisão, tendo em conta as sanções jurídicas existentes no contexto europeu (Objetivo O2).

O trabalho teve como referência um conjunto de orientações da Agência da União Europeia para a Segurança de Redes e Informações – ENISA, e a aplicação dos requisitos existentes na família ISO/IEC 27000, nomeadamente as normas ISO/IEC 27001:2013 e ISO/IEC 27701:2019, relativas à segurança da informação e à privacidade. Incluíram-se também critérios de apoio à decisão, tendo em conta as sanções jurídicas existentes no contexto europeu.

A revisão da literatura mostrou-nos que os modelos de referência também poderiam considerar as tendências das autoridades como critério de tomada de decisão e de priorização, nomeadamente ao nível das Pequenas e Médias Empresas, estruturas que, citando Brodin (2019), não dispõem de recursos ou conhecimentos para gerir este processo sozinhos. E que, portanto, poderiam ser aconselhadas a priorizar determinados requisitos em detrimento de outros, numa lógica de suporte à tomada de decisão. Freitas e Mira da Silva (2018), no contexto português, reforçaram a necessidade de definir uma metodologia para poder cumprir as obrigações do RGPD.

Adicionalmente, enquanto ponto de partida, para reforçar a pertinência do objetivo principal, analisou-se o impacto do RGPD nas PME, em Portugal (Objetivo O1). O inquérito apresentou também questões de continuidade do trabalho de investigação – Fase II, nomeadamente ao nível do interesse em realizar uma Prova de Conceito à solução proposta.

Por isto, pode afirmar-se que foram cumpridos todos os objetivos de pesquisa, propostos em 1.2:

- Relativamente ao objetivo O1, conseguiu verificar-se qual o impacto do RGPD nas Organizações – PME, através da participação de 34 PME. Destacam-se os seguintes pontos:
    - A falta de formação sobre o tema RGPD foi entendida como a principal dificuldade das PME na implementação do regulamento (17%). Em segundo lugar encontra-se a falta de orientações e práticas ou de normas de aplicação, representando 13% do total de dificuldades identificadas;
    - Em termos de principais benefícios do RGPD, foi indicado que a "garantia da confiança dos clientes" era o mais importante, tendo sido referido por 74% das organizações inquiridas;
    - Relativamente aos principais desafios que as PME percecionaram em relação à conformidade com o RGPD, a definição de processos foi o mais referido. Tendo em conta que a etapa "Definição da operação de tratamento e seu contexto" é o ponto de partida da avaliação do risco (ENISA, 2017, pág.10) – Fase 1 da solução de O2, considera-se que a utilização da ferramenta da ENISA, parte integrante da solução, permite ajudar as PME a definir os seus processos e, consequentemente, concretizar os passos seguintes que o regulamento exige.

- Conseguiu-se também, por via do objetivo O1, a aceitação de seis organizações para participarem na Fase II deste trabalho de investigação (objetivo O2).
- O objetivo O2 – desenvolver uma solução para conformidade, proteção e privacidade dos dados pessoais baseada em sanções jurídicas do RGPD, também foi conseguido, aplicando-se a metodologia DSR para sistemas de informação, através da definição inicial da solução, a Prova de Conceito, que testou a ferramenta (Fase II), através da participação de 6 PME, que aceitaram o desafio no momento do inquérito da Fase I, e que avaliaram a proposta, permitindo, deste modo, aceitar a solução proposta para conformidade, proteção e privacidade dos dados pessoais baseada em sanções jurídicas do RGPD como solução final.

Assim, de modo geral, considera-se que a proposta inicial foi aceite pelas 6 PME que participaram no trabalho de investigação.

Adicionalmente, reforçam-se as seguintes ideias que este trabalho de investigação permitiu aferir:

- A ENISA e as ISO 27001:2013 e 27701:2019 eram praticamente desconhecidas no universo das PME que participaram no inquérito da Fase I (apenas 7 respostas positivas). Contudo, as organizações participantes no PoC aceitaram bastante bem a proposta da Agência da União Europeia para a Segurança de Redes e Informações.
- Não obstante a ferramenta da ENISA, as PME apreciaram a completude da solução com o RGPD, incluindo os 66 novos controlos – dando, desta forma, segurança na aplicação e utilização da ferramenta.
- Estes 66 novos controlos estão, maioritariamente, alinhados com a extensão da ISO 27001:2013 para a privacidade, ou seja, a IS0 27701:2019, publicada apenas em 2019, quando as orientações da ENISA são anteriores, de 2016. Considera-se, portanto, que a ISO 27001 não é, por si só, suficiente no processo de conformidade com o RGPD, base de construção das orientações da ENISA.
- A solução baseada em sanções jurídicas identifica e prioriza as medidas em termos de multas RGPD, tanto pela incidência do valor monetário das multas como pela frequência da sua ocorrência, através da verificação dos artigos do RGPD que originaram as multas. Ou seja, esta integração aumenta a confiança do processo, melhora o nível de segurança e privacidade da informação e reduz o risco sancionatório.
- Das 10 medidas de segurança mais críticas, 7 são "novas" e 3 são das orientações da ENISA. Verifica-se também, deste modo, a pertinência do desenvolvimento dos novos controlos (66), sob pena de criar uma falsa sensação de segurança na utilização da ferramenta da ENISA, tal como ela se encontra. Considera-se que este *upgrade*, face às multas existentes, aumenta o nível de confiança do processo, uma das prioridades das PME, de acordo com os resultados obtidos na Figura 24 – Principais benefícios do RGPD para as empresas.
- A existência de um fator de tomada de decisão, associado às multas, para poder aplicar o RGPD de modo faseado foi um ponto que as 6 entidades participantes mencionaram como positivo.

- Todos os participantes consideraram que a apresentação do PoC foi satisfatória e a grande maioria das PME (5) consideraram que gostariam de ter a proposta aplicada a toda a sua organização.
- O trabalho desenvolvido no âmbito do PoC permitiu também às PME realizar uma avaliação do estado de maturidade da aplicação do RGPD nas suas organizações.

Com base na revisão da literatura, não se identificou quaisquer propostas de solução para aplicação e concretização da conformidade por parte das PME que introduzissem um critério relacionado com multas do RGPD, enquanto fator de tomada de decisão. Assim, considera-se que este trabalho trouxe novas contribuições não só para a comunidade académica e científica, ao iniciar uma vertente ainda não explorada, mas também a todas as PME que não dispõem de recursos e/ou conhecimentos para gerir este processo sozinhos.

Foi aceite para publicação e apresentação na 16ª Conferência Ibérica de Sistemas e Tecnologias de Informação (CISTI 2021) o artigo com o título "How can GDPR fines help SMEs ensuring the privacy and protection of processed personal data" (CISTI, 2021).

7.1 Limitações

O fator inovador de criar um critério de tomada de decisão associado a sanções jurídicas do RGPD transformou-se também numa limitação no trabalho de investigação, na medida em que o suporte literário apenas existiu ao nível concetual de modelos de referência para a conformidade do RGPD e não na componente metodológica da construção do fator de priorização, com base nas sanções jurídicas.

O quadro sancionatório em Portugal apresenta poucas multas, nomeadamente quando comparado com outros países como é o caso da vizinha Espanha, que apresenta quase um terço de todas as multas existentes no Espaço Económico Europeu (Anexo 10). Considera-se que este cenário nacional foi também, por si só, uma limitação no trabalho de investigação, não despertando o interesse num maior número de Pequenas e Médias Empresas, não obstante a forte divulgação realizada pela ANPME, tendo-se a perceção de que o regulamento e o seu quadro sancionatório não é, à data, uma ameaça real às organizações portuguesas.

7.2 Possíveis trabalhos futuros

A Prova de Conceito permitiu testar esta solução para conformidade, proteção e privacidade dos dados pessoais, tendo-se confirmado a sua aceitação, não obstante haver pontos relevantes que deverão ser considerados em trabalhos futuros, visto que a sua dimensão de aplicabilidade ultrapassa o âmbito deste trabalho. Seria interessante estender o estudo e validar a solução noutros setores de atividade onde prevalecem categorias especiais de dados pessoais, nomeadamente o setor da saúde.

De acordo com o ponto 5.3.2, indicam-se os seguintes trabalhos futuros que podem vir a ser realizados, na sequência desta investigação:

- Etapa de Avaliação do risco:
    - *Há perguntas formuladas na negativa que tornam difícil o preenchimento;*

      A formulação pela negativa é a forma como a ENISA considerou na sua ferramenta de gestão do risco. Não foi alvo deste trabalho alterar as orientações da ENISA. Contudo, para trabalhos futuros, sugere-se que se adapte a redação das questões existentes na etapa de avaliação do risco.

- Etapas de Tratamento do risco, de Aceitação do risco e de Comunicação do risco:
    - *A componente visual deveria estar mais simplificada. Tem muita informação. A informação deveria ser apresentada apenas quando é necessária;*

      Conforme desenvolvimento desta solução proposta, no ponto de outras recomendações e nos comentários finais, e na Etapa de Aceitação do risco, uma PME propôs a transformação desta proposta numa solução web-based. Neste sentido, propõe-se para trabalhos futuros o desenvolvimento da proposta alinhado a um ambiente gráfico mais amigável do utilizador final, que permita apresentar apenas a informação essencial, remetendo para segundo plano a componente de suporte e seu conteúdo explicativo.

      Propõe-se também uma revisão do nível de risco das medidas de segurança, alinhada ao fator multas RGPD. Por exemplo, de acordo com a Tabela 2, o risco "alto" da medida de segurança F.5 não permite que a medida seja considerada em todos os processos das PME, quando o risco dos processos é baixo ou médio. Sugere-se, portanto, a alteração da classificação definida pela ENISA.

- Etapa de Aceitação do risco:
    - *A componente de aceitação poderia ter uma vertente financeira associada às opções de melhoria, para além do ranking das multas;*

      Considera-se a observação relativa à vertente financeira associada às opções de melhoria, para além do ranking das multas, muito pertinente para a tomada de decisão das organizações. Ou seja, para além da componente do âmbito deste trabalho de investigação – as sanções jurídicas – verifica-se que a determinação do custo de aplicação/investimento pode também ajudar a tomar decisões. Neste sentido, e tendo em conta a necessidade de auscultar o mercado para todo um cenário de propostas de melhoria, propõe-se que para trabalhos futuros se possa desenvolver uma nova variável de tomada de decisão para a implementação do RGPD nas organizações, numa vertente financeira.

Relativamente a outras recomendações sobre como proceder numa implementação completa no contexto da organização e enquanto comentários finais, foi respondido no âmbito da Prova de Conceito que pode ser pertinente implementar a proposta de um modo global transformando o PoC numa solução web-based, enquanto ferramenta de auxílio às PME, que facilita a sua aplicação, aumentando a integridade dos processos e permitindo a escalabilidade da solução.

Referências bibliográficas

Associação Nacional das Pequenas e Médias Empresas (ANPME). (2021). Apresentação. Acedido a 18 de abril de 2021 em https://www.anpme.pt/apresentacao-anpme/

Banco de Portugal. (2021). Quadros do Setor. Acedido a 9 de janeiro de 2021 em https://www.bportugal.pt/QS/qsweb/Dashboards

Brodin, M. (2019). A Framework for GDPR Compliance for Small and Medium-Sized Enterprises. European Journal for Security Research. 4:243–264. https://doi.org/10.1007/s41125-019-00042-z

Carvalho Silva, G. (2019). RGPD aplicado nas PME Portuguesas. NOVA Information Management School – Instituto Superior de Estatística e Gestão de Informação da Universidade Nova de Lisboa. https://run.unl.pt/bitstream/10362/94888/4/TGI0280.pdf

Castets-Renard, C. (2019). Accountability of Algorithms in the GDPR and Beyond: A European Legal Framework on Automated Decision-Making, 30 Fordham Intell. Prop. Media & Ent. L.J. 91. https://ir.lawnet.fordham.edu/iplj/vol30/iss1/3

Chatzipoulidis, A., Tsiakis, T. & Kargidis, T. (2019). A readiness assessment tool for GDPR compliance certification. Computer Fraud & Security, 2019(8):14-19. https://doi.org/10.1016/S1361-3723(19)30086-7

CISTI. (2021). 16ª Conferência Ibérica de Sistemas e Tecnologias de Informação. Acedido a 13 de junho de 2021 em http://www.cisti.eu/2021/oc21/modules/request.php?module=oc_program&action=summary.php&id=161

CNCS. (2019). Quadro Nacional de Referência para a Cibersegurança, do Centro Nacional de Cibersegurança. Acedido a 10 de janeiro de 2021 em https://www.cncs.gov.pt/content/files/cncs_qnrcs_2019.pdf

CNCS. (2021). Glossário do Centro Nacional de Cibersegurança. Acedido a 18 de janeiro de 2021 em https://www.cncs.gov.pt/recursos/glossario/

CNPD. (2019). Modelos de registo de atividades de tratamento. Acedido a 18 de janeiro de 2021 em https://www.cnpd.pt/organizacoes/obrigacoes/registo-de-atividades-de-tratamento/

Comissão Europeia. (2020). Comunicação da Comissão ao Parlamento Europeu e ao Conselho - "A proteção de dados enquanto pilar da capacitação dos cidadãos e a abordagem da UE para a transição digital - dois anos de aplicação do Regulamento Geral sobre a Proteção de Dados". Acedido a 9 de janeiro de 2021 em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020DC0264&from=EN

Costa, N., Silva, J., Moehring, M. M. & Duarte de Almeida, I. (2018). Definition of key drivers for project success regarding the General Data Protection Regulation (GDPR).

European Commission. (2020). Commission Staff Working Document - Communication from the Commission to the European Parliament and the Council – "Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation". Acedido a 9 de janeiro de 2021 em https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020SC0115&from=EN

European Commission. (2020). Press corner "Two years of the GDPR: Questions and answers". Acedido a 10 de janeiro de 2021 em https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166

European Data Protection Board (EDPB). (2021). Members. Acedido a 17 de abril de 2021 em https://edpb.europa.eu/about-edpb/board/members_en

European Union Agency for Network and Information Security (ENISA). (2015). Big Data Security – Good Practices and Recommendations on the Security of Big Data

Systems. Acedido a 13 de junho de 2021 em https://www.enisa.europa.eu/publications/big-data-security

European Union Agency for Network and Information Security (ENISA). (2016). Guidelines for SMEs on the security of personal data processing. Acedido a 9 de janeiro de 2021 em https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

European Union Agency for Network and Information Security (ENISA). (2021). Inventory of Risk Management / Risk Assessment Methods and Tools. Acedido a 9 de janeiro de 2021 em https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory

European Union Agency for Network and Information Security (ENISA). (2017). Handbook on Security of Personal Data Processing. Acedido a 9 de janeiro de 2021 em https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

Freitas, M. C. & Mira da Silva, M. (2018). GDPR Compliance in SMEs: There is much to be done. Journal of Information Systems Engineering & Management, 3(4), 30. https://doi.org/10.20897/jisem/3941

Geko, M. e Tjoa, S. (2018). An Ontology Capturing the Interdependence of the General Data Protection Regulation (GDPR) and Information Security. 1-6. https://doi.org/10.1145/3277570.3277590.

Government of Newfoundland and Labrador. (2021). Governance of Evaluation, Proof of Concept and Pilot Projects. Acedido a 17 de janeiro de 2021 em https://www.gov.nl.ca/exec/ocio/files/pmo-docs-governance-evaluation-poc-pilot.pdf

Henderson, T. (2017). Does the GDPR Help or Hinder Fair Algorithmic Decision-Making?. LLM dissertation, Innovation, Technology & The Law, University of Edinburgh. http://dx.doi.org/10.2139/ssrn.3140887

Hevner, A.R., March, S. T., Park, J. & Ram, S. (2004). Design Science in Information Systems Research. Management Information Systems Quarterly. 28. 75-106. https://www.researchgate.net/publication/201168946_Design_Science_in_Information_Systems_Research

INE. (2020). Sociedade da Informação e do Conhecimento – Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Empresas. Acedido a 9 de janeiro de 2021 em https://ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=415621360&DESTAQUEStema=55579&DESTAQUESmodo=2

ISO/IEC 27001:2013, Tecnologia de informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. IPQ – Instituto Português da Qualidade

ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls, ISO/IEC, Switzerland.

ISO/IEC 27701:2019, Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines, ISO/IEC, Switzerland.

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. Department of Computer Science, Keele University, United Kingdom.

Laudon, K. C. & Laudon, J. P. (2018). Management Information Systems – Managing the Digital Firm. New York. Pearson Education Limited.

Lei n.º 58/2019 de 8 de agosto. (2019). Diário da República n.º 151/2019, Série I de 2019-08-08

Microsoft. (2018). Microsoft News Center: Apenas 2,5% dos decisores considera que a sua organização está preparada para lidar com o RGPD. Acedido a 9 de janeiro de 2021 em https://news.microsoft.com/pt-pt/2018/01/30/apenas-25-dos-decisores-considera-que-sua-organizacao-esta-preparada-para-lidar-com-o-rgpd/

Palmirani, M., Martoni, M., Rossi, A., Bartolini, C. & Robaldo, L. (2018). Legal ontology for modelling GDPR concepts and norms. Proc. 31st Int. Conf. Legal Knowledge and Information Systems (JURIX), 91-100. https://doi.org/10.3233/978-1-61499-935-5-91

Pordata. (2021). Base de Dados Portugal Contemporâneo. Acedido a 8 de janeiro de 2021 em https://www.pordata.pt/Portugal/Empresas+total+e+por+dimens%c3%a3o-2857

Recomendação EU 2003/361, de 6 de maio, relativa à definição de micro, pequenas e médias empresas, notificada com o número C(2003) 1422] (JO L 124 de 20.5.2003, p. 36-41). Comissão Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=LEGISSUM:n26026&from=PT

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). (2016). Jornal Oficial da União Europeia. 119(1):1–88

Resolução do Conselho de Ministros nº 41/2018. (2018). Diário da República n.º 62/2018, Série I de 2018-03-28

Saunders, M., Lewis, P. & Thornhill, A. (2009). Research Methods for Business Students. New York. Person Education Limited.

Slimani, T. (2014). A Study on Ontologies and their Classification. Recent Advances in Electrical Engineering and Educational Technologies. 86-92

Teixeira, G., Mira da Silva, M. & Pereira, R. (2019). The critical success factors of GDPR implementation - a systematic literature review. Digital Policy, Regulation and Governance. 21 (4), 402-418

UAG. (2020). The Standard Data Protection Model. A method for Data Protection advising and controlling on the basis of uniform protection goals. In Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder.

Anexos

Anexo 1 – Inquérito "Impacto do RGPD nas Pequenas e Médias Empresas, em Portugal"

Impacto do RGPD nas organizações

Bem-vindo ao inquérito sobre o impacto do RGPD nas Pequenas e Médias Empresas, em Portugal.

Este inquérito tem um tempo de preenchimento estimado em 10 minutos e insere-se num projeto de dissertação de mestrado em Gestão de Sistemas e Tecnologias da Informação na Atlântica Instituto Universitário, e que tem como objetivo apresentar uma Solução para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, sob a orientação da Professora Doutora Virgínia Araújo.

As suas respostas, que são muito importantes para nós, serão usadas apenas para a finalidade da investigação e serão consideradas estritamente confidenciais.

Para esclarecimento de qualquer dúvida acerca deste inquérito, pode contactar o investigador.

Contacto do Investigador:

Luís Pedroso

e: 201929286@academia.uatlantica.pt | w: http://www.linkedin.com/in/pedrosoluis

Atlântica Instituto Universitário

Departamento de informática

www.uatlantica.pt

Parte 1. Caracterização da PME

1. Distribuição da PME
   - 1.1 Micro
   - 1.2 Pequena
   - 1.3 Média

2. Antiguidade da PME
   - 2.1 Mais de 20 anos
   - 2.2 De 6 a 19 anos
   - 2.3 Menos de 5 anos

3. Localização geográfica (NUT II)
   - 3.1 Norte
   - 3.2 Centro
   - 3.3 Área Metropolitana de Lisboa
   - 3.4 Alentejo
   - 3.5 Algarve

3.6 Região Autónoma dos Açores
3.7 Região Autónoma da Madeira

4. Setor de atividade
   4.1 Agricultura, produção animal, caça, silvicultura e pesca
   4.2 Alojamento, restauração e similares
   4.3 Atividades de saúde humana e apoio social
   4.4 Atividades financeiras e de seguros
   4.5 Atividades imobiliárias
   4.6 Comércio por grosso e a retalho
   4.7 Construção
   4.8 Educação
   4.9 Eletricidade, gás e água
   4.10 Indústrias extrativas
   4.11 Indústrias transformadoras Transporte e armazenagem
   4.12 Outros setores

5. Função do/a inquirido/a na PME
   5.1 Gestor/a
   5.2 Administrativo/a
   5.3 Sócio/a
   5.4 Proprietário/a
   5.5 Diretor/a
   5.6 Colaborador/a interno/a
   5.7 Colaborador/a externo/a
   5.8 Outra, qual?

6. O/A inquirido/a tem responsabilidades na empresa na implementação do RGPD?
   6.1 Sim
   6.2 Não

7. Se a resposta anterior foi afirmativa, qual o cargo?
   7.1 Encarregado/a de Proteção de Dados (DPO)
   7.2 Chief Information Security Officer (CISO)
   7.3 Jurista
   7.4 Informático/a
   7.5 Gestor/a da Qualidade
   7.6 Auditor/a Interno/a
   7.7 Outro, qual?

Parte 2. Utilização de tecnologias da informação e da comunicação

8. A empresa tem website próprio ou do grupo económico a que pertence?
   8.1 Sim
   8.2 Não

9. A empresa realiza vendas de bens ou serviços através do comércio eletrónico?
   9.1 Sim
   9.2 Não

10. Se a resposta anterior foi afirmativa, qual a percentagem de vendas através do comércio eletrónico do total do volume de negócios do último ano fiscal (2020)?

11. A empresa tem serviços de computação em nuvem na internet? (ex: serviço de correio eletrónico; armazenamento de ficheiros)
    11.1 Sim
    11.2 Não

12. A empresa utiliza serviços de *big data*?
    12.1 Sim
    12.2 Não
    12.3 Não sei

13. A empresa tem pessoal especialista em TIC (Tecnologias de Informação e Comunicações)?
    13.1 Sim
    13.2 Não

14. A empresa utiliza dispositivos ou sistemas interconectados que podem ser monitorizados ou controlados remotamente através da Internet (IoT)?
    14.1 Sim
    14.2 Não

Parte 3. Conhecimentos sobre o RGPD – Regulamento Geral sobre a Proteção de Dados

15. A empresa tem conhecimento do que é o RGPD?
    15.1 Sim
    15.2 Não

16. Se a resposta anterior foi afirmativa, quando teve conhecimento?
    16.1 Antes de 2018
    16.2 Em 2018
    16.3 2019 e/ou 2020
    16.4 Só em 2021

17. Considera que a empresa, e os/as seus/suas colaboradores/as, têm um bom nível de conhecimento sobre o regulamento?
    17.1 Sim, muito bom
    17.2 Sim, bom
    17.3 Sim, suficiente
    17.4 Não, limitado
    17.5 Não, muito limitado

18. Considera que a empresa tem um bom nível de implementação do regulamento?
    18.1 Sim
    18.2 Não
    18.3 Não sei

19. Quais as principais dificuldades na implementação do regulamento?
    19.1 Sem dificuldades

19.2 Falta de conhecimento sobre o tema (RGPD)
19.3 Falta de formação (contínua) sobre o tema (RGPD)
19.4 Falta de Recursos Humanos
19.5 Incapacidade em identificar se os dados são alvo de um tratamento lícito
19.6 Falta de Recursos Informáticos / Tecnologia
19.7 Desconhecimento dos direitos dos titulares dos dados
19.8 Desconhecimento quanto aos contratos com prestadores de serviços relativamente à conformidade com o RGPD
19.9 Falta de recursos financeiros para as alterações necessárias
19.10 Falta de orientações práticas ou de normas de aplicação
19.11 Incapacidade em identificar todos os dados pessoais que a empresa possui
19.12 Necessidade de definir uma metodologia para cumprir as obrigações do RGPD
19.13 Inexistência de avaliação regular da conformidade com o RGPD
19.14 Desconhecimento da obrigação de notificação de uma violação de dados pessoais à Autoridade de Controlo
19.15 Outro, qual?

20. Quais os principais desafios que a empresa perceciona em relação à conformidade com o RGPD?
    20.1 Definição de processos
    20.2 Identificação, classificação e gestão dos dados
    20.3 Formação dos/as colaboradores/as
    20.4 Estabelecimento de medidas de segurança
    20.5 Gestão do consentimento
    20.6 Abordagem baseada em risco
    20.7 Outro, qual?

21. Quais os principais benefícios do RGPD para a sua empresa?
    21.1 Melhoria da segurança e privacidade da informação
    21.2 Melhoria da gestão da informação
    21.3 Garantia da confiança dos clientes
    21.4 Redução do risco sancionatório
    21.5 Melhoria da imagem pública e reputação da organização
    21.6 Outro, qual?

Parte 4. Implementação do RGPD em PME

22. Conhece a ENISA – Agência da União Europeia para a Segurança de Redes e Informações, e as suas orientações para as PME, no sentido de ajudá-las a avaliar os riscos de segurança e, consequentemente, adotar medidas de segurança para a proteção de dados pessoais, e garantir a conformidade com o RGPD?
    22.1 Sim
    22.2 Não

23. Conhece os controlos de segurança da ISO/IEC 27001:2013?
    23.1 Sim
    23.2 Não

24. Conhece a extensão da ISO/IEC 27001 para a gestão de informações de privacidade – ISO/IEC 27701:2019?
    24.1 Sim
    24.2 Não

Parte 5. Próximos passos – PROVA DE CONCEITO

25. Deseja realizar uma Prova de Conceito da solução proposta para proteção da privacidade e dos dados pessoais, do âmbito deste trabalho de mestrado?
    25.1 Sim
    25.2 Não

26. Se sim, indique por favor os dados para ser contactado/a (nome, email e/ou telefone). Em alternativa pode contactar diretamente para o email 201929286@academia.uatlantica.pt.

Anexo 2 – E-mail marketing de divulgação – Newsletter ANPME

https://mkt.anpme.pt/vl/44620102eaf4263ca7b559b6a5b48da2900590a8de8BeN01PeXuded034d70-cd

SOBRE O IMPACTO DO RGPD NAS PME

UAtlantica

"Em 25 de maio de 2018 foi implementado o **Regulamento Geral da Proteção de Dados (RGPD)** e desde então **foram aplicadas multas no valor de milhões de euros** no Espaço Económico Europeu (EEE).

Gostaria de convidá-lo(a) a participar no nosso inquérito, no link abaixo indicado, que visa explorar o **impacto do RGPD nas Pequenas e Médias Empresas**, em Portugal.

Este inquérito tem um tempo de preenchimento estimado em 10 minutos e insere-se num projeto de dissertação de **mestrado do Aluno Luís Pedroso, em Gestão de Sistemas e Tecnologias da Informação** na Universidade Atlântica, e que tem como objetivo apresentar uma proposta de **Solução para Proteção da Privacidade e dos Dados Pessoais baseada em Sanções Jurídicas do RGPD**, sob a orientação da Professora Doutora Virgínia Araújo."

CLICK AQUI PARA PARTICIPAR

QR CODE DO INQUÉRITO →

PARA MAIS INFORMAÇÕES
+351 226 052 340 | geral@anpme.pt

SEDE - LISBOA TAGUSPARK, NÚCLEO CENTRAL, 76 2740-122 OEIRAS | (+351) 213 867 597
DELEGAÇÃO NORTE - PORTO RUA JÚLIO DINIS, 210 4050 - 318 PORTO | (+351) 226 052 340
WWW.ANPME.PT

Anexo 3 – Etapa 0: caracterização geral

Etapa 0: caracterização geral

Esta etapa diz respeito à codificação do tratamento alvo de avaliação do risco, à caracterização geral da organização alvo da avaliação, e respetivo enquadramento em termos de tratamento de dados, por exemplo, se subcontratante, responsável pelo tratamento ou responsável conjunto, tendo como referência os modelos de registo das atividades de tratamento (CNPD, 2019).

1. # tratamento

1.1 Número do tratamento (ex: T000)

2. Enquadramento da Organização no tratamento de dados

2.1 Enquadramento da Organização (ex: subcontratante; responsável pelo tratamento; responsável conjunto)

3. Dados da Organização

3.1 Nome
3.2 Morada
3.3 E-mail
3.4 Telefone
3.5 Nome da pessoa de contacto
3.6 Área / Departamento

4. Dados do Encarregado de Proteção de Dados (se existir)

4.1 Nome
4.2 Morada
4.3 E-mail
4.4 Telefone

5. Dados do(s) Responsável(eis) Conjunto(s) (se existir(em))

5.1 Nome
5.2 Morada
5.3 E-mail
5.4 Telefone
5.5 Nome da pessoa de contacto
5.6 Referência par o(s) acordo(s) conjunto(s)

Anexo 4 – Etapa 1: Definição da operação de tratamento e seu contexto

Etapa 1: Definição da operação de tratamento e seu contexto

Esta etapa é o ponto de partida da avaliação do risco e é fundamental para a organização definir os limites do sistema de tratamento de dados (em avaliação) e o seu contexto. Para apoiar as PME na definição da atividade de tratamento, é fornecido um conjunto de perguntas.
Ao responder a essas perguntas, uma PME precisa considerar as várias fases do tratamento de dados (recolha, conservação, utilização, transferência, eliminação, etc.) e seus parâmetros subsequentes (ENISA, 2017, pág.10).

Pergunta n.º 1: Qual é a operação de tratamento de dados pessoais?
Um ponto importante a considerar aqui é que pode ser preferível executar diferentes processos de avaliação de risco para diferentes operações de tratamento de dados, mesmo que sejam geridos através dos mesmos meios técnicos (redes de TI, sistemas, aplicativos). Isso é especialmente importante no caso de operações de tratamento que envolvam dados de natureza e sensibilidade diferentes e, portanto, apresentam níveis de risco diferentes para o titular dos dados (ENISA, 2016, pág.18).

Exemplo: uma empresa gere por meio do seu sistema de TI os dados de RH (por exemplo, dados sobre salários, licenças, etc.) e dados sobre pedidos de compra com parceiros externos. Um processo de avaliação de risco diferente deve, em princípio, ser seguido para as duas operações, pois no primeiro caso os dados pessoais envolvidos são mais críticos (ou mesmo sensíveis) e, portanto, provavelmente resultariam num nível de risco mais alto do que no segundo caso. Isso também pode resultar em diferentes tipos de controlos de segurança. Se um único exercício de avaliação de risco for realizado, o risco mais alto deverá, no final, ser considerado (ou seja, o do sistema de RH) para ambas as operações de tratamento (ENISA, 2016, pág.18).

Pergunta n.º 2: Quais são os tipos de dados pessoais tratados?
Claramente relacionados com a pergunta anterior, os tipos de dados pessoais podem, por um lado, ajudar a definir a operação de tratamento, enquanto, por outro lado, dar uma indicação inicial do nível de risco potencial (ENISA, 2016, pág.18).

Exemplo: quando categorias especiais de dados ("dados confidenciais") estão envolvidas, o risco é, por padrão, maior. Categorias especiais de dados incluem (Artigo 9º RGPD):
dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa (ENISA, 2016, pág.18).

A pergunta 2 é densificada com os tipos de dados pessoais propostos pela CNPD, em especial para micro, pequenas e médias empresas, a saber (CNPD, 2019):
- Dados de identificação (ex: nome, fotografia, número de identificação civil);
- Dados de contacto (ex: morada, e-mail, telefone);
- Dados de faturação (ex: NIF, montante cobrado, data, IBAN);

- Dados de vida familiar (ex: situação familiar, dados do agregado familiar, estado civil);
- Dados de vida profissional (ex: CV, situação profissional, escolaridade, formação, distinções, diplomas);
- Dados de informações de ordem financeira e patrimonial (ex: vencimento, situação financeira, dados bancários, rendimentos, património);
- Dados de tráfego e de localização (ex: endereços IP, logs, identificadores dos terminais, identificadores de ligação, dados de data e hora, dados de GPS, GSM, pontos wi-fi);
- Dados de navegação na internet (ex: IP cookies de sessão, cookies de utilizador, cookies de terceiros, dados de navegação, device fingerprinting, medição de acesso a sites e interação através de ferramentas analíticas e de monitorização);
- Dados de outras categorias de dados pessoais não sensíveis (ex: cor dos sapatos na festa de Natal);
- Dados de perfis (ex: hábitos de vida, bom devedor, saudável);
- Dados de categorias especiais (Artigo 9º, n.º1) (ex: origem racial ou étnica, opiniões políticas, convicções religiosas e filosóficas, filiação sindical, dados genéticos, dados biométricos (controlo de acesso físico, controlo de acesso lógico), dados sobre a saúde, a vida sexual e a orientação sexual);
- Dados relacionados com condenações penais e infrações (Artigo 10º) (ex: dados relativos às condenações e às infrações penais);
- Seus prazos de conservação (ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual);

e de acordo com as várias categorias dos titulares dos dados:
- Recursos Humanos;
- Clientes;
- Potenciais clientes;
- Fornecedores;
- Outros.

Pergunta n.º 3: Qual é a finalidade do tratamento?
A finalidade está diretamente ligada à operação de tratamento de dados e pode ajudar a organização a compreender os limites do tratamento (por exemplo, no que diz respeito a quem obtém acesso aos dados e a forma como esse acesso é fornecido). No decorrer da avaliação de risco, pode ser necessário distinguir as operações de tratamento de dados com base na finalidade, mesmo quando os mesmos tipos de dados estão envolvidos (ENISA, 2016, pág.18).

Exemplo: uma PME trata o nome, endereço postal e / ou e-mail dos seus clientes no contexto de um serviço de compras online. Os mesmos tipos de dados podem ser tratados pela PME para o envio de material de marketing (ofertas, newsletters) aos clientes. Ainda assim, as duas operações de tratamento, pelas suas finalidades distintas, podem apresentar diferentes tipos de riscos que precisam ser tratados de forma mais específica (ENISA, 2016, pág.18).

A CNPD apresenta também os seguintes exemplos: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidade / gestão de clientes / marketing / gravação de chamadas na relação contratual / gestão de processos clínicos / gestão de crédito e solvabilidade (CNPD, 2019).

Pergunta n.º 4: Quais são os meios utilizados para o tratamento dos dados pessoais?
O tratamento de dados pessoais pode ocorrer de forma automatizada ou não automatizada ou ambas, incluindo redes, sistemas ou aplicações de TI específicos. As PME também podem

contar parcial ou totalmente com os meios técnicos de um subcontratante (por exemplo, cloud provider / fornecedor de serviços em nuvem) para a prestação de seu serviço. É importante, assim, compreender claramente os meios de tratamento, prestando particular atenção ao facto de estes poderem sofrer alterações nas diferentes fases do tratamento (recolha, conservação, utilização, transferência, eliminação de dados pessoais) (ENISA, 2016, pág.18).

Exemplo: Um sistema de CRM (Customer Relationship Management /Gestão de Relacionamento com o Cliente) pode ser usado por uma PME para o tratamento de dados pessoais do cliente. Uma plataforma de comércio eletrónico também pode ser usada para vendas online e tratamento de dados pessoais dos clientes. Estes sistemas podem ser hospedados e mantidos pela PME ou a PME pode usar aplicações relevantes de um cloud provider / fornecedor de serviços em nuvem (nuvem como soluções de serviço) (ENISA, 2016, pág.19).

Pergunta n.º 5: Onde ocorre o tratamento de dados pessoais?
A localização dos dados pessoais também é um fator importante, especialmente quando os serviços dos subcontratantes são utilizados. É importante observar que, quando os dados pessoais são tratados num país terceiro (não pertencente à UE), mecanismos de proteção adicionais devem ser implementados (Capítulo V do RGPD) (ENISA, 2016, pág.19).

Exemplo: De modo a minimizar custos e recursos, uma PME terceirizou parte da sua infraestrutura e serviços de TI (usados para o tratamento de dados pessoais) para um cloud provider / provedor de nuvem com servidores em todo o mundo. Nesse caso, a PME deve especificar claramente com o cloud provider a localização dos dados e adotar os controlos necessários, de acordo com o RGPD (ENISA, 2016, pág.19).

Pergunta n.º 6: Quais são as categorias dos titulares dos dados?
Definir claramente os titulares dos dados (por exemplo, clientes, fornecedores, outros) é importante para a organização como parte da compreensão da operação de tratamento de dados. Em alguns casos, dependendo das categorias dos titulares de dados, uma indicação do nível de risco potencial já pode ser obtida nesta fase (ENISA, 2016, pág.19).

Exemplo: O tratamento de dados pessoais de crianças pode requerer atenção especial devido ao fato de que muitas vezes as crianças não são informadas sobre o tratamento (ENISA, 2016, pág.19).

A pergunta 6 é densificada com as várias categorias dos titulares de dados propostos pela CNPD, em especial para micro, pequenas e médias empresas, alinhada à pergunta n. º2, a saber (CNPD, 2019):
- Recursos Humanos;
- Clientes;
- Potenciais clientes;
- Fornecedores;
- Outros (se sim, quais).

Pergunta n.º 7: Quais são os destinatários dos dados?
Definir os destinatários dos dados ajuda na compreensão das transferências autorizadas dos dados pessoais, bem como das condições dessas transferências. Às vezes, grupos de destinatários podem ser definidos. Certas transferências podem acarretar riscos específicos que já nesta fase é bom para a organização reconhecer (ENISA, 2016, pág.19).

Exemplo: um site de namoro on-line fornece acesso aos perfis dos utilizadores para todos os utilizadores registados (como parte da prestação do serviço). Também pode ser solicitado o acesso a informações relacionadas com taxas de assinatura e pagamentos aos serviços de auditoria financeira do Estado (ENISA, 2016, pág.19).

A pergunta 7 é densificada com os campos de preenchimento obrigatório propostos pela CNPD, em especial para micro, pequenas e médias empresas, a saber, por destinatário (CNPD, 2019):
- Nome do destinatário;
- NIF;
- País;
- Categorias de dados;
- Categoria do destinatário (ex: destinatário dentro da UE/EEE; destinatário fora da UE);
- Se transferência internacional nos termos do artigo 49º, n.º 1, segundo parágrafo, link para o documento que comprove a existência de garantias adequadas;
- Classificação do destinatário (ex: subcontratante; responsável pelo tratamento; responsável conjunto; terceiro).

Pergunta n.º 8: Qual a licitude do tratamento?
O tratamento só é lícito se e na medida em que se verifique pelo menos uma das situações do artigo 6º do RGPD.

Exemplo: consentimento, contrato, interesse legítimo, obrigação legal, prestação de serviços de saúde, interesse público ou exercício de autoridade pública (CNPD, 2019).

Esta pergunta não consta na metodologia da ENISA mas é um ponto essencial que se encontra nos modelos de registo das atividades de tratamento da CNPD (CNPD, 2019), desenvolvidos em especial para as micro, pequenas e médias empresas, através das várias opções de resposta, de acordo com o artigo 6º do Regulamento, a saber:
- Consentimento;
- Contrato ou diligências pré-contratuais;
- Obrigação jurídica;
- Interesses vitais;
- Interesse público;
- Interesses legítimos.

Anexo 5 – Etapa 2: Compreender e avaliar o impacto

Etapa 2: Compreender e avaliar o impacto

Com base na análise da Etapa 1, a organização, nesta fase, deve avaliar o impacto sobre os direitos e liberdades fundamentais dos titulares dos dados, resultante da possível perda de segurança dos dados pessoais. Quatro níveis de impacto são considerados (baixo, médio, alto, muito alto) (ENISA, 2017, pág.11).
O nível de impacto está sempre correlacionado com as consequências que uma violação de segurança de dados pessoais pode ter para os indivíduos (cujos dados foram violados). O incidente de segurança pode estar associado a qualquer tipo de violação de confidencialidade, integridade ou disponibilidade de dados pessoais (ENISA, 2016, pág.19).

A avaliação do impacto é um processo qualitativo e uma série de fatores precisam de ser considerados pelo responsável pelo tratamento, como os tipos de dados pessoais, criticidade da operação de tratamento, volume de dados pessoais, características especiais do responsável pelo tratamento, também como categorias especiais de titulares dos dados (ENISA, 2017, pág.11). De seguida são apresentados os fatores que precisam de ser considerados:

Tipo de dados pessoais: este parâmetro pode, por natureza, aumentar ou diminuir imediatamente o nível de impacto, com base na criticidade dos dados. Por exemplo, quando os dados incluem arquivos médicos ou informações sobre convicções políticas (ou qualquer outra categoria especial de dados constante no RGPD), o impacto de uma violação de segurança pode ser grave para os indivíduos. Ainda assim, a avaliação não pode basear-se apenas na distinção de dados entre "dados simples" e categorias especiais de dados. Na verdade, mesmo os dados pessoais que não se enquadram numa categoria especial podem revelar informações muito críticas sobre um indivíduo (por exemplo, localização, hábitos, informações financeiras) e, assim, trazer efeitos desastrosos sobre ele em caso de violação (ENISA, 2016, pág.21).

Criticidade da operação de tratamento: após o ponto acima mencionado, é importante avaliar a criticidade geral da operação de tratamento, além dos tipos particulares de dados. Deve-se dar atenção especial às operações de tratamento que se baseiam ou podem levar ao rastreamento, monitorização ou vigilância sistemáticos de indivíduos (ENISA, 2016, pág.21).

Volume dos dados pessoais tratados: este parâmetro refere-se à quantidade de dados pessoais que são tratados para um único indivíduo: quanto mais dados, mais potenciais efeitos adversos. O volume deve ser considerado em termos de tempo (por exemplo, o mesmo tipo de dados durante um determinado período de tempo) e conteúdo (complementando dados do mesmo tipo). Por exemplo, no caso de violação da confidencialidade dos dados de tráfego num ISP – *Internet Service Provider* / Prestador de serviço de acesso à internet, o impacto para um indivíduo seria maior se esses dados cobrissem todo o período de um ano, em vez de se limitarem a apenas uma semana (ENISA, 2016, pág.21).

Características especiais do responsável pelo tratamento / subcontratante: este parâmetro refere-se ao campo de operação e às atividades de negócios da organização, que podem por natureza revelar informações adicionais para um determinado conjunto de dados (assim, potencialmente afetando o nível de impacto). Por exemplo, a violação da confidencialidade de

uma lista de clientes pode ser maior se esta lista vier de uma farmácia online do que de uma papelaria (ENISA, 2016, pág.21).

Características especiais dos titulares dos dados: o impacto também pode aumentar caso os titulares dos dados pertençam a um grupo social com necessidades específicas (por exemplo, menores, figuras públicas). Por exemplo, o tratamento de uma lista de números de telefone torna-se mais crítico se diz respeito a membros conhecidos da Assembleia da República ou do Governo (ENISA, 2016, pág.21).

Exemplos:
Como referido pela ENISA (2016), estes exemplos devem ser considerados apenas como indicativos do nível de impacto. O responsável pelo tratamento / subcontratante deve sempre seguir uma análise aprofundada, com base nas especificidades da sua operação de tratamento de dados.

Caso 1 - Um supermercado / restaurante processa a lista de nomes e informações de contato dos seus clientes, que são utilizadas para realizar compras online. Nenhum outro dado pessoal de clientes é tratado. Nesse caso, o impacto pode ser considerado baixo, uma vez que uma potencial violação de segurança desses dados pode trazer apenas pequenos inconvenientes para os titulares dos dados (por exemplo, comunicação não solicitada por anunciantes), que podem ser facilmente superados (por exemplo, registo no *Do-Not-Call* do seu prestador de serviço telefónico) (ENISA, 2016, pág.21).

Caso 2 - O supermercado / restaurante também processa a lista de compras e preferências dos clientes ao longo do ano. Nesse caso, o impacto pode ser considerado médio se esta lista puder levar a um perfil dos hábitos e preferências dos titulares dos dados (por exemplo, com base no que eles compram e com que frequência) e / ou divulgação de informações adicionais (número de membros da família, especiais necessidades dietéticas, etc.). Em caso de violação desses dados, os indivíduos podem encontrar inconvenientes significativos que provavelmente ainda seriam capazes de se recuperar com algumas dificuldades (por exemplo, stress/ansiedade devido à divulgação de certos hábitos diários) (ENISA, 2016, pág.21).

Caso 3 - Uma farmácia com serviços especializados que, no âmbito do comércio eletrónico, processa a lista de nomes e informações de contato dos seus clientes, quando vende produtos para pacientes com diabetes. Nesse caso, devido às características especiais desta loja, que podem até revelar dados sensíveis sobre determinados indivíduos, o impacto deve ser considerado alto. Na verdade, em caso de violação da confidencialidade desses dados, suposições sobre o estado de saúde dos clientes (diabetes) podem ser feitas, o que pode levar a consequências significativas que são difíceis de superar (por exemplo, divulgação indesejada dessas informações sensíveis a membros da família e amigos) (ENISA, 2016, pág.22).

Caso 4 - Uma organização que apoia a recuperação de toxicodependentes para encontrar nomes de processos de emprego e currículos dessas pessoas. Nesse caso, o impacto poderia ser considerado muito alto, uma vez que uma violação de segurança (confidencialidade) relacionada a esses dados pode levar a consequências muito graves tanto para a sua situação física como psicológica, podendo até ser fatais (ENISA, 2016, pág.22).

Além dos parâmetros mencionados acima, outro aspeto importante que pode ser considerado pela organização é a identificabilidade dos titulares dos dados, ou seja, quão fácil é para uma

parte que tem acesso ao conjunto de dados relacioná-los univocamente a uma determinada pessoa. A fim de considerar a identificabilidade, deve-se levar em conta as possibilidades de identificação direta (por exemplo, com base no nome do titular dos dados), bem como aquelas de identificação indireta (por exemplo, com base num número de identificação ou outro identificador). Além disso, devem ser tidas em consideração medidas que possam reduzir a inteligibilidade dos dados pessoais (como por exemplo a encriptação), reduzindo assim a possibilidade de divulgação não autorizada de dados pessoais (ENISA, 2016, pág.22).

É importante notar que, ao avaliar o impacto, também devem ser considerados possíveis efeitos secundários (para os direitos e liberdades dos indivíduos). Por exemplo, quando o tratamento inclui nomes de utilizador / senhas para perfis online, deve-se levar em consideração que os indivíduos tendem a reutilizar as mesmas senhas em diferentes serviços online (e, portanto, uma possível violação dessas senhas também pode levar a mais violações de dados pessoais) (ENISA, 2016, pág.22).

O impacto, deste modo, é avaliado separadamente quanto à perda de confidencialidade, integridade e disponibilidade, de modo a, mais uma vez, melhor apoiar o responsável pelo tratamento / subcontratante na compreensão das especificidades do seu tratamento de dados pessoais. É importante considerar todos os casos possíveis de divulgação não autorizada, alteração ou destruição **e avaliar o impacto com base no pior cenário**.

Pergunta n.º 1 – perda de confidencialidade: Por favor, reflita sobre o impacto que uma divulgação não autorizada (perda de confidencialidade) de dados pessoais - no contexto em que a sua atividade comercial ocorre - poderia ter sobre a pessoa / titular dos dados e expresse uma classificação em conformidade.
Exemplos / cenários de perda de confidencialidade:
- Um arquivo de papel ou em laptop que contém dados pessoais é perdido durante o transporte.
- O equipamento foi eliminado sem destruição dos dados pessoais.
- Os dados pessoais são enviados indevidamente a vários destinatários não autorizados.
- Alguns clientes podem aceder a contas de outros clientes num serviço online.
- Os dados pessoais são publicados num contexto de mensagens na Internet ou site P2P (Peer-to-peer).
- Um CD-ROM com dados do cliente foi roubado das instalações.
- Um site configurado incorretamente torna publicamente acessível na internet os dados de utilizadores internos (ENISA, 2016, pág.23).

Pergunta n.º 2 – perda de integridade: Por favor, reflita sobre o impacto que uma alteração não autorizada (perda de integridade) de dados pessoais - no contexto em que a sua atividade comercial ocorre - poderia ter sobre a pessoa / titular dos dados e expresse uma classificação em conformidade.
Exemplos / cenários de perda de integridade:
- Foi alterado o cadastro necessário para a prestação do serviço social online e a pessoa / titular dos dados precisa solicitar o serviço offline.
- Um registo que é importante para a exatidão do arquivo de uma pessoa / titular dos dados num serviço médico online foi alterado (ENISA, 2016, pág.23).

Pergunta n.º 3 – perda de disponibilidade: Por favor, reflita sobre o impacto que uma destruição ou perda não autorizada (perda de disponibilidade) de dados pessoais - no

contexto em que a sua atividade comercial ocorre - poderia ter sobre a pessoa / titular dos dados e expresse uma classificação em conformidade.
Exemplos / cenários de perda de disponibilidade:
- Uma base de dados do cliente está corrompida e é necessário desenvolvimento de tarefas adicionais para colocar novamente o serviço online.
- Um arquivo pessoal é perdido e a pessoa / titular dos dados precisa de fornecer novamente algumas informações à organização.
- Um arquivo foi perdido / base de dados corrompida e não há backup dessas informações.
- Um serviço crítico (por exemplo, registo médico online) está indisponível e não pode ser recuperado imediatamente (ENISA, 2016, pág.23).

Respostas possíveis: 1 – Baixo; 2 – Médio; 3 – Alto; 4 - Muito Alto (ENISA, 2016, pág.20), onde:

1 - Baixo - As pessoas podem encontrar alguns pequenos inconvenientes, que serão superados sem problemas (tempo gasto para reintroduzir informações, aborrecimentos, irritações, etc.).

2 - Médio - As pessoas podem encontrar inconvenientes significativos, que serão capazes de superar apesar de algumas dificuldades (custos extras, recusa de acesso aos serviços comerciais, medo, falta de compreensão, ansiedade / stress, pequenas doenças físicas, etc.).

3 - Alto - As pessoas podem enfrentar consequências significativas, que devem ser capazes de superar, embora com sérias dificuldades (apropriação indevida de ativos financeiros, lista negra de instituições financeiras, danos materiais, perda de emprego, intimidação, degradação do estado de saúde, etc.).

4 - Muito Alto - As pessoas podem enfrentar consequências significativas, ou mesmo irreversíveis, que não podem superar (incapacidade para o trabalho, doenças físicas ou psicológicas de longo prazo, morte, etc.).

Anexo 6 – Etapa 3: Definição de possíveis ameaças e avaliação da sua probabilidade

Etapa 3: Definição de possíveis ameaças e avaliação da sua probabilidade

Nesta etapa, o objetivo da organização é entender as ameaças relacionadas com o ambiente geral do tratamento de dados pessoais (externos ou internos) e avaliar a sua probabilidade (probabilidade de ocorrência de ameaças) (ENISA, 2017, pág.12).

Neste contexto, uma ameaça é qualquer circunstância ou evento que tenha o potencial de afetar adversamente a segurança dos dados pessoais. Diferentes níveis e tipos de ameaças à confidencialidade, integridade e disponibilidade de dados pessoais podem ser considerados a este respeito. Deve-se notar que o contexto do tratamento de dados pessoais (tipos de dados, titulares dos dados, etc.) não é considerado como parte da probabilidade de ocorrência de ameaça, pois foi levado em consideração durante a avaliação do impacto (etapa 2) (ENISA, 2016, pág.24).

Exemplos de possíveis ameaças (a dados pessoais) (ENISA, 2016, pág.24):
- Um *hacker* injeta código num formulário de um website, com o objetivo de obter acesso aos dados pessoais armazenados no sistema.
- Um *hacker* executa um ataque *man-in-the-middle* para intercetar a comunicação eletrónica.
- Um funcionário rouba arquivos de dados pessoais do sistema interno.
- O funcionário de um hospital (de forma maliciosa ou acidental) altera um parâmetro crítico no arquivo médico de um paciente.
- Devido a um corte de energia, o sistema de TI da base de dados dos clientes está indisponível.
- Uma unidade flash USB com arquivos de dados pessoais é perdida durante o transporte por um subcontratante.

Para simplificar esta etapa para as PME, a ENISA definiu uma série de questões de avaliação que podem ajudar uma organização (atuando como responsável pelo tratamento ou subcontratante) a entender as ameaças e a calcular a sua probabilidade de ocorrência. Estas questões visam, na verdade, apoiar o processo de avaliação, tornando a organização ciente do ambiente de tratamento de dados (que é diretamente relevante para as ameaças). As questões estão agrupadas em quatro dimensões, a saber (ENISA, 2016, pág.24):

A - Rede e recursos técnicos (hardware e software)
B - Processos / procedimentos relacionados com o tratamento de dados pessoais
C - Diferentes partes e pessoas envolvidas no tratamento de dados pessoais
D - Setor empresarial e dimensão do tratamento

Como no caso da avaliação de impacto, a avaliação da probabilidade de ocorrência de uma ameaça só pode ser qualitativa, pois está muito relacionada com o ambiente específico de tratamento de dados pessoais. No contexto desta abordagem, estão definidos três níveis de probabilidade de ocorrência de uma ameaça (ENISA, 2016, pág.29):

1 - Baixo - é improvável que a ameaça se materialize.
2 - Médio - há uma possibilidade razoável de que a ameaça se materialize.

3 - Alto - a ameaça provavelmente se materializará.

Seguindo os níveis acima, a organização é solicitada a avaliar a probabilidade de ameaças para cada uma das quatro áreas diferentes apresentadas acima, ou seja, rede e recursos técnicos, processos / procedimentos relacionados com o tratamento de dados pessoais, diferentes partes e pessoas envolvidas no tratamento de dados pessoais, setor empresarial e dimensão do tratamento (ENISA, 2016, pág.29).

Se todas as respostas, numa área de avaliação, forem positivas, a organização deve considerar a probabilidade de ameaça para essa área como alta, enquanto que se todas forem negativas, a probabilidade de ameaça deve ser considerada baixa. Para casos com duas a três respostas positivas, a organização deve atribuir a probabilidade de ameaça média (ENISA, 2016, pág.29).

Em cada uma das perguntas, uma resposta positiva (SIM) indica uma alta probabilidade de ameaça, enquanto que uma resposta negativa (NÃO), uma menor probabilidade de ameaça. Com base nesse entendimento, a avaliação da probabilidade de ocorrência de uma ameaça é realizada (ENISA, 2016, pág.29).

Conforme discutido anteriormente, as perguntas não podem ser consideradas exaustivas, mas apenas indicativas e, consequentemente, a correlação de respostas positivas / negativas com os níveis de probabilidade de ocorrência de ameaças (ENISA, 2016, pág.30).
Apresentam-se de seguida as vinte questões, organizadas pelas suas quatro dimensões:

A - Rede e recursos técnicos (hardware e software)
As ligações de rede podem introduzir ameaças tanto de fontes externas (por exemplo, invasores externos com o objetivo de obter acesso remoto ao sistema ou derrubar o sistema), bem como fontes internas (por exemplo, interconexão com outros sistemas de TI dentro da mesma organização que têm falhas de segurança). Recursos de hardware e software também podem apresentar ameaças, por exemplo, devido à má manutenção e configuração, bem como devido a bugs e *backdoors* relacionados ao desenvolvimento de dispositivos e software. Ameaças comuns associadas aos recursos de rede e técnicos (hardware / software) incluem espionagem de canais de comunicação, acesso não autorizado a base de dados, indisponibilidade de serviços fornecidos, falha de links de comunicação, uso indevido / uso anormal de sistemas de informação, etc. (ENISA, 2016, pág.24).

1 - Alguma parte do tratamento de dados pessoais é realizada pela internet?
Quando o tratamento de dados pessoais é realizado total ou parcialmente por meio da Internet exposta, aumentam as possíveis ameaças de invasores online externos (por exemplo, negação de serviço / Denial of Service, injeção de SQL / SQL injection, ataques Man-in-the-Middle), especialmente quando o serviço está disponível (e, portanto, rastreável / conhecido) para todos os utilizadores da Internet (ENISA, 2016, pág.25).
Exemplos:
- Um mercado eletrónico que oferece a possibilidade de compra online de mercadorias.
- Um portal de notícias eletrónicas que fornece informações personalizadas para utilizadores registados.
- Um sistema de CRM oferecido por meio de uma solução de nuvem como serviço /Cloud as a Service (ENISA, 2016, pág.25).

2 - É possível fornecer acesso a um sistema interno de tratamento de dados pessoais através da Internet (por exemplo, para determinados utilizadores ou grupos de utilizadores)?

Quando o acesso a um sistema interno de tratamento de dados é fornecido pela Internet, a probabilidade de ameaças externas aumenta (por exemplo, devido a invasores online externos). Ao mesmo tempo, a probabilidade de uso indevido (acidental ou intencional) de dados pelos utilizadores também aumenta (por exemplo, divulgação acidental de dados pessoais ao trabalhar em espaços públicos). Deve ser dada atenção especial aos casos em que a gestão / administração remota do sistema de TI é permitida (ENISA, 2016, pág.25).

Exemplos:

- Uma seguradora permite aos seus gestores o acesso remoto (através da Internet) aos arquivos dos clientes.
- Uma empresa de consultoria permite que os funcionários acedam ao sistema interno de gestão de licenças e missões pela Internet.
- Uma empresa fornece acesso remoto ao sistema a contratados externos para manutenção e suporte de TI (ENISA, 2016, pág.25).

3 - O sistema de tratamento de dados pessoais está interconectado a outro sistema ou serviço de TI externo ou interno (à sua organização)?

A ligação com sistemas de TI externos pode apresentar ameaças adicionais devido às ameaças (e potenciais falhas de segurança) que são inerentes a esses sistemas. O mesmo se aplica aos sistemas internos, tendo em conta que, se não configurados de forma adequada, tais ligações podem permitir o acesso (aos dados pessoais) a mais pessoas dentro da organização (que em princípio não estão autorizadas para tal acesso) (ENISA, 2016, pág.26).

Exemplos:

- Uma *e-bookshop* está ligada a um sistema de pagamento online (para permitir compras eletrónicas).
- Um pequeno sistema TI financeiro de uma clínica de saúde está ligado ao sistema de TI do sistema central de seguros (para validar o status de seguro dos pacientes).
- Um sistema de CRM interconectado com o sistema de TI de tratamento de pedidos e sistemas de suporte a pagamentos e emissão de faturas (ENISA, 2016, pág.26).

4 - Pessoas não autorizadas podem aceder facilmente ao ambiente de tratamento de dados?

Embora o foco tenha sido colocado em sistemas e serviços eletrónicos, o ambiente físico (relevante para esses sistemas e serviços) é um aspeto importante que, se não for devidamente protegido, pode comprometer seriamente a segurança (por exemplo, permitindo que partes não autorizadas tenham acesso físico aos equipamentos de TI e componentes de rede ou a falta de proteção da sala de informática em caso de desastre físico) (ENISA, 2016, pág.26).

Exemplos:

- Uma PME não tem uma sala de informática dedicada para administrar o sistema de TI usado para o tratamento de dados pessoais.
- Uma PME terceirizou o armazenamento dos seus dados para uma empresa que oferece armazenamento remoto de dados. Não está claro que medidas de segurança foram aplicadas pela empresa para proteger as instalações do data center e/ou outro local de armazenamento dos dados (ENISA, 2016, pág.26).

5 - O sistema de tratamento de dados pessoais é projetado, implementado ou mantido sem seguir as melhores práticas relevantes?

Componentes de hardware e software mal projetados, implementados e / ou mantidos podem representar sérios riscos à segurança da informação. Portanto, as melhores práticas acumulam a experiência de eventos anteriores e podem ser consideradas diretrizes práticas de como evitar a exposição e atingir certos níveis de resiliência (ENISA, 2016, pág.26).
Exemplos (de melhores práticas):
- Os diferentes componentes da rede e do sistema são baseados em tecnologias e protocolos de TI padrão (ao contrário das soluções ad-hoc).
- Hardware e software são obtidos por fornecedores confiáveis e seguindo procedimentos contratuais formais.
- Um plano de manutenção adequado está em vigor, incluindo a manutenção regular da rede e dos dispositivos e aplicações do sistema (ENISA, 2016, pág.26).

B - Processos / procedimentos relacionados com o tratamento de dados pessoais
Em muitos casos, as ameaças à segurança surgem da falta de processos e procedimentos internos adequados, exigindo regras e práticas específicas dentro da organização para o tratamento de dados pessoais. Essas ameaças incluem o acesso aos dados por pessoas não autorizadas, corrupção (não) intencional de dados, modificação / destruição não autorizada de dados, eliminação acidental ou perda de equipamento de tratamento de dados, etc. (ENISA, 2016, pág.25).

6 - As funções e responsabilidades em relação ao tratamento de dados pessoais são vagas ou não estão claramente definidas?
Quando as funções e responsabilidades não estão claramente definidas, o acesso (e tratamento posterior) dos dados pessoais pode ser descontrolados, resultando no uso não autorizado de recursos e comprometendo a segurança geral do sistema (ENISA, 2016, pág.26).
Exemplos:
- Os assistentes do departamento financeiro não podem apenas inserir informações, mas também modificá-las e excluí-las, assim como os gestores dos processos.
- As enfermeiras numa clínica médica podem modificar a ficha clínica do paciente, embora apenas os médicos devam ser capazes de o fazer (ENISA, 2016, pág.26).

7 - O uso aceitável da rede, do sistema e dos recursos físicos dentro da organização é ambíguo ou não está claramente definido?
Quando o uso aceitável de recursos não é claramente obrigatório, podem surgir ameaças à segurança devido a mal-entendidos ou uso impróprio intencional do sistema. A definição clara de políticas para rede, sistema e recursos físicos pode reduzir riscos potenciais (ENISA, 2016, pág.27).
Exemplos:
- Não está claro se os funcionários podem usar o seu endereço de e-mail profissional para comunicações pessoais.
- Não há uma política em vigor que obrigue o nível de uso da largura de banda que os funcionários têm permissão para fazer diariamente (ENISA, 2016, pág.27).

8 - Os funcionários podem trazer e usar os seus próprios dispositivos para se ligarem ao sistema de tratamento de dados pessoais?
Os funcionários que usam os seus dispositivos pessoais dentro da organização podem aumentar o risco de fuga de dados ou acesso não autorizado ao sistema de informação. Além disso, como os dispositivos não são controlados centralmente, eles podem introduzir bugs/erros ou vírus adicionais no sistema (ENISA, 2016, pág.27).

Exemplos:
- Os funcionários podem-se ligar à rede da empresa com seus tablets / equipamentos pessoais ou outros dispositivos inteligentes.
- Os funcionários têm permissão para tratar dados utilizando aplicações específicas instaladas nos seus equipamentos pessoais / dispositivos inteligentes (ENISA, 2016, pág.27).

9 - Os funcionários estão autorizados a transferir, armazenar ou tratar dados pessoais fora das instalações da organização?
O tratamento de dados pessoais fora das instalações da organização pode oferecer muita flexibilidade, mas ao mesmo tempo apresenta riscos adicionais, tanto relacionados à transmissão de informações através de canais de rede possivelmente inseguros (por exemplo, redes Wi-Fi abertas), como no uso não autorizado desta informação (ENISA, 2016, pág.27).
Exemplos:
- Uma agência de viagens permite que os funcionários usem os seus laptops profissionais fora das instalações da organização para tratar os dados dos clientes.
- Uma empresa de entregas permite que os funcionários usem tablets dedicados ao fazer a entrega para validar os detalhes do destinatário (ENISA, 2016, pág.27).

10 - As atividades de tratamento de dados pessoais podem ser realizadas sem a criação de arquivos de log/registos?
A falta de mecanismos de registo e monitorização adequados pode aumentar o abuso intencional ou acidental de processos / procedimentos e recursos, resultando no subsequente abuso de dados pessoais (ENISA, 2016, pág.27).
Exemplos:
- Não há lista de pessoas que acedem diariamente à sala de informática de uma empresa.
- O acesso aos arquivos médicos dos pacientes numa clínica não é registado.
- Não há uma política em vigor determinando como os logs/registos são monitorizados e que ações devem ser tomadas em caso de abuso repetido sob o sistema (ENISA, 2016, pág.27).

C - Diferentes partes e pessoas envolvidas no tratamento de dados pessoais
As ameaças à segurança também podem surgir daqueles que realizam o tratamento de dados pessoais, ou seja, os funcionários da organização envolvidos diretamente no tratamento, bem como outras partes que realizam parte do tratamento (subcontratantes). Ameaças relevantes incluem potenciais ataques internos maliciosos (por exemplo, com o apoio de funcionários específicos), uso indevido acidental de dados pessoais devido a erro humano, divulgação não autorizada de dados por contratantes externos, etc. (ENISA, 2016, pág.25).

11 - O tratamento de dados pessoais é realizado por um número indefinido de funcionários?
Quando o acesso (e posterior tratamento) de dados pessoais é aberto a um grande número de funcionários, as possibilidades de abuso devido ao fator humano aumentam. Definir claramente quem realmente precisa de aceder aos dados e limitar o acesso apenas a essas pessoas pode contribuir para a segurança dos dados pessoais (ENISA, 2016, pág.27).
Exemplos:
- O sistema de tickets do departamento de RH de uma empresa pode ser visualizado por todos os membros da equipa.
- Os registos médicos dos pacientes podem ser tratados por pessoal administrativo, pese embora apenas a equipa médica que está a realizar o tratamento deva ter acesso (ENISA, 2016, pág.27).

12 - Alguma parte da operação de tratamento de dados é realizada por um prestador de serviços / terceiro (subcontratante)?

Quando o tratamento é realizado por contratados externos / prestadores de serviços, a organização pode perder parcialmente o controlo sobre esses dados. Além disso, ameaças de segurança adicionais podem ser introduzidas devido às ameaças que são inerentes a esses contratantes. É importante para a organização selecionar prestadores de serviços que possam oferecer um alto nível de segurança e definir claramente que parte do tratamento é lhes atribuída, mantendo, tanto quanto possível, um alto nível de controlo (ENISA, 2016, pág.27).

Exemplos:

- O sistema de TI de uma escola particular é hospedado num data center externo.
- Os arquivos do cliente de uma seguradora são tratados por parceiros externos da empresa.
- Empresa especializada na destruição de fichas clínicas é contratada por uma clínica médica.
- Uma empresa usa uma solução *Cloud as a Service* para gerir recursos internos (ENISA, 2016, pág.27).

13 - As obrigações das partes / pessoas envolvidas no tratamento de dados pessoais são ambíguas ou não estão claramente definidas?

Quando os funcionários não são claramente informados sobre as suas obrigações, as ameaças de uso indevido acidental (por exemplo, divulgação ou destruição) de dados aumentam significativamente (ENISA, 2016, pág.28).

Exemplos:

- Os funcionários não são informados com clareza de que estão a tratar informações confidenciais que não podem ser divulgadas a terceiros não autorizados.
- Os parceiros externos de uma empresa não recebem instruções claras sobre o nível exigido de segurança dos dados pessoais por eles tratados (ENISA, 2016, pág.28).

14 - O pessoal envolvido no tratamento de dados pessoais não está familiarizado com as questões de segurança da informação?

Quando os funcionários não estão cientes da necessidade de aplicar medidas de segurança, eles podem acidentalmente representar outras ameaças ao sistema. A formação pode contribuir muito para consciencializar os funcionários tanto sobre as suas obrigações de proteção de dados, quanto sobre a aplicação de medidas de segurança específicas (ENISA, 2016, pág.28).

Exemplos:

- Nem todas as pessoas envolvidas no tratamento de dados são informadas sobre possíveis ameaças à segurança e uso adequado dos recursos.
- A equipa que lida com a central telefónica de uma empresa não foi informada sobre possíveis ataques de *phishing* e ataques direcionados (ENISA, 2016, pág.28).

15 - As pessoas / partes envolvidas na operação de tratamento de dados negligenciam o armazenamento seguro e / ou destruição de dados pessoais?

Muitas violações de dados pessoais ocorrem devido à falta de medidas de proteção física, como bloqueios e sistemas de destruição seguros. Os arquivos em papel geralmente fazem parte da entrada ou saída de um sistema de informação, podendo conter dados pessoais. Também devem ser protegidos contra a divulgação não autorizada e/ou sua reutilização (ENISA, 2016, pág.28).

Exemplos:

- Os dados de RH dos funcionários não são mantidos em armários fechados à chave.
- As cópias das faturas recebidas com detalhes de cartão de crédito e número de conta bancária não são destruídas com trituradoras de papel, após o seu tratamento (ENISA, 2016, pág.28).

D - Setor empresarial e dimensão do tratamento

O setor de negócios de uma organização, bem como a escala (volume) dos dados tratados, podem também afetar significativamente o tipo e o nível das ameaças à segurança. Por exemplo, se o tipo de dados pessoais é considerado um ativo valioso e / ou se o tratamento diz respeito a toda a população de um país, os *hackers* podem estar mais interessados em obter acesso a esses dados (ENISA, 2016, pág.25).

16 - Considera que este setor empresarial está sujeito a ciber ataques?

Quando os ataques à segurança já ocorreram num setor empresarial específico, é um indicador de que a organização provavelmente precisa tomar medidas adicionais para evitar um evento semelhante (ENISA, 2016, pág.28).

Exemplos:

- Várias empresas (do mesmo setor) foram atacadas durante o ano passado.
- Foi dada publicidade a possíveis ameaças à segurança e vulnerabilidades de um determinado setor de negócios (por exemplo, enquanto resultado de um estudo) (ENISA, 2016, pág.28).

17 - A organização sofreu algum ciber ataque ou outro tipo de violação de segurança nos últimos dois anos?

Se a organização já foi atacada ou se há indícios de que esse possa ter sido o caso, medidas adicionais devem ser tomadas para evitar eventos semelhantes no futuro (ENISA, 2016, pág.28).

Exemplos:

- O departamento de TI descobriu um número crescente de tentativas mal sucedidas de sistemas externos para obter acesso não autorizado às bases de dados.
- Os bloqueios no centro de dados central foram violados (ENISA, 2016, pág.28).

18 - Recebeu alguma notificação e / ou reclamação relativa à segurança do sistema informático (utilizado para o tratamento de dados pessoais) no último ano?

Bugs/erros ou vulnerabilidades de segurança podem ser explorados para realizar ataques (digitais ou físicos) a sistemas e serviços. Devem ser considerados boletins de segurança contendo informações importantes sobre vulnerabilidades de segurança que podem afetar os sistemas e serviços mencionados (ENISA, 2016, pág.28).

Exemplos:

- Os utilizadores do serviço online de um comércio eletrónico notificaram que podem aceder acidentalmente a contas de outros utilizadores.
- Os auditores descobriram que a política de senha utilizada por um serviço online é fraca (ENISA, 2016, pág.28).

19 - Uma operação de tratamento diz respeito a um grande volume de pessoas individuais e / ou dados pessoais?

O tipo e o volume dos dados pessoais (escala) podem tornar a operação de tratamento atrativa para os invasores (devido ao valor inerente desses dados) (ENISA, 2016, pág.29).

Exemplos:

- Uma aplicação de um hospital para registo online de informações que armazena dados de pacientes com doenças crónicas, numa abrangência para todo o país.
- Um website de namoro online que armazena perfis de centenas de utilizadores (ENISA, 2016, pág.29).

20 - Existem práticas recomendadas de segurança, específicas para este setor empresarial, que não foram seguidas de forma adequada?
As medidas de segurança são geralmente ajustadas às necessidades (e riscos) do setor empresarial em questão. A falta de conformidade com as práticas relevantes recomendadas pode ser um indicador de uma gestão de segurança frágil (ENISA, 2016, pág.29).
Exemplos (de possíveis práticas específicas do setor):
- Uma empresa sujeita a medidas de segurança específicas para dispositivos médicos, serviços financeiros ou serviços de telecomunicações (ENISA, 2016, pág.29).

Deve-se notar que, embora as questões acima mencionadas (e abordagem geral) visem cobrir um amplo espectro de ameaças à segurança externa e interna, elas não podem ser consideradas exaustivas, mas sim percebidas como indicativas da avaliação prática das ameaças (e sua ocorrência). Nesse sentido, fatores adicionais e, portanto, áreas de avaliação, podem precisar de ser levados em consideração pela organização, seguindo as especificidades do seu ambiente de tratamento de dados pessoais (ENISA, 2016, pág.29).

A probabilidade final de ocorrência de uma ameaça é calculada após a soma das pontuações obtidas nas quatro dimensões já mencionadas, associando o resultado à seguinte escala (ENISA, 2017, pág.15):

– Nível de probabilidade de ocorrência de ameaça BAIXO, se a soma geral da probabilidade estiver compreendida entre 4 e 5;

– Nível de probabilidade de ocorrência de ameaça MÉDIO, se a soma geral da probabilidade estiver compreendida entre 6 e 8; e

– Nível de probabilidade de ocorrência de ameaça ALTO, se a soma geral da probabilidade estiver compreendida entre 9 e 12.

Anexo 7 – Tratamento do risco - Lista completa de medidas

Tratamento do risco – Lista completa de medidas

Nesta etapa, duas categorias principais de medidas são discutidas: as medidas técnicas e as medidas organizativas. Estas categorias foram divididas em subcategorias com uma breve descrição, explicando como cada subcategoria se relaciona com as disposições específicas do RGPD (ENISA, 2016, pág.33).

Em cada subcategoria, as medidas são apresentadas por nível de risco, seguindo o mesmo esquema de cores usado nas etapas anteriores (baixo: verde, médio: amarelo, alto: vermelho). Para alcançar escalabilidade, presume-se que todas as medidas descritas no nível inferior (verde) são aplicáveis a todos os níveis. Da mesma forma, as medidas apresentadas no nível médio (amarelo) são aplicáveis também no nível de risco alto. As medidas apresentadas no nível alto (vermelho) não são aplicáveis em nenhum outro nível de risco (ENISA, 2016, pág.33).

Também está incluído um mapeamento do conjunto de medidas proposto com os controlos de segurança da ISO/IEC 27001:2013, relativo à segurança da informação (ENISA, 2016, pág.33). Abrange, também, a extensão para a gestão de informações de privacidade – ISO/IEC 27701:2019, e as suas relações com os requisitos do RGPD.

Para garantir a completude do regulamento, foram desenvolvidos novos controlos, iniciativa alinhada com as recomendações da ENISA. Por estar em causa a completude do regulamento, o nível de risco das novas medidas é sempre o mais baixo, para permitir a conformidade legal em todos os níveis de risco.

Esta fase do processo de gestão do risco concretiza-se numa só etapa: o início da construção do **plano de tratamento do risco**, que inclui a lista completa de medidas propostas por nível de risco, e sua relação com o RGPD, com vista ao cumprimento total das obrigações do mesmo.

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.1	Gestão de segurança
Categoria da Medida	4.1.1.1	Política de segurança e procedimentos para a proteção de dados pessoais

Descrição da Medida:

A política de segurança é um documento de alto nível que estabelece os princípios básicos para a segurança e proteção de dados pessoais numa organização, formando a base para a implementação de todas as medidas técnicas e organizativas específicas, de acordo com o artigo 32º do RGPD , também complementado pelo artigo 24º do RGPD (implementação de políticas de proteção de dados).
Com base na política de segurança, as medidas técnicas e organizativas específicas são descritas num conjunto de políticas / procedimentos mais detalhados (por exemplo, controlo de acesso, gestão de dispositivos, gestão de recursos, etc.).
A política de segurança mostra o compromisso geral da gestão da organização com a segurança e proteção de dados. Pode ser baseado ou fazer parte da política geral de segurança de TI da organização. De qualquer forma, deve abordar explicitamente também a proteção de dados pessoais.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
A.1	A organização deve definir e documentar a sua política com base no tratamento de dados pessoais enquanto parte da sua política de segurança da informação.	Baixo	A.5.1.1	(24)(2)	ENISA
A.2	A política de segurança deve ser revista e renovada, se necessário, anualmente.	Baixo	A.5.1.2	---	ENISA
A.3	A organização deve documentar, de forma autónoma, a sua política de segurança no que diz respeito ao tratamento de dados pessoais. A política deve ser aprovada	Médio	A.5.1.1	(24)(2)	ENISA

	pela administração e comunicada a todos os funcionários e partes externas relevantes.				
A.4	A política de segurança deve referir-se, pelo menos, a funções e responsabilidades do pessoal, a medidas técnicas e organizativas básicas adotadas para a segurança dos dados pessoais e aos subcontratantes ou outros terceiros envolvidos no tratamento de dados pessoais.	Médio	A.5.1.1	(24)(2)	ENISA
A.5	Um inventário de políticas / procedimentos específicos relativos à segurança de dados pessoais deve ser criado e mantido, com base na política geral de segurança.	Médio	A.5.1.2	---	ENISA
A.6	A política de segurança deve ser reavaliada e revista, se necessário, semestralmente.	Alto	A.5.1.2	---	ENISA

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.1	Gestão de segurança
Categoria da Medida	4.1.1.1.1	Contexto da organização

Descrição da Medida:

O contexto da organização é o ponto de partida para a definição de um sistema de gestão de segurança da informação. Para tal, é necessário conhecer as questões internas e externas mais relevantes, quais as necessidades e expetativas das partes interessadas, quais os limites, interfaces e dependências da aplicabilidade do sistema (âmbito), e que processos devem ser considerados.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
A.6.1	A compreensão da organização e do seu contexto deve incluir, tanto as questões internas, como as questões externas que são relevantes para a sua finalidade. Na existência de dados pessoais, a organização deve determinar a sua função: se responsável pelo tratamento, subcontratante ou responsável conjunto.	Baixo	4.1	(24)(3), (25)(3), (28)(5), (28)(6), (28)(10), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)	NOVO
A.6.2	A organização deve determinar quais as necessidades, requisitos e expetativas das partes interessadas que são relevantes para o sistema de gestão de segurança da informação, relevando aquelas que tratam dados pessoais.	Baixo	4.2	(31), (35)(9), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)	NOVO
A.6.3	A definição do âmbito permite delimitar o sistema de gestão. Este pode incluir toda a organização ou apenas uma parte. Deve ser baseado no contexto da organização, nos requisitos das partes interessadas e nas interfaces e dependências com outras organizações, devendo ser incluído também o tratamento de dados pessoais.	Baixo	4.3	(32)(2)	NOVO
A.6.4	A organização deve estabelecer um sistema de gestão de segurança da informação, incorporando os requisitos de privacidade, através da implementação de um conjunto de atividades com um propósito e com definição de responsabilidades, por via da sistematização de processos.	Baixo	4.4	(32)(2)	NOVO

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.1	Gestão de segurança
Categoria da Medida	4.1.1.1.2	Planeamento - Ações para endereçar riscos e oportunidades

Descrição da Medida:

A organização, durante o planeamento do sistema de gestão, deve determinar os riscos associados à perda de confidencialidade, integridade e disponibilidade, e determinar as oportunidades para alcançar os resultados previstos, reduzir efeitos indesejáveis e garantir a melhoria contínua dos processos. Deverá, nomeadamente, avaliar o risco de segurança da informação e realizar o respetivo tratamento do risco.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
A.6.5	A organização deve aplicar um processo de avaliação do risco de segurança da informação e privacidade para identificar os riscos associados à perda de confidencialidade, integridade e disponibilidade, incluindo critérios de aceitação, de avaliação e de priorização, tendo por base os resultados da análise do risco.	Baixo	6.1.2	(32)(1)(b), (32)(2)	NOVO
A.6.6	A organização deve aplicar um processo de tratamento do risco de segurança da informação e privacidade que inclua a seleção de opções de tratamento, a	Baixo	6.1.3	(32)(1)(b), (32)(2)	NOVO

	determinação de controlos, a produção de uma declaração de aplicabilidade, a elaboração e a aceitação de um plano de tratamento do risco, e aceitação do risco residual.				

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.1	Gestão de segurança
Categoria da Medida	4.1.1.2	Papéis e responsabilidades

Descrição da Medida:

"De acordo com o n.º 4 do artigo 32º do RGPD, "o responsável pelo tratamento e o subcontratante tomam medidas para assegurar que qualquer pessoa singular que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, só procede ao seu tratamento mediante instruções do responsável pelo tratamento, exceto se tal lhe for exigido pelo direito da União Europeia ou de um Estado-Membro". Portanto, enquanto controlo primordial para a segurança de dados pessoais, todas as funções da organização, com acesso a dados pessoais, devem ter claramente definidas e documentadas as responsabilidades, os papéis e a necessidade de conhecer (que são regularmente revistas).
Uma função de particular importância é a do Responsável de Segurança, que é responsável por monitorizar a correta implementação da política de segurança. Outra função importante é a do Data Protection Officer (DPO) / Encarregado de Proteção de Dados (EPD), que monitoriza a conformidade com o RGPD e, portanto, também precisa de colaborar com o Responsável de Segurança na implementação adequada das medidas de segurança. De referir que, de acordo com o RGPD (artigo 37º), a designação de um DPO /EPD é obrigatória para certos tipos de operações de tratamento de dados (atividades de monitorização em grande escala, tratamento de categorias especiais de dados, etc.)."

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
B.1	As funções e responsabilidades relacionadas com o tratamento de dados pessoais devem ser claramente definidas e atribuídas de acordo com a política de segurança.	Baixo	A.6.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)	ENISA
B.2	Durante reorganizações internas ou rescisões e mudanças de funções, a revogação de direitos e responsabilidades com os respetivos procedimentos de transferência deve ser claramente definida.	Baixo	A.6.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)	ENISA
B.3	Deve ser realizada uma nomeação clara das pessoas encarregadas de tarefas específicas de segurança, incluindo a nomeação de um responsável de segurança.	Médio	A.6.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)	ENISA
B.4	O responsável de segurança deve ser formalmente nomeado (documentado). As tarefas e responsabilidades do responsável de segurança também devem ser claramente definidas e documentadas.	Alto	A.6.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)	ENISA
B.5	As áreas e funções que podem gerar conflitos de interesse, por exemplo, nas funções de responsável de segurança, auditor de segurança ou DPO/EPD, devem ser segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional ou uso indevido de dados pessoais.	Alto	A.6.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)	ENISA

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.1	Gestão de segurança
Categoria da Medida	4.1.1.3	Política de controlo de acesso

Descrição da Medida:

"Seguindo a definição de funções e responsabilidades, é essencial determinar uma política de controlo de acesso aos sistemas utilizados para o tratamento de dados pessoais. Deve basear-se no princípio da necessidade de conhecer; ou seja, cada função / utilizador deve apenas ter o nível de acesso aos dados pessoais estritamente necessário para o desempenho das suas funções. Este é um conceito central também no RGPD e está intimamente relacionado com o princípio da minimização de dados (artigo 5º (c) do RGPD).
A política de controlo de acesso será implementada com as medidas técnicas subsequentes (ver também 4.2.1 neste documento)."

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
C.1	Devem ser atribuídos direitos de controlo de acesso específicos a cada função, envolvida no tratamento de dados pessoais, de acordo com o princípio da necessidade de conhecer.	Baixo	A.9.1.1	---	ENISA
C.2	Uma política de controlo de acesso deve ser detalhada e documentada. A organização deve determinar, neste documento, as regras de controlo de acesso apropriadas, direitos de acesso e restrições para funções específicas do utilizador nos processos e procedimentos relacionados com dados pessoais.	Médio	A.9.1.1	---	ENISA

C.3	A segregação de funções de controlo de acesso (por exemplo, solicitação de acesso, autorização de acesso, administração de acesso) deve ser claramente definida e documentada.	Médio	A.9.1.1	---	ENISA
C.4	As funções com excessivos direitos de acesso devem ser claramente definidas e atribuídas a membros específicos e limitados da equipa.	Alto	A.9.1.1	---	ENISA

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.1	Gestão de segurança
Categoria da Medida	4.1.1.4	Gestão de recursos / ativos

Descrição da Medida:

A gestão adequada dos recursos de hardware, software e redes é essencial para a segurança dos dados pessoais, na medida em que permite o controlo dos meios de tratamento e, desta forma, o controlo das subsequentes medidas técnicas e organizativas. A gestão de recursos inclui, no mínimo, o registo de recursos de TI e a topologia de rede, usados para o tratamento de dados pessoais.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
D.1	A organização deve ter um registo dos recursos de TI usados para o tratamento de dados pessoais (hardware, software e rede). O registo pode incluir, pelo menos, as seguintes informações: recurso de TI, tipo (por exemplo: servidor, estação de trabalho), localização (física ou eletrónica). A tarefa de manter e atualizar o registo deve ser atribuída a uma pessoa específica, por exemplo, o responsável de TI.	Baixo	A.8.1.1	---	ENISA
D.2	Os recursos de TI devem ser revistos e atualizados regularmente.	Baixo	A.8.1.1	---	ENISA
D.3	Funções com acesso a determinados recursos devem ser definidas e documentadas.	Médio	A.8.1.2	---	ENISA
D.4	Os recursos de TI devem ser revistos e atualizados anualmente.	Alto	A.8.1.1	---	ENISA
D.4.1	A informação deve ser classificada, considerando os requisitos legais, a sua importância, o tipo e as categorias de dados pessoais. Deverão existir convenções para a sua classificação e critérios para a sua revisão.	Baixo	A.8.2.1	(5)(1)(f), (32)(2)	NOVO
D.4.2	A etiquetagem da informação deverá estar de acordo com a classificação da informação, devidamente procedimentada, abrangendo tanto os formatos físicos como os eletrónicos.	Baixo	A.8.2.2	(5)(1)(f)	NOVO
D.4.3	Os suportes de dados amovíveis deverão incluir procedimentos para a sua gestão. Sempre que se tratem de dados pessoais, deverão ser utilizados controlos criptográficos ou, na sua impossibilidade, embalagens à prova de violação para mitigar os riscos de perda de confidencialidade e integridade.	Baixo	A.8.3.1	(5)(1)(f), (32)(1)(a)	NOVO
D.4.4	Durante o seu transporte, os suportes de dados devem ser protegidos com base em procedimentos estabelecidos previamente. Nos casos em que as informações são confidenciais e não há encriptação, deverá ser considerada proteção física adicional.	Baixo	A.8.3.3	(5)(1)(f), (32)(1)(a)	NOVO

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.1	Gestão de segurança
Categoria da Medida	4.1.1.5	Gestão de alterações

Descrição da Medida:

A gestão de alterações visa sincronizar e controlar todas as alterações efetuadas no sistema informático utilizado para o tratamento de dados pessoais. É uma medida de segurança importante, pois uma tentativa de alteração mal sucedida pode levar à divulgação não autorizada, modificação ou destruição de dados.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
E.1	A organização deve certificar-se de que todas as mudanças no sistema de TI são registadas e monitorizadas por uma pessoa específica (por exemplo, o responsável de TI ou o responsável de segurança). Deve ocorrer a monitorização regular deste processo.	Baixo	A.12.1.2	---	ENISA
E.2	O desenvolvimento de software deve ser realizado num ambiente especial que não esteja conectado ao sistema de TI utilizado para o tratamento de dados pessoais. Quando o teste é necessário, dados fictícios devem ser usados (e não dados reais). Nos casos em que isso não seja possível, procedimentos específicos devem ser implementados para a proteção dos dados pessoais usados nos testes.	Baixo	A.14.3.1	(5)(1)(f)	ENISA
E.3	Uma política de mudança/gestão de alterações, detalhada e documentada, deve estar em vigor. Deve incluir: um processo para introduzir mudanças, as funções / utilizadores que têm direitos de mudança e cronogramas para introduzir mudanças. A política de mudança/gestão de alterações deve ser atualizada regularmente.	Médio	A.12.1.2	---	ENISA

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.1	Gestão de segurança
Categoria da Medida	4.1.1.6	Subcontratantes

Descrição da Medida:

De acordo com o n.º 1 do artigo de 28º do RGPD, "o responsável pelo tratamento recorre apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos dados". O mesmo artigo estabelece que o tratamento pelo subcontratante deve obrigatoriamente ser redigido por contrato ou outro ato jurídico, fixando também as cláusulas mínimas que este deve incluir, nomeadamente no que se refere à segurança dos dados pessoais, nos termos do artigo 32º do RGPD.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
F.1	As diretrizes e procedimentos formais que cobrem o tratamento de dados pessoais por subcontratantes (fornecedores / prestadores de serviços) devem ser definidos, documentados e acordados entre o responsável pelo tratamento e o subcontratante antes do início das atividades de tratamento. Estas diretrizes e procedimentos devem, obrigatoriamente, estabelecer o mesmo nível de segurança de dados pessoais, conforme determinado na política de segurança da organização.	Baixo	A.15.1.1	---	ENISA
F.2	Ao identificar uma violação de dados pessoais, o subcontratante deve notificar o responsável pelo tratamento sem demora injustificada.	Baixo	A.15.1.2	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)	ENISA
F.3	Os requisitos e as obrigações devem ser formalmente acordadas entre o responsável pelo tratamento e o subcontratante. O subcontratante deve fornecer evidências de conformidade suficientemente documentadas.	Baixo	A.15.1.2	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)	ENISA
F.4	O responsável pelo tratamento deve auditar regularmente a conformidade do subcontratante relativamente ao nível acordado de requisitos e obrigações.	Médio	A.15.2.1	---	ENISA
F.5	Os funcionários do subcontratante, que tratam dados pessoais, devem estar sujeitos a acordos de confidencialidade /de não divulgação, específicos e devidamente documentados.	Alto	A.15.1.2	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)	ENISA

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.2	Resposta a incidentes e continuidade do negócio
Categoria da Medida	4.1.2.1	Resposta a incidentes e continuidade do negócio

Descrição da Medida:

Em caso de violação de dados pessoais, a organização deve avaliar se isso leva a "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (n.º 12 do artigo 4º do RGPD). Os responsáveis pelo tratamento dos dados devem certificar-se de que cumprem as suas obrigações ao abrigo dos artigos 33º e 34º do RGPD, relativamente à notificação de uma violação de dados pessoais à Autoridade de Controlo e aos titulares dos dados. Os subcontratantes também devem certificar-se de que cumprem as suas obrigações, de acordo com o artigo 33º do RGPD, para notificação imediata do responsável pelo tratamento. Em qualquer caso, os responsáveis pelo tratamento e os subcontratantes devem ter procedimentos apropriados em vigor, não apenas para a notificação de violações de dados pessoais, mas também para o tratamento geral e gestão de tais eventos.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
G.1	Um plano de resposta a incidentes, com procedimentos detalhados, deve ser definido para garantir uma resposta eficaz e ordenada a incidentes relativos a dados pessoais.	Baixo	A.16.1.1	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)	ENISA
G.2	Violações de dados pessoais devem ser relatadas imediatamente à gestão. Os procedimentos de notificação para a comunicação das violações às autoridades competentes e aos titulares dos dados devem ser implementados nos termos dos artigos 33º e 34º do RGPD.	Baixo	A.16.1.2	---	ENISA
G.3	O plano de resposta aos incidentes deve ser documentado, incluindo uma lista de possíveis ações de mitigação e atribuição clara de funções.	Médio	A.16.1.5	(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)	ENISA
G.4	Incidentes e violações de dados pessoais devem ser registados, juntamente com os detalhes do evento e as ações de mitigação subsequentes realizadas.	Alto	A.16.1.7	---	ENISA

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.2	Resposta a incidentes e continuidade do negócio
Categoria da Medida	4.1.2.2	Continuidade do negócio

Descrição da Medida:

Um Plano de Continuidade do Negócio (bcp - *business continuity plan*) é essencial para determinar os processos e medidas técnicas que a organização deve seguir em caso de um incidente / violação de dados pessoais, complementando a política de segurança da organização, bem como o seu plano de resposta a incidentes. Esta medida está claramente relacionada com o artigo 32º do RGPD que exige ao responsável pelo tratamento / subcontratante, "a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico".

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
H.1	A organização deve estabelecer os principais procedimentos e controlos a serem seguidos para garantir o nível necessário de continuidade e disponibilidade do sistema de TI de tratamento de dados pessoais (no caso de um incidente / violação de dados pessoais).	Baixo	A.17.1.1	---	ENISA
H.2	Um Plano de Continuidade do Negócio deve ser detalhado e documentado, seguindo a política geral de segurança. Deve incluir ações claras e atribuição de funções.	Médio	A.17.1.1	---	ENISA
H.3	Um nível de garantia de qualidade de serviço deve ser definido no Plano de Continuidade do Negócio para os principais processos do negócio que contribuem para a segurança de dados pessoais.	Médio	A.17.1.3	---	ENISA
H.4	Deve ser nomeado pessoal específico com a responsabilidade, autoridade e competência necessárias para gerir a continuidade do negócio no caso de um incidente / violação de dados pessoais.	Alto	A.17.1.2	---	ENISA
H.5	Convém que existam instalações alternativas (redundância geográfica), dependendo da organização e do tempo de inatividade aceitável do sistema de TI.	Alto	A.17.2.1	---	ENISA

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.3	Recursos Humanos
Categoria da Medida	4.1.3.1	Confidencialidade do pessoal

Descrição da Medida:

De modo de garantir a confidencialidade dos dados pessoais nos termos do artigo 32º do RGPD, a organização deve assegurar que os seus funcionários também fornecem garantias de confidencialidade suficientes, tanto em termos de conhecimento técnico quanto de integridade pessoal. Além disso, de acordo com o n.º 4 do artigo 32º do RGPD, "o responsável pelo tratamento e o subcontratante tomam medidas para assegurar que qualquer pessoa singular que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, só procede ao seu tratamento mediante instruções do responsável pelo tratamento, exceto se tal lhe for exigido pelo direito da União Europeia ou de um Estado-Membro". Para o efeito, devem ser tomadas medidas específicas para garantir que o pessoal envolvido no tratamento de dados pessoais seja devidamente informado sobre o seu dever de confidencialidade, bem como para garantir que este dever está suficientemente estipulado nas políticas de recursos humanos da organização.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
I.1	A organização deve assegurar que todos os funcionários entendem as suas responsabilidades e obrigações relacionadas com o tratamento de dados pessoais. As funções e responsabilidades devem ser claramente comunicadas durante o processo de pré-contratação e / ou acolhimento.	Baixo	A.7.1.1	---	ENISA
I.2	Antes de assumirem as suas funções, deve ser solicitado aos funcionários a revisão e concordância com a política de segurança da organização, bem como a assinatura dos respetivos acordos de confidencialidade e de não divulgação.	Médio	A.7.1.2	---	ENISA
I.3	Os funcionários envolvidos no tratamento de alto risco de dados pessoais devem estar sujeitos a cláusulas de confidencialidade específicas (ao abrigo do seu contrato de trabalho ou outro diploma legal).	Alto	A.7.2.1	---	ENISA

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.3	Recursos Humanos
Categoria da Medida	4.1.3.2	Formação

Descrição da Medida:

A formação em proteção de dados e em procedimentos de segurança (por exemplo, uso de palavras-passe e acessos a sistemas de tratamento de dados específicos) é importante para a implementação correta das medidas técnicas e organizativas de segurança. Informação sobre obrigações legais específicas de proteção de dados também é fundamental, especialmente para o pessoal-chave envolvido no tratamento de dados pessoais de alto risco.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
J.1	A organização deve assegurar que todos os funcionários são adequadamente informados sobre os controlos de segurança do sistema de TI relacionados com o seu trabalho diário. Os funcionários envolvidos no tratamento de dados pessoais também devem ser devidamente informados sobre os requisitos relevantes de proteção de dados e obrigações legais por meio de campanhas frequentes de consciencialização.	Baixo	A.7.2.2	(39)(1)(b)	ENISA

J.2	A organização deve ter programas de formação estruturados e frequentes para os seus funcionários, incluindo programas específicos de proteção de dados aquando do acolhimento de novas contratações.	Médio	A.7.2.2	(39)(1)(b)	ENISA
J.3	Um plano de formação, com metas e objetivos definidos, deve ser preparado e executado anualmente.	Alto	A.7.2.2	(39)(1)(b)	ENISA

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.4	Conformidade
Categoria da Medida	4.1.4.1	Conformidade com requisitos legais e contratuais

Descrição da Medida:

A conformidade com as obrigações legais e contratuais, relativamente à segurança da informação e ao tratamento de dados pessoais, evita potenciais sanções legais.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
U.1.1	Deve haver um processo atualizado de todos os requisitos legais e contratuais ajustado à natureza da organização e aos seus sistemas de TI.	Baixo	A.18.1.1	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)	NOVO
U.1.2	A proteção de registos / evidências, devidamente classificados, deve ocorrer de acordo com procedimentos estabelecidos na organização, permitindo o cumprimento da legislação aplicável.	Baixo	A.18.1.3	(5)(2), (24)(2)	NOVO

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.4	Conformidade
Categoria da Medida	4.1.4.2	Revisões de segurança da informação

Descrição da Medida:

As revisões de segurança da informação permitem assegurar que a mesma é concretizada de acordo com as políticas e procedimentos existentes na organização. Para além de auditorias independentes aos processos implementados, deverão existir análises técnicas aos sistemas de informação que tratam dados pessoais. Sempre que possível, deve-se recorrer a ferramentas automatizadas, para posterior interpretação por um técnico especialista.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
U.2.1	As revisões da segurança da informação devem ocorrer de modo independente, periodicamente ou sempre que se justifique. Os resultados das revisões devem ser documentados.	Baixo	A.18.2.1	(32)(1)(d), (32)(2)	NOVO
U.2.2	Análises técnicas aos sistemas de informação que tratam dados pessoais devem ser revistos periodicamente, ou sempre que se justifique, e devem estar alinhados às políticas de segurança da organização.	Baixo	A.18.2.3	(32)(1)(d), (32)(2)	NOVO

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.5	Orientações adicionais para responsáveis pelo tratamento
Categoria da Medida	4.1.5.1	Condições para recolha e tratamento

Descrição da Medida:

As condições para a recolha e tratamento têm como objetivo determinar e documentar que o tratamento é lícito, tem enquadramento legal e está alinhado às finalidades, que são legítimas e estão claramente definidas.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
V.1.1	A organização deve identificar, detalhar e documentar a finalidade do tratamento dos dados pessoais, e comunicá-la claramente à gestão de topo.	Baixo	A.7.2.1 (27701)	(5)(1)(b), (32)(4)	NOVO
V.1.2	A licitude do tratamento de dados pessoais deve ser identificada e documentada para que seja possível demonstrar que a legalidade do tratamento foi devidamente estabelecida antes do mesmo ocorrer.	Baixo	A.7.2.2 (27701)	(5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(2), (6)(3), (6)(4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (10), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)	NOVO
V.1.3	As condições aplicáveis ao consentimento devem ser determinadas. A organização deve conseguir demonstrar, quando aplicável, quando e como o	Baixo	A.7.2.3 (27701)	(8)(1), (8)(2)	NOVO

	consentimento para o tratamento dos dados foi obtido.				
V.1.4	Sempre que se aplicar o consentimento, este deverá ser registado e ser rastreável, de modo a que a organização possa responder, mediante solicitação, aos pedidos realizados pelo titular dos dados.	Baixo	A.7.2.4 (27701)	(7)(1), (7)(2), (9)(2)(a)	NOVO
V.1.5	A organização deve, por meio de uma avaliação dos riscos, verificar a necessidade de haver, quando apropriado, uma avaliação de impacto sobre a proteção de dados, sempre que um novo tratamento de dados for planeado ou quando ocorrerem mudanças no atual tratamento.	Baixo	A.7.2.5 (27701)	(35)(1), (35)(2), (35)(3)(a), (35)(3)(b), (35)(3)(c), (35)(4), (35)(5), (35)(7)(a), (35)(7)(b), (35)(7)(c), (35)(7)(d), (35)(8), (35)(9), (35)(10), (35)(11), (36)(1), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)	NOVO
V.1.6	Devem existir contratos, por escrito, entre a organização e os subcontratantes, e estes contratos devem exigir que sejam implementados os controlos apropriados ao tratamento dos dados pessoais, em consonância com o processo de avaliação do risco de segurança da informação e privacidade.	Baixo	A.7.2.6 (27701)	(5)(2), (28)(3)(e), (28)(9)	NOVO
V.1.7	Quando há responsáveis conjuntos pelo tratamento, as funções e responsabilidades para o tratamento dos dados pessoais devem ser determinadas de forma clara e transparente, e devem ser documentadas num contrato ou em documento similar.	Baixo	A.7.2.7 (27701)	(26)(1), (26)(2), (26)(3)	NOVO
V.1.8	As evidências relacionadas com o tratamento dos dados pessoais devem ser elaboradas e mantidas em segurança por parte da organização. Para tal, deverá ser indicado um responsável para a sua conservação.	Baixo	A.7.2.8 (27701)	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(f), (30)(1)(g), (30)(3), (30)(4), (30)(5)	NOVO

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.5	Orientações adicionais para responsáveis pelo tratamento
Categoria da Medida	4.1.5.2	Obrigações para com os titulares dos dados

Descrição da Medida:

As obrigações para com os titulares dos dados estão diretamente relacionadas com os direitos dos mesmos e à forma como estes recebem informações adequadas por parte da organização sobre o tratamento dos seus dados pessoais.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
V.2.1	A organização deve determinar e documentar as suas obrigações legais e contratuais para com os titulares dos dados, nomeadamente no que diz respeito ao tratamento dos dados pessoais, garantindo os meios necessários para cumprir as respetivas obrigações, incluindo um meio de contacto atualizado.	Baixo	A.7.3.1 (27701)	(12)(2)	NOVO
V.2.2	Dependendo das obrigações legais e contratuais, a organização determina os requisitos que devem constar nas informações fornecidas aos titulares dos dados, tanto ao nível do seu conteúdo como ao nível da sua tempestividade.	Baixo	A.7.3.2 (27701)	(11)(2), (13)(1)(a), (13)(1)(b), (13)(1)(c), (13)(1)(d), (13)(1)(e), (13)(1)(f), (13)(2)(c), (13)(2)(d), (13)(2)(e), (13)(3), (13)(4), (14)(1)(a), (14)(1)(b), (14)(1)(c), (14)(1)(d), (14)(1)(e), (14)(1)(f), (14)(2)(b), (14)(2)(e), (14)(2)(f), (14)(3)(a), (14)(3)(b), (14)(3)(c), (14)(4), (14)(5)(a), (14)(5)(b), (14)(5)(c), (14)(5)(d), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (15)(2), (18)(3), (21)(4)	NOVO
V.2.3	A organização deve fornecer aos titulares dos dados informações adequadas ao público-alvo, utilizando uma linguagem clara e simples, de forma concisa, transparente, inteligível e de fácil acesso, e em momento oportuno.	Baixo	A.7.3.3 (27701)	(11)(2), (12)(1), (12)(7), (13)(3), (21)(4)	NOVO
V.2.4	Sempre que se aplicar o consentimento, a organização deverá fornecer um mecanismo que permita aos titulares dos dados alterar ou retirar o seu consentimento, consistente com o mecanismo utilizado para a sua obtenção.	Baixo	A.7.3.4 (27701)	(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)	NOVO
V.2.5	A organização deve fornecer um mecanismo para que os titulares dos dados possam exercer o direito de oposição, incluindo informações sobre este mesmo direito. Deve ainda documentar os requisitos relacionados com as objeções dos titulares dos dados.	Baixo	A.7.3.5 (27701)	(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(5), (21)(6)	NOVO
V.2.6	A organização deve implementar políticas, procedimentos e/ou mecanismos para cumprir as suas obrigações com os titulares dos dados em matéria de	Baixo	A.7.3.6 (27701)	(5)(1)(d), (13)(2)(b), (14)(2)(c), (16), (17)(1)(a), (17)(1)(b), (17)(1)(c), (17)(1)(d), (17)(1)(e), (17)(1)(f), (17)(2)	NOVO

	direitos de acesso, retificação e apagamento, sem demora injustificada.				
V.2.7	Sempre que os dados pessoais tenham sido transmitidos a terceiros, a organização comunica a cada destinatário qualquer retificação, apagamento ou limitação a que se tenha procedido, bem como estabelece políticas, procedimentos e/ou mecanismos apropriados para o realizar.	Baixo	A.7.3.7 (27701)	(19)	NOVO
V.2.8	A organização deve ser capaz de fornecer uma cópia dos dados pessoais em fase de tratamento, quando solicitada pelo titular dos dados, num formato estruturado, de uso corrente e de leitura automática, quando for tecnicamente possível.	Baixo	A.7.3.8 (27701)	(15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)	NOVO
V.2.9	A organização define, através de políticas e procedimentos, a gestão e resposta aos pedidos dos titulares dos dados.	Baixo	A.7.3.9 (27701)	(12)(3), (12)(4), (12)(5), (12)(6), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h)	NOVO
V.2.10	A organização define, através de políticas e procedimentos, como proceder nos casos em que o tratamento dos dados pessoais permite tomar decisões individuais automatizadas, incluindo a definição de perfis, que podem produzir efeitos na esfera jurídica do titular dos dados ou que o afete significativamente de forma similar.	Baixo	A.7.3.10 (27701)	(13)(2)(f), (14)(2)(g), (22)(1), (22)(3)	NOVO

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.5	Orientações adicionais para responsáveis pelo tratamento
Categoria da Medida	4.1.5.3	Proteção de dados desde a conceção e por defeito

Descrição da Medida:

A proteção de dados desde a conceção e por defeito permite projetar o tratamento de dados pessoais ao mínimo necessário para a finalidade identificada, tendo em consideração a quantidade de dados, a extensão do tratamento, o prazo de conservação e a sua acessibilidade, e também as medidas técnicas e organizativas mais adequadas.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
V.3.1	A organização deve limitar a recolha de dados pessoais apenas ao que é necessário relativamente às finalidades identificadas.	Baixo	A.7.4.1 (27701)	(5)(1)(b), (5)(1)(c)	NOVO
V.3.2	Por defeito, só devem ser tratados dados pessoais que sejam necessários, adequados e relevantes para cada finalidade específica do tratamento.	Baixo	A.7.4.2 (27701)	(25)(2)	NOVO
V.3.3	A organização deve assegurar e documentar que os dados pessoais são tão exatos e atualizados, como o necessário, para o cumprimento das finalidades de tratamento, ao longo do seu ciclo de vida.	Baixo	A.7.4.3 (27701)	(5)(1)(d)	NOVO
V.3.4	A organização deve definir e documentar os objetivos de minimização de dados e como é que os dados pessoais são limitados às finalidades do tratamento, bem como quais os mecanismos utilizados para alcançar a minimização dos dados (ex: técnicas de desidentificação).	Baixo	A.7.4.4 (27701)	(5)(1)(c), (5)(1)(e)	NOVO
V.3.5	A organização deve eliminar ou apresentar os dados pessoais de uma forma que não permita a sua identificação ou reidentificação, assim que os mesmos não sejam mais necessários para a(s) finalidade(s) do tratamento.	Baixo	A.7.4.5 (27701)	(5)(1)(c), (5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)	NOVO
V.3.6	A organização deve assegurar que os ficheiros temporários com dados pessoais, criados como resultado do tratamento de dados, são eliminados assim que deixem de ser necessários, através de procedimentos documentados e com verificações periódicas.	Baixo	A.7.4.6 (27701)	(5)(1)(c)	NOVO
V.3.7	Os prazos de conservação dos dados pessoais devem estar definidos ou, se tal não for possível, os critérios usados para definir esse prazo que, sempre que se aplique, devem estar alinhados aos requisitos legais, regulamentares e/ou de negócio. A organização deve desenvolver e manter cronogramas destes prazos de conservação.	Baixo	A.7.4.7 (27701)	(13)(2)(a), (14)(2)(a)	NOVO
V.3.8	A organização deve ter políticas, procedimentos e / ou mecanismos documentados para a eliminação de dados pessoais.	Baixo	A.7.4.8 (27701)	(5)(1)(f)	NOVO
V.3.9	A organização deve garantir que os dados pessoais são transmitidos apenas a pessoas / entidades autorizadas, seguindo processos apropriados para que os dados pessoais não sejam comprometidos.	Baixo	A.7.4.9 (27701)	(5)(1)(f)	NOVO

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.5	Orientações adicionais para responsáveis pelo tratamento
Categoria da Medida	4.1.5.4	Partilha, transferência e divulgação de dados pessoais

Descrição da Medida:					
A partilha, transferência e divulgação de dados pessoais visa determinar, enquadrar legalmente e documentar o modo como os dados pessoais podem ser transferidos para um país terceiro ou para uma organização internacional.					
	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
V.4.1	A organização deve identificar e documentar o enquadramento legal para a realização de transferências de dados pessoais, incluindo para países terceiros ou organizações internacionais.	Baixo	A.7.5.1 (27701)	(15)(2), (30)(1)(e), (44), (45)(1), (45)(2)(a), (45)(2)(b), (45)(2)(c), (45)(3), (45)(4), (45)(5), (45)(6), (45)(7), (45)(8), (45)(9), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (46)(4), (46)(5), (47)(1)(a), (47)(1)(b), (47)(1)(c), (47)(2)(a), (47)(2)(b), (47)(2)(c), (47)(2)(d), (47)(2)(e), (47)(2)(f), (47)(2)(g), (47)(2)(h), (47)(2)(i), (47)(2)(j), (47)(2)(k), (47)(2)(l), (47)(2)(m), (47)(2)(n), (47)(3), (48), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6)	NOVO
V.4.2	A organização deve especificar e documentar os países terceiros e organizações internacionais para os quais se podem transferir dados pessoais. Os titulares dos dados devem ser informados das garantias adequadas relativas à transferência de dados.	Baixo	A.7.5.2 (27701)	(15)(2), (30)(1)(e)	NOVO
V.4.3	A organização deve registar as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a sua identificação, e garantir a cooperação de forma a dar suporte a solicitações futuras relacionadas com as obrigações para com os titulares dos dados.	Baixo	A.7.5.3 (27701)	(30)(1)(e)	NOVO
V.4.4	A organização deve registar as categorias dos destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou em organizações internacionais.	Baixo	A.7.5.4 (27701)	(30)(1)(d)	NOVO

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.6	Orientações adicionais para subcontratantes
Categoria da Medida	4.1.6.1	Condições para recolha e tratamento

Descrição da Medida:					
As condições para a recolha e tratamento para subcontratantes têm como objetivo determinar e documentar que o tratamento é lícito, tem enquadramento legal e está alinhado às finalidades, que são legítimas e estão claramente definidas.					
	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
W.1.1	O subcontratante deve assegurar, quando relevante, que o contrato ou outro ato normativo para o tratamento de dados pessoais tem em consideração a natureza do tratamento e o papel da organização cliente, prestando assistência através de medidas técnicas e organizativas adequadas.	Baixo	A.8.2.1 (27701)	(28)(3)(e), (28)(3)(f), (28)(9), (35)(1)	NOVO
W.1.2	A organização deve garantir que os dados pessoais tratados em nome de um cliente ocorrem apenas mediante instruções documentadas do responsável pelo tratamento, limitadas às finalidades previstas.	Baixo	A.8.2.2 (27701)	(5)(1)(a), (5)(1)(b), (28)(3)(a), (29), (32)(4)	NOVO
W.1.3	Na existência de um contrato para fins de marketing e publicidade, a organização só trata dados pessoais depois de garantir que o consentimento foi dado previamente pelo titular dos dados.	Baixo	A.8.2.3 (27701)	(7)(4)	NOVO
W.1.4	Caso a organização percecione algum tipo de ilegalidade ou não conformidade no tratamento de dados pessoais deve informar o cliente.	Baixo	A.8.2.4 (27701)	(28)(3)(h)	NOVO
W.1.5	A organização deve disponibilizar ao cliente, sempre que tal seja possível e necessário, todas as informações para que o responsável pelo tratamento possa demonstrar a conformidade com as suas obrigações.	Baixo	A.8.2.5 (27701)	(28)(3)(h)	NOVO
W.1.6	As evidências relacionadas com o tratamento de dados pessoais, em nome do cliente, devem ser determinadas e mantidas com segurança por parte da organização.	Baixo	A.8.2.6 (27701)	(30)(2)(a), (30)(2)(b), (30)(3), (30)(4), (30)(5)	NOVO

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.6	Orientações adicionais para subcontratantes

Categoria da Medida	4.1.6.2	Obrigações para com os titulares dos dados

Descrição da Medida:

As obrigações para com os titulares dos dados estão diretamente relacionadas com os direitos dos mesmos e à forma como estes recebem informações adequadas por parte da organização sobre o tratamento dos seus dados pessoais.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
W.2.1	A organização deve garantir ao cliente / responsável pelo tratamento, os meios necessários para o cumprimento das obrigações perante o titular dos dados, nomeadamente através da existência de medidas técnicas e organizativas adequadas.	Baixo	A.8.3.1 (27701)	(15)(3), (17)(2), (28)(3)(e)	NOVO

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.6	Orientações adicionais para subcontratantes
Categoria da Medida	4.1.6.3	Proteção de dados desde a conceção e por defeito

Descrição da Medida:

A proteção de dados desde a conceção e por defeito permite projetar o tratamento de dados pessoais ao mínimo necessário para a finalidade identificada, tendo em consideração a quantidade de dados, a extensão do tratamento, o prazo de conservação e a sua acessibilidade, e também as medidas técnicas e organizativas mais adequadas.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
W.3.1	A organização deve assegurar que os ficheiros temporários com dados pessoais, criados como resultado do tratamento de dados, são eliminados assim que deixem de ser necessários, através de procedimentos documentados e com verificações periódicas.	Baixo	A.8.4.1 (27701)	(5)(1)(c)	NOVO
W.3.2	A organização, quando aplicável, deve garantir a capacidade de apagar ou devolver todos os dados pessoais, de maneira segura, depois de concluída a prestação dos serviços relacionados com o tratamento.	Baixo	A.8.4.2 (27701)	(28)(3)(g), (30)(1)(f)	NOVO
W.3.3	A organização deve garantir, incluindo no clausulado com o cliente, que os dados pessoais são transmitidos apenas a pessoas / entidades autorizadas, segundo processos apropriados para que os dados pessoais não sejam comprometidos.	Baixo	A.8.4.3 (27701)	(5)(1)(f)	NOVO

Categoria principal das medidas	4.1	Medidas organizativas de segurança
Subcategoria	4.1.6	Orientações adicionais para subcontratantes
Categoria da Medida	4.1.6.4	Partilha, transferência e divulgação de dados pessoais

Descrição da Medida:

A partilha, transferência e divulgação de dados pessoais visa determinar, enquadrar legalmente e documentar o modo como os dados pessoais podem ser transferidos para um país terceiro ou para uma organização internacional.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
W.4.1	A organização deve, em tempo útil, informar o cliente / responsável pelo tratamento sobre o enquadramento legal para a realização de transferências de dados pessoais, bem como de quaisquer alterações relacionadas com o mesmo, incluindo para países terceiros ou organizações internacionais, para que, consoante o caso, o cliente autorize ou tenha a oportunidade de se opor a tais alterações.	Baixo	A.8.5.1 (27701)	(44), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (48), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6)	NOVO
W.4.2	A organização deve especificar e documentar os países terceiros e organizações internacionais para os quais se podem transferir dados pessoais. Considerando que os titulares dos dados devem ser informados das garantias adequadas relativas à transferência dos dados, a organização deve partilhar esta informação com o cliente.	Baixo	A.8.5.2 (27701)	(30)(2)(c)	NOVO
W.4.3	A organização deve registar as categorias dos destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou em organizações internacionais.	Baixo	A.8.5.3 (27701)	(30)(1)(d)	NOVO
W.4.4	No caso da organização receber solicitações legalmente vinculativas para a divulgação de dados pessoais, nomeadamente de autoridades policiais, deve, desde que a lei o permita, notificar o cliente / responsável pelo tratamento, dentro dos prazos acordados e de acordo com um procedimento previamente estabelecido.	Baixo	A.8.5.4 (27701)	(28)(3)(a)	NOVO
W.4.5	A organização deve rejeitar quaisquer solicitações de transferências ou divulgações que não sejam juridicamente vinculadas, salvo devidamente contratualizado e autorizado pelo cliente / responsável pelo tratamento.	Baixo	A.8.5.5 (27701)	(48)	NOVO

W.4.6	Se a organização contratar outro subcontratante para a realização de operações específicas de tratamento de dados por conta do cliente, as disposições para o uso de subcontratados devem estar incluídas no contrato com o cliente / responsável pelo tratamento.	Baixo	A.8.5.6 (27701)	(28)(2), (28)(4)	NOVO
W.4.7	A organização só contrata outro subcontratante caso o cliente / responsável pelo tratamento tenha dado, previamente e por escrito, autorização.	Baixo	A.8.5.7 (27701)	(28)(2), (28)(3)(d)	NOVO
W.4.8	Quando a organização muda de subcontratante necessita de autorização, por escrito, do cliente / responsável pelo tratamento, para a mudança, dando assim ao cliente a oportunidade de se opor a tais alterações.	Baixo	A.8.5.8 (27701)	(28)(2)	NOVO

Categoria principal das medidas	4.2	Medidas técnicas de segurança
Subcategoria	4.2.1	Medidas técnicas de segurança
Categoria da Medida	4.2.1	Medidas técnicas de segurança

Descrição da Medida:

O controlo de acessos e a autenticação são medidas básicas de segurança para a proteção contra o acesso não autorizado ao sistema de TI utilizado para o tratamento de dados pessoais. Implementam a política de controlo de acessos da organização (consulte a Seção 4.1.1.3), impondo-a tecnicamente em componentes e aplicativos específicos.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
K.1.1	Deve existir um processo formal de registo e cancelamento de utilizadores que assegure o acesso autorizado e previna o acesso não autorizado.	Baixo	A.9.2.1	(5)(1)(f)	NOVO
K.1	Deve ser implementado um sistema de controlo de acesso aplicável a todos os utilizadores que acedem o sistema de TI. O sistema deve permitir a criação, aprovação, revisão e exclusão de contas de utilizadores.	Baixo	A.9.2.2	(5)(1)(f)	ENISA
K.2	O uso de contas comuns deve ser evitado. Nos casos em que isso for necessário, deve-se assegurar que todos os utilizadores da conta comum tenham as mesmas funções e responsabilidades.	Baixo	A.9.4.1	---	ENISA
K.3	Deve haver um mecanismo de autenticação que permita o acesso ao sistema de TI (com base na política e sistema de controlo de acessos). No mínimo, uma combinação de nome de utilizador / senha deve ser usada. As senhas devem respeitar um certo nível (configurável) de complexidade.	Baixo	A.9.4.2	(5)(1)(f)	ENISA
K.4	O sistema de controlo de acessos deve ter a capacidade de detetar e não permitir o uso de senhas que não respeitem um determinado nível (configurável) de complexidade.	Baixo	A.9.4.3	---	ENISA
K.5	Uma política específica de senhas deve ser definida e documentada. A política deve incluir, pelo menos, o comprimento da senha, complexidade, período de validade, bem como o número de tentativas de login mal-sucedidas aceitáveis.	Médio	A.9.4.3	---	ENISA
K.6	As senhas do utilizador devem ser armazenadas num formato “hash”.	Médio	A.9.4.3	---	ENISA
K.7	A autenticação de dois fatores deve ser usada preferencialmente para aceder a sistemas que tratam dados pessoais. Os fatores de autenticação podem ser senhas, tokens de segurança, pen drives com um token secreto, biometria, etc.	Alto	A.9.4.2	(5)(1)(f)	ENISA
K.8	A autenticação do dispositivo deve ser utilizada para garantir que o tratamento dos dados pessoais seja realizado apenas por meio de recursos específicos da rede.	Alto	A.9.4.2	(5)(1)(f)	ENISA

Categoria principal das medidas	4.2	Medidas técnicas de segurança
Subcategoria	4.2.2	Registo e monitorização
Categoria da Medida	4.2.2	Registo e monitorização

Descrição da Medida:

A utilização de arquivos de log é uma medida de segurança essencial que permite a identificação e o rastreamento das ações do utilizador (no que diz respeito ao tratamento de dados pessoais), apoiando, assim, a responsabilização em caso de divulgação não autorizada, modificação ou destruição de dados pessoais. A monitorização dos arquivos de log é importante para identificar possíveis tentativas internas ou externas de violação do sistema.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
L.1	Os arquivos de log devem ser ativados para cada sistema / aplicativo usado para o tratamento de dados pessoais. Devem incluir todos os tipos de acesso aos dados (visualização, modificação, eliminação).	Baixo	A.12.4.1	(5)(1)(f)	ENISA
L.2	Os arquivos de log devem ter um carimbo de data / hora e ser protegidos adequadamente contra adulteração e acesso não autorizado. Os relógios devem ser sincronizados com uma única fonte de tempo de referência.	Baixo	A.12.4.4	---	ENISA

L.3	As ações dos administradores e operadores do sistema, incluindo adição / eliminação / alteração dos direitos do utilizador, devem ser registadas.	Médio	A.12.4.3	---	ENISA
L.4	Não deve haver possibilidade de eliminação ou modificação do conteúdo dos arquivos de log. O acesso aos arquivos de log também deve ser registado, além da monitorização para detetar atividades incomuns.	Médio	A.12.4.2	(5)(1)(f)	ENISA
L.5	Um sistema de monitorização deve processar os arquivos de log e produzir relatórios sobre o status do sistema e notificar possíveis alertas.	Médio	A.12.4.1	(5)(1)(f)	ENISA

Categoria principal das medidas	4.2	Medidas técnicas de segurança
Subcategoria	4.2.3	Segurança de servidor/base de dados
Categoria da Medida	4.2.3.1	Segurança de servidor/base de dados

Descrição da Medida:

Os servidores e bases de dados são a espinha dorsal do sistema de informação que trata dados pessoais. Devem ter segurança reforçada para garantir um ambiente operacional seguro.
Dados em repouso são aqueles que não se movem ativamente de um dispositivo para outro, ou de rede para rede, como dados armazenados num disco rígido, laptop, unidade flash USB ou de qualquer outra forma. Esta categoria de medidas está principalmente relacionada com o tratamento de dados pessoais em bases de dados ou outros sistemas relevantes (incluindo armazenamento em nuvem). Também se relaciona com o tratamento de dados pessoais por funcionários que utilizam estações de trabalho específicas ou outros dispositivos. O RGPD reconhece a capacidade de pseudonimização para ajudar a proteger os direitos dos indivíduos e, simultaneamente, habilitar a utilidade de dados, tal como mencionado no artigo 32º: "pseudonimização e a cifragem dos dados pessoais".

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
M.1	Os servidores de bases de dados e de aplicações devem ser configurados usando uma conta separada, com privilégios mínimos de sistema operacional para funcionarem corretamente.	Baixo	A.12.1.4	---	ENISA
M.2	Os servidores de base de dados e de aplicações devem tratar apenas os dados pessoais realmente necessários, a fim de atingir os seus objetivos de tratamento.	Baixo	A.12.1.4	---	ENISA
M.3	As soluções de criptografia devem ser consideradas em arquivos ou registos específicos por meio da implementação de software ou hardware.	Médio	A.10.1.1	(32)(1)(a)	ENISA
M.4	Deve ser considerada a criptografia das unidades de armazenamento / drives.	Médio	A.10.1.1	(32)(1)(a)	ENISA
M.5	As técnicas de pseudonimização devem ser aplicadas por meio da separação de dados de identificadores diretos para evitar a identificação do titular dos dados sem informações adicionais.	Médio	A.10.1.1	(32)(1)(a)	ENISA
M.6	Devem ser consideradas técnicas de suporte à privacidade ao nível da base de dados, como consultas autorizadas, consultas à base de dados que preservam a privacidade, criptografia pesquisável, etc.	Alto	A.12.1.4	---	ENISA

Categoria principal das medidas	4.2	Medidas técnicas de segurança
Subcategoria	4.2.3	Segurança de servidor/base de dados
Categoria da Medida	4.2.3.2	Segurança da estação de trabalho

Descrição da Medida:

Esta medida está principalmente relacionada com a configuração de segurança das estações de trabalho ou outros dispositivos dos utilizadores, sendo importante para permitir aplicar políticas de segurança específicas, restringindo a realização por parte dos utilizadores de certas ações capazes de comprometer a segurança do sistema de TI (por exemplo, desativação de programas anti-vírus ou instalação de software não autorizado).
Dados em repouso são aqueles que não se movem ativamente de um dispositivo para outro, ou de rede para rede, como dados armazenados num disco rígido, laptop, unidade flash USB ou de qualquer outra forma. Esta categoria de medidas está principalmente relacionada com o tratamento de dados pessoais em bases de dados ou outros sistemas relevantes (incluindo armazenamento em nuvem). Também se relaciona com o tratamento de dados pessoais por funcionários que utilizam estações de trabalho específicas ou outros dispositivos. O RGPD reconhece a capacidade de pseudonimização para ajudar a proteger os direitos dos indivíduos e, simultaneamente, habilitar a utilidade de dados, tal como mencionado no artigo 32º: "pseudonimização e a cifragem dos dados pessoais".

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
N.1	Os utilizadores não devem ser capazes de desativar ou ignorar as configurações de segurança.	Baixo	A.14.1.1	---	ENISA
N.2	Aplicações de antivírus e deteção baseada em assinaturas devem ser configuradas semanalmente.	Baixo	A.14.1.1	---	ENISA
N.3	Os utilizadores não devem ter privilégios para instalar ou desativar aplicações de software não autorizados.	Baixo	A.14.1.3	---	ENISA

N.4	O sistema deve ter tempos limite de sessão quando o utilizador não estiver ativo, e este deve estar determinado.	Baixo	A.14.1.1	---	ENISA
N.5	As atualizações críticas de segurança lançadas pelo fornecedor do sistema operativo devem ser instaladas regularmente.	Baixo	A.14.1.1	---	ENISA
N.6	Aplicações antivírus e assinaturas de deteção devem ser configuradas diariamente.	Médio	A.14.1.1	---	ENISA
N.7	Não deve ser permitido transferir dados pessoais de estações de trabalho para dispositivos de armazenamento externos (por exemplo, USB, DVD, discos rígidos externos).	Alto	A.14.1.3	---	ENISA
N.8	As estações de trabalho usadas para o tratamento de dados pessoais não devem estar ligadas à Internet, a menos que haja medidas de segurança em vigor para impedir o tratamento, cópia e transferência não autorizada de dados pessoais armazenados.	Alto	A.14.1.2	(5)(1)(f), (32)(1)(a)	ENISA
N.9	A criptografia de software de disco completo deve ser ativada nas unidades do sistema operativo da estação de trabalho.	Alto	A.14.1.2	(5)(1)(f), (32)(1)(a)	ENISA

Categoria principal das medidas	4.2	Medidas técnicas de segurança
Subcategoria	4.2.4	Segurança de rede / comunicações
Categoria da Medida	4.2.4	Segurança de rede / comunicações

Descrição da Medida:

A segurança da rede é importante para a proteção dos dados pessoais, tanto no que diz respeito às ligações externas (por exemplo, à Internet), como também à ligação com outros sistemas (externos ou internos) da organização.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
O.1	Sempre que o acesso for realizado pela Internet, a comunicação deve ser criptografada por meio de protocolos criptográficos (TLS / SSL).	Baixo	A.13.2.1	(5)(1)(f)	ENISA
O.2	O acesso sem fio ao sistema de TI deve ser permitido apenas para utilizadores e processos específicos. Deve ser protegido por mecanismos de criptografia.	Médio	A.13.1.2	---	ENISA
O.3	Em geral, o acesso remoto ao sistema de TI deve ser evitado. Nos casos em que isso for absolutamente necessário, deve ser realizado apenas sob o controlo e monitorização de uma pessoa específica da organização (por exemplo, administrador de TI / responsável de segurança) por meio de dispositivos pré-definidos.	Médio	A.13.1.2	---	ENISA
O.4	O tráfego de entrada e saída do sistema de TI deve ser monitorizado e controlado por meio de firewalls e sistemas de deteção de intrusão.	Médio	A.13.1.1	---	ENISA
O.5	A ligação com a Internet não deve ser permitida a servidores e estações de trabalho usados para o tratamento de dados pessoais.	Alto	A.13.2.1	(5)(1)(f)	ENISA
O.6	A rede do sistema de informação do responsável pelo tratamento deve ser segregada das outras redes.	Alto	A.13.1.3	---	ENISA
O.7	O acesso ao sistema de TI deve ser realizado apenas por dispositivos e terminais pré-autorizados, usando técnicas como filtragem MAC ou Controlo de Acesso à Rede (NAC) - Network Access Control.	Alto	A.13.1.1	---	ENISA
O.7.1	Os acordos de confidencialidade ou de não divulgação devem refletir as necessidades da organização e devem ser revistos periodicamente ou sempre que se justifique.	Baixo	A.13.2.4	(5)(1)(f), (28)(3)(b), (38)(5)	NOVO

Categoria principal das medidas	4.2	Medidas técnicas de segurança
Subcategoria	4.2.5	Backups
Categoria da Medida	4.2.5	Backups

Descrição da Medida:

Um sistema de backup é um meio essencial de recuperação da perda ou destruição de dados. Ainda que seja essencial a existência de um sistema, a frequência e a natureza do backup dependerão, entre outros fatores, do tipo de organização e da natureza dos dados que são tratados. De acordo com o artigo 32º do RGPD, deve-se considerar a "capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais", enquanto parte das obrigações de segurança de dados do responsável pelo tratamento ou do subcontratante.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
P.1	Os procedimentos de backup e restauração de dados devem ser definidos, documentados e claramente vinculados às funções e responsabilidades.	Baixo	A.12.3.1	(5)(1)(f), (32)(1)(c)	ENISA

P.2	Os backups devem receber um nível apropriado de proteção física e ambiental, consistente com os padrões aplicados aos dados de origem.	Baixo	A.12.3.1	(5)(1)(f), (32)(1)(c)	ENISA
P.3	A execução de backups deve ser monitorizada para garantir a sua completude.	Baixo	A.12.3.1	(5)(1)(f), (32)(1)(c)	ENISA
P.4	Devem ser realizados backups completos frequentemente.	Baixo	A.12.3.1	(5)(1)(f), (32)(1)(c)	ENISA
P.5	A cópia de segurança deve ser testada regularmente para garantir que é confiável em caso de emergência.	Médio	A.12.3.1	(5)(1)(f), (32)(1)(c)	ENISA
P.6	Os backups incrementais programados devem ser executados pelo menos diariamente.	Médio	A.12.3.1	(5)(1)(f), (32)(1)(c)	ENISA
P.7	As cópias do backup devem ser armazenadas com segurança e em locais diferentes.	Médio	A.12.3.1	(5)(1)(f), (32)(1)(c)	ENISA
P.8	No caso de ser usado um prestador de serviços para armazenamento do backup, o responsável pelo tratamento deve encriptar a cópia antes desta ser transmitida.	Médio	A.12.3.1	(5)(1)(f), (32)(1)(c)	ENISA
P.9	As cópias dos backups também devem ser encriptadas e armazenadas offline, com segurança.	Alto	A.12.3.1	(5)(1)(f), (32)(1)(c)	ENISA

Categoria principal das medidas	4.2	Medidas técnicas de segurança
Subcategoria	4.2.6	Dispositivos móveis / portáteis
Categoria da Medida	4.2.6	Dispositivos móveis / portáteis

Descrição da Medida:

Dispositivos móveis / portáteis podem alargar o nível de serviços oferecidos pelo responsável pelo tratamento, mas também aumentam a exposição ao roubo e/ou perda acidental. No caso de dispositivos móveis, como smartphones ou tablets, os utilizadores também podem utilizá-los para uso pessoal, pelo que cuidados especiais devem ser tomados para garantir que os dados do negócio não são comprometidos.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
Q.1	Os procedimentos de gestão de dispositivos móveis e portáteis devem ser definidos e documentados, estabelecendo regras claras para o seu uso adequado.	Baixo	A.6.2.1	(5)(1)(f)	ENISA
Q.2	Os dispositivos móveis que têm permissão para aceder aos sistemas de informação devem ser pré-registados e pré-autorizados.	Baixo	A.6.2.1	(5)(1)(f)	ENISA
Q.3	Os dispositivos móveis devem estar sujeitos aos mesmos níveis de procedimentos de controlo de acesso (ao sistema de tratamento de dados) que outros equipamentos terminais.	Baixo	A.6.2.1	(5)(1)(f)	ENISA
Q.4	As funções e responsabilidades específicas relativas à gestão de dispositivos móveis e portáteis devem ser claramente definidas.	Médio	A.6.2.1	(5)(1)(f)	ENISA
Q.5	A organização deve ser capaz de apagar remotamente dados pessoais (relacionados com a sua operação de tratamento) num dispositivo móvel que seja comprometido.	Médio	A.6.2.1	(5)(1)(f)	ENISA
Q.6	Os dispositivos móveis devem permitir separar a utilização privada da utilização profissional por meio de *conteinerização* de softwares seguros.	Médio	A.6.2.1	(5)(1)(f)	ENISA
Q.7	Os dispositivos móveis, quando não estão a uso, devem ser protegidos fisicamente contra o roubo.	Médio	A.6.2.1	(5)(1)(f)	ENISA
Q.8	A autenticação de dois fatores deve ser considerada para aceder a dispositivos móveis	Alto	A.6.2.1	(5)(1)(f)	ENISA
Q.9	Os dados pessoais armazenados no dispositivo móvel (como parte da operação de tratamento de dados da organização) devem estar encriptados.	Alto	A.6.2.1	(5)(1)(f)	ENISA

Categoria principal das medidas	4.2	Medidas técnicas de segurança
Subcategoria	4.2.7	Segurança do ciclo de vida da aplicação
Categoria da Medida	4.2.7	Segurança do ciclo de vida da aplicação

Descrição da Medida:

Durante todas as fases do ciclo de vida de desenvolvimento de aplicações, a organização deve garantir que a conformidade com a proteção de dados, incluindo a segurança de dados pessoais, é tida em consideração. No artigo 25º, o RGPD apresenta os princípios de proteção de dados, desde a conceção e por defeito, que exigem que os responsáveis pelo tratamento projetem e implementem atividades de tratamento tendo presente a proteção de dados, aplicando as configurações de privacidade mais rígidas.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
R.1	Durante o ciclo de vida de desenvolvimento das aplicações, devem ser seguidas as melhores práticas existentes e os melhores padrões de desenvolvimento.	Baixo	A.14.2.5	(25)(1)	ENISA
R.2	Requisitos específicos de segurança devem ser definidos durante as fases iniciais do ciclo de vida de desenvolvimento.	Baixo	A.14.2.1	(25)(1)	ENISA
R.3	Devem ser adotadas tecnologias e técnicas específicas destinadas a apoiar a proteção da privacidade e dos dados, também conhecidas como tecnologias de reforço da privacidade (PETs - *Privacy Enhancing Technologies*), em analogia com os requisitos de segurança.	Baixo	A.14.2.1	(25)(1)	ENISA
R.4	Padrões e práticas de código seguro devem ser seguidas.	Baixo	A.14.2.1	(25)(1)	ENISA
R.5	Durante o desenvolvimento devem ser realizados testes e validações à implementação dos requisitos de segurança iniciais.	Baixo	A.14.2.8	---	ENISA
R.6	As avaliações de vulnerabilidades e os testes de penetração em aplicações e nas infraestruturas devem ser realizados por uma entidade terceira de confiança antes da aceitação operacional. A aceitação não deve ocorrer sem que o nível de segurança exigido seja alcançado.	Médio	A.12.6.1	---	ENISA
R.7	Testes de penetração devem ser realizados periodicamente.	Médio	A.14.2.8	---	ENISA
R.8	Devem ser obtidas informações sobre vulnerabilidades técnicas dos sistemas de informação em uso.	Médio	A.12.6.1	---	ENISA
R.9	Os *patches* de software devem ser testados e avaliados antes de serem instalados num ambiente produtivo.	Médio	A.12.6.2	---	ENISA

Categoria principal das medidas	4.2	Medidas técnicas de segurança
Subcategoria	4.2.8	Eliminação de dados
Categoria da Medida	4.2.8	Eliminação de dados

Descrição da Medida:

O objetivo da eliminação / remoção é eliminar ou destruir irreversivelmente os dados pessoais para que não possam ser recuperados. O(s) método(s) usado(s) devem, portanto, corresponder ao tipo de tecnologia de armazenamento, incluindo cópias em papel. Ao eliminar equipamentos obsoletos ou redundantes, o responsável pelo tratamento deve garantir que todos os dados, previamente armazenados nos dispositivos, foram removidos antes da eliminação dos equipamentos. De acordo com o artigo 5º do RGPD, os dados pessoais não devem ser retidos por mais tempo do que o necessário em relação aos fins para os quais foram recolhidos ou para os quais são posteriormente tratados. Em alguns casos, os titulares dos dados também têm o direito de solicitar a eliminação antes do final do período máximo de conservação.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
S.1	A sobregravação baseada em software deve ser executada em todos os suportes antes de ser eliminada. Nos casos em que isso não seja possível (CDs, DVDs, etc.), a destruição física deve ser executada.	Baixo	A.11.2.7	(5)(1)(f)	ENISA
S.2	Deve ser realizada a trituração de papel e suportes portáteis usados para armazenar dados pessoais.	Baixo	A.8.3.2	(5)(1)(f)	ENISA
S.3	Várias sequências de sobregravação baseada em software devem ser executadas em todas os suportes antes de serem eliminadas.	Médio	A.8.3.2	(5)(1)(f)	ENISA
S.4	Se serviços de terceiros forem utilizados para a eliminação segura dos suportes de informação ou dos registos em papel, um contrato de serviço deve ser estabelecido e deve existência evidência da destruição dos registos.	Médio	A.11.2.7	(5)(1)(f)	ENISA
S.5	Após a eliminação do software, medidas adicionais baseadas em hardware, como desmagnetização, devem ser executadas. Dependendo do caso, a destruição física também pode ser considerada.	Alto	A.11.2.7	(5)(1)(f)	ENISA
S.6	Se um prestador de serviço, incluindo subcontratantes, tiver a tarefa de destruição dos dispositivos de informação ou arquivos em papel, o processo deve acontecer nas instalações do responsável pelo tratamento, evitando transferências de dados pessoais para fora do local de tratamento.	Alto	A.8.3.2	(5)(1)(f)	ENISA

Categoria principal das medidas	4.2	Medidas técnicas de segurança
Subcategoria	4.2.9	Segurança física
Categoria da Medida	4.2.9	Segurança física

Descrição da Medida:

A segurança física é igualmente importante no que concerne as medidas de segurança orientadas para a tecnologia, visto que o acesso físico aos sistemas de informação pode ser a base para a estratégia geral de segurança.

	Descrição da Medida	Nível de Risco	Relação com ISO	Relação com RGPD	Obs:
T.1	O perímetro físico da infraestrutura do sistema de TI não deve ser acessível a pessoal não autorizado.	Baixo	A.11.1.1	---	ENISA
T.2	Devem ser estabelecidas medidas de identificação claras, nomeadamente através de meios apropriados como crachás de identificação para todo o pessoal e visitantes que acedem às instalações da organização.	Médio	A.11.1.2	---	ENISA
T.3	As zonas seguras devem ser definidas e protegidas por controlos de entrada apropriados. Um livro de registo físico ou pista de auditoria eletrónica de todos os acessos deve ser mantido e monitorizado com segurança.	Médio	A.11.1.2	---	ENISA
T.4	Os sistemas de deteção de intrusão devem ser instalados em todas as zonas de segurança.	Médio	A.11.1.1	---	ENISA
T.5	Devem ser construídas, quando aplicável, barreiras físicas para impedir o acesso físico não autorizado.	Médio	A.11.1.1	---	ENISA
T.6	As áreas seguras vazias devem ser fisicamente fechadas e revistas periodicamente.	Médio	A.11.1.5	---	ENISA
T.7	Um sistema automático de supressão de incêndio, um sistema de ar condicionado dedicado de controlo fechado e uma fonte de alimentação ininterrupta (UPS - *uninterruptible power supply*) devem ser implementados na sala do servidor.	Médio	A.11.2.1	---	ENISA
T.8	Ao pessoal de serviço de suporte, entidades terceiras / prestadoras de serviço, deve ser concedido acesso restrito às áreas seguras.	Médio	A.11.1.2	---	ENISA
T.8.1	A política de secretária limpa e ecrã limpo deverá ter em consideração a classificação da informação, os requisitos legais e contratuais e os riscos correspondentes, restringindo ao máximo a impressão documental.	Baixo	A.11.2.9	(5)(1)(f)	NOVO

Anexo 8 – Propostas de resolução para as não conformidades

Propostas de resolução para as não conformidades

As propostas para as não conformidades foram desenvolvidas com base na informação disponível das Autoridades de Controlo dos vários Estados-Membros da União Europeia e Espaço Económico Europeu, orientações oficiais do EDPB – European Data Protection Board, e do anterior Grupo de Trabalho do artigo 29, documentação da Organização Internacional de Normalização (ISO), mais propriamente através dos documentos ISO/IEC 27001:2013, ISO/IEC 27002:2013 e ISO/IEC 27701:2019, e outros documentos relevantes tais como a Resolução do Conselho de Ministros nº 41/2018, relativa aos requisitos técnicos mínimos das redes e sistemas de informação ou o boletim do National Institute of Standards and Technology (NIST) relativo à integração da segurança no ciclo de vida de desenvolvimento de software (SDLC).

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
A.1	Baixo	incluir os requisitos legais da proteção de dados pessoais na política de segurança da informação da organização tendo por referência, por exemplo, as ISOs 27701 e 27001	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html
A.2	Baixo	cumprir as obrigações de renovação e revisão regulares preconizadas, por exemplo, pelas ISOs 27701 e 27001	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html
A.3	Médio	incluir e documentar os requisitos legais da proteção de dados pessoais na política de segurança da informação da organização tendo por referência, por exemplo, as ISOs 27701 e 27001	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html
A.4	Médio	De acordo com a descrição da medida, incluir os requisitos legais da proteção de dados pessoais na política de segurança da informação da organização tendo por referência, por exemplo, as ISOs 27701 e 27001	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html
A.5	Médio	De acordo com a descrição da medida, incluir os requisitos legais da proteção de dados pessoais na política de segurança da informação da organização tendo por referência, por exemplo, as ISOs 27701 e 27001	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html
A.6	Alto	cumprir as obrigações de renovação e revisão regulares preconizadas, por exemplo, pelas ISOs 27701 e 27001	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
A.6.1	Baixo	para auxiliar a classificação da função da organização, poderá ser utilizado o documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
A.6.2	Baixo	Em coordenação com as diversas partes interessadas e alinhado com a descrição da medida, incluir os requisitos legais da proteção de dados pessoais na política de segurança da informação da organização tendo por referência, por exemplo, as ISOs 27701 e 27001	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html
A.6.3	Baixo	incluir os requisitos legais da proteção de dados pessoais na política de segurança da informação da organização tendo por referência, por exemplo, as ISOs 27701 e 27001	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html
A.6.4	Baixo	cumprir as obrigações de renovação e revisão regulares preconizadas, por exemplo, pelas ISOs 27701 e 27001	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
A.6.5	Baixo	cumprir o preconizado nesta Solução proposta para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, tendo como base as orientações da ENISA e densificados com esclarecimentos da CNPD e da Organização Internacional de Normalização (ISO)	https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing
A.6.6	Baixo	cumprir o preconizado nesta Solução proposta para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, tendo como base as orientações da ENISA e densificados com esclarecimentos da CNPD e da Organização Internacional de Normalização (ISO)	https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
B.1	Baixo	incluir os requisitos legais da proteção de dados pessoais na política de segurança da informação da organização, incluindo as obrigações do Encarregado da Proteção de Dados, quando aplicável, tendo por referência, por exemplo, as ISOs 27701 e 27001, as orientações da CNPD e da EDPB/WP29 relativas ao Encarregado de Proteção de Dados (wp243rev.01)	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html; https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#d1e4673-1-1; https://www.cnpd.pt/organizacoes/obrigacoes/encarregado-de-protecao-de-dados/; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
B.2	Baixo	incluir os requisitos legais da proteção de dados pessoais na política de segurança da informação da organização, incluindo as obrigações do Encarregado da Proteção de Dados, quando aplicável, tendo por referência, por exemplo, as ISOs 27701 e 27001, as orientações da CNPD e da EDPB/WP29 relativas ao Encarregado de Proteção de Dados (wp243rev.01)	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html; https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#d1e4673-1-1; https://www.cnpd.pt/organizacoes/obrigacoes/encarregado-de-protecao-de-dados/; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
B.3	Médio	incluir os requisitos legais da proteção de dados pessoais na política de segurança da informação da organização, incluindo as obrigações do Encarregado da Proteção de Dados, quando aplicável, tendo por referência, por exemplo, as ISOs 27701 e 27001, as orientações da CNPD e da EDPB/WP29 relativas ao Encarregado de Proteção de Dados (wp243rev.01)	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html; https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#d1e4673-1-1; https://www.cnpd.pt/organizacoes/obrigacoes/encarregado-de-protecao-de-dados/; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
B.4	Alto	incluir os requisitos legais da proteção de dados pessoais na política de segurança da informação da organização, incluindo as obrigações do Encarregado da Proteção de Dados, quando aplicável, tendo por referência, por exemplo, as ISOs 27701 e 27001 e as orientações da CNPD	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html; https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#d1e4673-1-1; https://www.cnpd.pt/organizacoes/obrigacoes/encarregado-de-protecao-de-dados/
B.5	Alto	incluir os requisitos legais da proteção de dados pessoais na política de segurança da informação da organização, incluindo as obrigações do Encarregado da Proteção de Dados, quando aplicável, tendo por referência, por exemplo, as ISOs 27701 e 27001 e as orientações da CNPD	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html; https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#d1e4673-1-1; https://www.cnpd.pt/organizacoes/obrigacoes/encarregado-de-protecao-de-dados/

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
C.1	Baixo	considerar, como referência, a atribuição de direitos de acesso e privilégio de forma restrita e controlada, da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034
C.2	Médio	incluir os requisitos de direitos de acesso e privilégio na política de segurança da informação da organização tendo por referência, por exemplo, as ISOs 27701 e 27001, bem como a Arquitetura de	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html; https://dre.pt/application/conteudo/114937034

		segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	
C.3	Médio	incluir os requisitos de direitos de acesso e privilégio na política de segurança da informação da organização tendo por referência, por exemplo, as ISOs 27701 e 27001, bem como a Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html; https://dre.pt/application/conteudo/114937034
C.4	Alto	incluir os requisitos de direitos de acesso e privilégio na política de segurança da informação da organização tendo por referência, por exemplo, as ISOs 27701 e 27001, bem como a Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html; https://dre.pt/application/conteudo/114937034

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
D.1	Baixo	incluir os requisitos de direitos de acesso e privilégio na política de segurança da informação da organização tendo por referência, por exemplo, as ISOs 27701 e 27001, bem como a Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html; https://dre.pt/application/conteudo/114937034
D.2	Baixo	cumprir as obrigações de renovação e revisão regulares preconizadas, por exemplo, pelas ISOs 27701 e 27001, bem como a Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html; https://dre.pt/application/conteudo/114937034
D.3	Médio	incluir os requisitos de direitos de acesso e privilégio na política de segurança da informação da organização tendo por referência, por exemplo, as ISOs 27701 e 27001, bem como a Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html; https://dre.pt/application/conteudo/114937034
D.4	Alto	cumprir as obrigações de renovação e revisão regulares preconizadas, por exemplo, pelas ISOs 27701 e 27001	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html
D.4.1	Baixo	incluir os requisitos de classificação da informação constantes da ISO 27002 e as categorias de dados pessoais existentes nesta Solução proposta para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, tendo como referência a proposta da CNPD	https://www.iso.org/standard/54533.html
D.4.2	Baixo	incluir os requisitos de rotulagem da informação constantes da ISO 27002 e as categorias de dados pessoais existentes nesta Solução proposta para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, tendo como referência a proposta da CNPD	https://www.iso.org/standard/54533.html
D.4.3	Baixo	incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis	https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf
D.4.4	Baixo	incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis	https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
E.1	Baixo	Implementar uma política de gestão de alterações, por exemplo, aplicando as boas práticas do ITIL – Information Techonology Infrastructure Library.	https://www.axelos.com/news/blogs/january-2016/itil-practitioner-organizational-change-management
E.2	Baixo	considerar a integração das questões de segurança em cada fase do ciclo de vida do desenvolvimento de software (SDLC) preconizado pelo NIST – National Institute of Standards and Technology	Radack, S. (2009), The System Development Life Cycle (SDLC), ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm ? pub_id = 902622 (acedido em 7 de abril de 2021). https://www.nist.gov/publications/system-development-life-cycle-sdlc
E.3	Médio	Implementar uma política de gestão de alterações, por exemplo, aplicando as boas práticas do ITIL – Information Techonology Infrastructure Library.	https://www.axelos.com/news/blogs/january-2016/itil-practitioner-organizational-change-management

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
F.1	Baixo	para auxiliar a classificação da função da organização, poderá ser utilizado o documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
F.2	Baixo	considerar as orientações do documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
F.3	Baixo	considerar as orientações do documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
F.4	Médio	considerar as orientações do documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
F.5	Alto	considerar as orientações do documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
G.1	Baixo	cumprir as obrigações dos artigos 33º e 34º do RGPD, tendo como referência as orientações da CNPD, e EDPB, incluindo formulário de notificação de violação de dados pessoais	https://www.cnpd.pt/organizacoes/obrigacoes/violacao-de-dados-ou-data-breach/; https://www.cnpd.pt:8086/databreach/?AspxAutoDetectCookieSupport=1; https://www.cnpd.pt/media/zgkec1q0/data-breach-_wp250rev01_pt.pdf
G.2	Baixo	cumprir as obrigações dos artigos 33º e 34º do RGPD, tendo como referência as orientações da CNPD, e EDPB, incluindo formulário de notificação de violação de dados pessoais	https://www.cnpd.pt/organizacoes/obrigacoes/violacao-de-dados-ou-data-breach/; https://www.cnpd.pt:8086/databreach/?AspxAutoDetectCookieSupport=1; https://www.cnpd.pt/media/zgkec1q0/data-breach-_wp250rev01_pt.pdf
G.3	Médio	cumprir as obrigações dos artigos 33º e 34º do RGPD, tendo como referência as orientações da CNPD, e EDPB, incluindo formulário de notificação de violação de dados pessoais	https://www.cnpd.pt/organizacoes/obrigacoes/violacao-de-dados-ou-data-breach/; https://www.cnpd.pt:8086/databreach/?AspxAutoDetectCookieSupport=1; https://www.cnpd.pt/media/zgkec1q0/data-breach-_wp250rev01_pt.pdf
G.4	Alto	cumprir as obrigações dos artigos 33º e 34º do RGPD, tendo como referência as orientações da CNPD, e EDPB, incluindo formulário de notificação de violação de dados pessoais	https://www.cnpd.pt/organizacoes/obrigacoes/violacao-de-dados-ou-data-breach/; https://www.cnpd.pt:8086/databreach/?AspxAutoDetectCookieSupport=1; https://www.cnpd.pt/media/zgkec1q0/data-breach-_wp250rev01_pt.pdf

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
H.1	Baixo	cumprir as obrigações dos artigos 33º e 34º do RGPD, tendo como referência as orientações da CNPD, e EDPB, incluindo formulário de notificação de violação de dados pessoais	https://www.cnpd.pt/organizacoes/obrigacoes/violacao-de-dados-ou-data-breach/; https://www.cnpd.pt:8086/databreach/?AspxAutoDetectCookieSupport=1; https://www.cnpd.pt/media/zgkec1q0/data-breach-_wp250rev01_pt.pdf
H.2	Médio	cumprir os aspetos de segurança da informação na gestão da continuidade do negócio preconizadas, por exemplo, pelas ISOs 27701 e 22301	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/75106.html
H.3	Médio	cumprir os aspetos de segurança da informação na gestão da continuidade do negócio preconizadas, por exemplo, pelas ISOs 27701 e 22301	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/75106.html
H.4	Alto	cumprir os aspetos de segurança da informação na gestão da continuidade do negócio preconizadas, por exemplo, pelas ISOs 27701 e 22301	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/75106.html
H.5	Alto	cumprir os aspetos de segurança da informação na gestão da continuidade do negócio preconizadas, por exemplo, pelas ISOs 27001 e 22301	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/75106.html

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
I.1	Baixo	cumprir os aspetos de segurança na gestão de recursos humanos preconizadas, por exemplo, pelas ISO 27001	https://www.iso.org/standard/54534.html
I.2	Médio	cumprir os aspetos de segurança na gestão de recursos humanos preconizadas, por exemplo, pelas ISO 27001	https://www.iso.org/standard/54534.html
I.3	Alto	cumprir os aspetos de segurança na gestão de recursos humanos preconizadas, por exemplo, pelas ISO 27001	https://www.iso.org/standard/54534.html

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
J.1	Baixo	incluir os requisitos legais da proteção de dados pessoais na política de segurança da informação da organização, incluindo as obrigações do Encarregado da Proteção de Dados, quando aplicável, tendo por referência, por exemplo, as ISOs 27701 e 27001 e as orientações da CNPD	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html; https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#d1e4673-1-1; https://www.cnpd.pt/organizacoes/obrigacoes/encarregado-de-protecao-de-dados/
J.2	Médio	cumprir os aspetos de segurança na gestão de recursos humanos preconizadas, por exemplo, pelas ISO 27001	https://www.iso.org/standard/54534.html
J.3	Alto	cumprir os aspetos de segurança na gestão de recursos humanos preconizadas, por exemplo, pelas ISO 27001	https://www.iso.org/standard/54534.html

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
U.1.1	Baixo	De acordo com a descrição da medida, incluir os requisitos legais da proteção de dados pessoais na política de segurança da informação da organização tendo por referência, por exemplo, as ISOs 27701 e 27001	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html
U.1.2	Baixo	De acordo com a descrição da medida, incluir os requisitos legais da proteção de dados pessoais na política de segurança da informação da organização tendo por referência, por exemplo, as ISOs 27701 e 27001	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
U.2.1	Baixo	cumprir as obrigações de renovação e revisão regulares preconizadas, por exemplo, pelas ISOs 27701 e 27001	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html
U.2.2	Baixo	cumprir as obrigações de renovação e revisão regulares preconizadas, por exemplo, pelas ISOs 27701 e 27001	https://www.iso.org/standard/71670.html; https://www.iso.org/standard/54534.html

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
V.1.1	Baixo	cumprir o preconizado nesta Solução proposta para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, tendo como base as orientações da ENISA e densificados com esclarecimentos da CNPD e da Organização Internacional de Normalização (ISO)	https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing; https://www.cnpd.pt/organizacoes/obrigacoes/registo-de-atividades-de-tratamento/
V.1.2	Baixo	cumprir o preconizado nesta Solução proposta para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, tendo como base as orientações da ENISA e densificados com esclarecimentos da CNPD e da Organização Internacional de Normalização (ISO)	https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing; https://www.cnpd.pt/organizacoes/obrigacoes/registo-de-atividades-de-tratamento/
V.1.3	Baixo	considerar as orientações do documento 5/2020 do EDPB sobre o consentimento nos termos do RGPD	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
V.1.4	Baixo	considerar as orientações do documento 5/2020 do EDPB sobre o consentimento nos termos do RGPD	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
V.1.5	Baixo	considerar as informações da CNPD, orientações do EDPB e a ferramenta de avaliação de impacto da CNIL	https://www.cnpd.pt/organizacoes/obrigacoes/avaliacao-de-impacto/; https://www.cnpd.pt/media/f0ide5i0/aipd_wp248rev-01_pt.pdf; https://www.cnil.fr/en/privacy-impact-assessment-pia; https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
V.1.6	Baixo	considerar as orientações do documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
V.1.7	Baixo	considerar as orientações do documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento, responsáveis conjuntos e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
V.1.8	Baixo	cumprir o preconizado nesta Solução proposta para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, tendo como base as orientações da CNPD e respetivos modelos de registo	https://www.cnpd.pt/organizacoes/obrigacoes/registo-de-atividades-de-tratamento/

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
V.2.1	Baixo	considerar as orientações do documento wp260rev.01 do EDPB/WP29 sobre transparência e regras para o exercício dos direitos dos titulares dos dados nos termos do RGPD	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
V.2.2	Baixo	considerar as orientações do documento wp260rev.01 do EDPB/WP29 sobre transparência e regras para o exercício dos direitos dos titulares dos dados nos termos do RGPD, os dossiers temáticos relativos aos direitos individuais, direito de ser informado, e responsabilidade e governaça da Autoridade de Controlo do Reino Unido (ICO), e ter como referência o modelo de aviso de privacidade disponibilizado pela ICO	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/; https://ico.org.uk/for-organisations/guide-to-data-

			protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/; https://ico.org.uk/for-organisations/make-your-own-privacy-notice/
V.2.3	Baixo	considerar as orientações do documento wp260rev.01 do EDPB/WP29 sobre transparência e regras para o exercício dos direitos dos titulares dos dados nos termos do RGPD	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
V.2.4	Baixo	considerar as orientações do documento 5/2020 do EDPB sobre o consentimento nos termos do RGPD	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
V.2.5	Baixo	considerar as explicações da CNPD relativas ao direito de oposição assim como o dossier temático da Autoridade de Controlo do Reino Unido, ICO, relativo ao direito de oposição	https://www.cnpd.pt/cidadaos/direitos/direito-de-oposicao/; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/
V.2.6	Baixo	considerar as orientações do documento wp260rev.01 do EDPB/WP29 sobre transparência e regras para o exercício dos direitos dos titulares dos dados nos termos do RGPD, assim como o dossier temático da Autoridade de Controlo do Reino Unido, ICO, relativo aos direitos individuais	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/
V.2.7	Baixo	considerar as orientações do documento wp260rev.01 do EDPB/WP29 sobre transparência e regras para o exercício dos direitos dos titulares dos dados nos termos do RGPD, assim como o dossier temático da Autoridade de Controlo do Reino Unido, ICO, relativo aos direitos individuais	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/
V.2.8	Baixo	considerar as explicações da CNPD relativas ao direito de portabilidade assim como as orientações do documento wp242rev.01 do EDPB/WP29 sobre o direito de portabilidade de dados	https://www.cnpd.pt/cidadaos/direitos/direito-de-portabilidade/; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233
V.2.9	Baixo	considerar as orientações da Autoridade de Controlo Francesa, CNIL, relativas ao direito de acesso do titular dos dados	https://www.cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-dacces
V.2.10	Baixo	considerar as orientações do documento wp251rev.01 do EDPB/WP29 sobre decisões individuais automatizadas, incluindo definição de perfis	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
V.3.1	Baixo	considerar os dossiers temáticos da Autoridade de Controlo do Reino Unido, ICO, relativos à limitação das finalidades e à minimização dos dados	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/
V.3.2	Baixo	considerar as orientações do documento 4/2019 do EDPB sobre a proteção de dados desde a conceção e por defeito	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en
V.3.3	Baixo	considerar o dossier temático da Autoridade de Controlo do Reino Unido, ICO, relativo à exatidão dos dados pessoais	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/
V.3.4	Baixo	considerar os dossiers temáticos da Autoridade de Controlo do Reino Unido, ICO, relativos à minimização dos dados e à limitação da conservação, bem como o relatório da ENISA relativo à pseudonimização de dados	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/; https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases
V.3.5	Baixo	considerar os dossiers temáticos da Autoridade de Controlo do Reino Unido, ICO, relativos à minimização dos dados e à limitação da conservação, bem como o relatório da ENISA relativo à pseudonimização de dados	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/; https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases
V.3.6	Baixo	considerar o dossier temático da Autoridade de Controlo do Reino Unido, ICO, relativo à minimização dos dados e incluir	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/; https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf

		as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis	
V.3.7	Baixo	considerar as orientações do documento wp260rev.01 do EDPB/WP29 sobre transparência e regras para o exercício dos direitos dos titulares dos dados nos termos do RGPD	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
V.3.8	Baixo	considerar o dossier temático da Autoridade de Controlo do Reino Unido, ICO, relativo à integridade e confidencialidade (segurança)	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/
V.3.9	Baixo	considerar o dossier temático da Autoridade de Controlo do Reino Unido, ICO, relativo à integridade e confidencialidade (segurança)	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
V.4.1	Baixo	considerar as orientações do documento 2/2020 do EDPB sobre transferências de dados pessoais sujeitas a garantias adequadas, e as informações da Comissão Europeia relativas à dimensão internacional da proteção de dados, com destaque para as regras sobre transferências internacionais de dados, decisões de adequação, cláusulas contratuais padrão e regras vinculativas aplicáveis às empresas	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation-2016679_en; https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_en
V.4.2	Baixo	considerar as orientações da Autoridade de Controlo Francesa, CNIL, relativas ao direito de acesso do titular dos dados e cumprir o preconizado nesta Solução proposta para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, tendo como base as orientações da CNPD e respetivos modelos de registo	https://www.cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-dacces; https://www.cnpd.pt/organizacoes/obrigacoes/registo-de-atividades-de-tratamento/
V.4.3	Baixo	cumprir o preconizado nesta Solução proposta para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, tendo como base as orientações da CNPD e respetivos modelos de registo	https://www.cnpd.pt/organizacoes/obrigacoes/registo-de-atividades-de-tratamento/
V.4.4	Baixo	cumprir o preconizado nesta Solução proposta para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, tendo como base as orientações da CNPD e respetivos modelos de registo	https://www.cnpd.pt/organizacoes/obrigacoes/registo-de-atividades-de-tratamento/

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
W.1.1	Baixo	considerar o documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
W.1.2	Baixo	considerar o documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
W.1.3	Baixo	considerar as orientações do documento 5/2020 do EDPB sobre o consentimento nos termos do RGPD	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
W.1.4	Baixo	considerar o documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
W.1.5	Baixo	considerar o documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
W.1.6	Baixo	cumprir o preconizado nesta Solução proposta para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, tendo como base as orientações da CNPD e respetivos modelos de registo, bem	https://www.cnpd.pt/organizacoes/obrigacoes/registo-de-atividades-de-tratamento/; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045

	como o documento de posição do EDPB/WP29 sobre as derrogações à obrigação de manter registos das atividades de tratamento de acordo com o Artigo 30 (5) do RGPD

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
W.2.1	Baixo	considerar o documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD e as orientações do documento wp260rev.01 do EDPB/WP29 sobre transparência e regras para o exercício dos direitos dos titulares dos dados nos termos do RGPD, assim como o dossier temático da Autoridade de Controlo do Reino Unido, ICO, relativo aos direitos individuais	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
W.3.1	Baixo	considerar o dossier temático da Autoridade de Controlo do Reino Unido, ICO, relativo à minimização dos dados e incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/; https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf
W.3.2	Baixo	considerar o documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD e cumprir o preconizado nesta Solução proposta para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, tendo como base as orientações da CNPD e respetivos modelos de registo	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en; https://www.cnpd.pt/organizacoes/obrigacoes/registo-de-atividades-de-tratamento/
W.3.3	Baixo	considerar o dossier temático da Autoridade de Controlo do Reino Unido, ICO, relativo à integridade e confidencialidade (segurança) e o documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/; https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
W.4.1	Baixo	considerar as orientações do documento 2/2020 do EDPB sobre transferências de dados pessoais sujeitas a garantias adequadas, e as informações da Comissão Europeia relativas à dimensão internacional da proteção de dados, com destaque para as regras sobre transferências internacionais de dados, decisões de adequação, cláusulas contratuais padrão e regras vinculativas aplicáveis às empresas	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation-2016679_en; https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_en
W.4.2	Baixo	cumprir o preconizado nesta Solução proposta para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, tendo como base as orientações da CNPD e respetivos modelos de registo	https://www.cnpd.pt/organizacoes/obrigacoes/registo-de-atividades-de-tratamento/
W.4.3	Baixo	cumprir o preconizado nesta Solução proposta para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, tendo como base as orientações da CNPD e respetivos modelos de registo	https://www.cnpd.pt/organizacoes/obrigacoes/registo-de-atividades-de-tratamento/
W.4.4	Baixo	considerar o documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
W.4.5	Baixo	considerar as orientações do documento 2/2020 do EDPB sobre transferências de dados pessoais sujeitas a garantias adequadas, e as informações da Comissão Europeia relativas à dimensão internacional da proteção de dados, com destaque para as regras sobre transferências internacionais de dados, decisões de	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation-2016679_en; https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_en

		adequação, cláusulas contratuais padrão e regras vinculativas aplicáveis às empresas	
W.4.6	Baixo	considerar o documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
W.4.7	Baixo	considerar o documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
W.4.8	Baixo	considerar o documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
K.1.1	Baixo	considerar os dossiers temáticos da Autoridade de Controlo do Reino Unido, ICO, relativo à integridade e confidencialidade (segurança) e relativo aos direitos individuais, bem como as orientações do documento wp260rev.01 do EDPB/WP29 sobre transparência e regras para o exercício dos direitos dos titulares dos dados nos termos do RGPD	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
K.1	Baixo	considerar os dossiers temáticos da Autoridade de Controlo do Reino Unido, ICO, relativo à integridade e confidencialidade (segurança) e relativo aos direitos individuais, bem como as orientações do documento wp260rev.01 do EDPB/WP29 sobre transparência e regras para o exercício dos direitos dos titulares dos dados nos termos do RGPD	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
K.2	Baixo	considerar, como referência, a atribuição de direitos de acesso e privilégio de forma restrita e controlada, da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034
K.3	Baixo	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034
K.4	Baixo	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034
K.5	Médio	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034
K.6	Médio	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034
K.7	Alto	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034
K.8	Alto	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
L.1	Baixo	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034
L.2	Baixo	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034
L.3	Médio	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034
L.4	Médio	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034

L.5	Médio	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
M.1	Baixo	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034
M.2	Baixo	considerar o dossier temático da Autoridade de Controlo do Reino Unido, ICO, relativo à minimização dos dados	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/
M.3	Médio	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018 e o documento "Recommended cryptographic measures - Securing personal data" da ENISA	https://dre.pt/application/conteudo/114937034; https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data
M.4	Médio	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018 e os documentos "Recommended cryptographic measures - Securing personal data" e "Encrypted Traffic Analysis" da ENISA	https://dre.pt/application/conteudo/114937034; https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data; https://www.enisa.europa.eu/publications/encrypted-traffic-analysis
M.5	Médio	considerar o relatório da ENISA relativo à pseudonimização de dados	https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases
M.6	Alto	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
N.1	Baixo	De acordo com a descrição da medida, incluir os requisitos das ISOs 27001 e 27002 nas configurações de segurança dos sistemas de informação	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
N.2	Baixo	De acordo com a descrição da medida, incluir os requisitos das ISOs 27001 e 27002 nas configurações de segurança dos sistemas de informação	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
N.3	Baixo	De acordo com a descrição da medida, incluir os requisitos das ISOs 27001 e 27002 nas configurações de segurança dos sistemas de informação	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
N.4	Baixo	De acordo com a descrição da medida, incluir os requisitos das ISOs 27001 e 27002 nas configurações de segurança dos sistemas de informação	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
N.5	Baixo	De acordo com a descrição da medida, incluir os requisitos das ISOs 27001 e 27002 nas configurações de segurança dos sistemas de informação	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
N.6	Médio	De acordo com a descrição da medida, incluir os requisitos das ISOs 27001 e 27002 nas configurações de segurança dos sistemas de informação	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
N.7	Alto	De acordo com a descrição da medida, incluir os requisitos das ISOs 27001 e 27002 nas configurações de segurança dos sistemas de informação, bem como as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf
N.8	Alto	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034
N.9	Alto	considerar, como referência, os documentos "Recommended cryptographic measures - Securing personal data" e "Encrypted Traffic Analysis" da ENISA	https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data; https://www.enisa.europa.eu/publications/encrypted-traffic-analysis

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
O.1	Baixo	considerar, como referência, os documentos "Recommended cryptographic measures - Securing personal data" e "Encrypted Traffic Analysis" da ENISA	https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data; https://www.enisa.europa.eu/publications/encrypted-traffic-analysis
O.2	Médio	considerar, como referência, os documentos "Recommended cryptographic measures - Securing personal data" e "Encrypted Traffic Analysis" da ENISA	https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data; https://www.enisa.europa.eu/publications/encrypted-traffic-analysis
O.3	Médio	De acordo com a descrição da medida, incluir os requisitos de segurança de comunicações das ISOs 27001 e 27002	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
O.4	Médio	De acordo com a descrição da medida, incluir os requisitos de segurança de comunicações das ISOs 27001 e 27002	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
O.5	Alto	considerar, como referência, as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://dre.pt/application/conteudo/114937034
O.6	Alto	De acordo com a descrição da medida, incluir os requisitos de segurança de comunicações das ISOs 27001 e 27002 bem como as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://dre.pt/application/conteudo/114937034
O.7	Alto	De acordo com a descrição da medida, incluir os requisitos de segurança de comunicações das ISOs 27001 e 27002 bem como as regras da Arquitetura de segurança das redes e sistemas de informação da Resolução do Conselho de Ministros n.º 41/2018	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://dre.pt/application/conteudo/114937034
O.7.1	Baixo	considerar o documento 7/2020 do EDPB sobre os conceitos relativos a responsável pelo tratamento e subcontratante no RGPD, bem como as obrigações do Encarregado da Proteção de Dados, tendo por referência as orientações da CNPD e da EDPB/WP29 relativas ao Encarregado de Proteção de Dados (wp243rev.01)	https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en; https://www.cnpd.pt/organizacoes/obrigacoes/encarregado-de-protecao-de-dados/; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
P.1	Baixo	De acordo com a descrição da medida, incluir os requisitos de salvaguarda de dados das ISOs 27001 e 27002 e as orientações sobre como fazer backups da NCSC - National Cyber Security Centre, do Reino Unido	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data
P.2	Baixo	De acordo com a descrição da medida, incluir os requisitos de salvaguarda de dados das ISOs 27001 e 27002 e as orientações sobre como fazer backups da NCSC - National Cyber Security Centre, do Reino Unido	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data
P.3	Baixo	De acordo com a descrição da medida, incluir os requisitos de salvaguarda de dados das ISOs 27001 e 27002 e as orientações sobre como fazer backups da NCSC - National Cyber Security Centre, do Reino Unido	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data
P.4	Baixo	De acordo com a descrição da medida, incluir os requisitos de salvaguarda de dados das ISOs 27001 e 27002 e as orientações sobre como fazer backups da NCSC - National Cyber Security Centre, do Reino Unido	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data
P.5	Médio	De acordo com a descrição da medida, incluir os requisitos de salvaguarda de dados das ISOs 27001 e 27002 e as orientações sobre como fazer backups da NCSC - National Cyber Security Centre, do Reino Unido	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data
P.6	Médio	De acordo com a descrição da medida, incluir os requisitos de salvaguarda de dados das ISOs 27001 e 27002 e as orientações sobre como fazer backups da NCSC - National Cyber Security Centre, do Reino Unido	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data
P.7	Médio	De acordo com a descrição da medida, incluir os requisitos de salvaguarda de dados das ISOs 27001 e 27002 e as orientações sobre como fazer backups da NCSC - National Cyber Security Centre, do Reino Unido	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data

P.8	Médio	De acordo com a descrição da medida, incluir os requisitos de salvaguarda de dados das ISOs 27001 e 27002 e as orientações sobre como fazer backups da NCSC - National Cyber Security Centre, do Reino Unido	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data
P.9	Alto	De acordo com a descrição da medida, incluir os requisitos de salvaguarda de dados das ISOs 27001 e 27002 e as orientações sobre como fazer backups da NCSC - National Cyber Security Centre, do Reino Unido	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
Q.1	Baixo	incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis e de acordo com a descrição da medida, incluir os requisitos de dispositivos móveis e teletrabalho das ISOs 27001 e 27002	https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf; https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
Q.2	Baixo	incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis e de acordo com a descrição da medida, incluir os requisitos de dispositivos móveis e teletrabalho das ISOs 27001 e 27002	https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf; https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
Q.3	Baixo	incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis e de acordo com a descrição da medida, incluir os requisitos de dispositivos móveis e teletrabalho das ISOs 27001 e 27002	https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf; https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
Q.4	Médio	incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis e de acordo com a descrição da medida, incluir os requisitos de dispositivos móveis e teletrabalho das ISOs 27001 e 27002	https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf; https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
Q.5	Médio	incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis e de acordo com a descrição da medida, incluir os requisitos de dispositivos móveis e teletrabalho das ISOs 27001 e 27002	https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf; https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
Q.6	Médio	incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis e de acordo com a descrição da medida, incluir os requisitos de dispositivos móveis e teletrabalho das ISOs 27001 e 27002	https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf; https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
Q.7	Médio	incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis e de acordo com a descrição da medida, incluir os requisitos de dispositivos móveis e teletrabalho das ISOs 27001 e 27002	https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf; https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
Q.8	Alto	incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis e de acordo com a descrição da medida, incluir os requisitos de dispositivos móveis e teletrabalho das ISOs 27001 e 27002	https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf; https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
Q.9	Alto	incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis e de acordo com a descrição da medida, incluir os requisitos de dispositivos móveis e teletrabalho das ISOs 27001 e 27002	https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf; https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
R.1	Baixo	considerar a integração das questões de segurança em cada fase do ciclo de vida do desenvolvimento de software (SDLC) preconizado pelo NIST – National Institute of Standards and Technology, bem como as orientações do documento 4/2019 do EDPB sobre a proteção de dados desde a conceção e por defeito	Radack, S. (2009), The System Development Life Cycle (SDLC), ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm ? pub_id = 902622 (acedido em 7 de abril de 2021). https://www.nist.gov/publications/system-development-life-cycle-sdlc; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en
R.2	Baixo	considerar a integração das questões de segurança em cada fase do ciclo de vida do desenvolvimento de software (SDLC) preconizado pelo NIST – National Institute of Standards and Technology, bem como as orientações do documento 4/2019 do EDPB sobre a proteção de dados desde a conceção e por defeito	Radack, S. (2009), The System Development Life Cycle (SDLC), ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm ? pub_id = 902622 (acedido em 7 de abril de 2021). https://www.nist.gov/publications/system-development-life-cycle-sdlc; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en
R.3	Baixo	considerar a integração das questões de segurança em cada fase do ciclo de vida do desenvolvimento de software (SDLC) preconizado pelo NIST – National Institute of Standards and Technology, bem como as orientações do documento 4/2019 do EDPB sobre a proteção de dados desde a conceção e por defeito, e o dossier sobre as tecnologias de reforço da privacidade (PETs) da ENISA	Radack, S. (2009), The System Development Life Cycle (SDLC), ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm ? pub_id = 902622 (acedido em 7 de abril de 2021). https://www.nist.gov/publications/system-development-life-cycle-sdlc; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en; https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies?tab=details
R.4	Baixo	considerar a integração das questões de segurança em cada fase do ciclo de vida do desenvolvimento de software (SDLC) preconizado pelo NIST – National Institute of Standards and Technology, bem como as orientações do documento 4/2019 do EDPB sobre a proteção de dados desde a conceção e por defeito	Radack, S. (2009), The System Development Life Cycle (SDLC), ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm ? pub_id = 902622 (acedido em 7 de abril de 2021). https://www.nist.gov/publications/system-development-life-cycle-sdlc; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en
R.5	Baixo	De acordo com a descrição da medida, incluir os requisitos de segurança no desenvolvimento e nos processos de suporte das ISOs 27001 e 27002	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
R.6	Médio	De acordo com a descrição da medida, incluir os requisitos de gestão de vulnerabilidades técnicas das ISOs 27001 e 27002	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
R.7	Médio	De acordo com a descrição da medida, incluir os requisitos de segurança no desenvolvimento e nos processos de suporte das ISOs 27001 e 27002	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
R.8	Médio	De acordo com a descrição da medida, incluir os requisitos de gestão de vulnerabilidades técnicas das ISOs 27001 e 27002	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
R.9	Médio	De acordo com a descrição da medida, incluir os requisitos de gestão de vulnerabilidades técnicas das ISOs 27001 e 27002	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
S.1	Baixo	incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis e de acordo com a descrição da medida, incluir os requisitos sobre equipamentos das ISOs 27001 e 27002	https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf; https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
S.2	Baixo	De acordo com a descrição da medida, incluir os requisitos de manuseamento de suportes de dados das ISOs 27001 e 27002	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
S.3	Médio	incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis e de acordo com a	https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf; https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html

		descrição da medida, incluir os requisitos sobre equipamentos das ISOs 27001 e 27002	
S.4	Médio	incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis e de acordo com a descrição da medida, incluir os requisitos relativos a equipamentos / segurança física e ambiental das ISOs 27001 e 27002	https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf; https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
S.5	Alto	incluir as recomendações da Autoridade de Controlo Irlandesa para o uso de dispositivos de armazenamento portáteis e de acordo com a descrição da medida, incluir os requisitos relativos a equipamentos / segurança física e ambiental das ISOs 27001 e 27002	https://www.dataprotection.ie/sites/default/files/uploads/2019-11/General%20Portable%20Storage%20Device%20Recommendations_Oct19.pdf; https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html
S.6	Alto	De acordo com a descrição da medida, incluir os requisitos de manuseamento de suportes de dados das ISOs 27001 e 27002	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html

ID Medida	Nível de Risco	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
T.1	Baixo	De acordo com a descrição da medida, incluir os requisitos de segurança física e ambiental das ISOs 27001 e 27002, a decisão do Conselho da União Europeia relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (2013/488/UE), e considerar as informações da Autoridade de Controlo Francesa (CNIL) relativas à proteção de instalações físicas	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:02013D0488-20191230; https://www.cnil.fr/fr/securite-proteger-les-locaux
T.2	Médio	De acordo com a descrição da medida, incluir os requisitos de segurança física e ambiental das ISOs 27001 e 27002, a decisão do Conselho da União Europeia relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (2013/488/UE), e considerar as informações da Autoridade de Controlo Francesa (CNIL) relativas à proteção de instalações físicas	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:02013D0488-20191230; https://www.cnil.fr/fr/securite-proteger-les-locaux
T.3	Médio	De acordo com a descrição da medida, incluir os requisitos de segurança física e ambiental das ISOs 27001 e 27002, a decisão do Conselho da União Europeia relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (2013/488/UE), e considerar as informações da Autoridade de Controlo Francesa (CNIL) relativas à proteção de instalações físicas	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:02013D0488-20191230; https://www.cnil.fr/fr/securite-proteger-les-locaux
T.4	Médio	De acordo com a descrição da medida, incluir os requisitos de segurança física e ambiental das ISOs 27001 e 27002, a decisão do Conselho da União Europeia relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (2013/488/UE), e considerar as informações da Autoridade de Controlo Francesa (CNIL) relativas à proteção de instalações físicas	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:02013D0488-20191230; https://www.cnil.fr/fr/securite-proteger-les-locaux
T.5	Médio	De acordo com a descrição da medida, incluir os requisitos de segurança física e ambiental das ISOs 27001 e 27002, a decisão do Conselho da União Europeia relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (2013/488/UE), e considerar as informações da Autoridade de Controlo Francesa (CNIL) relativas à proteção de instalações físicas	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:02013D0488-20191230; https://www.cnil.fr/fr/securite-proteger-les-locaux
T.6	Médio	De acordo com a descrição da medida, incluir os requisitos de segurança física e ambiental das ISOs 27001 e 27002, a decisão do Conselho da União Europeia relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (2013/488/UE), e considerar as informações da Autoridade de Controlo Francesa (CNIL) relativas à proteção de instalações físicas	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:02013D0488-20191230; https://www.cnil.fr/fr/securite-proteger-les-locaux
T.7	Médio	De acordo com a descrição da medida, incluir os requisitos de segurança física e ambiental das ISOs 27001 e 27002, a decisão do Conselho da União Europeia relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (2013/488/UE), e considerar as informações da Autoridade de Controlo Francesa (CNIL) relativas à proteção de instalações físicas	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:02013D0488-20191230; https://www.cnil.fr/fr/securite-proteger-les-locaux
T.8	Médio	De acordo com a descrição da medida, incluir os requisitos de segurança física e ambiental das ISOs 27001 e 27002, a decisão do Conselho da União Europeia relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (2013/488/UE), e considerar as informações da Autoridade de Controlo Francesa (CNIL) relativas à proteção de instalações físicas	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html; https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:02013D0488-20191230; https://www.cnil.fr/fr/securite-proteger-les-locaux
T.8.1	Baixo	De acordo com a descrição da medida, incluir os requisitos de política de secretária limpa e ecrã limpo das ISOs 27001 e 27002	https://www.iso.org/standard/54534.html; https://www.iso.org/standard/54533.html

Anexo 9 – Fator de priorização com base nas sanções jurídicas do RGPD

Fator de priorização com base nas sanções jurídicas do RGPD

ID Medida	Nível de Risco	Obs:	Fator de priorização, com base nas sanções jurídicas
A.1	Baixo	ENISA	112
A.2	Baixo	ENISA	121
A.3	Médio	ENISA	112
A.4	Médio	ENISA	112
A.5	Médio	ENISA	121
A.6	Alto	ENISA	121
A.6.1	Baixo	NOVO	71
A.6.2	Baixo	NOVO	105
A.6.3	Baixo	NOVO	87
A.6.4	Baixo	NOVO	87
A.6.5	Baixo	NOVO	64
A.6.6	Baixo	NOVO	64
B.1	Baixo	ENISA	81
B.2	Baixo	ENISA	81
B.3	Médio	ENISA	81
B.4	Alto	ENISA	81
B.5	Alto	ENISA	81
C.1	Baixo	ENISA	121
C.2	Médio	ENISA	121
C.3	Médio	ENISA	121
C.4	Alto	ENISA	121
D.1	Baixo	ENISA	121
D.2	Baixo	ENISA	121
D.3	Médio	ENISA	121
D.4	Alto	ENISA	121
D.4.1	Baixo	NOVO	25
D.4.2	Baixo	NOVO	29
D.4.3	Baixo	NOVO	11
D.4.4	Baixo	NOVO	11
E.1	Baixo	ENISA	121
E.2	Baixo	ENISA	29
E.3	Médio	ENISA	121
F.1	Baixo	ENISA	121
F.2	Baixo	ENISA	3
F.3	Baixo	ENISA	3
F.4	Médio	ENISA	121
F.5	Alto	ENISA	3
G.1	Baixo	ENISA	26
G.2	Baixo	ENISA	121
G.3	Médio	ENISA	93
G.4	Alto	ENISA	121
H.1	Baixo	ENISA	121
H.2	Médio	ENISA	121
H.3	Médio	ENISA	121
H.4	Alto	ENISA	121
H.5	Alto	ENISA	121
I.1	Baixo	ENISA	121
I.2	Médio	ENISA	121
I.3	Alto	ENISA	121
J.1	Baixo	ENISA	121
J.2	Médio	ENISA	121
J.3	Alto	ENISA	121
U.1.1	Baixo	NOVO	3
U.1.2	Baixo	NOVO	81
U.2.1	Baixo	NOVO	67
U.2.2	Baixo	NOVO	67
V.1.1	Baixo	NOVO	28
V.1.2	Baixo	NOVO	1
V.1.3	Baixo	NOVO	119
V.1.4	Baixo	NOVO	89

ID Medida	Nível de Risco	Obs:	Fator de priorização, com base nas sanções jurídicas
V.1.5	Baixo	NOVO	70
V.1.6	Baixo	NOVO	72
V.1.7	Baixo	NOVO	111
V.1.8	Baixo	NOVO	76
V.2.1	Baixo	NOVO	100
V.2.2	Baixo	NOVO	2
V.2.3	Baixo	NOVO	66
V.2.4	Baixo	NOVO	63
V.2.5	Baixo	NOVO	60
V.2.6	Baixo	NOVO	24
V.2.7	Baixo	NOVO	121
V.2.8	Baixo	NOVO	106
V.2.9	Baixo	NOVO	69
V.2.10	Baixo	NOVO	74
V.3.1	Baixo	NOVO	9
V.3.2	Baixo	NOVO	108
V.3.3	Baixo	NOVO	73
V.3.4	Baixo	NOVO	10
V.3.5	Baixo	NOVO	7
V.3.6	Baixo	NOVO	61
V.3.7	Baixo	NOVO	74
V.3.8	Baixo	NOVO	29
V.3.9	Baixo	NOVO	29
V.4.1	Baixo	NOVO	109
V.4.2	Baixo	NOVO	110
V.4.3	Baixo	NOVO	115
V.4.4	Baixo	NOVO	115
W.1.1	Baixo	NOVO	77
W.1.2	Baixo	NOVO	8
W.1.3	Baixo	NOVO	98
W.1.4	Baixo	NOVO	95
W.1.5	Baixo	NOVO	95
W.1.6	Baixo	NOVO	107
W.2.1	Baixo	NOVO	92
W.3.1	Baixo	NOVO	61
W.3.2	Baixo	NOVO	94
W.3.3	Baixo	NOVO	29
W.4.1	Baixo	NOVO	120
W.4.2	Baixo	NOVO	115
W.4.3	Baixo	NOVO	115
W.4.4	Baixo	NOVO	95
W.4.5	Baixo	NOVO	121
W.4.6	Baixo	NOVO	91
W.4.7	Baixo	NOVO	90
W.4.8	Baixo	NOVO	99
K.1.1	Baixo	NOVO	29
K.1	Baixo	ENISA	29
K.2	Baixo	ENISA	121
K.3	Baixo	ENISA	29
K.4	Baixo	ENISA	121
K.5	Médio	ENISA	121
K.6	Médio	ENISA	121
K.7	Alto	ENISA	29
K.8	Alto	ENISA	29
L.1	Baixo	ENISA	29
L.2	Baixo	ENISA	121
L.3	Médio	ENISA	121
L.4	Médio	ENISA	29
L.5	Médio	ENISA	29
M.1	Baixo	ENISA	121
M.2	Baixo	ENISA	121
M.3	Médio	ENISA	78
M.4	Médio	ENISA	78
M.5	Médio	ENISA	78
M.6	Alto	ENISA	121
N.1	Baixo	ENISA	121
N.2	Baixo	ENISA	121
N.3	Baixo	ENISA	121
N.4	Baixo	ENISA	121
N.5	Baixo	ENISA	121
N.6	Médio	ENISA	121
N.7	Alto	ENISA	121
N.8	Alto	ENISA	11

ID Medida	Nível de Risco	Obs:	**Fator de priorização, com base nas sanções jurídicas**
N.9	Alto	ENISA	11
O.1	Baixo	ENISA	29
O.2	Médio	ENISA	121
O.3	Médio	ENISA	121
O.4	Médio	ENISA	121
O.5	Alto	ENISA	29
O.6	Alto	ENISA	121
O.7	Alto	ENISA	121
O.7.1	Baixo	NOVO	27
P.1	Baixo	ENISA	11
P.2	Baixo	ENISA	11
P.3	Baixo	ENISA	11
P.4	Baixo	ENISA	11
P.5	Médio	ENISA	11
P.6	Médio	ENISA	11
P.7	Médio	ENISA	11
P.8	Médio	ENISA	11
P.9	Alto	ENISA	11
Q.1	Baixo	ENISA	29
Q.2	Baixo	ENISA	29
Q.3	Baixo	ENISA	29
Q.4	Médio	ENISA	29
Q.5	Médio	ENISA	29
Q.6	Médio	ENISA	29
Q.7	Médio	ENISA	29
Q.8	Alto	ENISA	29
Q.9	Alto	ENISA	29
R.1	Baixo	ENISA	101
R.2	Baixo	ENISA	101
R.3	Baixo	ENISA	101
R.4	Baixo	ENISA	101
R.5	Baixo	ENISA	121
R.6	Médio	ENISA	121
R.7	Médio	ENISA	121
R.8	Médio	ENISA	121
R.9	Médio	ENISA	121
S.1	Baixo	ENISA	29
S.2	Baixo	ENISA	29
S.3	Médio	ENISA	29
S.4	Médio	ENISA	29
S.5	Alto	ENISA	29
S.6	Alto	ENISA	29
T.1	Baixo	ENISA	121
T.2	Médio	ENISA	121
T.3	Médio	ENISA	121
T.4	Médio	ENISA	121
T.5	Médio	ENISA	121
T.6	Médio	ENISA	121
T.7	Médio	ENISA	121
T.8	Médio	ENISA	121
T.8.1	Baixo	NOVO	29

Anexo 10 – Dataset multas RGPD no Espaço Económico Europeu

Dataset multas RGPD no Espaço Económico Europeu

ID	País	Nome da Autoridade de Controlo	URL da multa	Data da Multa	Valor da Multa (em Euros)	Artigo RGPD	Nome entidade multada	Relação RGPD: Responsável / Subcontratante	Classificação (Público / Privado)	Tipo de organização (Pública; Privada - PME / Grande Empresa)
1	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9556958	25/02/2021	300 000,00 €	(5)(1)(a);(5)(1)(c);(5)(1)(d);(5)(2);(25);(35)	Istituto Nazionale Previdenza Sociale (INPS)	Responsável pelo tratamento	Entidade Pública	Entidade Pública
2	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9565258	25/02/2021	2 000,00 €	(5)(1)(a);(5)(1)(c);(6)(1)(c);(6)(1)(e);(6)(2);(6)(3)	Comune di Conflenti	Responsável pelo tratamento	Entidade Pública	Entidade Pública
3	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9556625	11/02/2021	75 000,00 €	(5)(1)(a);(5)(1)(b);(5)(1)(c);(6)(1)(c);(6)(1)(e);(6)(2);(6)(3);(37)(1);(37)(7)	Ministero dello Sviluppo Economico	Responsável pelo tratamento	Entidade Pública	Entidade Pública
4	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9544504	27/01/2021	50 000,00 €	(5)(1)(a);(5)(1)(d);(5)(1)(f);(9);(32)(1)(b)	Autoridade Sanitária Local da Romagna	Responsável pelo tratamento	Entidade Pública	Entidade Pública
5	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9544457	27/01/2021	10 000,00 €	(5)(1)(f);(9)	Hospital Universitário de Siena	Responsável pelo tratamento	Entidade Pública	Entidade Pública
6	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9544092	27/01/2021	10 000,00 €	(5)(1)(f);(9)	Hospital Universitário de Parma	Responsável pelo tratamento	Entidade Pública	Entidade Pública
7	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9538748	14/01/2021	8 000,00 €	(5)(1)(f);(32)	Agência Regional de Proteção Ambiental da Campania (ARPAC)	Responsável pelo tratamento	Entidade Pública	Entidade Pública
8	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9542071	14/01/2021	30 000,00 €	(5)(1)(a);(6);(9)	Azienda sanitaria provinciale di Enna	Responsável pelo tratamento	Entidade Pública	Entidade Pública
9	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9542096	14/01/2021	2 000,00 €	(12)(3);(15)	Poliambulatorio Talenti Srl	Responsável pelo tratamento	Entidade Privada	PME
10	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9542155	14/01/2021	18 000,00 €	(5)(1)(f);(9)	Unidade Local de Saúde de Bolonha	Responsável pelo tratamento	Entidade Pública	Entidade Pública
11	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9524175	17/12/2020	500 000,00 €	(5);(13);(14);(28);(32)	Município de Roma	Responsável pelo tratamento	Entidade Pública	Entidade Pública

12	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9525315	17/12/2020	40 000,00 €	(5)(1)(a);(5)(1)(e);(6);(9);(28)	Miropass Srl	Responsável pelo tratamento	Entidade Privada	PME
13	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9529527	17/12/2020	100 000,00 €	(5)(1)(f);(13);(14);(28);(30);(32);(35)	Unidade Local de Saúde da Toscana Sudeste	Responsável pelo tratamento	Entidade Pública	Entidade Pública
14	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9533587	26/11/2020	3 000,00 €	(5)(1)(a);(13)	Charly Mike srl	Responsável pelo tratamento	Entidade Privada	PME
15	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9509558	26/11/2020	10 000,00 €	(5)(1)(a)	RTI - Reti Televisive Italiane Spa	Responsável pelo tratamento	Entidade Privada	Grande
16	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9509515	26/11/2020	20 000,00 €	(5)(1)(a);(5)(1)(c);(6)(1)(b);(6)(1)(c);(9)(1)(b)	Concentrix Cvg Italy srl	Responsável pelo tratamento	Entidade Privada	PME
17	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9474649	09/07/2020	20 000,00 €	(5)(1)(a);(13)	Burgo Group SpA	Responsável pelo tratamento	Entidade Privada	Grande
18	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9483375	01/10/2020	30 000,00 €	(5)(1)(a);(5)(1)(c);(9)(1);(9)(2);(9)(4);(37)(7)	Autoridade Provincial de Saúde de Cosenza	Responsável pelo tratamento	Entidade Pública	Entidade Pública
19	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9486531	15/10/2020	2 000,00 €	(12)(1);(12)(3);(12)(4)	Município de Collegno	Responsável pelo tratamento	Entidade Pública	Entidade Pública
20	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9485681	12/11/2020	12 251 601,00 €	(5)(1);(5)(2);(6)(1);(7);(15)(1);(16);(21);(24);(25)(1);(32);(33)(1)	Vodafone Italia SpA	Responsável pelo tratamento	Entidade Privada	Grande
21	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9518890	29/10/2020	20 000,00 €	(5)(1)(a);(5)(1)(c);(5)(1)(e);(12);(13);(88)	Gaypa srl	Responsável pelo tratamento	Entidade Privada	PME
22	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9518849	29/10/2020	4 000,00 €	(5)(1)(a);(13);(88)	Borgo Fonte Scura srl	Responsável pelo tratamento	Entidade Privada	PME
23	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9469345	01/10/2020	20 000,00 €	(5)(1)(a);(5)(1)(f);(9)	Università Campus Bio-medico di Roma (Policlínica)	Responsável pelo tratamento	Entidade Privada	PME
24	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9461168	17/09/2020	80 000,00 €	(5)(1)(a);(6)(1)(c);(6)(1)(e);(13);(28);(32)	Azienda Ospedaliera di Rilievo Nazionale 'Antonio Cardarelli' (Hospital Privado)	Responsável pelo tratamento	Entidade Privada	PME
25	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9461321	17/09/2020	60 000,00 €	(5)(1)(a);(6);(9);(32)	Scanshare srl	Subcontratante	Entidade Privada	PME
26	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9451734	09/07/2020	2 000,00 €	(5)(1)(a);(5)(1)(c);(6)(1)(c);(6)(1)(e);(6)(2);(6)(3)(b);(9)(1);(9)(2);(9)(4)	Instituto Estatal de Integração "Crucoli Torretta" de Crucoli	Responsável pelo tratamento	Entidade Pública	Entidade Pública
27	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9468523	03/09/2020	2 000,00 €	(5)(1)(a);(5)(1)(c);(6)(1)(c);(6)(1)(e);(6)(2);(6)(3)(b)	Município de Casaloldo	Responsável pelo tratamento	Entidade Pública	Entidade Pública
28	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9446730	26/03/2020	10 000,00 €	(5);(6);(13);(32)	Cavauto SRL	Responsável pelo tratamento	Entidade Privada	PME

29	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9446659	09/07/2020	2 000,00 €	(5)(1)(a);(5)(1)(c);(6)(1)(c);(6)(1)(e);(6)(2);(6)(3)(b)	Município de Baronissi	Responsável pelo tratamento	Entidade Pública	Entidade Pública
30	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445710	02/07/2020	3 000,00 €	(12);(15)	GTL SRL	Responsável pelo tratamento	Entidade Privada	PME
31	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445324	02/07/2020	2 000,00 €	(5)(1)(a);(5)(1)(c);(6)(1)(c);(6)(1)(e)	Istituto Comprensivo di Uggiano La Chiesa	Responsável pelo tratamento	Entidade Privada	PME
32	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445180	02/07/2020	15 000,00 €	(5)(1)(a);(5)(1)(c);(5)(1)(e);(12);(13);(15)	Mapei SpA	Responsável pelo tratamento	Entidade Privada	Grande
33	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445550	02/07/2020	5 000,00 €	(15)	Instituto Nacional de Segurança Social - Departamento da Província de Brescia	Responsável pelo tratamento	Entidade Pública	Entidade Pública
34	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445567	02/07/2020	1 000,00 €	(5)(1)(a);(5)(1)(c);(6)	Supermercado TB srl	Responsável pelo tratamento	Entidade Privada	PME
35	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9440000	02/07/2020	2 000,00 €	(6)(1)(c);(6)(1)(e);(6)(2);(6)(3)(b)	Município de Manduria	Responsável pelo tratamento	Entidade Pública	Entidade Pública
36	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9361186	05/03/2020	3 000,00 €	(5)(1)(c);(6)(1)(c);(6)(1)(e);(6)(2);(6)(3)(b)	Comunidade de San Giorgio Jonico	Responsável pelo tratamento	Entidade Pública	Entidade Pública
37	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9440075	02/07/2020	4 000,00 €	(5)(1)(a);(5)(1)(c);(6)(1)(c);(6)(1)(e);(6)(2);(6)(3)(b)	Região da Campânia	Responsável pelo tratamento	Entidade Pública	Entidade Pública
38	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9435774	09/07/2020	200 000,00 €	(5)(1);(5)(2);(6);(7);(28);(29)	Merlini srl	Subcontratante	Entidade Privada	PME
39	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9435753	09/07/2020	16 729 600,00 €	(5)(1);(5)(1)(d);(5)(2);(6)(1)(a);(7);(12)(1);(12)(2);(24);(24)(1);(25);(25)(1)	Wind Tre SpA	Responsável pelo tratamento	Entidade Privada	Grande
40	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9435807	09/07/2020	800 000,00 €	(5)(1)(a);(25)	Iliad Italia SpA	Responsável pelo tratamento	Entidade Privada	Grande
41	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445180	02/07/2020	15 000,00 €	(5)(1)(a);(5)(1)(c);(5)(1)(e);(12);(13);(15)	Mapei SpA	Responsável pelo tratamento	Entidade Privada	Grande
42	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9283029	06/02/2020	4 000,00 €	(5)(1)(a);(5)(1)(c);(6)(1)(c);(6)(1)(e);(6)(2);(6)(3)(b);(9)(1);(9)(2);(9)(4)	Liceo Artistico Statale di Napoli	Responsável pelo tratamento	Entidade Pública	Entidade Pública
43	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9283014	30/01/2020	4 000,00 €	(5)(1)(a);(5)(1)(c);(6)(1)(c);(6)(1)(e);(6)(2);(6)(3)(b);(9)(1);(9)(2);(9)(4)	Liceo Scientifico Nobel di Torre del Greco	Responsável pelo tratamento	Entidade Pública	Entidade Pública
44	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9361186	05/03/2020	3 000,00 €	(5)(1)(c);(6)(1)(c);(6)(1)(e);(6)(2);(6)(3)(b)	Município de San Giorgio Jonico	Responsável pelo tratamento	Entidade Pública	Entidade Pública
45	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9285411	13/02/2020	4 000,00 €	(5)(1)(a);(5)(1)(c);(6)(1)(c);(6)(1)(e);(6)(2);(6)(3)(b)	Município de Urago d'Oglio	Responsável pelo tratamento	Entidade Pública	Entidade Pública

46	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9283121	06/02/2020	20 000,00 €	(5)(1)(a)	RTI - Spa Reti Televisive Italiane	Responsável pelo tratamento	Entidade Privada	Grande
47	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9302897	30/01/2020	4 000,00 €	(5)(1)(a);(5)(1)(c);(6)(1)(c);(6)(1)(e);(6)(2);(6)(3)(b)	Município de Colledara	Responsável pelo tratamento	Entidade Pública	Entidade Pública
48	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9269629	23/01/2020	30 000,00 €	(5)(1)(f)	Hospital Universitário Integrado de Verona	Responsável pelo tratamento	Entidade Privada	Grande
49	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9269618	23/01/2020	30 000,00 €	(32)	Sapienza Università di Roma	Responsável pelo tratamento	Entidade Pública	Entidade Pública
50	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9256486	15/01/2021	27 802 946,00 €	(5)(1)(d);(5)(1)(f);(5)(2);(24)(1);(24)(2);(25)(1);(32)(1);(33)(1)	TIM	Responsável pelo tratamento	Entidade Privada	Grande
51	Itália	Garante per la protezione dei dati personali	https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9261227	15/01/2021	10 000,00 €	(5)(1)(c);(9)(1);(9)(2);(9)(4)	Município de Francavilla Fontana	Responsável pelo tratamento	Entidade Pública	Entidade Pública
52	Itália	Garante per la protezione dei dati personali	https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9244365	11/12/2019	8 500 000,00 €	(5)(1)(a);(5)(1)(c);(5)(1)(e);(5)(2);(6)(1)(a);(7)(1);(25)	Eni Gas e Luce	Responsável pelo tratamento	Entidade Privada	Grande
53	Itália	Garante per la protezione dei dati personali	https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9244358	11/12/2019	3 000 000,00 €	(5)(1)(f);(32)	Eni Gas e Luce	Responsável pelo tratamento	Entidade Privada	Grande
54	Itália	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9101974	04/04/2019	50 000,00 €	(32)	Movimento 5 Stelle	Responsável pelo tratamento	Entidade Privada	PME
55	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/2020-12-14-beslut-tillsyn-uppsalahem.pdf	14/12/2021	29 500,00 €	(6)(1)(f)	Uppsalahem AB	Responsável pelo tratamento	Entidade Privada	PME
56	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/2020-12-10-beslut-tillsyn-umea-universitet.pdf	10/12/2020	44 000,00 €	(5)(1)(f);(32)(1);(32)(2)	Universidade de Umeå	Responsável pelo tratamento	Entidade Pública	Entidade Pública
57	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/2020-12-10-beslut-tillsyn-umea-universitet.pdf	10/12/2020	10 000,00 €	(33)(1);(33)(5)	Universidade de Umeå	Responsável pelo tratamento	Entidade Pública	Entidade Pública
58	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-aleris-sjukvard-di-2019-3844.pdf	02/12/2020	1 470 000,00 €	(5)(1)(f);(5)(2);(32)(1);(32)(2)	Aleris Sjukvård AB	Responsável pelo tratamento	Entidade Privada	Grande
59	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-aleris-narsjukvard-di-2019-3842.pdf	02/12/2020	1 180 000,00 €	(5)(1)(f);(5)(2);(32)(1);(32)(2)	Aleris Närsjukvård AB	Responsável pelo tratamento	Entidade Privada	Grande
60	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-region-ostergotland-di-2019-3843.pdf	02/12/2020	246 400,00 €	(5)(1)(f);(5)(2);(24)(1);(32)(1);(32)(2)	Região de Östergötland	Responsável pelo tratamento	Entidade Pública	Entidade Pública
61	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-region-vasterbotten-di-2019-3841.pdf	02/12/2020	246 400,00 €	(5)(1)(f);(5)(2);(32)(1);(32)(2)	Conselho de Saúde e Cuidados Médicos na Região Västerbotten	Responsável pelo tratamento	Entidade Pública	Entidade Pública
62	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-	02/12/2020	345 000,00 €	(5)(1)(f);(5)(2);(32)(1);(32)(2)	Hospital Universitário Sahlgrenska	Responsável pelo tratamento	Entidade Pública	Entidade Pública

			sahlgrenska-universitetssjukhuset-di-2019-3840.pdf							
63	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-karolinska-universitetssjukhuset-di-2019-3839.pdf	02/12/2020	394 000,00 €	(5)(1)(f);(5)(2);(32)(1);(32)(2)	Hospital Universitário Karolinska de Solna	Responsável pelo tratamento	Entidade Pública	Entidade Pública
64	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-capio-st-gorans-sjukhus-di-2019-3846.pdf	02/12/2020	2 900 000,00 €	(5)(1)(f);(5)(2);(32)(1);(32)(2)	Hospital de emergência	Responsável pelo tratamento	Entidade Privada	Grande
65	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-gnosjo-2020-11-25.pdf	24/11/2020	19 700,00 €	(5)(1)(a);(6)(1);(9)(2);(13);(35);(36)	Município de Gnosjö - Comité de Assuntos Sociais	Responsável pelo tratamento	Entidade Pública	Entidade Pública
66	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-stockholms-stad.pdf	23/11/2020	394 000,00 €	(5)(1)(f);(32)(1)	Conselho de Educação da cidade de Estocolmo	Responsável pelo tratamento	Entidade Pública	Entidade Pública
67	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/2020-06-16-kamerabevakning-hos-brf.pdf	15/06/2020	1 900,00 €	(5);(6);(13)	BRF Gårdsbjörken em Halmstad	Responsável pelo tratamento	Entidade Privada	PME
68	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-region-orebro-2020-05-11.pdf	11/05/2020	7 900,00 €	(5);(6);(9)	Conselho de Saúde e Cuidados Médicos na Região do Condado de Örebro	Responsável pelo tratamento	Entidade Pública	Entidade Pública
69	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-region-orebro-2020-05-11.pdf	11/05/2020	3 900,00 €	(32)	Conselho de Saúde e Cuidados Médicos na Região do Condado de Örebro	Responsável pelo tratamento	Entidade Pública	Entidade Pública
70	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-ssc-20200428.pdf	28/04/2020	14 700,00 €	(33)(2)	Centro Nacional de Serviços do Governo (NGSC)	Responsável pelo tratamento	Entidade Pública	Entidade Pública
71	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/2020-03-11-beslut-google.pdf	10/03/2020	7 300 000,00 €	(5);(6);(9);(10);(17)	Google LLC	Responsável pelo tratamento	Entidade Privada	Grande
72	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-mrkoll.pdf	13/12/2019	35 000,00 €	(5);(10)	Nusvar AB	Responsável pelo tratamento	Entidade Privada	PME
73	Suécia	Swedish Authority for Privacy Protection	https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf	20/08/2019	19 700,00 €	(5);(9);(35);(36)	Conselho de Educação Secundária do município de Skellefteå	Responsável pelo tratamento	Entidade Pública	Entidade Pública
74	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00295-2020.pdf	23/03/2021	1 000,00 €	(5)(1)(c)	Laboratorio Octogón, SL	Responsável pelo tratamento	Entidade Privada	PME
75	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00483-2020.pdf	18/03/2021	2 000,00 €	(5)(1)(f)	Asesoría Alpi-Clúa SL	Responsável pelo tratamento	Entidade Privada	PME
76	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00483-2020.pdf	18/03/2021	1 000,00 €	(32)(1)	Asesoría Alpi-Clúa SL	Responsável pelo tratamento	Entidade Privada	PME
77	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00484-2020.pdf	16/03/2021	60 000,00 €	(6)(1)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande

78	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00417-2020.pdf	15/03/2021	5 000,00 €	(5)(1)(b)	Certime SA	Responsável pelo tratamento	Entidade Privada	PME
79	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00405-2020.pdf	15/03/2021	3 000,00 €	(6)(1)(a)	Associação cultural	Responsável pelo tratamento	Entidade Privada	PME
80	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00375-2020.pdf	15/03/2021	2 000,00 €	(13)	Heredad de Urueña SA	Responsável pelo tratamento	Entidade Privada	PME
81	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00179-2020.pdf	15/03/2021	500 000,00 €	(32)(1)	Air Europa Lineas Aereas, SA.	Responsável pelo tratamento	Entidade Privada	Grande
82	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00179-2020.pdf	15/03/2021	100 000,00 €	(33)	Air Europa Lineas Aereas, SA.	Responsável pelo tratamento	Entidade Privada	Grande
83	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00193-2020.pdf	12/03/2021	1 500,00 €	(5)(1)(c)	Pessoa privada	Responsável pelo tratamento	Pessoa individual	Pessoa individual
84	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00061-2021.pdf	12/03/2021	12 000,00 €	(6)(1)	Tecnologia NBQ, SAU	Responsável pelo tratamento	Entidade Privada	PME
85	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00059-2020.pdf	11/03/2021	2 000 000,00 €	(21)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
86	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00059-2020.pdf	11/03/2021	2 000 000,00 €	(44)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
87	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00059-2020.pdf	11/03/2021	4 000 000,00 €	(24);(28)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
88	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00074-2020.pdf	10/03/2021	10 000,00 €	(5)(1)(f)	CENTRO DE DIAGNÓSTICO	Responsável pelo tratamento	Entidade Privada	PME
89	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00136-2020.pdf	10/03/2021	4 000,00 €	(13)	Filigrana Comunicación SLU	Responsável pelo tratamento	Entidade Privada	PME
90	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00136-2020.pdf	10/03/2021	2 000,00 €	(14)	Filigrana Comunicación SLU	Responsável pelo tratamento	Entidade Privada	PME
91	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00136-2020.pdf	10/03/2021	2 000,00 €	(6)(1)	Filigrana Comunicación SLU	Responsável pelo tratamento	Entidade Privada	PME
92	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00406-2020.pdf	10/03/2021	50 000,00 €	(6)(1)(f)	Equifax Iberica SL	Responsável pelo tratamento	Entidade Privada	Grande
93	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00448-2020.pdf	10/03/2021	50 000,00 €	(17)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
94	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00448-2020.pdf	10/03/2021	30 000,00 €	(32)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
95	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00448-2020.pdf	10/03/2021	50 000,00 €	(5)(1)(f)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande

96	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00378-2019.pdf	09/03/2021	15 000,00 €	(5)(1)(f)	Associação de Proprietários de Imóveis	Responsável pelo tratamento	Entidade Privada	PME
97	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00279-2020.pdf	02/03/2021	5 000,00 €	(6)	Desconhecido	Responsável pelo tratamento	N/A	N/A
98	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00279-2020.pdf	02/03/2021	4 000,00 €	(13)	Desconhecido	Responsável pelo tratamento	N/A	N/A
99	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00197-2020.pdf	02/03/2021	200 000,00 €	(5)(1)(b);(5)(1)(c);(6)(1)(b)	I-DE Redes Eléctricas Inteligentes, SAU	Responsável pelo tratamento	Entidade Privada	Grande
100	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00502-2020.pdf	24/02/2021	12 000,00 €	(21)	AVILON CENTER 2016, S.L.	Responsável pelo tratamento	Entidade Privada	PME
101	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00268-2020.pdf	16/02/2021	1 000,00 €	(13)	The Washpoint SL	Responsável pelo tratamento	Entidade Privada	PME
102	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00191-2020.pdf	22/02/2021	1 600,00 €	(5)(1)(c)	RIPOBRUNA 2007,S.L	Responsável pelo tratamento	Entidade Privada	PME
103	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00430-2020.pdf	11/02/2021	120 000,00 €	(6)	Vodafone España, SAU	Responsável pelo tratamento	Entidade Privada	Grande
104	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00026-2021.pdf	10/02/2021	24 000,00 €	(28)	Vamavi Phone S.L.	Subcontratante	Entidade Privada	PME
105	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00062-2020.pdf	08/02/2021	5 000,00 €	(13)	Predase Servicios Integrales S.L.	Responsável pelo tratamento	Entidade Privada	PME
106	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00440-2020.pdf	05/02/2021	3 000,00 €	(6)	Patio Ancestral S.L.	Responsável pelo tratamento	Entidade Privada	PME
107	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00253-2020.pdf	08/02/2021	5 000,00 €	(5)(1)(c)	Pessoa individual - senhorio	Responsável pelo tratamento	Pessoa individual	Pessoa individual
108	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00270-2020.pdf	04/02/2021	2 000,00 €	(5)(1)(c)	Pessoa individual - dono estabelecimento	Responsável pelo tratamento	Pessoa individual	Pessoa individual
109	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00220-2020.pdf	02/02/2021	50 000,00 €	(5)(1)(d)	Iberdrola Clientes	Responsável pelo tratamento	Entidade Privada	Grande
110	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00220-2020.pdf	02/02/2021	50 000,00 €	(17)	Iberdrola Clientes	Responsável pelo tratamento	Entidade Privada	Grande
111	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00433-2020.pdf	03/02/2021	24 000,00 €	(58)(2)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
112	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00335-2020.pdf	02/02/2021	3 000,00 €	(5)(1)(f)	IDFINANCE Spain, S.L.	Responsável pelo tratamento	Entidade Privada	Grande
113	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00232-2020.pdf	21/01/2021	50 000,00 €	(6)(1)(b)	Alterna Operador Integral S.L.	Responsável pelo tratamento	Entidade Privada	Grande

114	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00235-2020.pdf	26/01/2021	75 000,00 €	(6)(1)	Telefónica Móviles España, SAU	Responsável pelo tratamento	Entidade Privada	Grande
115	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00215-2020.pdf	20/01/2021	1 200,00 €	(5)(1)(c)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual
116	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00477-2019.pdf	13/01/2021	2 000 000,00 €	(13);(14)	Caixabank S.A.	Responsável pelo tratamento	Entidade Privada	Grande
117	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00477-2019.pdf	13/01/2021	4 000 000,00 €	(6)	Caixabank S.A.	Responsável pelo tratamento	Entidade Privada	Grande
118	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00415-2020.pdf	04/01/2021	54 000,00 €	(5)(1)(d);(5)(1)(f)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
119	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00368-2020.pdf	22/12/2020	6 000,00 €	(21)	Iberdrola Clientes, SAU	Responsável pelo tratamento	Entidade Privada	Grande
120	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00219-2019.pdf	21/12/2020	36 000,00 €	(5)(1)(d)	Banco Bilbao Vizcaya Argentaria, S.A.	Responsável pelo tratamento	Entidade Privada	Grande
121	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00438-2019.pdf	14/12/2020	10 000,00 €	(6)(1)(a);(8);(13)	Pessoa individual	Responsável pelo tratamento	Entidade Privada	PME
122	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00070-2019.pdf	13/01/2021	2 000 000,00 €	(13);(14)	Banco Bilbao Vizcaya Argentaria, S.A.	Responsável pelo tratamento	Entidade Privada	Grande
123	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00070-2019.pdf	13/01/2021	3 000 000,00 €	(6)	Banco Bilbao Vizcaya Argentaria, S.A.	Responsável pelo tratamento	Entidade Privada	Grande
124	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00332-2020.pdf	11/12/2020	4 000,00 €	(7)	Borjamotor, S.A.	Responsável pelo tratamento	Entidade Privada	PME
125	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00262-2020.pdf	09/12/2020	40 000,00 €	(6)(1)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
126	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00324-2020.pdf	09/12/2020	10 000,00 €	(5)(1)(f)	Desconhecido	Responsável pelo tratamento	N/A	N/A
127	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00317-2020.pdf	02/12/2020	2 400,00 €	(13)	Dr Marín Cirugia Plástica, S.L.P.	Responsável pelo tratamento	Entidade Privada	PME
128	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00320-2020.pdf	02/12/2020	6 000,00 €	(6)(1)	Servicio de Alojamientos Responsables, S.L.	Responsável pelo tratamento	Entidade Privada	PME
129	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00287-2020.pdf	02/12/2020	1 000,00 €	(5)(1)(f)	Comercio Online Levante, S.L.	Responsável pelo tratamento	Entidade Privada	PME
130	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00287-2020.pdf	02/12/2020	2 000,00 €	(32)(1)	Comercio Online Levante, S.L.	Responsável pelo tratamento	Entidade Privada	PME
131	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00141-2020.pdf	02/12/2020	5 000,00 €	(6)(1)	Asociación de Víctimas por Arbitrariedades Judiciales (JAVA)	Responsável pelo tratamento	Entidade Privada	PME

132	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00322-2020.pdf	02/12/2020	6 000,00 €	(5)(1)(f)	Losada Advocats S.L.	Responsável pelo tratamento	Entidade Privada	PME
133	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00278-2020.pdf	27/11/2020	1 200,00 €	(5)(1)(a)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual
134	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00416-2019.pdf	25/11/2020	20 000,00 €	(13);(14)	Miraclia Telecomunicaciones S.L.	Responsável pelo tratamento	Entidade Privada	PME
135	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00416-2019.pdf	25/11/2020	20 000,00 €	(6)	Miraclia Telecomunicaciones S.L.	Responsável pelo tratamento	Entidade Privada	PME
136	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00227-2020.pdf	23/11/2020	10 000,00 €	(6)	Recambios Villalegre S.L.	Responsável pelo tratamento	Entidade Privada	PME
137	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00227-2020.pdf	23/11/2020	2 000,00 €	(13)	Recambios Villalegre S.L.	Responsável pelo tratamento	Entidade Privada	PME
138	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00308-2020.pdf	19/11/2020	36 000,00 €	(6)(1)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
139	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00189-2020.pdf	18/11/2020	2 000,00 €	(58)(2)	Anmavas 61, S.L.	Responsável pelo tratamento	Entidade Privada	PME
140	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00353-2019.pdf	16/11/2020	1 600,00 €	(5)(1)(c)	Associação de proprietários	Responsável pelo tratamento	Entidade Privada	PME
141	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00356-2020.pdf	18/11/2020	42 000,00 €	(6)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
142	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00348-2020.pdf	11/11/2020	42 000,00 €	(6)(1)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
143	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00185-2020.pdf	10/11/2020	1 000,00 €	(32)	Miguel Ibáñez Bezanilla, S.L.	Responsável pelo tratamento	Entidade Privada	PME
144	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00185-2020.pdf	10/11/2020	1 000,00 €	(13)	Miguel Ibáñez Bezanilla, S.L.	Responsável pelo tratamento	Entidade Privada	PME
145	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00365-2019.pdf	06/11/2020	20 000,00 €	(31)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
146	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00182-2020.pdf	05/11/2020	75 000,00 €	(6)	Telefónica Móviles España, SAU	Responsável pelo tratamento	Entidade Privada	Grande
147	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00341-2020.pdf	03/11/2020	30 000,00 €	(6)(1)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
148	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00303-2020.pdf	27/10/2020	36 000,00 €	(6)(1)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
149	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00003-2020.pdf	28/10/2020	4 000,00 €	(5)(1)(c)	Play Orenes, S.L.	Responsável pelo tratamento	Entidade Privada	PME

150	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00247-2020.pdf	10/11/2020	4 000,00 €	(13)	Organic Natur 03 S.L.	Responsável pelo tratamento	Entidade Privada	PME
151	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00251-2020.pdf	10/11/2020	50 000,00 €	(37)(1)(b)	Conseguridad SL	Responsável pelo tratamento	Entidade Privada	PME
152	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00035-2020.pdf	09/10/2020	900,00 €	(5)(1)(c)	Café Restaurante B.B.B	Responsável pelo tratamento	Entidade Privada	PME
153	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00312-2019.pdf	09/10/2020	2 000,00 €	(5)(1)(c)	Pessoa individual - senhorio	Responsável pelo tratamento	Pessoa individual	Pessoa individual
154	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00206-2020.pdf	09/10/2020	50 000,00 €	(6)	Centro de Investigación y Estudio para la Obesidad, SL	Responsável pelo tratamento	Entidade Privada	PME
155	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00058-2020.pdf	15/10/2020	5 000,00 €	(5)(1)(f)	Caja Rural San José de Nules S. Cooperativa de Crédito	Responsável pelo tratamento	Entidade Privada	PME
156	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00069-2020.pdf	06/10/2020	60 000,00 €	(6)(1)(a)	Lycamobile	Responsável pelo tratamento	Entidade Privada	Grande
157	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00028-2020.pdf	06/10/2020	4 000,00 €	(6)	Callesgarcia, S.L.	Responsável pelo tratamento	Entidade Privada	PME
158	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00245-2020.pdf	03/11/2020	3 000,00 €	(28)(3)(g)	Avata Hispania, S.L.	Subcontratante	Entidade Privada	Grande
159	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00249-2020.pdf	29/09/2020	3 000,00 €	(5)(1)(b)	Venu Sanz Chef, S.L.	Responsável pelo tratamento	Entidade Privada	PME
160	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00024-2020.pdf	29/09/2020	60 000,00 €	(6)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
161	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00079-2020.pdf	22/09/2020	60 000,00 €	(6)(1)	GLP Instalaciones 86, SL	Responsável pelo tratamento	Entidade Privada	PME
162	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00234-2020.pdf	24/09/2020	3 000,00 €	(13)	Iweb Internet Learning, S.L.	Responsável pelo tratamento	Entidade Privada	PME
163	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00234-2020.pdf	24/09/2020	5 000,00 €	(7)	Iweb Internet Learning, S.L.	Responsável pelo tratamento	Entidade Privada	PME
164	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00186-2020.pdf	01/09/2020	60 000,00 €	(6)(1)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
165	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00311-2019.pdf	16/09/2020	3 000,00 €	(5)(1)(c)	Grupo Carolizan	Responsável pelo tratamento	Entidade Privada	PME
166	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00034-2020.pdf	15/09/2020	10 000,00 €	(5)(1)(f)	Condomínio	Responsável pelo tratamento	Entidade Privada	PME
167	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00051-2020.pdf	10/09/2020	1 500,00 €	(6)(1)(a)	Partido político	Responsável pelo tratamento	Entidade Privada	PME

168	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00188-2020.pdf	07/09/2020	3 000,00 €	(5)(1)(f)	Barcelona Airport Security Guard Association ('AVSAB')	Responsável pelo tratamento	Entidade Privada	PME
169	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00198-2020.pdf	01/09/2020	45 000,00 €	(6)	Telefónica Móviles España, SAU	Responsável pelo tratamento	Entidade Privada	Grande
170	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00076-2020.pdf	28/08/2020	40 000,00 €	(5)(1)(b)	Bankia S.A.	Responsável pelo tratamento	Entidade Privada	Grande
171	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00200-2020.pdf	28/08/2020	3 000,00 €	(6)	Basketball Federation of Castilla and Leon	Responsável pelo tratamento	Entidade Privada	PME
172	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00449-2019.pdf	17/08/2020	5 000,00 €	(5)(1)(b)	Party of the Socialists of Catalonia	Responsável pelo tratamento	Entidade Privada	PME
173	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00092-2020.pdf	06/08/2020	0,00 €	(13)	GROW BEATS SL	Responsável pelo tratamento	Entidade Privada	PME
174	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00036-2020.pdf	06/08/2020	0,00 €	(13)	Just Landed S.L.	Responsável pelo tratamento	Entidade Privada	PME
175	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00479-2019.pdf	05/08/2020	3 000,00 €	(5)(1)(c)	Restaurant	Responsável pelo tratamento	Entidade Privada	PME
176	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00009-2020.pdf	04/08/2020	60 000,00 €	(6)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
177	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00168-2020.pdf	31/07/2020	45 000,00 €	(6)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
178	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00031-2020.pdf	31/07/2020	0,00 €	(21)	Tour & People Max S.L.	Responsável pelo tratamento	Entidade Privada	PME
179	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00422-2019.pdf	24/07/2020	10 000,00 €	(6)	El Periódico de Catalunya, S.L.U.	Responsável pelo tratamento	Entidade Privada	Grande
180	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00114-2019.pdf	23/07/2020	55 000,00 €	(6)(1)	Telefónica Móviles España, SAU	Responsável pelo tratamento	Entidade Privada	Grande
181	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00010-2020.pdf	23/07/2020	70 000,00 €	(6)(1)	Telefónica Móviles España, SAU	Responsável pelo tratamento	Entidade Privada	Grande
182	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00014-2020.pdf	23/07/2020	75 000,00 €	(6)	Telefónica Móviles España, SAU	Responsável pelo tratamento	Entidade Privada	Grande
183	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00115-2020.pdf	23/07/2020	3 000,00 €	(58)(1)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
184	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00134-2020.pdf	23/07/2020	3 000,00 €	(7)	El Real Sporting de Gijón S.A.D.	Responsável pelo tratamento	Entidade Privada	PME
185	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00068-2020.pdf	20/07/2020	18 000,00 €	(6)(1)	Banco Bilbao Vizcaya Argentaria, S.A.	Responsável pelo tratamento	Entidade Privada	Grande

186	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00060-2020.pdf	20/07/2020	24 000,00 €	(58)(2)	IBERIA LÍNEAS AÉREAS DEESPAÑA, SA OPERADORA UNIPERSONAL	Responsável pelo tratamento	Entidade Privada	Grande
187	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00459-2019.pdf	20/07/2020	1 500,00 €	(5)(1)(c)	Comercial Vigobrandy, SL	Responsável pelo tratamento	Entidade Privada	PME
188	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00452-2019.pdf	20/07/2020	80 000,00 €	(6)(1)	Orange Espagne S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
189	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00450-2019.pdf	20/07/2020	70 000,00 €	(5)(1)(f)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
190	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00004-2020.pdf	10/07/2020	900,00 €	(5)(1)(c)	Auto Desguaces Iglesias S.L.	Responsável pelo tratamento	Entidade Privada	PME
191	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00149-2020.pdf	10/07/2020	0,00 €	(58)(2)	Centro Internacional De Crecimiento Laboral Y Profesional S.L.	Responsável pelo tratamento	Entidade Privada	PME
192	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00139-2020.pdf	10/07/2020	9 000,00 €	(5)(1)(d)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
193	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00247-2019.pdf	10/07/2020	5 000,00 €	(32)(4)	Global Business Travel Spain SLU	Responsável pelo tratamento	Entidade Privada	Grande
194	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00135-2020.pdf	10/07/2020	3 000,00 €	(13)	School Fitness Holiday & Franchising S.L.	Responsável pelo tratamento	Entidade Privada	PME
195	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00104-2020.pdf	10/07/2020	33 000,00 €	(5)(1)(f);(32)(1)(b);(32)(1)(c)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
196	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00102-2020.pdf	02/07/2020	24 000,00 €	(5)(1)(f)	Iberdrola Clientes, SAU	Responsável pelo tratamento	Entidade Privada	Grande
197	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00475-2019.pdf	02/07/2020	4 000,00 €	(21)	De Vere Spain S.L.	Responsável pelo tratamento	Entidade Privada	Grande
198	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00122-2020.pdf	02/07/2020	3 600,00 €	(33);(34)	Saunier-Tec Mantenimientos de Calor y Frio, SL.	Responsável pelo tratamento	Entidade Privada	PME
199	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00090-2020.pdf	02/07/2020	3 000,00 €	(58)(1)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
200	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Noticias-Judiciales/El-Tribunal-Supremo-confirma-la-multa-de-7-500-euros-a-una-empresa-de-bromas-telefonicas-por-infraccion-de-la-ley-de-Proteccion-Datos	23/06/2020	7 500,00 €	(5);(6)	Miraclia Telecomunicaciones S.L.	Responsável pelo tratamento	Entidade Privada	PME
201	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00273-2019.pdf	19/06/2020	2 000,00 €	(5)(1)(c)	Comunidad de propietarios demelza beach	Responsável pelo tratamento	Entidade Privada	PME

202	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00379-2019.pdf	15/06/2020	3 600,00 €	(6)(1)(a)	Desconhecido	Responsável pelo tratamento	Entidade Privada	PME
203	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00306-2019.pdf	15/06/2020	2 000,00 €	(5)(1)(c)	Café Bar	Responsável pelo tratamento	Entidade Privada	PME
204	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00415-2019.pdf	15/06/2020	75 000,00 €	(6)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
205	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00434-2019.pdf	08/06/2020	5 000,00 €	(6)	Consulting de Seguridad e Investigacion Mira Dp Madrid S.L.	Responsável pelo tratamento	Entidade Privada	PME
206	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00433-2019.pdf	09/06/2020	540,00 €	(12)	Chenming Ye (Bazar Real)	Responsável pelo tratamento	Entidade Privada	PME
207	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00373-2019.pdf	09/06/2020	1 000,00 €	(5)(1)(c);(13)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual
208	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00451-2019.pdf	09/06/2020	75 000,00 €	(6)(1)(f)	Equifax Iberica, S.L.	Responsável pelo tratamento	Entidade Privada	Grande
209	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00033-2020.pdf	09/06/2020	39 000,00 €	(5)(1)(f)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
210	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00417-2019.pdf	09/06/2020	25 000,00 €	(37)	Glovoapp23	Responsável pelo tratamento	Entidade Privada	Grande
211	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00453-2019.pdf	09/06/2020	40 000,00 €	(6)(1)	Telefónica Móviles España, SAU	Responsável pelo tratamento	Entidade Privada	Grande
212	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00048-2020.pdf	09/06/2020	0,00 €	(13)	Salad Market S.L.	Responsável pelo tratamento	Entidade Privada	PME
213	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00390-2019.pdf	09/06/2020	2 000,00 €	(32)	Advogado	Responsável pelo tratamento	Entidade Privada	PME
214	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00359-2019.pdf	09/06/2020	2 000,00 €	(5)(1)(c)	Pessoa individual - proprietário	Responsável pelo tratamento	Pessoa individual	Pessoa individual
215	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00444-2019.pdf	04/06/2020	4 000,00 €	(58)(1)	Iberdrola Clientes, SAU	Responsável pelo tratamento	Entidade Privada	Grande
216	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00436-2019.pdf	25/03/2020	5 000,00 €	(58)(1)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
217	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00008-2020.pdf	19/03/2020	6 000,00 €	(6)(1)	Oliveros Ustrell, S.L.	Responsável pelo tratamento	Entidade Privada	PME
218	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00351-2019.pdf	18/03/2020	30 000,00 €	(58)(2)	Telefónica Móviles España, SAU	Responsável pelo tratamento	Entidade Privada	Grande

219	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00425-2019.pdf	16/03/2020	5 000,00 €	(5)(1)(f)	Centro De Estudio Dirigidos Delta, S.L.	Responsável pelo tratamento	Entidade Privada	PME
220	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00335-2019.pdf	16/03/2020	4 000,00 €	(6)(1)(a)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual
221	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00317-2019.pdf	17/03/2020	3 600,00 €	(5)(1)(c)	Amalfi Servicios de Restauracion S.L.	Responsável pelo tratamento	Entidade Privada	PME
222	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00272-2019.pdf	12/03/2020	2 000,00 €	(5)(1)(c)	Comunidade de proprietários	Responsável pelo tratamento	Entidade Privada	PME
223	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00358-2019.pdf	09/03/2020	15 000,00 €	(5)(1)(f)	Gesthotel Activos Balagares	Responsável pelo tratamento	Entidade Privada	PME
224	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00293-2019.pdf	06/03/2020	4 000,00 €	(5)(1)(c)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual
225	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00360-2019.pdf	06/03/2020	2 400,00 €	(5)(1)(f)	Bazar Susana	Responsável pelo tratamento	Entidade Privada	PME
226	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00429-2019.pdf	04/03/2020	60 000,00 €	(6)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
227	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00469-2019.pdf	03/03/2020	1 800,00 €	(13)	Solo Embrague	Responsável pelo tratamento	Entidade Privada	PME
228	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00474-2019.pdf	03/03/2020	42 000,00 €	(5)(1)(f)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
229	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00421-2019.pdf	03/03/2020	40 000,00 €	(6)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
230	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00426-2019.pdf	03/03/2020	24 000,00 €	(6)(1)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
231	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00212-2019.pdf	28/02/2020	48 000,00 €	(32)	Vodafone ONO, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
232	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00455-2019.pdf	28/02/2020	3 600,00 €	(5)(1)(f)	AEMA Hispánica	Responsável pelo tratamento	Entidade Privada	PME
233	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00235-2019.pdf	27/02/2020	120 000,00 €	(5)(1)(a);(6)(1)(a)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
234	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00187-2019.pdf	25/02/2020	48 000,00 €	(5)(1)(a)	HM HOSPITALES 1989 SA.	Responsável pelo tratamento	Entidade Privada	Grande
235	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00369-2019.pdf	25/02/2020	6 000,00 €	(5)(1)(c)	Casa Gracio Operation	Responsável pelo tratamento	Entidade Privada	PME
236	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00423-2019.pdf	18/02/2020	1 500,00 €	(13)	MYMOVILES EUROPA 2000, SL	Responsável pelo tratamento	Entidade Privada	PME

237	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00298-2019.pdf	14/02/2020	2 500,00 €	(5)(1)(f)	Grupo Valsor Y Losan, S.L.	Responsável pelo tratamento	Entidade Privada	PME
238	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00466-2019.pdf	14/02/2020	3 000,00 €	(6)(1)(a)	Colegio Arenales Carabanchel	Responsável pelo tratamento	Entidade Privada	PME
239	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00181-2019.pdf	23/03/2020	80 000,00 €	(6)	Iberdrola Clientes, SAU	Responsável pelo tratamento	Entidade Privada	Grande
240	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00471-2019.pdf	14/02/2020	42 000,00 €	(5)(1)(f)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
241	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00385-2019.pdf	14/02/2020	30 000,00 €	(5)(1)(f)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
242	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00427-2018.pdf	04/02/2020	1 500,00 €	(5)(1)(c)	Cafetería Nagasaki	Responsável pelo tratamento	Entidade Privada	PME
243	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00227-2019.pdf	04/02/2020	60 000,00 €	(6)(1)(a)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
244	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00270-2019.pdf	03/02/2020	75 000,00 €	(6)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
245	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00405-2019.pdf	03/02/2020	60 000,00 €	(6)(1)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
246	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00275-2019.pdf	03/02/2020	50 000,00 €	(5)(1)(f)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
247	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00402-2019.pdf	03/02/2020	20 000,00 €	(6)(1)	IBERIA LÍNEAS AÉREAS DEESPAÑA, SA OPERADORA UNIPERSONAL	Responsável pelo tratamento	Entidade Privada	Grande
248	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00278-2019.pdf	03/02/2020	75 000,00 €	(6)(1)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
249	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00400-2019.pdf	03/02/2020	0,00 €	(57)	Banco Bilbao Vizcaya Argentaria, S.A.	Responsável pelo tratamento	Entidade Privada	Grande
250	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00259-2019.pdf	03/02/2020	5 000,00 €	(6)(1)	Queseria Artesenal Ameco S.L.	Responsável pelo tratamento	Entidade Privada	PME
251	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00292-2019.pdf	04/02/2020	800,00 €	(6)(1)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual
252	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00397-2019.pdf	03/02/2020	3 600,00 €	(5)(1)(c)	Zhang Bordeta 2006, S.L. (Store and Restaurant)	Responsável pelo tratamento	Entidade Privada	PME
253	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00445-2019.pdf	09/01/2020	3 000,00 €	(58)(1)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande

254	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00093-2019.pdf	07/01/2020	44 000,00 €	(5)(1)(f)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
255	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00109-2019.pdf	14/01/2020	75 000,00 €	(6)(1)	EDP España S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
256	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00025-2019.pdf	09/12/2020	75 000,00 €	(6)(1)	EDP Comercializadora, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
257	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00231-2019.pdf	07/01/2020	10 000,00 €	(6)(1)(a)	Asociación de Médicos Demócratas	Responsável pelo tratamento	Entidade Privada	PME
258	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00279-2019.pdf	18/12/2019	1 600,00 €	(5)(1)(c)	Megastar SL	Responsável pelo tratamento	Entidade Privada	PME
259	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00320-2019.pdf	18/12/2019	5 000,00 €	(5)(1)(f)	Shop Macoyn, S.L.	Responsável pelo tratamento	Entidade Privada	PME
260	Espanha	Agencia Española de Protección de Datos (AEPD)	https://egida.es/wp-content/uploads/2019/12/ps-00265-2019-1.pdf	13/12/2019	1 500,00 €	(13)	Cerrajeria Verin S.L.	Responsável pelo tratamento	Entidade Privada	PME
261	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00250-2019.pdf	16/12/2019	0,00 €	(6)	Linea Directa Aseguradora	Responsável pelo tratamento	Entidade Privada	Grande
262	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00140-2019.pdf	04/12/2019	75 000,00 €	(6)(1)(a)	CURENERGIA COMERCIALIZADORA DE ULTIMO RECURSO, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
263	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00233-2019.pdf	21/11/2019	60 000,00 €	(6)	ViaAqua Gestión Integral Aguas de Galicia	Responsável pelo tratamento	Entidade Privada	PME
264	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00305-2019.pdf	19/11/2019	60 000,00 €	(32)	Corporación radiotelevisión espanola	Responsável pelo tratamento	Entidade Privada	Grande
265	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00237-2019.pdf	25/11/2019	60 000,00 €	(32)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
266	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00236-2019.pdf	04/12/2019	6 000,00 €	(5)(1)(c)	MALONEY'S SPORT BAR S. L.	Responsável pelo tratamento	Entidade Privada	PME
267	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00251-2019.pdf	22/11/2019	30 000,00 €	(5)	Telefónica Móviles España, SAU	Responsável pelo tratamento	Entidade Privada	Grande
268	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00174-2019.pdf	15/11/2019	3 000,00 €	(5)(1)(f)	CONFEDERACION GENERAL DEL TRABAJO	Responsável pelo tratamento	Entidade Privada	PME
269	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00268-2019.pdf	11/11/2019	900,00 €	(13)	TODOTECNICOS24H S.L.	Responsável pelo tratamento	Entidade Privada	PME
270	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00266-2019.pdf	08/11/2019	900,00 €	(13)	CERRAJERO ONLINE S.L.	Responsável pelo tratamento	Entidade Privada	PME

271	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/td-00140-2020.pdf	28/12/2020	60 000,00 €	(6)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
272	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00291-2019.pdf	08/11/2019	6 000,00 €	(6)	JOKER PREMIUM INVEX, S.L.	Responsável pelo tratamento	Entidade Privada	PME
273	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00301-2019.pdf	04/11/2019	36 000,00 €	(5);(6)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
274	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00249-2019.pdf	04/11/2019	60 000,00 €	(5)(1)(f)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
275	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00262-2018.pdf	14/01/2019	0,00 €	(58)(2)	Xfera Moviles S.A.	Responsável pelo tratamento	Entidade Privada	Grande
276	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00304-2019.pdf	21/10/2019	8 000,00 €	(31)	Iberdrola Clientes, SAU	Responsável pelo tratamento	Entidade Privada	Grande
277	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00300-2019.pdf	10/10/2019	30 000,00 €	(5);(6)	VUELING AIRLINES, S.L.	Responsável pelo tratamento	Entidade Privada	Grande
278	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00159-2019.pdf	03/10/2019	60 000,00 €	(6)	Avon Cosmetics Sa	Responsável pelo tratamento	Entidade Privada	Grande
279	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00326-2018.pdf	20/08/2019	250 000,00 €	(5)(1)(a)	LIGA NACIONAL DE FÚTBOL PROFESIONAL	Responsável pelo tratamento	Entidade Privada	Grande
280	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00087-2019.pdf	03/07/2019	21 000,00 €	(6)(1)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
281	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00092-2019.pdf	22/05/2019	36 000,00 €	(5)(1)(f)	Vodafone ONO, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
282	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00212-2019.pdf	28/02/2019	48 000,00 €	(32)	Vodafone ONO, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
283	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00173-2019.pdf	22/08/2019	48 000,00 €	(5)(1)(a)	Telefónica Móviles España, SAU	Responsável pelo tratamento	Entidade Privada	Grande
284	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00205-2019.pdf	31/07/2019	30 000,00 €	(5)(1)(f);(32)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
285	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00064-2019.pdf	03/07/2019	40 000,00 €	(6)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
286	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00150-2019.pdf	08/08/2019	20 000,00 €	(5)(1)(c)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual
287	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00050-2019.pdf	19/08/2019	9 000,00 €	(5)(1)(c)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual
288	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00135-2019.pdf	10/07/2019	3 600,00 €	(5)(1)(c)	AMADOR RECREATIVOS, S.L	Responsável pelo tratamento	Entidade Privada	PME

289	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00331-2018.pdf	28/03/2019	5 000,00 €	(5)(1)(d)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
290	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00121-2019.pdf	10/06/2019	60 000,00 €	(5)(1)(f)	GESTIÓN DE COBROS, YO COBRO SL	Responsável pelo tratamento	Entidade Privada	PME
291	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00411-2018.pdf	28/03/2019	27 000,00 €	(5)(1)(d)	Vodafone España, S.A.U.	Responsável pelo tratamento	Entidade Privada	Grande
292	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00074-2019.pdf	22/05/2019	60 000,00 €	(5)(1)(f)	ENDESA	Responsável pelo tratamento	Entidade Privada	Grande
293	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/documento/ps-00401-2018.pdf	02/09/2019	9 600,00 €	(5)(1)(a);(6)	SANTI 3000, S.L.	Responsável pelo tratamento	Entidade Privada	PME
294	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00188-2019.pdf	08/09/2019	12 000,00 €	(5)(1)(f)	Madrileña Red de Gas	Responsável pelo tratamento	Entidade Privada	Grande
295	Espanha	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/es/documento/ps-00127-2019.pdf	02/12/2019	0,00 €	(58)(2)	IKEA IBERICA, S.A.U	Responsável pelo tratamento	Entidade Privada	Grande
296	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.baden-wuerttemberg.datenschutz.de/vfb-stuttgart-bussgeld-erlassen/	10/03/2021	300 000,00 €	(5)(2)	VfB Stuttgart 1893 AG	Responsável pelo tratamento	Entidade Privada	Grande
297	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://twitter.com/EinRobert1/status/1367163781508440066	03/03/2021	200,00 €	(5);(32)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual
298	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.deutsche-wohnen.com/fileadmin/user_upload/21-02-23_PM_Landgericht_Berlin_stellt_Bussgeldverfahren_gegen_Deutsche_Wohnen_ein.pdf	23/02/2021	0,00 €	(32)	Deutsche Wohnen SE	Responsável pelo tratamento	Entidade Privada	Grande
299	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-verhangt-bussgeld-uber-10-4-millionen-euro-gegen-notebooksbilliger-de-196019.html	01/08/2021	10 400 000,00 €	(5);(6)	notebooksbilliger.de	Responsável pelo tratamento	Entidade Privada	Grande
300	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.lg-bonn.nrw.de/behoerde/presse/zt_archiv_060/Archiv-2020/Pressemitteilung27-2020-vom-11_11_2020-Bussgeld-gegen-Telekommunikationsd___.pdf	11/11/2020	900 000,00 €	(32)(1)	1 & 1 Telecom GmbH	Responsável pelo tratamento	Entidade Privada	Grande
301	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren	01/10/2020	35 258 708,00 €	(5);(6)	H&M Hennes & Mauritz Online Shop AB & Co. KG	Responsável pelo tratamento	Entidade Privada	Grande
302	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-bussgeld-gegen-aok-baden-wuerttemberg-wirksamer-datenschutz-erfordert-regelmaessige-kontrolle-und-anpassung/	30/06/2020	1 240 000,00 €	(32)	Allgemeine Ortskrankenkasse	Responsável pelo tratamento	Entidade Privada	Grande

303	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/30_BfDIverh%C3%A4ngtGeldbu%C3%9Fe1u1.html	09/12/2019	10 000,00 €	(37)	Rapidata GmbH	Responsável pelo tratamento	Entidade Privada	PME
304	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/geldbusse-gegen-krankenhaus-aufgrund-von-datenschutz-defiziten-beim-patientenmanagement/	03/12/2019	105 000,00 €	(32)	Clínica da Universidade de Mainz	Responsável pelo tratamento	Entidade Pública	Entidade Pública
305	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf	05/11/2019	17 000,00 €	(5);(25)(1)	Deutsche Wohnen SE	Responsável pelo tratamento	Entidade Privada	Grande
306	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/01/35.-T%C3%A4tigkeitsbericht-f%C3%BCr-den-Datenschutz-Web.pdf#page=44&zoom=100,0,0	24/10/2019	100 000,00 €	(5);(32)	Empresa de alimentos	Responsável pelo tratamento	Entidade Privada	Grande
307	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20190919-PM-Bussgelder.pdf	19/09/2019	195 407,00 €	(15);(17);(21)	Delivery Hero Germany GmbH	Responsável pelo tratamento	Entidade Privada	Grande
308	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://lfd.niedersachsen.de/download/158404	05/08/2019	200,00 €	(5);(6)	Pessoa privada	Responsável pelo tratamento	Pessoa individual	Pessoa individual
309	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-erstes-bussgeld-gegen-polizeibeamten/	09/05/2019	1 400,00 €	(6)	Polícia	Responsável pelo tratamento	Entidade Pública	Entidade Pública
310	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/01/35.-T%C3%A4tigkeitsbericht-f%C3%BCr-den-Datenschutz-Web.pdf#page=44&zoom=100,0,0	12/04/2019	80 000,00 €	(5)(1)(f)	Empresa do setor financeiro	Responsável pelo tratamento	Entidade Privada	Grande
311	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20190919-PM-Bussgelder.pdf	01/03/2019	50 000,00 €	(6)	N26	Responsável pelo tratamento	Entidade Privada	Grande
312	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20190919-PM-Bussgelder.pdf	05/02/2019	2 500,00 €	(5);(6)	Pessoa privada	Responsável pelo tratamento	Pessoa individual	Pessoa individual
313	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/07/PM-Datenschutzverletzungen-bereiten-zunehmend-Sorge-30.07.2019.pdf	12/04/2019	80 000,00 €	(32)	Desconhecido	Responsável pelo tratamento	N/A	N/A
314	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Taetigkeitsberichte/lfdmvtb14.pdf	01/09/2018	800,00 €	(6)	Polícia	Responsável pelo tratamento	Entidade Pública	Entidade Pública

315	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20190919-PM-Bussgelder.pdf	01/06/2019	294 000,00 €	(5)	Desconhecido	Responsável pelo tratamento	N/A	N/A
316	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf	01/03/2019	51 000,00 €	(37)(7)	Facebook Germany GmbH	Responsável pelo tratamento	Entidade Privada	Grande
317	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf	06/07/2018	20 000,00 €	(33);(34)	Hamburger Verkehrsverbund GmbH (HVV GmbH)	Responsável pelo tratamento	Entidade Privada	Grande
318	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf	01/06/2019	0,00 €	(21)	Hamburger Volksbank eG	Responsável pelo tratamento	Entidade Privada	Grande
319	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/tberichte/tb28_2019.pdf	01/06/2019	2 000,00 €	(6)(1)(f)	Restaurante	Responsável pelo tratamento	Entidade Privada	PME
320	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.lda.brandenburg.de/sixcms/media.php/9/TB_2019_Web.pdf	01/06/2019	50 000,00 €	(12);(28)(9)	Empresa Desconhecida	Responsável pelo tratamento	Entidade Privada	N/A
321	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://kolibri-image.com/causa-datenschutz/	17/12/2018	0,00 €	(28)(3)	Kolibri Image Regina und Dirk Maass GbR	Responsável pelo tratamento	Entidade Privada	PME
322	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/	21/11/2018	20 000,00 €	(32)(1)(a)	Desconhecido	Responsável pelo tratamento	Entidade Privada	N/A
323	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://datenschutz-hamburg.de/assets/pdf/27._Taetigkeitsbericht_Datenschutz_2018_HmbBfDI.pdf	10/07/1905	20 000,00 €	(33)(1);(34)(1)	Desconhecido	Responsável pelo tratamento	N/A	N/A
324	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://datenschutz-hamburg.de/assets/pdf/27._Taetigkeitsbericht_Datenschutz_2018_HmbBfDI.pdf	10/07/1905	5 000,00 €	(28)(3)	Desconhecido	Responsável pelo tratamento	N/A	N/A
325	Alemanha	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	https://indd.adobe.com/view/d639298c-3165-4e30-85d8-0730de2a3598	10/07/1905	118,00 €	(6)	Desconhecido	Responsável pelo tratamento	N/A	N/A
326	Portugal	Comissão Nacional de Proteção de Dados - CNPD	https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121677	25/03/2019	2 000,00 €	(13)(1);(13)(2)	Desconhecido	Responsável pelo tratamento	N/A	N/A
327	Portugal	Comissão Nacional de Proteção de Dados - CNPD	https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121679	19/03/2019	2 000,00 €	(13)(1);(13)(2)	Desconhecido	Responsável pelo tratamento	N/A	N/A
328	Portugal	Comissão Nacional de Proteção de Dados - CNPD	https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121678	05/02/2019	20 000,00 €	(15)(1)	Desconhecido	Responsável pelo tratamento	N/A	N/A
329	Portugal	Comissão Nacional de Proteção de Dados - CNPD	https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121680	09/10/2018	150 000,00 €	(5)(1)(c)	Hospital Público	Responsável pelo tratamento	Entidade Pública	Entidade Pública

330	Portugal	Comissão Nacional de Proteção de Dados - CNPD	https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121680	09/10/2018	150 000,00 €	(5)(1)(f)	Hospital Público	Responsável pelo tratamento	Entidade Pública	Entidade Pública
331	Portugal	Comissão Nacional de Proteção de Dados - CNPD	https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121680	09/10/2018	100 000,00 €	(32)(1)(b);(32)(1)(d)	Hospital Público	Responsável pelo tratamento	Entidade Pública	Entidade Pública
332	Reino Unido	Information Commissioner's Office (ICO)	https://ico.org.uk/media/action-weve-taken/2618609/ticketmaster-uk-limited-mpn.pdf	13/11/2020	1 405 000,00 €	(5)(1)(f);(32)	Ticketmaster UK Limited	Responsável pelo tratamento	Entidade Privada	Grande
333	Reino Unido	Information Commissioner's Office (ICO)	https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf	30/10/2020	20 450 000,00 €	(5)(1)(f);(32)	Marriott International, Inc	Responsável pelo tratamento	Entidade Privada	Grande
334	Reino Unido	Information Commissioner's Office (ICO)	https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf	16/10/2020	22 046 000,00 €	(5)(1)(f);(32)	British Airways	Responsável pelo tratamento	Entidade Privada	Grande
335	Reino Unido	Information Commissioner's Office (ICO)	https://ico.org.uk/media/action-weve-taken/mpns/2616742/doorstop-mpn-20191217.pdf	17/12/2019	320 000,00 €	(5)(1)(e);(5)(1)(f);(13);(14);(24)(1);(32)	Doorstep Dispensaree Ltd.	Responsável pelo tratamento	Entidade Privada	PME
336	Noruega	Datatilsynet	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/dragefossen-as-far-gebyr/	25/03/2021	14 829,00 €	(5)(1)(a);(6)(1)	Dragefossen AS	Responsável pelo tratamento	Entidade Privada	Grande
337	Noruega	Datatilsynet	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/gebyr-til-alesund-kommune-for-bruk-av-strava/	24/03/2021	4 900,00 €	(24)(1);(32)(1)(b);(35)	Município de Ålesund	Responsável pelo tratamento	Entidade Pública	Entidade Pública
338	Noruega	Datatilsynet	https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2021/far-gebyr-for-ulovleg-vidaresending-av-e-post/	02/03/2021	24 400,00 €	(5);(6)	Desconhecido	Responsável pelo tratamento	Entidade Privada	N/A
339	Noruega	Datatilsynet	https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2021/cyberbook-as-far-gebyr/	03/02/2021	19 300,00 €	(5);(6)	Cyberbook AS	Responsável pelo tratamento	Entidade Privada	PME
340	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/c5f433a97050467497810b9e891d5b83/vedtak-om-palegg-og-overtredelsesgebyr---aquateknikk-as.pdf	01/04/2021	9 700,00 €	(6)(1)(f)	Aquateknikk AS	Responsável pelo tratamento	Entidade Privada	PME
341	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/5cd2e76bd5d2481f9578ffe721b7e24d/vedtak-om-overtredelsesgebyr-til-coop-finnmark-sa.pdf	14/01/2021	38 600,00 €	(5)(1)(a);(6)	Coop Finnmark SA	Responsável pelo tratamento	Entidade Privada	PME
342	Noruega	Datatilsynet	https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2021/far-gebyr-for-videresending-av-e-post/	12/01/2021	38 600,00 €	(5);(6)	Desconhecido	Responsável pelo tratamento	Entidade Privada	N/A

343	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/c4e89c78222a40e09740b7ade6e8cfcf/vedtak-om-palegg-og-overtredelsesgebyr---gveik-as.pdf	07/01/2021	7 250,00 €	(5)(2);(6)	Gveik AS	Responsável pelo tratamento	Entidade Privada	PME
344	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/a5ac87c91d9f4835b2b7abfa5e907cf7/vedtak-om-overtredelsesgebyr-lindstrand-trading-as.pdf	06/01/2021	9 700,00 €	(6)(1)(f)	Lindstrand Trading AS	Responsável pelo tratamento	Entidade Privada	PME
345	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/004f43fe684445c29e4fc8393a9a714d/varsel-om-overtredelsesgebyr---innovasjon-norge.pdf	04/01/2021	95 500,00 €	(6)(1)(f)	Innovasjon Norge	Responsável pelo tratamento	Entidade Privada	Grande
346	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/1679986c04f54694b734ab883eebfde1/endelig-vedtak-til-indre-ostfold-kommune.pdf	03/12/2020	18 840,00 €	(5);(6);(32)(1)(b)	Município de Indre Østfold	Responsável pelo tratamento	Entidade Pública	Entidade Pública
347	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/44c6c9df0ee64fdc9f704f8ca930d4ce/vedtak-om-otg-odin-flissenter.pdf	25/09/2020	13 900,00 €	(6)(1)(f)	Odin Flissenter AS	Responsável pelo tratamento	Entidade Privada	PME
348	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/fd5c454b4eae4924af94943ba68002bf/20_02181-3-vedtak-om-overtredelsesgebyr---bergen-kommune.pdf	03/09/2020	294 000,00 €	(5)(1)(f);(32)(1)(b)	Município de Bergen	Responsável pelo tratamento	Entidade Pública	Entidade Pública
349	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/9d5792264c884f3a903d3981c38812ac/~-20_02191-1-vedtak-om-overtredelsesgebyr---ralingen-kommune-202444_10_1.pdf	02/07/2020	46 660,00 €	(5);(24);(32)(1)(b);(32)(1)(d);(35)	Município de Rælingen	Responsável pelo tratamento	Entidade Pública	Entidade Pública
350	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/bce6b7225a2146dbb5dd416bd9f19b9c/20-02220-1---sladdet---varsel-om-vedtak-odin-flissenter-as.pdf	02/07/2020	0,00 €	(6)(1)(f)	Odin Flissenter AS	Responsável pelo tratamento	Entidade Privada	PME
351	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/580ab399d02d4d369de8c5905757d4b2/~-20_02291-4-vedtak-om-overtredelsesgebyr-og-palegg-208484_13_1.pdf	22/10/2020	73 539,80 €	(5)(1)(f);(24)(32)	Østfold HF Hospital	Responsável pelo tratamento	Entidade Pública	Entidade Pública
352	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/2b5da07f91fe4cf0a95684c149516c6d/varsel-om-otg---aquateknikk.pdf	19/06/2020	0,00 €	(5);(6)	Aquateknikk AS	Responsável pelo tratamento	Entidade Privada	PME
353	Noruega	Datatilsynet	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/varsel-om-irettesettelse-mot-telenor-norge-as/	27/05/2020	147 000,00 €	(32)(1);(33)	Telenor Norge AS	Responsável pelo tratamento	Entidade Privada	Grande
354	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/8dbf5b4b2a33471aacf375b1f0032347/varsel-om-overtredelsesgebyr.pdf	28/02/2020	0,00 €	(5)(1)(a);(6)	Coop Finnmark SA	Responsável pelo tratamento	Entidade Privada	PME

355	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/bc26a2a8b78b4b30b4b060a4cac80d90/varsel-ralingen.pdf	26/02/2020	0,00 €	(5);(24);(32)(1)(b);(32)(1)(d);(35)	Município de Rælingen	Responsável pelo tratamento	Entidade Pública	Entidade Pública
356	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/ae65e212c134455c93f36a10c5a8c792/vedtak-oslo-kommune-oktober2019.pdf	11/10/2019	117 000,00 €	(5)(1);(32)(1)(b);(32)(1)(d)	Departamento Municipal de Educação de Oslo	Responsável pelo tratamento	Entidade Pública	Entidade Pública
357	Noruega	Datatilsynet	https://www.datatilsynet.no/contentassets/67033efe6b8a48d7aa679be2c8fd436d/18-02140-13-vedtak-om-overtredelsesgebyr---melding-om-avvik-hos-bergen-kommune-253778_15_1.pdf	19/03/2019	156 000,00 €	(5)(1)(f);(32)(1)(a);(32)(1)(b)	Município de Bergen	Responsável pelo tratamento	Entidade Pública	Entidade Pública
358	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_Presa_23_/_03_/_2021&lang=ro	23/03/2021	2 000,00 €	(32)(1)(b);(32)(2);(32)(4)	SC Medicover SRL	Responsável pelo tratamento	Entidade Privada	Grande
359	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_Presa_04_03_2021&lang=ro	04/03/2021	500,00 €	(32)(1);(32)(2);(58)(1)(a);(58)(1)(e)	Pessoa privada	Responsável pelo tratamento	Pessoa individual	Pessoa individual
360	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_Presa_10_/_02_/_21&lang=ro	10/02/2021	1 000,00 €	(29);(32)(2);(32)(4)	ING Bank N.V. Amsterdam - Bucharest office	Responsável pelo tratamento	Entidade Privada	Grande
361	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_presa_30_12_2020&lang=ro	30/12/2020	3 000,00 €	(5)(1)(a);(5)(1)(d);(6)(1)	ING Bank N.V. Amsterdam - Bucharest office	Responsável pelo tratamento	Entidade Privada	Grande
362	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_Presa_29_12_2020&lang=ro	29/12/2020	1 000,00 €	(32)	Qualitance QBS SA	Responsável pelo tratamento	Entidade Privada	Grande
363	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_Presa_22_12_2020&lang=ro	22/12/2020	2 000,00 €	(58)(1)(a);(58)(1)(e);(58)(2)(i)	S.C. C&V Water Control S.A.	Responsável pelo tratamento	Entidade Privada	Grande
364	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_17_12_2020&lang=ro	17/12/2020	100 000,00 €	(5)(1)(f);(32)(1);(32)(2)	Banca Transilvania SA	Responsável pelo tratamento	Entidade Privada	Grande
365	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_Presa_24_11_2020&lang=ro	24/11/2020	5 000,00 €	(32)(1);(32)(2);(33)(1)	Dada Creation S.R.L.	Responsável pelo tratamento	Entidade Privada	PME
366	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_de_presa_23_/_11_/_2020&lang=ro	23/11/2020	4 000,00 €	(12);(15);(17)	Vodafone România SA	Responsável pelo tratamento	Entidade Privada	Grande
367	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Alta_amenda_pentru_incalcarea_RGPD_oct_2020&lang=ro	20/10/2020	2 000,00 €	(58)(1)	Globus Score SRL	Responsável pelo tratamento	Entidade Privada	PME

368	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Amenda_pentru_incalcarea_RGPD_15_/_10_/_2020&lang=ro	15/10/2020	3 000,00 €	(25);(32)	SC Marsorom SRL	Responsável pelo tratamento	Entidade Privada	PME
369	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_Presa_01_/_10_/_2020&lang=ro	01/10/2020	3 000,00 €	(31);(58)	Megareduceri TV S.R.L.	Responsável pelo tratamento	Entidade Privada	PME
370	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_Presa_01_/_10_/_2020&lang=ro	01/10/2020	2 000,00 €	(31);(58)	Asociația de proprietari Militari R	Responsável pelo tratamento	Entidade Privada	PME
371	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_Presa_08_/_09_/_20&lang=ro	08/09/2020	2 000,00 €	(5)(1)(f);(32)(1);(32)(2)	Sanatatea Press Group S.R.L.	Responsável pelo tratamento	Entidade Privada	PME
372	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_Presa_01_09_2020&lang=ro	01/09/2020	500,00 €	(5);(6)(1)	Apartment building owners association	Responsável pelo tratamento	Entidade Privada	PME
373	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Amenda_pentru_incalcarea_RGPD_Viva_Credit_IFN&lang=ro	30/07/2020	2 000,00 €	(12)(3);(12)(4);(17)	SC Viva Credit IFN SA	Responsável pelo tratamento	Entidade Privada	PME
374	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Sanctiune_pentru_incalcarea_RGPD_Posta_Romana&lang=ro	30/07/2020	2 000,00 €	(32)	Romanian Post National Company	Responsável pelo tratamento	Entidade Privada	PME
375	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Sanctiune%20pentru%20incalcare%20RGPD%2027_07_20&lang=ro	27/07/2020	5 000,00 €	(32)(1)(b);(32)(2);(32)(4)	SC Cntar Tarom SA	Responsável pelo tratamento	Entidade Privada	Grande
376	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_09_07_20&lang=ro	09/07/2020	15 000,00 €	(32)(1);(32)(2)	Proleasing Motors SRL	Responsável pelo tratamento	Entidade Privada	PME
377	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Amenda_pentru_incalcarea_RGPD_Enel_iunie2020&lang=ro	18/06/2020	4 000,00 €	(32)	ENEL ENERGIE MUNTENIA SA	Responsável pelo tratamento	Entidade Privada	Grande
378	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=O_noua_sanctiune_pentru_incalcarea_RGPD_iunie_2020&lang=ro	11/06/2020	3 000,00 €	(32)	Telekom Romania	Responsável pelo tratamento	Entidade Privada	Grande
379	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Sanctiune_pentru_incalcarea_RGPD_BCR&lang=ro	05/05/2020	5 000,00 €	(32)(1);(32)(2);(32)(4)	Banca Comercială Română SA	Responsável pelo tratamento	Entidade Privada	Grande
380	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Amenda_pentru_incalcarea_RGPD_iunie_2020&lang=ro	23/04/2020	3 000,00 €	(6);(7);(9)	Estee Lauder Romania	Responsável pelo tratamento	Entidade Privada	PME
381	Roménia	The National Supervisory Authority	https://www.dataprotection.ro/?page=O_noua_sanctiune_pentru_incalcarea_RGPD_iunie_2020&lang=ro	23/04/2020	3 000,00 €	(32)	Telekom Romania Communications SA	Responsável pelo tratamento	Entidade Privada	Grande

		for Personal Data Processing								
382	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_amenda_asociatia_sos_infertilitatea&lang=ro	25/03/2020	2 000,00 €	(58)(1)(a);(58)(1)(e)	SOS Infertility Association	Responsável pelo tratamento	Entidade Privada	PME
383	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_amenda_enel_martie_2020&lang=ro	25/03/2020	3 000,00 €	(32)	ENEL ENERGIE MUNTENIA SA	Responsável pelo tratamento	Entidade Privada	Grande
384	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_noua_amenda_vodafone&lang=ro	25/03/2020	4 150,00 €	(32)	Vodafone Romania	Responsável pelo tratamento	Entidade Privada	Grande
385	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_amenda_dante_international_martie_2020&lang=ro	25/03/2020	3 000,00 €	(6);(21)(3)	Dante International	Responsável pelo tratamento	Entidade Privada	Grande
386	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=sanctiune_vodafone_februarie_2020&lang=ro	11/02/2020	3 000,00 €	(5)(1)(d);(5)(1)(f);(5)(2)	Vodafone Romania	Responsável pelo tratamento	Entidade Privada	Grande
387	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=O_noua_amenda_pentru_incalcarea_RGPD_comunicat_decembrie&lang=ro	18/12/2019	2 000,00 €	(5)(1)(d)	Telekom Romania Mobile Communications SA	Responsável pelo tratamento	Entidade Privada	Grande
388	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Alta_amenda_pentru_incalcarea_GDPR&lang=en	16/12/2019	2 000,00 €	(58)(1)(a);(58)(1)(e)	Globus Score SRL	Responsável pelo tratamento	Entidade Privada	PME
389	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=sanctiune_pentru_incalcarea_RGPD_2020_2&lang=ro	16/12/2019	3 000,00 €	(5)(1)(d);(6)(1)(a);(7)(1)	SC Enel Energie S.A. (Electricity Distributor)	Responsável pelo tratamento	Entidade Privada	Grande
390	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=sanctiune_pentru_incalcarea_RGPD_2020_2&lang=ro	16/12/2019	3 000,00 €	(21)(1)	SC Enel Energie S.A. (Electricity Distributor)	Responsável pelo tratamento	Entidade Privada	Grande
391	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=O_noua_sanctiune_pentru_incalcarea_RGPD_2020_3&lang=ro	13/12/2019	5 000,00 €	(5)(1);(6);(7)	Entirely Shipping & Trading S.R.L.	Responsável pelo tratamento	Entidade Privada	PME
392	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=O_noua_sanctiune_pentru_incalcarea_RGPD_2020_3&lang=ro	13/12/2019	5 000,00 €	(5)(1);(7);(9)	Entirely Shipping & Trading S.R.L.	Responsável pelo tratamento	Entidade Privada	PME
393	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Alta_amenda_pentru_incalcarea_RGPD_2020_1&lang=ro	10/12/2019	3 000,00 €	(5);(25);(32);(33)	Hora Credit IFN SA	Responsável pelo tratamento	Entidade Privada	PME
394	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Sanctiune_CN_TAROM&lang=ro	04/12/2019	20 000,00 €	(32)(1);(32)(2);(32)(4)	S CNTAR TAROM SA	Responsável pelo tratamento	Entidade Privada	Grande

395	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Noi_amenzi_in_aplicarea_RGPD&lang=ro	02/12/2019	2 000,00 €	(58)(1)(a);(58)(1)(e)	Nicola Medical Team 17 SRL	Responsável pelo tratamento	Entidade Privada	PME
396	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=alta_sanctiune_Royal_President&lang=ro	29/11/2019	2 500,00 €	(5)(1)(f);(32)(1)(b)	Royal President SRL	Responsável pelo tratamento	Entidade Privada	PME
397	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Amenda_asociatie_proprietari&lang=ro	29/11/2019	500,00 €	(32)	Associação de Proprietários de Imóveis	Responsável pelo tratamento	Entidade Privada	PME
398	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Amenda_ING_RGPD&lang=ro	28/11/2019	80 000,00 €	(5)(1)(f);(25)(1)	ING Bank N.V. Amsterdam - Bucharest office	Responsável pelo tratamento	Entidade Privada	Grande
399	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Noi_amenzi_in_aplicarea_RGPD&lang=ro	26/11/2019	3 000,00 €	(58)(1)(a);(58)(1)(e)	Modern Barber SRL	Responsável pelo tratamento	Entidade Privada	PME
400	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=O_noua_amenda_in_baza_RGPD&lang=ro	25/11/2019	11 000,00 €	(32)(1);(32)(2)	FAN COURIER EXPRESS SRL	Responsável pelo tratamento	Entidade Privada	Grande
401	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Amenda_pentru_incalcarea_RGPD&lang=ro	22/11/2019	2 000,00 €	(12)(3)	BNP Paribas Personal Finance SA	Responsável pelo tratamento	Entidade Privada	Grande
402	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=A_patra_amenda&lang=ro	17/10/2019	1 000,00 €	(12)	UTTIS INDUSTRIES SRL	Responsável pelo tratamento	Entidade Privada	PME
403	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=A_patra_amenda&lang=ro	17/10/2019	1 500,00 €	(5)(1)(c);(6)	UTTIS INDUSTRIES SRL	Responsável pelo tratamento	Entidade Privada	PME
404	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_Presa_09_10_2019&lang=ro	09/10/2019	150 000,00 €	(32)(1);(32)(2);(32)(4)	Raiffeisen Bank SA	Responsável pelo tratamento	Entidade Privada	Grande
405	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_Presa_09_10_2019&lang=ro	09/10/2019	20 000,00 €	(32)(1);(32)(2);(32)(4);(33)(1)	Vreau Credit SRL	Responsável pelo tratamento	Entidade Privada	PME
406	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Alta_sanctiune_RGPD&lang=ro	26/09/2019	9 000,00 €	(5)(1)(a);(5)(1)(b);(6)(1)(a);(7)	Inteligo Media SA	Responsável pelo tratamento	Entidade Privada	PME
407	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=2019%20A%20treia%20amenda%20in%20aplicarea%20RGPD&lang=ro	05/07/2019	3 000,00 €	(32)(1);(32)(2)	LEGAL COMPANY & TAX HUB SRL	Responsável pelo tratamento	Entidade Privada	PME
408	Roménia	The National Supervisory Authority	https://www.dataprotection.ro/?page=O_noua_amenda_GDPR&lang=ro	02/07/2019	15 000,00 €	(32)(1);(32)(2);(32)(4)	WORLD TRADE CENTER BUCHAREST SA	Responsável pelo tratamento	Entidade Privada	PME

		for Personal Data Processing								
409	Roménia	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/?page=Comunicat_Amenda_Unicredit&lang=ro	27/06/2019	130 000,00 €	(25)(1)	UNICREDIT BANK SA	Responsável pelo tratamento	Entidade Privada	Grande
410	Austria	Österreichische Datenschutzbehörde	https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=f40e6a89-d994-4e49-af4a-fcf3d89c1ccd&Position=1&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20201019_2020_0_111_488_00	19/10/2020	600,00 €	(5)(1)(a);(9)(1);(9)(2)	Pessoa individual	Responsável pelo tratamento	Entidade Privada	PME
411	Austria	Österreichische Datenschutzbehörde	https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=3e78f5a9-f724-41df-a8b6-4f95524b02a4&Position=1&SkipToDocumentPage=True&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.10.2020&BisDatum=03.12.2020&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20201019_2020_0_550_322_00	19/10/2020	150,00 €	(5)(1)(a);(6)(1)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual
412	Austria	Österreichische Datenschutzbehörde	https://www.dsb.gv.at/documents/22758/115212/Newsletter_DSB_3_2020.pdf/90579856-6cb5-4206-823a-cacc724cf94e	05/08/2020	100,00 €	(5);(6)	Bank	Responsável pelo tratamento	Entidade Privada	Grande
413	Austria	Österreichische Datenschutzbehörde	https://www.bvwg.gv.at/presse/Datenschutzverfahren_Oesterreichische_Post.html	29/10/2019	0,00 €	(5)(1)(a);(6)	Österreichische Post AG	Responsável pelo tratamento	Entidade Privada	Grande
414	Austria	Österreichische Datenschutzbehörde	https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181116_DSB_D213_692_0001_DSB_2018_00/DSBT_20181116_DSB_D213_692_0001_DSB_2018_00.html	16/11/2018	50 000,00 €	(13);(37)	Company in the medical sector	Responsável pelo tratamento	Entidade Privada	PME
415	Austria	Österreichische Datenschutzbehörde	https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=875606c8-283c-4523-8a39-c37451d99169&Position=1&Sort=2%7cDesc&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&	11/07/2019	11 000,00 €	(5)(1)(a);(5)(1)(b);(6)(1)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual

			VonDatum=01.01.2017&BisDatum=13.03.2021&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20190711_DSB_D550_185_0002_DSB_2019_00							
416	Austria	Österreichische Datenschutzbehörde	https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=875606c8-283c-4523-8a39-c37451d99169&Position=1&Sort=2%7cDesc&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.2017&BisDatum=13.03.2021&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20181220_DSB_D550_037_0003_DSB_2018_00	20/12/2018	2 200,00 €	(5)(1)(a);(5)(1)(c);(6)(1)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual
417	Austria	Österreichische Datenschutzbehörde	https://www.dsb.gv.at/documents/22758/116802/Straferkenntnis+DSB-D550.038+0003-DSB+2018.pdf/fb0bb313-8651-44ac-a713-c286d83e3f19	09/12/2018	4 800,00 €	(13)	Lugar de apostas	Responsável pelo tratamento	Entidade Privada	N/A
418	Austria	Österreichische Datenschutzbehörde	https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=875606c8-283c-4523-8a39-c37451d99169&Position=1&Sort=2%7cDesc&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.2017&BisDatum=13.03.2021&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20180927_DSB_D550_084_0002_DSB_2018_00	27/09/2018	300,00 €	(5)(1)(a);(5)(1)(c);(6)(1)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual
419	Austria	Österreichische Datenschutzbehörde	https://www.dsb.gv.at/documents/22758/115212/Newsletter_DSB_1_2020.pdf/a640bbb8-9297-4230-86e4-163bc9ccb844	01/06/2018	1 800,00 €	(5);(13);(14)	Kebab restaurant	Responsável pelo tratamento	Entidade Privada	PME
420	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-36-2021.pdf	15/03/2021	1 000,00 €	(5)(1)(c);(6)(1);(8)	Escola	Responsável pelo tratamento	Entidade Pública	Entidade Pública

421	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-04-2021.pdf	27/01/2021	50 000,00 €	(5);(6);(7);(13);(24);(25);(28)	Family Service / NDPK nv.	Responsável pelo tratamento	Entidade Privada	PME
422	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-05-2021.pdf	22/01/2021	25 000,00 €	(5)(1)(f);(5)(2);(24);(32);(33)(1);(33)(5);(34)(1)	Desconhecido	Responsável pelo tratamento	Entidade Privada	N/A
423	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-02-2021.pdf	12/01/2021	10 000,00 €	(6)(1);(12)(3);(21)(1)	Desconhecido	Responsável pelo tratamento	N/A	N/A
424	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-81-2020.pdf	23/12/2020	50 000,00 €	(5)(1)(c);(5)(2);(6);(12)(3);(14)(1);(14)(2);(24)(1);(24)(2)	Desconhecido	Responsável pelo tratamento	Entidade Privada	N/A
425	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-81-2020.pdf	23/12/2020	15 000,00 €	(5)(1)(c);(5)(2);(6);(12)(3);(14)(1);(14)(2);(24)(1);(24)(2)	Desconhecido	Responsável pelo tratamento	Entidade Privada	N/A
426	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-74-2020.pdf	24/11/2020	1 500,00 €	(25)(1)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual
427	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-73-2020.pdf	13/11/2013	1 500,00 €	(5)(1)(a);(5)(1)(b);(5)(2);(6)(1);(12)(1);(13)(1)(b);(13)(1)(c);(13)(2)(b);(15)(1);(25)(2);(37)(5);(37)(7);(38)(1);(38)(3);(39)	Desconhecido	Responsável pelo tratamento	Entidade Privada	N/A
428	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-53-2020.pdf	01/09/2020	0,00 €	(5)(1)(a);(5)(1)(b);(6)(1);(25)(1);(25)(2);(32)(1);(32)(4)	Político	Responsável pelo tratamento	Entidade Pública	Entidade Pública
429	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-39-2020.pdf	28/07/2020	3 000,00 €	(5);(6);(12);(14)	Associação política	Responsável pelo tratamento	Entidade Privada	N/A
430	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-37-2020.pdf	14/07/2020	500 000,00 €	(6)(1)(f);(17)(1)(a)	Google Belgium SA	Responsável pelo tratamento	Entidade Privada	Grande
431	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-37-2020.pdf	14/07/2020	100 000,00 €	(12)(1);(12)(4)	Google Belgium SA	Responsável pelo tratamento	Entidade Privada	Grande
432	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-36-2020.pdf	09/07/2020	5 000,00 €	(6)(1)	Operadora de CCTV em edifício residencial	Responsável pelo tratamento	N/A	N/A
433	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Beslissing_GK_33-2020_NL.pdf	19/06/2020	10 000,00 €	(5);(6);(15)	Desconhecido	Responsável pelo tratamento	N/A	N/A
434	Bélgica	Autorité de la protection des données -	https://www.autoriteprotectiondonnees.be/sites/privacycommission/fi	16/06/2020	1 000,00 €	(17);(21);(31)	Desconhecido	Responsável pelo tratamento	N/A	N/A

		Gegevensbeschermingsautoriteit (APD-GBA)	les/documents/D%C3%A9cision_CC_32-2020_FR.pdf							
435	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Decision_CC_30-2020_FR.pdf	08/06/2020	5 000,00 €	(5);(6)	Funcionário municipal	Responsável pelo tratamento	Entidade Pública	Entidade Pública
436	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Beslissing_GK_28-2020_NL.pdf	29/05/2020	1 000,00 €	(6);(21)	Organização sem fins lucrativos	Responsável pelo tratamento	Entidade Privada	N/A
437	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/Beslissing_GK_25-2020_EN.pdf	14/05/2020	50 000,00 €	(6)	Provedor de mídia social	Responsável pelo tratamento	Entidade Privada	N/A
438	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Beslissing_GK_18-2020_NL.pdf	28/04/2020	50 000,00 €	(31);(37);(58)	Proximus SA	Responsável pelo tratamento	Entidade Privada	Grande
439	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/DEQF_13-2019_FR_ANO.pdf	17/12/2019	2 000,00 €	(12);(15);(17)	Organização de cuidados de enfermagem	Responsável pelo tratamento	Entidade Privada	N/A
440	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/BETG_12-2019_NL.PDF	17/12/2019	15 000,00 €	(6);(12);(13)	Site que fornece informações legais	Responsável pelo tratamento	N/A	N/A
441	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.autoriteprotectiondonnees.be/news/la-chambre-contentieuse-sanctionne-deux-candidats-aux-elections-communales-de-2018	28/11/2019	5 000,00 €	(6)	Político	Responsável pelo tratamento	Entidade Pública	Entidade Pública
442	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.autoriteprotectiondonnees.be/news/la-chambre-contentieuse-sanctionne-deux-candidats-aux-elections-communales-de-2018	28/11/2019	5 000,00 €	(6)	Político	Responsável pelo tratamento	Entidade Pública	Entidade Pública
443	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.gegevensbeschermingsautoriteit.be/burger/de-gegevensbeschermingsautoriteit-sanctioneert-een-handelaar-voor-het-disproportionele-gebruik-van-de-eid-om-een-klantenkaart-aan-te-maken	17/09/2019	10 000,00 €	(5)(1)(c)	Comerciante	Responsável pelo tratamento	Entidade Privada	N/A
444	Bélgica	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.autoriteprotectiondonnees.be/news/lautorite-de-protection-des-donnees-prononce-une-sanction-dans-le-cadre-dune-campagne	28/05/2019	2 000,00 €	(5)(1)(b);(6)	Político	Responsável pelo tratamento	Entidade Pública	Entidade Pública
445	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/?p=element&aid=1247	14/04/2020	2 000,00 €	(6)	Político	Responsável pelo tratamento	Entidade Pública	Entidade Pública
446	Bulgária	Commission for Personal Data Protection	http://www.cpdp.bg/download.php?part=rubric_element&aid=4563	20/02/2020	2 560,00 €	(25)(1);(32)	T.K. EOOD	Responsável pelo tratamento	Entidade Privada	PME

447	Bulgária	Commission for Personal Data Protection	http://www.cpdp.bg/download.php?part=rubric_element&aid=4563	20/02/2020	2 560,00 €	(6);(25)(1);(32)	L.E. EOOD	Responsável pelo tratamento	Entidade Privada	PME
448	Bulgária	Commission for Personal Data Protection	http://www.cpdp.bg/download.php?part=rubric_element&aid=4563	06/01/2020	5 110,00 €	(6)(1)	Utility Company	Responsável pelo tratamento	Entidade Pública	Entidade Pública
449	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/index.php?p=element&aid=1219	28/10/2019	511,00 €	(12)(3);(15)(1)	Pessoa individual	Responsável pelo tratamento	N/A	N/A
450	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/index.php?p=element&aid=1219	08/10/2019	5 112,00 €	(5)(1);(6)(1)	The Ministry of Interior Affairs	Responsável pelo tratamento	Entidade Pública	Entidade Pública
451	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/index.php?p=element&aid=1219	07/10/2019	511,00 €	(31)	Desconhecido	Responsável pelo tratamento	N/A	N/A
452	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/?p=element_view&aid=2226	03/09/2019	28 100,00 €	(6)(1)	National Revenue Agency	Responsável pelo tratamento	Entidade Pública	Entidade Pública
453	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/index.php?p=element&aid=1219	03/09/2019	1 022,00 €	(6)(1);(25)(1)	Telecommunication service provide	Responsável pelo tratamento	Entidade Privada	N/A
454	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/index.php?p=element&aid=1219	03/09/2019	5 113,00 €	(6)(1);(25)(1)	Telecommunication service provide	Responsável pelo tratamento	Entidade Privada	N/A
455	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/index.php?p=element&aid=1219	03/09/2019	11 706,00 €	(6)(1)	Commercial representative of telecommunication service provider	Responsável pelo tratamento	Entidade Privada	N/A
456	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/index.php?p=element&aid=1219	03/09/2019	1 121,00 €	(12)(4);(15)	Private enforcement agent	Responsável pelo tratamento	Entidade Privada	N/A
457	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/index.php?p=news_view&aid=1519	28/08/2019	2 600 000,00 €	(32)(1)(b)	National Revenue Agency	Responsável pelo tratamento	Entidade Pública	Entidade Pública
458	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/index.php?p=news_view&aid=1514	28/08/2019	511 313,00 €	(32)(1)(b)	DSK Bank	Responsável pelo tratamento	Entidade Privada	Grande
459	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/?p=element_view&aid=2192	08/04/2019	510,00 €	(5)(1)(b);(6)(1)	Medical centers	Responsável pelo tratamento	Entidade Pública	Entidade Pública
460	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/?p=element_view&aid=2191	26/03/2019	5 100,00 €	(6)(1)	A.P. EOOD	Responsável pelo tratamento	Entidade Privada	PME
461	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/?p=element_view&aid=2180	26/02/2019	27 100,00 €	(6)(1)	Telecommunication service provider	Responsável pelo tratamento	Entidade Privada	Grande
462	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/?p=element_view&aid=2177	22/02/2019	500,00 €	(12);(15)(1)(a);(15)(1)(b);(15)(1)(c);(15)(1)(g);(15)(3)	Pessoa individual	Responsável pelo tratamento	N/A	N/A
463	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/?p=element&aid=1195	17/01/2019	500,00 €	(5)(1)(a);(6)	Bank	Responsável pelo tratamento	Entidade Privada	Grande
464	Bulgária	Commission for Personal Data Protection	https://www.cpdp.bg/?p=element_view&aid=2152	04/12/2018	500,00 €	(5)(1)(b)	Bank	Responsável pelo tratamento	Entidade Privada	Grande
465	Croácia	Croatian Personal Data Protection Agency	https://azop.hr/izdana-nova-upravna-novcana-kazna/	22/02/2021	0,00 €	(32)(1)(b);(32)(1)(d);(32)(2);(32)(4)	Security company	Responsável pelo tratamento	N/A	N/A
466	Croácia	Croatian Personal Data Protection Agency	https://azop.hr/rjesenje-kojim-se-izrice-upravno-novcana-kazna-zbog-odbijanja-dostave-osobnih-podataka-ispitanicima/	13/03/2020	0,00 €	(15)(3)	Bank	Responsável pelo tratamento	Entidade Privada	Grande

467	Chipre	Commissioner for Personal Data Protection	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/B0CED3EDDC2EE5EDC225868D0037E7A4?OpenDocument	03/03/2021	25 000,00 €	(5)(1)(e);(5)(1)(f);(32)(1)(b);(32)(1)(c);(33)(1)	Hellenic Bank	Responsável pelo tratamento	Entidade Privada	Grande
468	Chipre	Commissioner for Personal Data Protection	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/B0CED3EDDC2EE5EDC225868D0037E7A4?OpenDocument	03/03/2021	10 000,00 €	(12);(15);(31);(58)(1)(e)	Autoridade cipriota de registro de bens imóveis	Responsável pelo tratamento	Entidade Pública	Entidade Pública
469	Chipre	Commissioner for Personal Data Protection	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/B0CED3EDDC2EE5EDC225868D0037E7A4?OpenDocument	03/03/2021	6 000,00 €	(32)(4)	KEPIDES	Responsável pelo tratamento	Entidade Privada	Grande
470	Chipre	Commissioner for Personal Data Protection	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/news02_gr/news02_gr?OpenDocument	03/03/2021	40 000,00 €	(6)(1);(9)(2)	Autoridade de Eletricidade do Chipre	Responsável pelo tratamento	Entidade Pública	Entidade Pública
471	Chipre	Commissioner for Personal Data Protection	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/B64595978C98EFCEC2258606003EC47E/$file/%CE%A0%CE%95%CE%A1%CE%99%CE%9B%CE%97%CE%A8%CE%97%20%CE%91%CE%A0%CE%9F%CE%A6%CE%91%CE%A3%CE%97%CE%A3%20%CE%91%CE%A3%CE%A4%CE%A5%CE%9D%CE%9F%CE%9C%CE%99%CE%91%CE%A3%2068-2017.pdf?openelement	19/10/2020	6 000,00 €	(32)(1)(b);(32)(1)(d)	Polícia de Chipre	Responsável pelo tratamento	Entidade Pública	Entidade Pública
472	Chipre	Commissioner for Personal Data Protection	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/B64595978C98EFCEC2258606003EC47E?OpenDocument	19/10/2020	1 000,00 €	(5);(6)	Grant Ideas Ltd	Responsável pelo tratamento	Entidade Privada	PME
473	Chipre	Commissioner for Personal Data Protection	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/B64595978C98EFCEC2258606003EC47E?OpenDocument	19/10/2020	15 000,00 €	(5)(1)(f);(5)(2);(15);(32);(33)	Bank of Cyprus Public Company Ltd	Responsável pelo tratamento	Entidade Privada	Grande
474	Chipre	Commissioner for Personal Data Protection	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/ACDFDC478581BEE1C22584EE002EE9C2?OpenDocument	13/01/2013	9 000,00 €	(32)(1)(b);(32)(1)(d);(32)(4)	Serviços de Seguro Social do Ministério do Trabalho, Previdência e Seguro Social	Responsável pelo tratamento	Entidade Pública	Entidade Pública
475	Chipre	Commissioner for Personal Data Protection	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/ACDFDC478581BEE1C22584EE002EE9C2?OpenDocument	13/01/2013	1 000,00 €	(6)	ML PRO.FIT SOLUTIONS LTD	Responsável pelo tratamento	Entidade Privada	Grande
476	Chipre	Commissioner for Personal Data Protection	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/ACDFDC478581BEE1C22584EE002EE9C2?OpenDocument	25/10/2019	70 000,00 €	(6)(1);(9)(2)	LGS Handling Ltd, Louis Travel Ltd e Louis Aviation Ltd	Responsável pelo tratamento	Entidade Privada	Grande
477	Chipre	Commissioner for Personal Data Protection	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/ACDFDC478581BEE1C22584EE002EE9C2?OpenDocument	25/10/2019	10 000,00 €	(6)(1);(9)(2)	LGS Handling Ltd, Louis Travel Ltd e Louis Aviation Ltd	Responsável pelo tratamento	Entidade Privada	Grande

478	Chipre	Commissioner for Personal Data Protection	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/ACDFDC478581BEE1C22584EE002EE9C2?OpenDocument	25/10/2019	2 000,00 €	(6)(1);(9)(2)	LGS Handling Ltd, Louis Travel Ltd e Louis Aviation Ltd	Responsável pelo tratamento	Entidade Privada	Grande
479	Chipre	Commissioner for Personal Data Protection	https://www.agplaw.com/cyprus-gdpr-commissioner-fines-newspaper-and-hospital/	01/06/2019	5 000,00 €	(15)	Hospital	Responsável pelo tratamento	Entidade Pública	Entidade Pública
480	Chipre	Commissioner for Personal Data Protection	https://www.agplaw.com/cyprus-gdpr-commissioner-fines-newspaper-and-hospital/	01/06/2019	10 000,00 €	(6)	Jornal	Responsável pelo tratamento	Entidade Privada	N/A
481	Chipre	Commissioner for Personal Data Protection	https://cyprus-mail.com/2019/10/11/doctor-fined-e14000-for-violating-patient-data-on-instagram/	01/06/2019	14 000,00 €	(5);(6)	Médico	Responsável pelo tratamento	N/A	N/A
482	República Checa	Office for Personal Data Protection	https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=47199	05/01/2021	118 500,00 €	(6)(1);(14)	Desconhecido	Responsável pelo tratamento	Entidade Privada	N/A
483	República Checa	Office for Personal Data Protection	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34472	06/05/2019	194,00 €	(15)(1)	empresa de utilidade pública	Responsável pelo tratamento	N/A	N/A
484	República Checa	Office for Personal Data Protection	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34470	21/03/2019	10 000,00 €	(5)(1)(a);(5)(1)(c);(5)(1)(e)	Desconhecido	Responsável pelo tratamento	N/A	N/A
485	República Checa	Office for Personal Data Protection	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34466	28/02/2019	582,00 €	(5)(1)(a);(5)(1)(f);(28)(3)	Desconhecido	Responsável pelo tratamento	N/A	N/A
486	República Checa	Office for Personal Data Protection	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34469	26/02/2019	776,00 €	(15)(1)	Desconhecido	Responsável pelo tratamento	N/A	N/A
487	República Checa	Office for Personal Data Protection	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34465	04/02/2019	1 165,00 €	(5)(1)(a)	Empresa	Responsável pelo tratamento	Entidade Privada	N/A
488	República Checa	Office for Personal Data Protection	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34467	04/02/2019	1 165,00 €	(5)(1)(a);(5)(1)(f)	Corretora de crédito	Responsável pelo tratamento	Entidade Privada	N/A
489	República Checa	Office for Personal Data Protection	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34464	10/01/2019	388,00 €	(6)(1)	Empresa	Responsável pelo tratamento	N/A	N/A
490	República Checa	Office for Personal Data Protection	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34468	25/10/2018	388,00 €	(15)(1)	Desconhecido	Responsável pelo tratamento	N/A	N/A
491	República Checa	Office for Personal Data Protection	https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-bankou-unicredit-bank-czech-republic-and-slovakia-a-s/ds-5705/archiv=0&p1=5653	01/06/2019	3 140,00 €	(5)(1)(a);(5)(1)(b);(5)(1)(f);(6)(1)	UniCredit Bank República Tcheca e Eslováquia	Responsável pelo tratamento	Entidade Privada	Grande
492	República Checa	Office for Personal Data Protection	https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-po-odvolani-souhlasu-spolecnost-alza-cz-a-s/ds-5717/archiv=0&p1=5653	01/06/2019	582,00 €	(6)(1);(7);(12);(29)	Alza.cz as	Responsável pelo tratamento	Entidade Privada	Grande
493	República Checa	Office for Personal Data Protection	https://www.uoou.cz/kontrola-zabezpeceni-osobnich-udaju-pri-provozovani-online-hry-fyzicka-osoba-podnikajici/ds-5723/archiv=0&p1=5653	01/06/2019	980,00 €	(5)(1)(a);(5)(1)(f);(5)(2);(28)(3);(32)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual

494	Dinamarca	Datatilsynet	https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/jun/tilsyn-med-iddesigns-behandling-af-personoplysninger/	12/02/2021	13 450,00 €	(5)(1)(e);(5)(2)	IDdesign A / S	Responsável pelo tratamento	Entidade Privada	Grande
495	Dinamarca	Datatilsynet	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/aug/datatilsynet-indstiller-privatbo-til-boede	04/08/2020	20 100,00 €	(32)	PrivatBo AMBA	Responsável pelo tratamento	Entidade Privada	PME
496	Dinamarca	Datatilsynet	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/jul/arp-hansen-hotel-group-a/s-indstilles-til-boede	28/07/2020	147 800,00 €	(5)(1)(e)	Arp Hansen Hotel Group A / S	Responsável pelo tratamento	Entidade Privada	Grande
497	Dinamarca	Datatilsynet	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/jun/lejre-kommune-indstilles-til-boede	30/06/2020	6 700,00 €	(5);(6);(33);(34)	Município de Lejre	Responsável pelo tratamento	Entidade Pública	Entidade Pública
498	Dinamarca	Datatilsynet	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/maj/jobteam-indstillet-til-boede/	15/05/2020	6 700,00 €	(15)	JobTeam A / S DK	Responsável pelo tratamento	Entidade Privada	PME
499	Dinamarca	Datatilsynet	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/to-kommuner-indstillet-til-boede/	03/10/2020	6 700,00 €	(5)(1)(f);(32)	Município de Hørsholm	Responsável pelo tratamento	Entidade Pública	Entidade Pública
500	Dinamarca	Datatilsynet	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/to-kommuner-indstillet-til-boede/	03/10/2020	13 400,00 €	(5)(1)(f);(32)	Município de Gladsaxe	Responsável pelo tratamento	Entidade Pública	Entidade Pública
501	Dinamarca	Datatilsynet	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/mar/datatilsynet-indstiller-taxaselskab-til-boede-paa-1-2-mio-kr/	01/06/2019	160 000,00 €	(5)(1)(e)	Taxa 4x35	Responsável pelo tratamento	Entidade Privada	Grande
502	Estónia	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)	https://www.aki.ee/et/uudised/andmekaitse-inspektsioon-kohustas-e-apteeke-lopetama-koheselt-ligipaas-teise-inimese	01/12/2020	100 000,00 €	(5);(6)	Apotheka e-apteek	Responsável pelo tratamento	Entidade Privada	PME
503	Estónia	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)	https://www.aki.ee/et/uudised/andmekaitse-inspektsioon-kohustas-e-apteeke-lopetama-koheselt-ligipaas-teise-inimese	01/12/2020	100 000,00 €	(5);(6)	Südameapteegi e-apteek	Responsável pelo tratamento	Entidade Privada	PME
504	Estónia	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)	https://www.aki.ee/et/uudised/andmekaitse-inspektsioon-kohustas-e-apteeke-lopetama-koheselt-ligipaas-teise-inimese	01/12/2020	100 000,00 €	(5);(6)	Azeta.ee e-apteek	Responsável pelo tratamento	Entidade Privada	PME
505	Estónia	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)	https://www.aki.ee/et/uudised/uudishimuparing-toi-vaarteotrahvi	17/08/2020	48,00 €	(5);(6)	Polícia	Responsável pelo tratamento	Pessoa individual	Pessoa individual
506	Estónia	Estonian Data Protection Inspectorate	https://www.aki.ee/sites/default/files/ettekirjutused/2019/ettekirjutus-hoiatus_isikuandmete_kaitse_asjas	30/04/2020	500,00 €	(6)	Associação de Habitação	Responsável pelo tratamento	Entidade Privada	PME

		(Andmekaitse Inspektsioon)	_30.04.2020_nr_2.1.-6-20-19_korteriuhistu_outokumpu_19.pdf							
507	Finlândia	Office of the Data Protection Ombudsman	https://tietosuoja.fi/-/yritykselle-seuraamusmaksu-sahkoisen-suoramarkkinoinnin-harjoittamisesta-ilman-ennalta-annettua-suostumusta-ja-rekisteroidyn-oikeuksien-laiminlyonnista	08/05/2020	7 000,00 €	(5);(6)	Acc Consulting Varsinais-Suomi	Responsável pelo tratamento	Entidade Privada	PME
508	Finlândia	Office of the Data Protection Ombudsman	https://tietosuoja.fi/-/tietosuojavaltuutetun-toimiston-seuraamuskollegio-maarasi-hallinnollisen-seuraamusmaksun-useista-puutteista-henkilotietojen-kasittelyssa	29/05/2020	72 000,00 €	(5);(6);(12);(25);(26);(28);(30);(35)	aksi Helsinki Oy	Responsável pelo tratamento	Entidade Privada	PME
509	Finlândia	Office of the Data Protection Ombudsman	https://tietosuoja.fi/-/tietosuojavaltuutetun-toimiston-seuraamuskollegio-maarasi-kolme-seuraamusmaksua-tietosuojarikkomuksista	22/05/2020	100 000,00 €	(12);(13);(14);(15)	Posti Oy	Responsável pelo tratamento	Entidade Privada	Grande
510	Finlândia	Office of the Data Protection Ombudsman	https://tietosuoja.fi/-/tietosuojavaltuutetun-toimiston-seuraamuskollegio-maarasi-kolme-seuraamusmaksua-tietosuojarikkomuksista	22/05/2020	16 000,00 €	(35)	Kymen Vesi Oy	Responsável pelo tratamento	Entidade Privada	PME
511	Finlândia	Office of the Data Protection Ombudsman	https://tietosuoja.fi/-/tietosuojavaltuutetun-toimiston-seuraamuskollegio-maarasi-kolme-seuraamusmaksua-tietosuojarikkomuksista	22/05/2020	12 500,00 €	(5);(6)	Empresa	Responsável pelo tratamento	N/A	N/A
512	França	Commission Nationale de l'Informatique et des Libertés - CNIL	https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant	27/01/2021	150 000,00 €	(32)	Desconhecido	Responsável pelo tratamento	N/A	N/A
513	França	Commission Nationale de l'Informatique et des Libertés - CNIL	https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant	27/01/2021	75 000,00 €	(32)	Desconhecido	Subcontratante	N/A	N/A
514	França	Commission Nationale de l'Informatique et des Libertés - CNIL	https://www.cnil.fr/fr/prospection-commerciale-sanction-de-20-000-euros-lencontre-de-la-societe-nestor	05/01/2021	20 000,00 €	(12);(13)	Nestor SAS	Responsável pelo tratamento	Entidade Privada	PME
515	França	Commission Nationale de l'Informatique et des Libertés - CNIL	https://www.cnil.fr/fr/violations-de-donnees-de-sante-la-cnil-sanctionne-deux-medecins	17/12/2020	3 000,00 €	(32);(33)	Médico	Responsável pelo tratamento	N/A	N/A
516	França	Commission Nationale de l'Informatique et des Libertés - CNIL	https://www.cnil.fr/fr/violations-de-donnees-de-sante-la-cnil-sanctionne-deux-medecins	17/12/2020	6 000,00 €	(32);(33)	Médico	Responsável pelo tratamento	N/A	N/A
517	França	Commission Nationale de l'Informatique et des Libertés - CNIL	https://www.cnil.fr/fr/prospection-commerciale-sanction-publique-lencontre-de-la-societe-performeclic	31/12/2020	7 300,00 €	(5)(1)(c);(5)(1)(e);(14);(21);(28)	Perfomeclic	Responsável pelo tratamento	Entidade Privada	PME

518	França	Commission Nationale de l'Informatique et des Libertés - CNIL	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042564657	18/11/2020	800 000,00 €	(5)(1)(a);(12);(13)	Carrefour Banque	Responsável pelo tratamento	Entidade Privada	Grande
519	França	Commission Nationale de l'Informatique et des Libertés - CNIL	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042563756	18/11/2020	2 250 000,00 €	(5)(1)(e);(12);(13);(15);(17);(21);(32);(33)	Carrefour França	Responsável pelo tratamento	Entidade Privada	Grande
520	França	Commission Nationale de l'Informatique et des Libertés - CNIL	https://www.cnil.fr/fr/spartoo-sanction-de-250-000-euros-et-injonction-sous-astreinte-de-se-conformer-au-rgpd	05/08/2020	250 000,00 €	(5)(1)(c);(5)(1)(e);(13);(32)	Spartoo	Responsável pelo tratamento	Entidade Privada	Grande
521	França	Commission Nationale de l'Informatique et des Libertés - CNIL	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000041537429/	30/01/2020	0,00 €	(5)(1)(c);(12);(13);(14);(21);(31);(44)	Futura Internationale	Responsável pelo tratamento	Entidade Privada	PME
522	França	Commission Nationale de l'Informatique et des Libertés - CNIL	https://www.cnil.fr/fr/active-assurances-sanction-de-180-000-euros-pour-atteinte-la-securite-des-donnees-des-clients	25/07/2019	180 000,00 €	(32)	ACTIVE ASSURANCES	Responsável pelo tratamento	Entidade Privada	Grande
523	França	Commission Nationale de l'Informatique et des Libertés - CNIL	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038629823/	13/06/2019	20 000,00 €	(32)	Empresa	Responsável pelo tratamento	Entidade Privada	PME
524	França	Commission Nationale de l'Informatique et des Libertés - CNIL	https://www.cnil.fr/fr/sergic-sanction-de-400-000eu-pour-atteinte-la-securite-des-donnees-et-non-respect-des-durees-de	06/06/2019	400 000,00 €	(5);(32)	SERGIC	Responsável pelo tratamento	Entidade Privada	Grande
525	França	Commission Nationale de l'Informatique et des Libertés - CNIL	https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc	21/01/2019	50 000 000,00 €	(5);(6);(13);(14)	Google Inc.	Responsável pelo tratamento	Entidade Privada	Grande
526	Grécia	Hellenic Data Protection Authority	https://www.dpa.gr/sites/default/files/2020-12/33_2020.anonym.pdf	29/10/2020	1 000,00 €	(12)(3);(12)(4)	American College of Greece	Responsável pelo tratamento	Entidade Privada	PME
527	Grécia	Hellenic Data Protection Authority	https://www.dpa.gr/sites/default/files/2020-09/30_2020anonym.pdf	26/08/2020	8 000,00 €	(5)(1)	Pessoa privada	Responsável pelo tratamento	Pessoa individual	Pessoa individual
528	Grécia	Hellenic Data Protection Authority	https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-dioikitikoy-prostimoy-se-ypopsifio-boyleyti-gia-paranomi	03/08/2020	3 000,00 €	(15)	Candidato às eleições parlamentares	Responsável pelo tratamento	Entidade Pública	Entidade Pública
529	Grécia	Hellenic Data Protection Authority	https://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=252,140,181,222,128,166,229,159	29/06/2020	5 000,00 €	(5)	New York College SA	Responsável pelo tratamento	Entidade Privada	PME
530	Grécia	Hellenic Data Protection Authority	https://www.dpa.gr/sites/default/files/2020-05/4_2020anonym.pdf	20/03/2020	8 000,00 €	(15);(58)	Centro Modelo para Fala e Educação Especial - Michos Dimitra	Responsável pelo tratamento	Entidade Privada	PME
531	Grécia	Hellenic Data Protection Authority	https://www.dpa.gr/sites/default/files/2020-05/2_2020anonym.pdf	21/02/2020	5 000,00 €	(12)(3);(12)(4)	Public Power Corporation SA	Responsável pelo tratamento	Entidade Privada	Grande
532	Grécia	Hellenic Data Protection Authority	https://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=126,92,211,86,111,236,222,151	13/01/2013	15 000,00 €	(5)(1)(a);(5)(2)	Allseas Marine SA	Responsável pelo tratamento	Entidade Privada	PME
533	Grécia	Hellenic Data Protection Authority	https://www.dpa.gr/sites/default/files/2020-05/44_2019anonym.pdf	19/12/2019	150 000,00 €	(5)(1);(5)(2);(6)(1)	Aegean Marine Petroleum Network Inc.	Responsável pelo tratamento	Entidade Privada	Grande

534	Grécia	Hellenic Data Protection Authority	https://www.dpa.gr/sites/default/files/2019-12/38_2019anonym%20%281%29.pdf	18/10/2019	20 000,00 €	(21)	Wind Hellas Telecommunications	Responsável pelo tratamento	Entidade Privada	Grande
535	Grécia	Hellenic Data Protection Authority	https://www.dpa.gr/sites/default/files/2019-12/31_2019anonym%20%281%29.pdf	07/10/2019	200 000,00 €	(5)(1)(c);(25)	Provedor de serviços de telecomunicações	Responsável pelo tratamento	Entidade Privada	Grande
536	Grécia	Hellenic Data Protection Authority	https://www.dpa.gr/sites/default/files/2019-12/34_2019anonym%20%281%29.pdf	07/10/2019	200 000,00 €	(21);(25)(1)	Provedor de serviços de telecomunicações	Responsável pelo tratamento	Entidade Privada	Grande
537	Grécia	Hellenic Data Protection Authority	https://www.dpa.gr/el/enimerwtiko/deltia/deltio-typoy-shetika-me-tin-askisi-diorthotikon-exoysion-tis-arhis-basei-toy	30/07/2019	150 000,00 €	(5)(1);(5)(2);(6)(1)	PWC Business Solutions	Responsável pelo tratamento	Entidade Privada	Grande
538	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2020-2729-15-hatarozat.pdf	14/10/2020	1 940,00 €	(5)(1)(b);(5)(1)(c);(13)(1)	Desconhecido	Responsável pelo tratamento	Entidade Privada	N/A
539	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2020-0066-21-hatarozat.pdf	09/12/2020	55 400,00 €	(25)(1);(25)(2);(32)(1)(b);(34)(1)	Robinson Tours Ltd.	Responsável pelo tratamento	Entidade Privada	PME
540	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2020-0066-21-hatarozat.pdf	09/12/2020	1 385,00 €	(32)(1)	Next Time Media Ügynökség Kft.	Subcontratante	Entidade Privada	PME
541	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/hatarozatok-vegzesek?download=326:babavaro-kolcsonnel-osszefuggesben-vegzett-adatkezeles-varandosgondozasi-konyvekrol-valo-masolatkeszites-jogszerusege	16/12/2020	97 150,00 €	(5)(1)(b);(5)(1)(c);(6)(1);(9);(12)(1)	Desconhecido	Responsável pelo tratamento	N/A	N/A
542	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://naih.hu/hatarozatok-vegzesek?download=325:1-rendszeres-szocialis-osztondijakkal-kapcsolatos-adatkezeles-a-budapesti-muszaki-es-gazdasagtudomanyi-egyetemen-modositasokkal-egyseges-szerkezetben	10/12/2020	22 200,00 €	(5)(1)(a);(5)(1)(b);(5)(1)(c);(6)(1);(9)(2);(12)(1);(13)	Budapesti Műszaki és Gazdaságtudományi Egyetem	Responsável pelo tratamento	Entidade Pública	Entidade Pública
543	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2020-3479-hatarozat.pdf	18/11/2020	28,00 €	(5)(1)(d);(16)	Desconhecido	Responsável pelo tratamento	N/A	N/A
544	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2020-2204-8-hatarozat.pdf	23/10/2020	55 400,00 €	(12)(4);(15)(1);(18)(1)(c)	Deichmann	Responsável pelo tratamento	Entidade Privada	Grande
545	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2020-1154-9-hatarozat.pdf	23/07/2020	5 419,00 €	(5)(1)(a);(5)(2);(6)(1)(f);(12)(1);(12)(4);(14);(15);(21)(4)	Forbes Hungria	Responsável pelo tratamento	Entidade Privada	Grande

546	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2020-193-hatarozat.pdf	23/07/2020	1 620,00 €	(5)(1)(d);(6)(1);(12);(13);(17)(1)	Desconhecido	Responsável pelo tratamento	N/A	N/A
547	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2020-5553-hatarozat.pdf	16/07/2020	28,00 €	(15)(3)	Google Ireland Ltd.	Responsável pelo tratamento	Entidade Privada	Grande
548	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2020-1160-10-hatarozat.pdf	18/05/2020	288 000,00 €	(5)(1)(b);(5)(1)(e);(32)(1);(32)(2)	Digi Távközlési Szolgáltató Kft.	Responsável pelo tratamento	Entidade Privada	Grande
549	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2020-32-4-hatarozat.pdf	04/03/2020	270,00 €	(5)(1)(a);(5)(1)(b);(5)(1)(c);(6)(1);(12)(1);(12)(2);(12)(3);(12)(4);(12)(5);(15)(1);(17)(1)	Banco	Responsável pelo tratamento	Entidade Privada	Grande
550	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2020-200-hatarozat.pdf	19/03/2020	5 800,00 €	(6);(15)	Empresa Desconhecida	Responsável pelo tratamento	N/A	N/A
551	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2020-2555-hatarozat.pdf	09/03/2020	870,00 €	(6)(1)	Empresa Desconhecida	Responsável pelo tratamento	N/A	N/A
552	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2020-32-4-hatarozat.pdf	04/03/2020	290,00 €	(5)(1)(a);(5)(1)(b);(5)(1)(c);(6)(1);(12)(1);(12)(2);(12)(3);(12)(4);(12)(5);(15)(1);(17)(1)	Representante de um governo local	Responsável pelo tratamento	N/A	N/A
553	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2020-1137-hatarozat.pdf	24/01/2020	1 450,00 €	(24)(1);(24)(2);(32)(1)	Empresa de contabilidade	Responsável pelo tratamento	Entidade Privada	N/A
554	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://naih.hu/files/NAIH-2019-51-hatarozat.pdf	11/12/2019	1 430,00 €	(5);(6);(13);(24);(25)	Empresa Desconhecida	Responsável pelo tratamento	N/A	N/A
555	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2019-2485-hatarozat.pdf	24/10/2019	7 400,00 €	(24)(1);(24)(2);(32)(1);(33)(1)	Hospital militar	Responsável pelo tratamento	Entidade Pública	Entidade Pública
556	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2019-769-hatarozat.pdf	15/10/2019	2 860,00 €	(5);(6);(13);(24);(25)	Empresa Desconhecida	Responsável pelo tratamento	N/A	N/A
557	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2019-2076-hatarozat.pdf	01/06/2019	15 100,00 €	(6)(1)	Cidade de Kerepes	Responsável pelo tratamento	Entidade Pública	Entidade Pública
558	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2019-1590-hatarozat.pdf	08/08/2019	1 715,00 €	(5);(14)	Escritório do governo	Responsável pelo tratamento	Entidade Pública	Entidade Pública
559	Hungria	Hungarian National Authority for Data	https://www.naih.hu/files/NAIH_2019_2466_hatarozat.pdf	02/08/2019	4 290,00 €	(5);(6);(13)	Empresa de manutenção de áreas públicas	Responsável pelo tratamento	N/A	N/A

		Protection and Freedom of Information								
560	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2019-2472_hatarozat.pdf	17/07/2019	8 575,00 €	(5)(1)(b);(6)	Tribunal Regional de Environs de Budapeste	Responsável pelo tratamento	Entidade Pública	Entidade Pública
561	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2019-2402_hatarozat.pdf	26/06/2019	2 850,00 €	(5);(6);(17)	Desconhecido	Responsável pelo tratamento	N/A	N/A
562	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH_2019_1837_hatarozat.pdf	26/06/2019	2 850,00 €	(5);(6);(21)	Empresa Financeira	Responsável pelo tratamento	Entidade Privada	N/A
563	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2019-2471-hatarozat.pdf	25/06/2019	15 150,00 €	(33)(1)	Desconhecido	Responsável pelo tratamento	N/A	N/A
564	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH_2019_1598_hatarozat.pdf	03/06/2019	2 850,00 €	(5)(1)(a);(5)(1)(b);(6)(1)	Empresa de gestão de reclamações	Responsável pelo tratamento	N/A	N/A
565	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH_2019_1859_hatarozat.pdf	31/05/2019	2 000,00 €	(12)(3);(12)(4);(12)(5);(15);(18)	Banco local	Responsável pelo tratamento	N/A	N/A
566	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2019-55_hatarozat.pdf	23/05/2019	92 146,00 €	(5)(1)(b);(6);(13)	Organizador do festival SZIGET e do festival VOLT	Responsável pelo tratamento	N/A	N/A
567	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2019-3854_hatarozat.pdf	21/05/2019	286,00 €	(33)(1)	Instituições Sociais e de Bem-Estar Infantil do Distrito Ferencvaros de Budapeste	Responsável pelo tratamento	Entidade Pública	Entidade Pública
568	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2019-167-hatarozat.pdf	17/04/2019	9 400,00 €	(5)(1)(a);(6)	Desconhecido	Responsável pelo tratamento	N/A	N/A
569	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/hatarozatok-vegzesek?download=159:hozzaferesi-jog-gyakorlasara-iranyulo-kerelem-teljesitese	05/04/2019	34 375,00 €	(33)(1);(33)(5);(34)(1)	Partido político húngaro	Responsável pelo tratamento	Entidade Pública	Entidade Pública
570	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH_2019_133_hatarozat.pdf	05/04/2019	1 900,00 €	(15)	Desconhecido	Responsável pelo tratamento	N/A	N/A
571	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2019-2526-2-H-hatarozat.pdf	04/03/2019	3 200,00 €	(5)(1)(b);(5)(1)(c);(6)(4);(13)(3);(17)(1)	Instituição financeira	Responsável pelo tratamento	Entidade Privada	Grande
572	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2019-596-hatarozat.pdf	28/02/2019	3 200,00 €	(5)(1)(a);(6)	Município de Kecdkemét	Responsável pelo tratamento	Entidade Pública	Entidade Pública

573	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2019-1841_hatarozat.pdf	20/02/2019	1 560,00 €	(5)(1)(a);(5)(1)(c)	Desconhecido	Responsável pelo tratamento	N/A	N/A
574	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2019_363_hatarozat.pdf	08/02/2019	1 560,00 €	(5)(1)(d)	Banco	Responsável pelo tratamento	Entidade Privada	Grande
575	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/files/NAIH-2018-5559-H-hatarozat.pdf	21/12/2018	3 200,00 €	(12)(4);(13);(15);(18)(1)(c)	Desconhecido	Responsável pelo tratamento	N/A	N/A
576	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/hatarozatok-vegzesek?download=172:khr-ben-szereplo-szemelyes-adatok-torlese-iranti-kerelem-elutasitasa	18/06/2019	1 354,00 €	(12)(2);(15)	Desconhecido	Responsável pelo tratamento	N/A	N/A
577	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/hatarozatok-vegzesek/birosagi-jogorvoslatok?download=337:masodfoku-itelet-a-naih-2019-2485-sz-ugyben-kuria-kfv-ii-37-701-2020-5	22/10/2019	2 167,00 €	(5);(6)(1)	Desconhecido	Responsável pelo tratamento	N/A	N/A
578	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/hatarozatok-vegzesek/birosagi-jogorvoslatok?download=341:itelet-a-naih-2019-3107-sz-ugyben-fovarosi-torvenyszek-106-k-700-570-2019-24	11/11/2019	4 064,00 €	(5)(1)(a)	Desconhecido	Responsável pelo tratamento	N/A	N/A
579	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/hatarozatok-vegzesek?download=193:hozzaferesi-jog-megsertese-masolasi-dij-jogellenes-megallapitasa	15/11/2019	67 740,00 €	(6)(1);(12)(1);(13)(1)	RaiffeisenBank Zrt.	Responsável pelo tratamento	Entidade Privada	Grande
580	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/hatarozatok-vegzesek?download=211:a-digitavkozlesi-es-szolgaltato-kft-nel-bekovetkezett-adatvedelmi-incidensben-erintett-adatbazisok-celhoz-kotottseggel-korlatozott-tarolhatosaggal-es-adatbiztonsaggal-kapcsolatos-hianyossagai	27/04/2020	20 322,00 €	(32)(1)(b);(33)(1);(34)(1)	Hungária Med-M	Responsável pelo tratamento	Entidade Pública	Entidade Pública
581	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/hatarozatok-vegzesek?download=213:szakertoi-vizsgalat-soran-keletkezett-hangfelvetel-masolatanak-kiadasa-kiskoru-vizsgalata-soran-keletkezett-hangfelvetel-vonatkozasaban-is	28/05/2020	2 709,00 €	(5)(1)(b);(5)(1)(c);(15)(1);(15)(2);(15)(3)	Desconhecido	Responsável pelo tratamento	N/A	N/A
582	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/hatarozatok-vegzesek?download=218:szemelyes-adatok-koveteleskezelesi-celu-kezelesenek-jogalapja	16/07/2020	2 709,00 €	(5)(1)(a);(5)(2);(21)(4)	Desconhecido	Responsável pelo tratamento	N/A	N/A
583	Hungria	Hungarian National Authority for Data	https://www.naih.hu/hatarozatok-vegzesek?download=221:adatpont	17/07/2020	1 354,00 €	(5)(1)(a);(5)(1)(b);(6);(13)(1);(13)(2)	Desconhecido	Responsável pelo tratamento	N/A	N/A

		Protection and Freedom of Information	ossag-elve-szemelyes-adatok-tovabbitasa							
584	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/hatarozatok-vegzesek?download=291:engedmenyezes-utan-kezelt-telefonszam-es-e-mail-cim	06/08/2020	5 419,00 €	(5)(1)(d);(6)(1);(14)(1)(c);(15)(1)(f);(15)(1)(g);(18)(1)(a)	Desconhecido	Responsável pelo tratamento	N/A	N/A
585	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/hatarozatok-vegzesek?download=324:az-ugyintezes-folyamatarol-valo-hangfelvetel-keszites-a-upc-szemelyes-ugyfelfogadasra-alkalmas-irodaiban	03/09/2020	1 354,00 €	(12);(15);(18)(1)(c)	Desconhecido	Responsável pelo tratamento	N/A	N/A
586	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/hatarozatok-vegzesek?download=231:pontossag-elvenek-megsertese	29/09/2020	162 578,00 €	(5)(1)(a);(5)(1)(b);(5)(1)(c);(6)(1);(12)(1);(13)	UPCHungria Telecommunications Limited Liability Company	Responsável pelo tratamento	Entidade Privada	Grande
587	Hungria	Hungarian National Authority for Data Protection and Freedom of Information	https://www.naih.hu/hatarozatok-vegzesek?download=227:a-tajekoztatashoz-es-a-hozzafereshez-fuzodo-erintetti-jogok-es-az-atlathatosag-serelme	05/10/2020	1 625,00 €	(5)(1)	Desconhecido	Responsável pelo tratamento	N/A	N/A
588	Islândia	Persónuvernd	https://www.personuvernd.is/personuvernd/frettir/oryggisbrestur-hja-saa-sektarakvordun-1	03/10/2020	20 600,00 €	(5)(1)(f);(32)	Centro Nacional de Medicina do Vício ('SAA')	Responsável pelo tratamento	Entidade Pública	Entidade Pública
589	Islândia	Persónuvernd	https://www.personuvernd.is/personuvernd/frettir/oryggisbrestur-hja-fjolbrautaskolanum-i-breidholti-sektarakvordun	03/10/2020	9 000,00 €	(5)(1)(f);(32)	Breiðholt Upper Secondary School	Responsável pelo tratamento	Entidade Pública	Entidade Pública
590	Irlanda	Data Protection Commission	https://www.dataprotection.ie/sites/default/files/uploads/2021-02/Inquiry%20University%20College%20Dublin_0.pdf	17/12/2020	70 000,00 €	(5)(1)(e);(5)(1)(f);(32)(1);(33)(1)	University College Dublin	Responsável pelo tratamento	Entidade Pública	Entidade Pública
591	Irlanda	Data Protection Commission	https://edpb.europa.eu/sites/edpb/files/decisions/final_decision_-_in-19-1-1_9.12.2020.pdf	15/12/2020	450 000,00 €	(33)(1);(33)(5)	Twitter International Company	Responsável pelo tratamento	Entidade Privada	Grande
592	Irlanda	Data Protection Commission	https://www.irishexaminer.com/news/arid-40075673.html	18/08/2020	65 000,00 €	(5)(1)(f);(32)(1)	Cork University Maternity Hospital	Responsável pelo tratamento	Entidade Pública	Entidade Pública
593	Irlanda	Data Protection Commission	https://www.dataprotection.ie/sites/default/files/uploads/2021-02/12.08.2020_Decision_Tusla_IN-18-11-04.pdf	12/08/2020	85 000,00 €	(32)(1)	Agência Tusla para Crianças e Famílias	Responsável pelo tratamento	Entidade Pública	Entidade Pública
594	Irlanda	Data Protection Commission	https://www.dataprotection.ie/sites/default/files/uploads/2021-02/21.05.2020_Decision_IN-19-12-8_Tusla.pdf	30/06/2020	40 000,00 €	(32)(1);(33)(1)	Agência Tusla para Crianças e Famílias	Responsável pelo tratamento	Entidade Pública	Entidade Pública
595	Irlanda	Data Protection Commission	https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-fine-tusla-child-and-family-agency-confirmed-court	17/05/2020	75 000,00 €	(32)(1);(33)(1)	Agência Tusla para Crianças e Famílias	Responsável pelo tratamento	Entidade Pública	Entidade Pública
596	Letónia	Data State Inspectorate	https://www.dvi.gov.lv/lv/media/273/download	09/02/2021	65 000,00 €	(5)(1)(a);(5)(1)(b);(5)(1)(c);(6)(1)	Lursoft IT SIA	Responsável pelo tratamento	Entidade Privada	PME

597	Letónia	Data State Inspectorate	https://www.dvi.gov.lv/lv/media/271/download	26/11/2020	15 000,00 €	(5)(1)(a);(5)(2);(12)(1);(13)	HH Invest SIA	Responsável pelo tratamento	Entidade Privada	PME
598	Letónia	Data State Inspectorate	https://www.dvi.gov.lv/lv/media/269/download	15/09/2020	6 250,00 €	(5)(1)	Desconhecido	Responsável pelo tratamento	N/A	N/A
599	Letónia	Data State Inspectorate	https://www.dvi.gov.lv/lv/media/275/download	08/11/2019	150 000,00 €	(13)	sia shopping service	Responsável pelo tratamento	Entidade Privada	PME
600	Letónia	Data State Inspectorate	https://www.dvi.gov.lv/lv/jaunums/datu-valsts-inspekcija-piemero-7000-eiro-lielu-naudas-sodu-internetveikalam-par-personas-datu-apstrades-parkapumiem	29/08/2019	7 000,00 €	(17)	Serviços online	Responsável pelo tratamento	Entidade Privada	N/A
601	Letónia	Data State Inspectorate	https://www.dvi.gov.lv/lv/media/889/download	15/06/2020	200,00 €	(5);(6);(7);(9)	Serviços públicos	Responsável pelo tratamento	N/A	N/A
602	Letónia	Data State Inspectorate	https://www.dvi.gov.lv/lv/media/895/download	15/06/2020	2 964,20 €	(58)(1)(e)	VVV Auto	Responsável pelo tratamento	Entidade Privada	PME
603	Letónia	Data State Inspectorate	https://www.dvi.gov.lv/lv/media/897/download	19/06/2020	600,60 €	(58)(1)(e)	restaurante SIA KINKI	Responsável pelo tratamento	Entidade Privada	PME
604	Lituânia	State Data Protection Inspectorate	https://vdai.lrv.lt/lt/naujienos/skirta-bauda-del-bendrojo-duomenu-apsaugos-reglamento-pazeidimu-registru-centre	02/03/2021	15 000,00 €	(32)(1)(b);(32)(1)(c)	SE Register Center	Responsável pelo tratamento	Entidade Pública	Entidade Pública
605	Lituânia	State Data Protection Inspectorate	https://vdai.lrv.lt/lt/naujienos/skirta-bauda-del-bendrojo-duomenu-apsaugos-reglamento-pazeidimu-programeleje-karantinas	26/02/2021	12 000,00 €	(5);(13);(24);(32);(35);(58)(2)(f)	Centro Nacional de Saúde Pública (NVSC)	Responsável pelo tratamento	Entidade Pública	Entidade Pública
606	Lituânia	State Data Protection Inspectorate	https://vdai.lrv.lt/lt/naujienos/skirta-bauda-del-bendrojo-duomenu-apsaugos-reglamento-pazeidimu-programeleje-karantinas	26/02/2021	3 000,00 €	(5);(13);(24);(32);(35)	UAB IT Solutions Success	Responsável pelo tratamento	Entidade Privada	PME
607	Lituânia	State Data Protection Inspectorate	https://vdai.lrv.lt/lt/naujienos/pagal-bendraji-duomenu-apsaugos-reglamenta-skirta-bauda-del-netinkamai-tvarkomu-ivaikinto-vaiko-tevu-asmens-duomenu	28/09/2020	15 000,00 €	(5)(1)(d);(5)(1)(f)	Município de Vilnius	Responsável pelo tratamento	Entidade Pública	Entidade Pública
608	Lituânia	State Data Protection Inspectorate	https://www.ada.lt/go.php/lit/Imones-atsakomybes-neisvengs--lietuvoje-skirta-zenkli-bauda-uz-bendrojo-duomenu-apsaugos-reglamento-pazeidimus-/1	16/05/2019	61 500,00 €	(5);(32);(33)	UAB MisterTango	Responsável pelo tratamento	Entidade Privada	Grande
609	Malta	Office of the Information and Data Protection Commissioner	https://idpc.org.mt/decisions/	18/02/2019	5 000,00 €	(5)(1)(f);(32)(1)(b)	Desconhecido	Responsável pelo tratamento	N/A	N/A
610	Malta	Office of the Information and Data Protection Commissioner	https://idpc.org.mt/decisions/	01/06/2019	2 500,00 €	(32)(1)(b)	Desconhecido	Responsável pelo tratamento	N/A	N/A
611	Malta	Office of the Information and Data Protection Commissioner	https://idpc.org.mt/decisions/	01/06/2019	2 500,00 €	(32)(1)(b)	Desconhecido	Responsável pelo tratamento	N/A	N/A

612	Malta	Office of the Information and Data Protection Commissioner	https://idpc.org.mt/decisions/	01/06/2019	2 000,00 €	(32)(1)(b)	Desconhecido	Responsável pelo tratamento	N/A	N/A
613	Malta	Office of the Information and Data Protection Commissioner	https://idpc.org.mt/decisions/	01/06/2019	2 500,00 €	(5)(1)(f);(32)(1)(b)	Desconhecido	Responsável pelo tratamento	N/A	N/A
614	Malta	Office of the Information and Data Protection Commissioner	https://idpc.org.mt/decisions/	01/06/2019	15 000,00 €	(6);(7);(21)	Desconhecido	Responsável pelo tratamento	N/A	N/A
615	Malta	Office of the Information and Data Protection Commissioner	https://idpc.org.mt/decisions/	01/06/2019	20 000,00 €	(13);(15)	Desconhecido	Responsável pelo tratamento	N/A	N/A
616	Malta	Office of the Information and Data Protection Commissioner	https://idpc.org.mt/decisions/	01/06/2019	4 000,00 €	(13);(15)	Desconhecido	Responsável pelo tratamento	N/A	N/A
617	Malta	Office of the Information and Data Protection Commissioner	https://idpc.org.mt/decisions/	01/06/2019	3 000,00 €	(5)(1);(6)	Desconhecido	Responsável pelo tratamento	N/A	N/A
618	Malta	Office of the Information and Data Protection Commissioner	https://idpc.org.mt/decisions/	01/06/2019	3 000,00 €	(5)(1)(f);(32)(1)(b)	Desconhecido	Responsável pelo tratamento	N/A	N/A
619	Malta	Office of the Information and Data Protection Commissioner	https://idpc.org.mt/decisions/	01/06/2019	5 000,00 €	(12)(3);(15)(3)	Desconhecido	Responsável pelo tratamento	N/A	N/A
620	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://www.uodo.gov.pl/decyzje/DKN.5130.2024.2020	11/02/2021	22 200,00 €	(5)(1)(f);(25)(1);(28)(3);(32)(1);(32)(2)	Ministério Público	Responsável pelo tratamento	Entidade Pública	Entidade Pública
621	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/DKE.561.16.2020	05/01/2021	4 600,00 €	(31);(58)(1)(a)	Anwara Sp. jardim zoológico	Responsável pelo tratamento	Entidade Pública	Entidade Pública
622	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://www.uodo.gov.pl/decyzje/DKN.5131.7.2020	11/01/2021	30 000,00 €	(33)(1)	Enea SA	Responsável pelo tratamento	Entidade Privada	Grande
623	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/DKN.5131.6.2020	05/01/2021	5 500,00 €	(33)(1);(34)(1)	Śląski Uniwersytet Medyczny	Responsável pelo tratamento	Entidade Pública	Entidade Pública
624	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/DKE.561.11.2020	05/01/2021	19 000,00 €	(34)(1);(34)(2);(58)(2)(e)	Desconhecido	Responsável pelo tratamento	N/A	N/A
625	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/DKN.5131.5.2020	28/12/2020	18 930,00 €	(33)(1);(34)(1)	Towarzystwo Ubezpieczeń i Reasekuracji WARTA SA	Responsável pelo tratamento	Entidade Privada	Grande
626	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/DKN.5130.1354.2020	17/12/2020	235 300,00 €	(5)(1)(f);(25)(1);(32)(1)(b);(32)(1)(d);(32)(2)	ID Finance Polônia Sp. z oo	Responsável pelo tratamento	Entidade Privada	Grande

627	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://www.uodo.gov.pl/decyzje/DKN.5112.1.2020	03/12/2020	443 000,00 €	(5)(1)(f);(5)(2);(25)(1);(32)(1)(b);(32)(1)(d);(32)(2)	Virgin Mobile Polska	Responsável pelo tratamento	Entidade Privada	Grande
628	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/DKN.5131.5.2020	09/12/2020	18 850,00 €	(33)(1);(34)(1)	TUiR Warta SA	Responsável pelo tratamento	Entidade Privada	Grande
629	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://www.uodo.gov.pl/decyzje/DKE.561.13.2020%20	09/12/2020	2 850,00 €	(31);(58)(1)(e)	Smart Cities Sp. z oo	Responsável pelo tratamento	Entidade Privada	PME
630	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://www.uodo.gov.pl/decyzje/ZSO%C5%9AS.421.25.2019	21/08/2020	11 200,00 €	(5)(1)(e);(5)(2);(25)(1);(32)(1)(b);(32)(1)(d);(32)(2);(38)(1);(39)(1);(39)(2)	Universidade de Ciências da Vida de Varsóvia	Responsável pelo tratamento	Entidade Pública	Entidade Pública
631	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/DKN.5112.13.2020	24/08/2020	22 700,00 €	(5)(1);(6)(1)	Sede de Geodésia e Cartografia	Responsável pelo tratamento	Entidade Pública	Entidade Pública
632	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/DKE.561.3.2020	02/07/2020	22 300,00 €	(31);(58)(1)(e);(58)(1)(f)	Escritório de geodésia e cartografia	Responsável pelo tratamento	Entidade Pública	Entidade Pública
633	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/DKE.561.1.2020	29/05/2020	3 505,00 €	(58)(1)(e)	East Power Sp. z oo	Responsável pelo tratamento	Entidade Privada	PME
634	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/DKE.561.2.2020	03/06/2020	1 168,00 €	(31);(58)(1)(e)	Pessoa individual	Responsável pelo tratamento	Pessoa individual	Pessoa individual
635	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/ZSPR.421.19.2019	09/03/2020	4 673,00 €	(31);(58)(1)(e);(58)(1)(f)	Vis Consulting Sp. z oo	Responsável pelo tratamento	Entidade Privada	PME
636	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	http://orzeczenia.nsa.gov.pl/doc/2A2CFDE9D2	18/02/2020	0,00 €	(5);(9)	Município de Gdansk	Responsável pelo tratamento	Entidade Pública	Entidade Pública
637	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	http://orzeczenia.nsa.gov.pl/doc/942DE6198F	01/11/2019	1 770,00 €	(5)(1)(a);(5)(1)(f)	L. Sp. z oo	Responsável pelo tratamento	Entidade Privada	PME
638	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/ZSPU.421.3.2019	18/10/2019	9 380,00 €	(5)(1)(a);(5)(1)(e);(5)(1)(f);(5)(2);(28);(30)(1)(d);(30)(1)(f);(32)	Major de Aleksandrów Kujawski	Responsável pelo tratamento	Entidade Pública	Entidade Pública
639	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/ZSPR.421.7.2019	16/10/2019	47 000,00 €	(5)(1)(a);(6)(1);(7)(3);(12)(2);(17)(1)(b);(24)(1)	ClickQuickNow	Responsável pelo tratamento	Entidade Privada	PME
640	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/ZSPR.421.2.2019	10/09/2019	610 690,00 €	(5)(1)(a);(5)(2);(6)(1);(7)(1);(24)(1);(25)(1);(32)(1)(b);(32)(1)(d);(32)(2)	Morele.net	Responsável pelo tratamento	Entidade Privada	Grande
641	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/ZSPR.440.43.2019	25/04/2019	13 000,00 €	(5)(1);(32)(1);(32)(2)	Associação desportiva	Responsável pelo tratamento	Entidade Privada	PME
642	Polónia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/decyzje/ZSPR.440.43.2019	26/03/2019	203 563,00 €	(14)(1);(14)(2)	Empresa	Responsável pelo tratamento	Entidade Privada	N/A
643	Eslováquia	Office for Personal Data Protection of the Slovak Republic	https://dataprotection.gov.sk/uoou/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_obdobie_25.maj_2018_az_24_maj_2019.pdf	01/03/2019	3 489,00 €	(15)	Desconhecido	Responsável pelo tratamento	N/A	N/A

644	Eslováquia	Office for Personal Data Protection of the Slovak Republic	https://dataprotection.gov.sk/uoou/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_obdobie_25.maj_2018_az_24_maj_2019.pdf	01/03/2019	3 489,00 €	(5)(1)(f);(32)	Desconhecido	Responsável pelo tratamento	N/A	N/A
645	Eslováquia	Office for Personal Data Protection of the Slovak Republic	https://dataprotection.gov.sk/uoou/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_obdobie_25.maj_2018_az_24_maj_2019.pdf	01/03/2019	3 489,00 €	(5)(1)(f);(32)	Desconhecido	Responsável pelo tratamento	N/A	N/A
646	Eslováquia	Office for Personal Data Protection of the Slovak Republic	https://dataprotection.gov.sk/uoou/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_obdobie_25.maj_2018_az_24_maj_2019.pdf	01/03/2019	3 489,00 €	(5)(1)(a);(6)(1)(a)	Desconhecido	Responsável pelo tratamento	N/A	N/A
647	Eslováquia	Office for Personal Data Protection of the Slovak Republic	https://www.trend.sk/spravy/gdpr-zacina-hryzt-znamy-operator-dostal-pokutu-40-tisic-eur	27/09/2019	40 000,00 €	(32)	Slovak Telekom	Responsável pelo tratamento	Entidade Privada	Grande
648	Eslováquia	Office for Personal Data Protection of the Slovak Republic	https://www.trend.sk/spravy/social na-poistovna-porusila-gdpr-rekordnu-pokutu-nechce-zaplatit	13/11/2019	50 000,00 €	(32)	Segurança Social	Responsável pelo tratamento	Entidade Pública	Entidade Pública
649	Holanda	Autoriteit Persoonsgegevens	https://autoriteitpersoonsgegevens.nl/nl/nieuws/ziekenhuis-olvg-beboet-om-onvoldoende-beveiliging-medische-dossiers	11/02/2021	440 000,00 €	(32)	OLVG	Responsável pelo tratamento	Entidade Pública	Entidade Pública
650	Holanda	Autoriteit Persoonsgegevens	https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-bkr-vanwege-kosten-bij-inzage-persoonsgegevens	06/07/2020	830 000,00 €	(12)(1);(12)(2);(12)(5);(15)	Bureau Krediet Registratie (BKR)	Responsável pelo tratamento	Entidade Privada	Grande
651	Holanda	Autoriteit Persoonsgegevens	https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-bedrijf-voor-verwerken-vingerafdrukken-werknemers	30/04/2020	725 000,00 €	(9)	Desconhecido	Responsável pelo tratamento	N/A	N/A
652	Holanda	Autoriteit Persoonsgegevens	https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-tennisbond-vanwege-verkoop-van-persoonsgegevens	03/03/2020	525 000,00 €	(5)(1);(6)(1)	Associação Real Holandesa de Tênis ('KNLTB')	Responsável pelo tratamento	Entidade Privada	PME
653	Holanda	Autoriteit Persoonsgegevens	https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-dwingt-uwv-met-sanctie-gegevens-beter-te-beveiligen	30/10/2019	900 000,00 €	(32)	UWV	Responsável pelo tratamento	Entidade Privada	Grande
654	Holanda	Autoriteit Persoonsgegevens	https://autoriteitpersoonsgegevens.nl/nl/nieuws/sancties-voor-menzis-en-vgz-voor-overtreding-van-de-privacywet	04/11/2019	50 000,00 €	(5);(32)	VGZ e Menzis	Responsável pelo tratamento	Entidade Privada	Grande
655	Holanda	Autoriteit Persoonsgegevens	https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%Abntendossiers	18/06/2019	460 000,00 €	(32)	Haga Hospital	Responsável pelo tratamento	Entidade Pública	Entidade Pública

Anexo 11 – Prova de Conceito junto das PME

Prova de Conceito junto das PME

A presente Prova de Conceito enquadra-se num projeto de dissertação de mestrado em Gestão de Sistemas e Tecnologias da Informação na Atlântica Instituto Universitário, que tem como objetivo apresentar uma Solução para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD, sob a orientação da Professora Doutora Virgínia Araújo.

Destina-se a todas as PME – Pequenas e Médias Empresas, nomeadamente às que participaram no inquérito "Impacto do RGPD nas Organizações". A Prova de Conceito tem um tempo total estimado de 6 horas, por tratamento.

Por definição, uma Prova de Conceito (PoC) é a entrega de um sistema funcional para provar que a tecnologia funciona e funciona conforme pretendido. Geralmente é um processo pequeno e pode incluir todas as funções ou apenas parte das mesmas. Em simultâneo, é um processo que envolve um número relativamente pequeno de utilizadores. No fim do processo, o PoC deve ser dado como concluído, desmontado, caso se aplique, e considerado completo após os resultados terem sido documentados (Government of Newfoundland and Labrador, 2021).

As suas respostas, que são muito importantes para nós, serão usadas apenas para a finalidade da investigação e serão consideradas estritamente confidenciais.

Para esclarecimento de qualquer dúvida acerca desta iniciativa, pode contactar o investigador.

Contacto do Investigador:

Luís Pedroso

e: 201929286@academia.uatlantica.pt | w: http://www.linkedin.com/in/pedrosoluis

Atlântica Instituto Universitário

Departamento de informática

www.uatlantica.pt

FASE 1 – Iniciação – Identificação da PME

4. Nome
5. Morada
6. Telefone de contacto
7. E-mail de contacto

FASE 1 – Iniciação – Identificação do responsável da PME

8. Nome
9. Telefone de contacto
10. E-mail de contacto
11. Função dentro da empresa
    - 8.1 Gestor/a
    - 8.2 Administrativo/a
    - 8.3 Sócio/a
    - 8.4 Proprietário/a
    - 8.5 Diretor/a
    - 8.6 Colaborador/a interno/a
    - 8.7 Colaborador/a externo/a
    - 8.8 Outra, qual?

12. O responsável da PME é também responsável pela implementação do RGPD?
    - 9.1 Sim
    - 9.2 Não

13. Se a resposta anterior foi afirmativa, qual o cargo?
    - 10.1Encarregado de Proteção de Dados (DPO)
    - 10.2Chief Information Security Officer (CISO)
    - 10.3Jurista
    - 10.4Informático/a
    - 10.5Gestor/a da Qualidade
    - 10.6Auditor/a Interno/a
    - 10.7Outro

FASE 1 – Iniciação – Planeamento

14. Proposta de data para reunião

15. Horário proposto

16. Modo de apresentação

17. Lista de contactos (nomes) para a apresentação

18. Lista de contatos (endereço eletrónico) para a apresentação

FASE 2 – Planeamento e Análise – Plano de projeto

2.1 Nome da PME

2.2 Definição do âmbito (ex: máximo 2 tratamentos de dados pessoais)

2.3 Definição da calendarização (datas e duração de cada sessão – ex: 6 horas por tratamento)

2.4 Entregas previstas (ex: preenchimento integral de uma proposta de solução)

2.5 Definição de prazos de concretização da iniciativa (ex: data início e data fim. A data fim deve ocorrer no máximo no mês de maio de 2021)

FASE 2 – Planeamento e Análise – Plano de recursos

2.6 Nome do/a gestor/a do projeto

2.7 Endereço eletrónico do/a gestor/a do projeto

2.8 Função dentro da organização do/a gestor/a do projeto

- 8.1 Gestor/a
- 8.2 Administrativo/a
- 8.3 Sócio/a
- 8.4 Proprietário/a
- 8.5 Diretor/a
- 8.6 Colaborador/a interno/a
- 8.7 Colaborador/a externo/a
- 8.8 Outra, qual?

2.9 Definição da equipa de projeto (ex: pessoa responsável pelo tratamento de dados, diretor/a responsável, responsável TI, responsável jurídico, Encarregado de Proteção de Dados, etc.)

2.10 Partes interessadas no PoC (ex: prestadores de serviços, fornecedores, instituições púbicas, etc.)

2.11 Definição das sessões (ex: presencial, remoto, misto)

2.12 Declaro que concordo em não utilizar de forma alguma a informação confidencial no âmbito deste PoC, fabricar ou testar qualquer produto que incorpore esta informação confidencial, exceto para os fins autorizados pelos seus autores

- 12.1 Aceito as condições do PoC

FASE 3 – Fecho do Projeto

Na fase de conclusão do PoC, o gestor do projeto, consultando a equipa de projeto, finaliza as entregas. A avaliação do PoC deverá ser escrita, e deve incluir toda a documentação necessária. A sua concretização não deverá demorar mais de 10 dias úteis após a concretização do mesmo. Proposta de data fim: 31 de maio de 2021.

1.18.1 A proposta de apresentação do PoC à PME foi satisfatória?
- 1.1 Sim
- 1.2 Não

1.18.2 Comentários sobre a pergunta anterior (apresentação do PoC)

1.18.3 Que lições foram aprendidas com o PoC?

1.18.4 A definição do âmbito foi ajustada ao PoC?

1.18.5 Comentários sobre a pergunta anterior (definição do âmbito)

1.18.6 Os prazos definidos foram cumpridos?

1.18.7 Comentários sobre a pergunta anterior (prazos)

1.18.8 A duração do PoC foi satisfatória?

1.18.9 Comentários sobre a pergunta anterior (duração)

1.18.10 A alocação de recursos foi ajustada às necessidades?

1.18.11 Comentários sobre a pergunta anterior (alocação de recursos)

1.18.12 As entregas previstas foram cumpridas?
- 12.1 Sim
- 12.2 Não

2.13 Comentários sobre a pergunta anterior (entregas)

2.14 Gostava de ter esta solução implementada em toda a organização?
- 14.1 Sim
- 14.2 Não

2.15 Comentários sobre a pergunta anterior (implementação)

FASE 3 – Fecho do Projeto – propostas de melhoria da Solução para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD

2.16 Etapa de Avaliação do risco

2.17 Etapa de Tratamento do risco

2.18 Etapa de Aceitação do risco

2.19 Etapa de Comunicação do risco

2.20 Nível global de satisfação do PoC
- 20.1 Muito bom
- 20.2 Bom
- 20.3 Suficiente
- 20.4 Insuficiente
- 20.5 Muito insuficiente

2.21 Outras recomendações sobre como proceder numa implementação completa no contexto da organização

2.22 Comentários finais

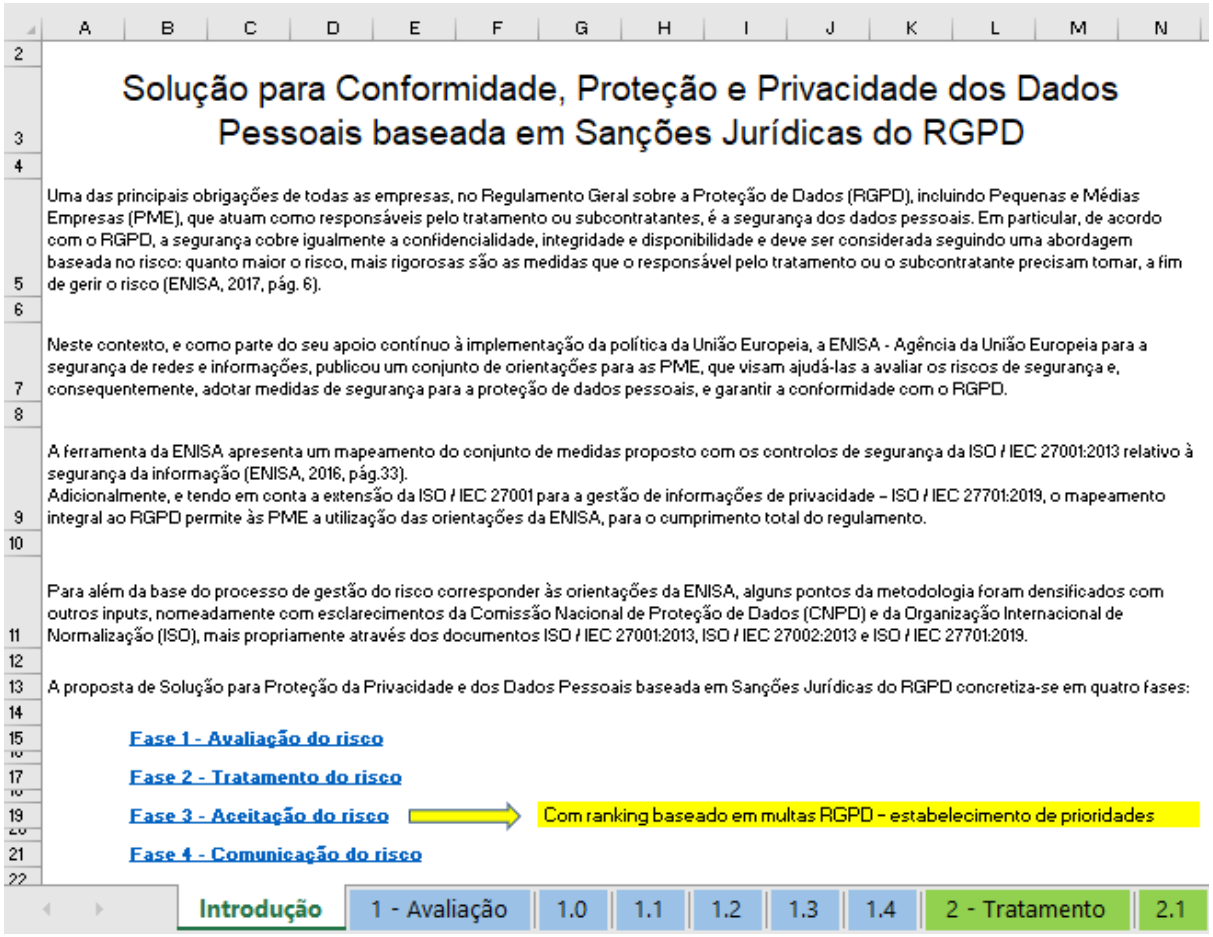
2.23 Data de submissão

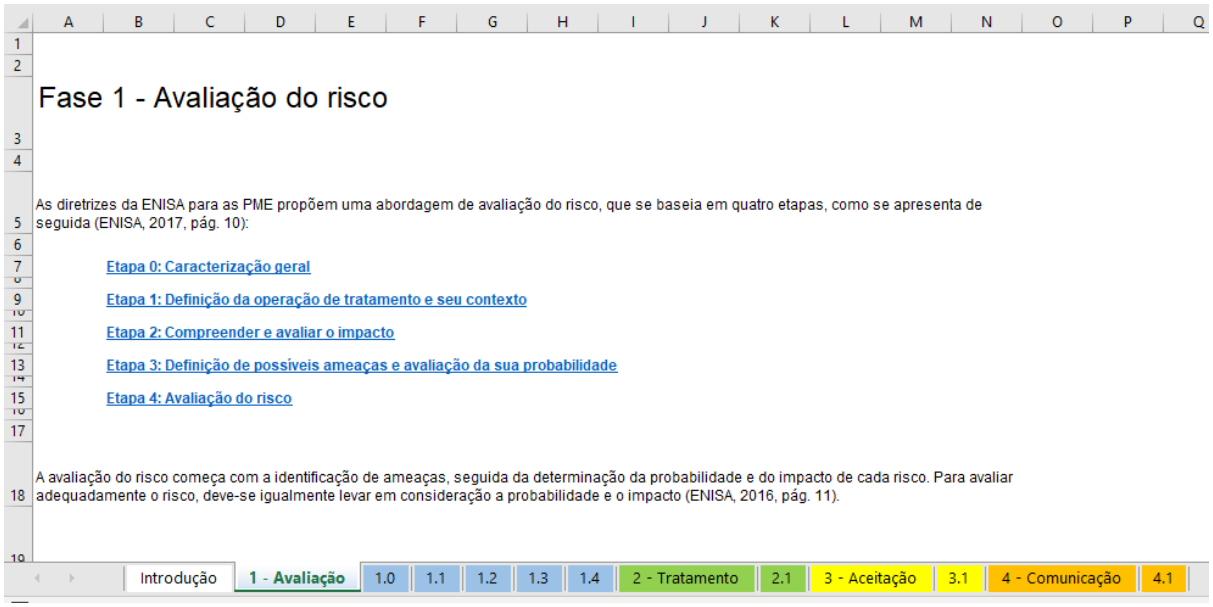
Anexo 12 – Modelo desenvolvido para a concretização do PoC

Modelo desenvolvido para a concretização do PoC

A Solução proposta para Conformidade, Proteção e Privacidade dos Dados Pessoais baseada em Sanções Jurídicas do RGPD (conjunto das quatro etapas do ponto 4.1.1, a saber: avaliação do risco, tratamento do risco, aceitação do risco e comunicação do risco) foi apresentada a cada PME em reunião de início de projeto, e disponibilizada em ficheiro próprio, em formato Excel.

Exemplos do modelo desenvolvido para a concretização do PoC:





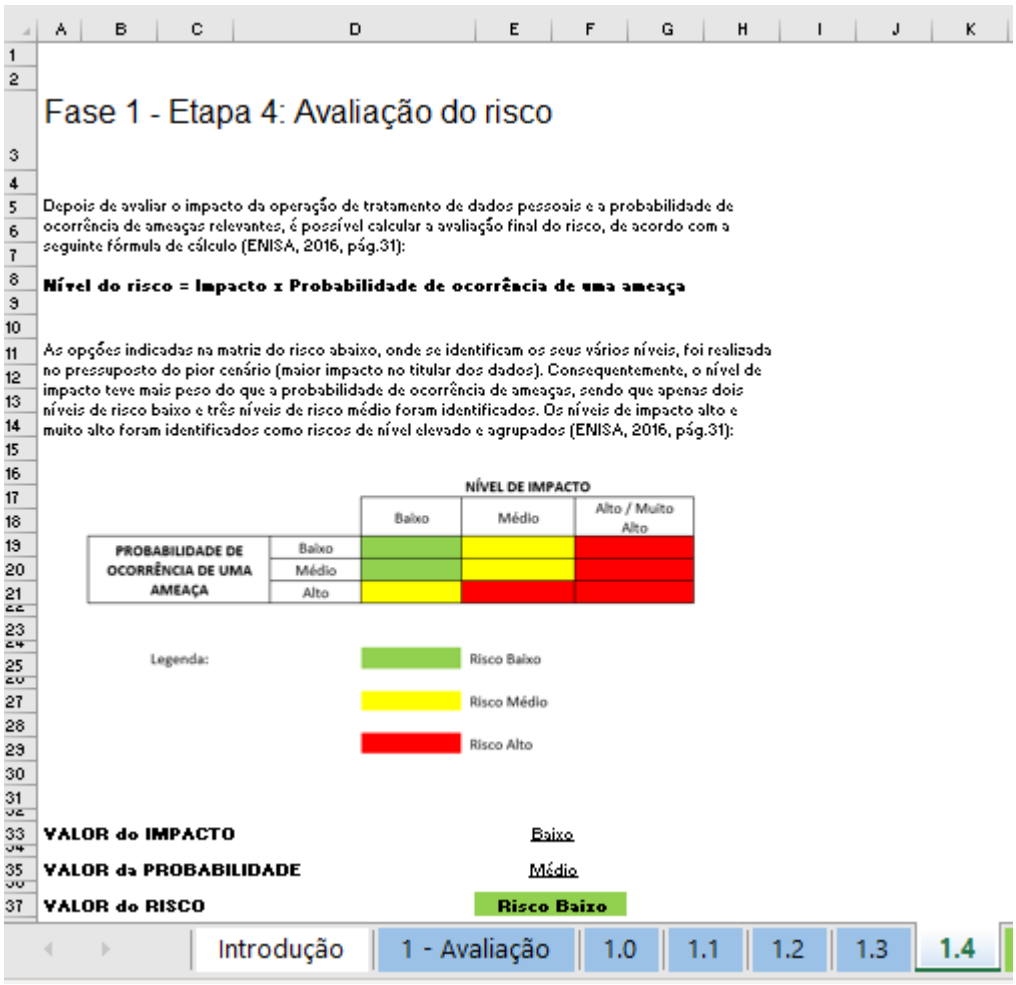
Fase 1 - Avaliação do risco

As diretrizes da ENISA para as PME propõem uma abordagem de avaliação do risco, que se baseia em quatro etapas, como se apresenta de seguida (ENISA, 2017, pág. 10):

- Etapa 0: Caracterização geral
- Etapa 1: Definição da operação de tratamento e seu contexto
- Etapa 2: Compreender e avaliar o impacto
- Etapa 3: Definição de possíveis ameaças e avaliação da sua probabilidade
- Etapa 4: Avaliação do risco

A avaliação do risco começa com a identificação de ameaças, seguida da determinação da probabilidade e do impacto de cada risco. Para avaliar adequadamente o risco, deve-se igualmente levar em consideração a probabilidade e o impacto (ENISA, 2016, pág. 11).

Introdução | 1 - Avaliação | 1.0 | 1.1 | 1.2 | 1.3 | 1.4 | 2 - Tratamento | 2.1 | 3 - Aceitação | 3.1 | 4 - Comunicação | 4.1



Fase 1 - Etapa 4: Avaliação do risco

Depois de avaliar o impacto da operação de tratamento de dados pessoais e a probabilidade de ocorrência de ameaças relevantes, é possível calcular a avaliação final do risco, de acordo com a seguinte fórmula de cálculo (ENISA, 2016, pág.31):

Nível do risco = Impacto x Probabilidade de ocorrência de uma ameaça

As opções indicadas na matriz do risco abaixo, onde se identificam os seus vários níveis, foi realizada no pressuposto do pior cenário (maior impacto no titular dos dados). Consequentemente, o nível de impacto teve mais peso do que a probabilidade de ocorrência de ameaças, sendo que apenas dois níveis de risco baixo e três níveis de risco médio foram identificados. Os níveis de impacto alto e muito alto foram identificados como riscos de nível elevado e agrupados (ENISA, 2016, pág.31):

		NÍVEL DE IMPACTO		
		Baixo	Médio	Alto / Muito Alto
PROBABILIDADE DE OCORRÊNCIA DE UMA AMEAÇA	Baixo			
	Médio			
	Alto			

Legenda:

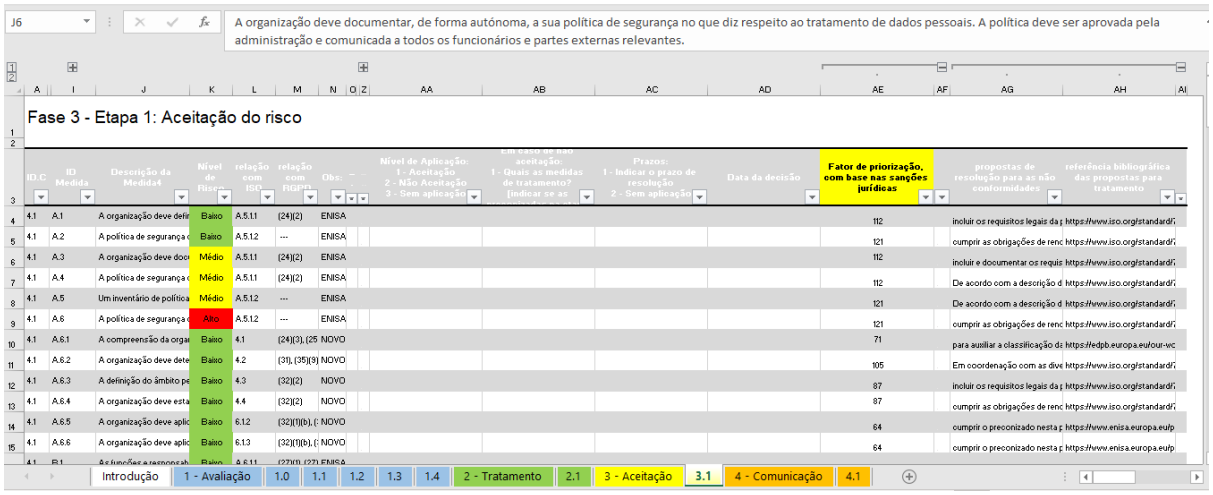
- Risco Baixo
- Risco Médio
- Risco Alto

VALOR do IMPACTO Baixo

VALOR da PROBABILIDADE Médio

VALOR do RISCO **Risco Baixo**

Introdução | 1 - Avaliação | 1.0 | 1.1 | 1.2 | 1.3 | 1.4



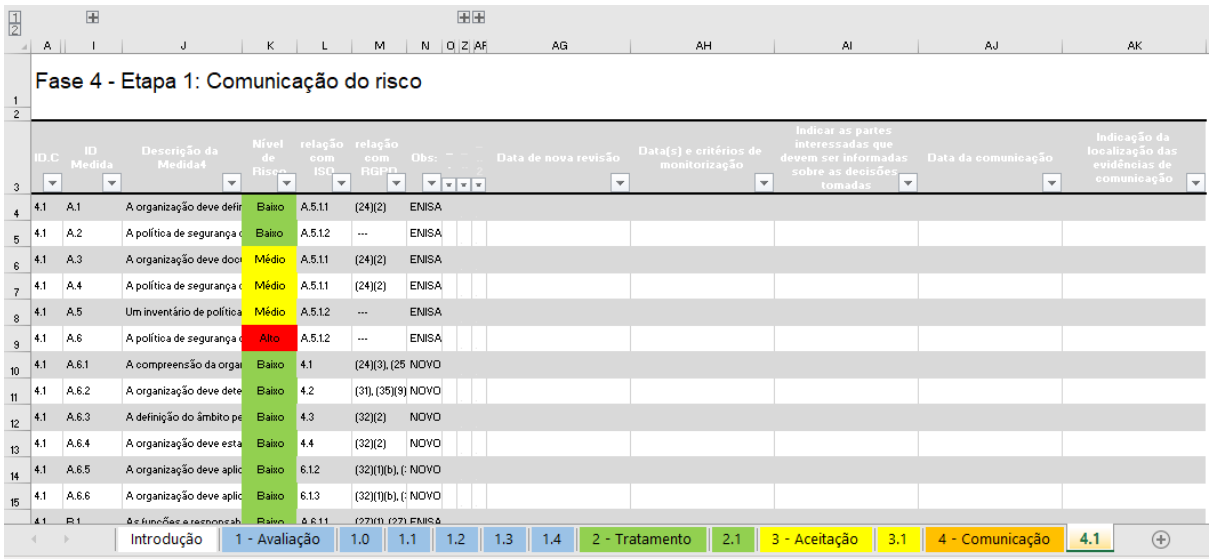
J6

A organização deve documentar, de forma autónoma, a sua política de segurança no que diz respeito ao tratamento de dados pessoais. A política deve ser aprovada pela administração e comunicada a todos os funcionários e partes externas relevantes.

Fase 3 - Etapa 1: Aceitação do risco

ID.C	ID Medida	Descrição da Medida4	Nível de Risco	relação com ISO	relação com RGPD	Obs:	Nível de Aplicação: 1 - Aceitação 2 - Não Aceitação 3 - Sem aplicação	Em caso de não aceitação: 1 - Quais as medidas de tratamento? [indicar se as	Prazos: 1 - Indicar o prazo de resolução 2 - Sem aplicação	Data da decisão	Fator de priorização, com base nas sanções jurídicas	propostas de resolução para as não conformidades	referência bibliográfica das propostas para tratamento
4.1	A.1	A organização deve defi	Baixo	A.5.1.1	(24)(2)	ENISA					112	incluir os requisitos legais da p	https://www.iso.org/standard/
4.1	A.2	A política de segurança d	Baixo	A.5.1.2	---	ENISA					121	cumprir as obrigações de rend	https://www.iso.org/standard/
4.1	A.3	A organização deve doc	Médio	A.5.1.1	(24)(2)	ENISA					112	incluir e documentar os requis	https://www.iso.org/standard/
4.1	A.4	A política de segurança d	Médio	A.5.1.1	(24)(2)	ENISA					112	De acordo com a descrição d	https://www.iso.org/standard/
4.1	A.5	Um inventário de política	Médio	A.5.1.2	---	ENISA					121	De acordo com a descrição d	https://www.iso.org/standard/
4.1	A.6	A política de segurança d	Alto	A.5.1.2	---	ENISA					121	cumprir as obrigações de rend	https://www.iso.org/standard/
4.1	A.6.1	A compreensão da orga	Baixo	4.1	(24)(3), (25	NOVO					71	para auxiliar a classificação da	https://edpb.europa.eu/our-wc
4.1	A.6.2	A organização deve dete	Baixo	4.2	(31), (35)(9	NOVO					105	Em coordenação com as dive	https://www.iso.org/standard/
4.1	A.6.3	A definição do âmbito pe	Baixo	4.3	(32)(2)	NOVO					87	incluir os requisitos legais da p	https://www.iso.org/standard/
4.1	A.6.4	A organização deve esta	Baixo	4.4	(32)(2)	NOVO					87	cumprir as obrigações de rend	https://www.iso.org/standard/
4.1	A.6.5	A organização deve aplic	Baixo	6.1.2	(32)(1)(b), (:	NOVO					64	cumprir o preconizado nesta p	https://www.enisa.europa.eu/p
4.1	A.6.6	A organização deve aplic	Baixo	6.1.3	(32)(1)(b), (:	NOVO					64	cumprir o preconizado nesta p	https://www.enisa.europa.eu/p
4.1	B.1	As funções e responsab	Baixo	A.6.1.1	(27)(1), (27	ENISA							

Introdução | 1 - Avaliação | 1.0 | 1.1 | 1.2 | 1.3 | 1.4 | 2 - Tratamento | 2.1 | 3 - Aceitação | 3.1 | 4 - Comunicação | 4.1



Fase 4 - Etapa 1: Comunicação do risco

ID.C	ID Medida	Descrição da Medida4	Nível de Risco	relação com ISO	relação com RGPD	Obs:	Data de nova revisão	Data(s) e critérios de monitorização	Indicar as partes interessadas que devem ser informadas sobre as decisões tomadas:	Data da comunicação	Indicação da localização das evidências de comunicação
4.1	A.1	A organização deve defir	Baixo	A.5.1.1	(24)(2)	ENISA					
4.1	A.2	A política de segurança d	Baixo	A.5.1.2	---	ENISA					
4.1	A.3	A organização deve doc	Médio	A.5.1.1	(24)(2)	ENISA					
4.1	A.4	A política de segurança d	Médio	A.5.1.1	(24)(2)	ENISA					
4.1	A.5	Um inventário de política	Médio	A.5.1.2	---	ENISA					
4.1	A.6	A política de segurança d	Alto	A.5.1.2	---	ENISA					
4.1	A.6.1	A compreensão da orga	Baixo	4.1	(24)(3), (25	NOVO					
4.1	A.6.2	A organização deve dete	Baixo	4.2	(31), (35)(9	NOVO					
4.1	A.6.3	A definição do âmbito pe	Baixo	4.3	(32)(2)	NOVO					
4.1	A.6.4	A organização deve esta	Baixo	4.4	(32)(2)	NOVO					
4.1	A.6.5	A organização deve aplic	Baixo	6.1.2	(32)(1)(b), (:	NOVO					
4.1	A.6.6	A organização deve aplic	Baixo	6.1.3	(32)(1)(b), (:	NOVO					
4.1	B.1	As funções e responsab	Baixo	A.6.1.1	(27)(1), (27	ENISA					

Introdução | 1 - Avaliação | 1.0 | 1.1 | 1.2 | 1.3 | 1.4 | 2 - Tratamento | 2.1 | 3 - Aceitação | 3.1 | 4 - Comunicação | 4.1

Anexo 13 – Respostas ao inquérito "Impacto do RGPD nas organizações"

Respostas ao inquérito "Impacto do RGPD nas organizações"

ID	Dimensão da PME	Antiguidade da PME	Localização geográfica (NUT II)	Setor de atividade	Função do/a inquirido/a na PME
1	Pequena	Mais de 20 anos	Centro	Comércio por grosso e a retalho	Colaborador/a interno/a
2	Média	Mais de 20 anos	Área Metropolitana de Lisboa	Outros setores	Proprietário/a
3	Micro	De 6 a 19 anos	Centro	Outros setores	Colaborador/a interno/a
4	Pequena	De 6 a 19 anos	Área Metropolitana de Lisboa	Outros setores	Gestor/a
5	Micro	Menos de 5 anos	Área Metropolitana de Lisboa	Atividades de saúde humana e apoio social	Administrativo/a
6	Micro	De 6 a 19 anos	Área Metropolitana de Lisboa	Atividades imobiliárias	Proprietário/a
7	Micro	Menos de 5 anos	Norte	Construção	Proprietário/a
8	Micro	Menos de 5 anos	Centro	Atividades de saúde humana e apoio social	Gestor/a
9	Micro	De 6 a 19 anos	Região Autónoma da Madeira	Outros setores	Administrativo/a
10	Micro	Menos de 5 anos	Área Metropolitana de Lisboa	Outros setores	Sócio/a
11	Pequena	De 6 a 19 anos	Alentejo	Alojamento, restauração e similares	Sócio/a
12	Pequena	Menos de 5 anos	Área Metropolitana de Lisboa	Outros setores	Colaborador/a interno/a
13	Micro	Menos de 5 anos	Norte	Atividades financeiras e de seguros	Sócio/a
14	Micro	Menos de 5 anos	Norte	Outros setores	Proprietário/a
15	Micro	Menos de 5 anos	Área Metropolitana de Lisboa	Outros setores	Proprietário/a
16	Micro	Menos de 5 anos	Norte	Atividades financeiras e de seguros	Administrativo/a
17	Micro	De 6 a 19 anos	Norte	Outros setores	Gestor/a
18	Micro	Menos de 5 anos	Norte	Outros setores	Proprietário/a
19	Micro	Menos de 5 anos	Centro	Outros setores	Gestor/a
20	Média	Mais de 20 anos	Região Autónoma da Madeira	Comércio por grosso e a retalho	Colaborador/a interno/a
21	Micro	De 6 a 19 anos	Norte	Outros setores	Proprietário/a
22	Micro	De 6 a 19 anos	Área Metropolitana de Lisboa	Outros setores	Administrativo/a
23	Média	Mais de 20 anos	Norte	Educação	Colaborador/a interno/a
24	Pequena	De 6 a 19 anos	Norte	Outros setores	Gestor/a
25	Micro	Mais de 20 anos	Área Metropolitana de Lisboa	Comércio por grosso e a retalho	Gestor/a
26	Micro	De 6 a 19 anos	Área Metropolitana de Lisboa	Outros setores	Proprietário/a
27	Pequena	Mais de 20 anos	Área Metropolitana de Lisboa	Outros setores	Colaborador/a interno/a
28	Micro	De 6 a 19 anos	Área Metropolitana de Lisboa	Outros setores	Gestor/a
29	Pequena	De 6 a 19 anos	Área Metropolitana de Lisboa	Outros setores	Gestor/a
30	Micro	De 6 a 19 anos	Área Metropolitana de Lisboa	Atividades de saúde humana e apoio social	Proprietário/a

31	Pequena	Mais de 20 anos	Norte	Outros setores	Gestor/a
32	Micro	Mais de 20 anos	Área Metropolitana de Lisboa	Outros setores	Gestor/a
33	Micro	Menos de 5 anos	Área Metropolitana de Lisboa	Outros setores	Proprietário/a
34	Pequena	Menos de 5 anos	Área Metropolitana de Lisboa	Comércio por grosso e a retalho	Sócio/a

ID	O/A inquirido/a tem responsabilidades na implementação do RGPD?	Se a resposta anterior foi afirmativa, qual o cargo?	A empresa tem website próprio ou do grupo económico a que pertence?	A empresa realiza vendas de bens ou serviços através do comércio eletrónico?	Se a resposta anterior foi afirmativa, qual a percentagem de vendas através do comércio eletrónico do total do volume de negócios do último ano fiscal (2020)?
1	Não		Sim	Não	
2	Não		Sim	Não	
3	Não		Sim	Não	
4	Sim	Encarregado/a de Proteção de Dados (DPO)	Sim	Não	
5	Sim	Administrativa/Recepção	Sim	Não	
6	Sim	Gestor/a da Qualidade	Sim	Não	
7	Não		Sim	Não	
8	Não		Sim	Não	
9	Não		Sim	Não	
10	Sim	Auditor/a Interno/a	Sim	Não	
11	Não		Não	Não	
12	Sim		Não	Não	
13	Não		Sim	Sim	100%
14	Sim	Responsável	Sim	Não	
15	Sim	Encarregado/a de Proteção de Dados (DPO)	Sim	Não	
16	Sim	Informático/a	Sim	Não	
17	Sim	Encarregado/a de Proteção de Dados (DPO)	Sim	Não	
18	Sim	Jurista	Não	Não	
19	Sim	Informático/a	Não	Sim	24%
20	Não		Não	Não	
21	Sim	Encarregado/a de Proteção de Dados (DPO)	Sim	Sim	100%
22	Sim	Auditor/a Interno/a	Sim	Não	
23	Não		Sim	Não	
24	Sim	Jurista	Sim	Não	
25	Sim	Encarregado/a de Proteção de Dados (DPO)	Sim	Não	
26	Sim	Gerente	Não	Não	
27	Não		Sim	Não	
28	Sim	Encarregado/a de Proteção de Dados (DPO)	Sim	Não	
29	Não		Sim	Não	

30	Sim	Encarregado/a de Proteção de Dados (DPO)	Sim	Não	
31	Sim	Informático/a	Não	Não	
32	Sim	Diretor Geral	Sim	Não	
33	Sim	Como proprietário da empresa, tenho responsabilidades indiretas.	Sim	Não	
34	Não		Não	Não	

ID	A empresa tem serviços de computação em nuvem na internet? (ex: serviço de correio eletrónico; armazenamento de ficheiros)	A empresa utiliza serviços de big data?	A empresa tem pessoal especialista em TIC (Tecnologias de Informação e Comunicações)?	A empresa utiliza dispositivos ou sistemas interconectados que podem ser monitorizados ou controlados remotamente através da Internet (IoT)?	A empresa tem conhecimento do que é o RGPD?
1	Sim	Não	Sim	Não	Sim
2	Sim	Não	Sim	Sim	Sim
3	Sim	Não sei	Sim	Sim	Sim
4	Sim	Não sei	Não	Não	Sim
5	Sim	Não sei	Não	Sim	Sim
6	Sim	Não	Não	Sim	Sim
7	Não	Não	Não	Não	Sim
8	Sim	Não sei	Não	Não	Sim
9	Não	Não	Sim	Não	Sim
10	Sim	Sim	Não	Não	Sim
11	Sim	Não	Não	Não	Não
12	Sim	Não	Sim	Sim	Sim
13	Sim	Não	Não	Não	Sim
14	Não	Não	Não	Não	Sim
15	Sim	Não	Sim	Não	Sim
16	Sim	Não sei	Sim	Sim	Sim
17	Não	Não	Não	Não	Sim
18	Sim	Não sei	Não	Sim	Não
19	Sim	Não	Sim	Sim	Sim
20	Sim	Não sei	Sim	Sim	Sim
21	Sim	Não sei	Sim	Sim	Sim
22	Sim	Sim	Sim	Sim	Sim
23	Sim	Não	Sim	Sim	Sim
24	Sim	Sim	Sim	Sim	Sim
25	Sim	Não	Sim	Não	Sim
26	Não	Não	Não	Não	Sim
27	Não	Não	Não	Sim	Sim
28	Sim	Sim	Sim	Sim	Sim
29	Sim	Não	Sim	Não	Sim
30	Sim	Não sei	Não	Não	Sim
31	Sim	Não	Não	Não	Sim
32	Sim	Não sei	Não	Sim	Sim

33	Sim	Não	Sim	Não	Sim
34	Sim	Não sei	Não	Não	Sim

ID	Se a resposta anterior foi afirmativa, quando teve conhecimento?	Considera que a empresa, e os/as seus/suas colaboradores/as, têm um bom nível de conhecimento sobre o regulamento?	Considera que a empresa tem um bom nível de implementação do regulamento?
1	Em 2018	Não, limitado	Não
2	Antes de 2018	Sim, suficiente	Sim
3	Em 2018	Sim, bom	Não sei
4	Em 2018	Sim, suficiente	Sim
5	Em 2018	Sim, suficiente	Não
6	Em 2018	Não, limitado	Não sei
7	Em 2018	Não, limitado	Não
8	Só em 2021	Não, limitado	Não
9	Antes de 2018	Sim, bom	Sim
10	2019 e/ou 2020	Sim, muito bom	Sim
11		Não, limitado	Não sei
12	Antes de 2018	Sim, suficiente	Sim
13	Antes de 2018	Sim, suficiente	Sim
14	Antes de 2018	Sim, suficiente	Não sei
15	Em 2018	Sim, bom	Sim
16	Só em 2021	Sim, suficiente	Não sei
17	Em 2018	Não, limitado	Não
18		Não, muito limitado	Não sei
19	2019 e/ou 2020	Sim, suficiente	Sim
20	Antes de 2018	Sim, suficiente	Não sei
21	Em 2018	Sim, suficiente	Sim
22	2019 e/ou 2020	Sim, suficiente	Sim
23	Antes de 2018	Sim, suficiente	Sim
24	Antes de 2018	Sim, bom	Sim
25	Antes de 2018	Sim, bom	Sim
26	Antes de 2018	Sim, suficiente	Não
27	Antes de 2018	Sim, suficiente	Não
28	Antes de 2018	Sim, suficiente	Sim
29	2019 e/ou 2020	Sim, bom	Não
30	2019 e/ou 2020	Sim, suficiente	Sim
31	2019 e/ou 2020	Sim, suficiente	Não sei
32	Em 2018	Não, muito limitado	Não
33	Em 2018	Sim, suficiente	Sim
34	Só em 2021	Sim, suficiente	Sim

ID	Quais as principais dificuldades na implementação do regulamento?	Quais os principais desafios que a empresa perceciona em relação à conformidade com o RGPD?
1	Desconhecimento da obrigação de notificação de uma violação de dados pessoais à Autoridade de Controlo; Inexistência de avaliação regular da conformidade com o RGPD;	Definição de processos;
2	Sem dificuldades;	Definição de processos;

3	Necessidade de definir uma metodologia para cumprir as obrigações do RGPD;	Gestão do consentimento;Definição de processos;Identificação, classificação e gestão dos dados;
4	Falta de conhecimento sobre o tema (RGPD);Falta de formação (contínua) sobre o tema (RGPD);Falta de Recursos Humanos;Incapacidade em identificar se os dados são alvo de um tratamento lícito;Falta de Recursos Informáticos / Tecnologia;Falta de recursos financeiros para as alterações necessárias;Falta de orientações práticas ou de normas de aplicação;Inexistência de avaliação regular da conformidade com o RGPD;	Definição de processos;Identificação, classificação e gestão dos dados;Gestão do consentimento;
5	Falta de formação (contínua) sobre o tema (RGPD);Incapacidade em identificar se os dados são alvo de um tratamento lícito;Desconhecimento quanto aos contratos com prestadores de serviços relativamente à conformidade com o RGPD;Necessidade de definir uma metodologia para cumprir as obrigações do RGPD;	Identificação, classificação e gestão dos dados;Gestão do consentimento;
6	Falta de conhecimento sobre o tema (RGPD);Falta de Recursos Humanos;	Definição de processos;Formação dos/as colaboradores/as;
7	Falta de conhecimento sobre o tema (RGPD);Falta de formação (contínua) sobre o tema (RGPD);Incapacidade em identificar se os dados são alvo de um tratamento lícito;Falta de Recursos Informáticos / Tecnologia;Desconhecimento dos direitos dos titulares dos dados;Desconhecimento quanto aos contratos com prestadores de serviços relativamente à conformidade com o RGPD;Falta de orientações práticas ou de normas de aplicação;Incapacidade em identificar todos os dados pessoais que a empresa possui;Necessidade de definir uma metodologia para cumprir as obrigações do RGPD;Inexistência de avaliação regular da conformidade com o RGPD;Desconhecimento da obrigação de notificação de uma violação de dados pessoais à autoridade de controlo;	Identificação, classificação e gestão dos dados;Estabelecimento de medidas de segurança;Definição de processos;Gestão do consentimento;Abordagem baseada em risco;
8	Falta de conhecimento sobre o tema (RGPD);Falta de formação (contínua) sobre o tema (RGPD);Falta de Recursos Humanos;Falta de recursos financeiros para as alterações necessárias;	Formação dos/as colaboradores/as;
9	Incapacidade em identificar se os dados são alvo de um tratamento lícito;	Definição de processos;
10	Desconhecimento da obrigação de notificação de uma violação de dados pessoais à autoridade de controlo;	Estabelecimento de medidas de segurança;
11	Falta de orientações práticas ou de normas de aplicação;Falta de formação (contínua) sobre o tema (RGPD);	Abordagem baseada em risco;
12	Sem dificuldades;	Gestão do consentimento;
13	Sem dificuldades;	Definição de processos;
14	Necessidade de definir uma metodologia para cumprir as obrigações do RGPD;	Abordagem baseada em risco;
15	Sem dificuldades;	Gestão do consentimento;
16	Falta de formação (contínua) sobre o tema (RGPD);Falta de conhecimento sobre o tema (RGPD);Falta de Recursos Humanos;Falta de orientações práticas ou de normas de aplicação;Falta de recursos financeiros para as alterações necessárias;	Definição de processos;Formação dos/as colaboradores/as;Estabelecimento de medidas de segurança;Gestão do consentimento;
17	Falta de conhecimento sobre o tema (RGPD);Falta de Recursos Informáticos / Tecnologia;Falta de recursos financeiros para as alterações necessárias;	Definição de processos;Identificação, classificação e gestão dos dados;Formação dos/as colaboradores/as;Gestão do consentimento;
18	Desconhecimento quanto aos contratos com prestadores de serviços relativamente à conformidade com o RGPD;Falta de conhecimento sobre o tema (RGPD);	Definição de processos;
19	Falta de formação (contínua) sobre o tema (RGPD);Falta de recursos financeiros para as alterações necessárias;Falta de Recursos Humanos;Desconhecimento quanto aos contratos com prestadores de serviços relativamente à conformidade com o RGPD;Necessidade de definir uma metodologia para cumprir as obrigações do RGPD;	Formação dos/as colaboradores/as;Gestão do consentimento;Definição de processos;
20	Falta de formação (contínua) sobre o tema (RGPD);Falta de recursos financeiros para as alterações necessárias;Necessidade de definir uma metodologia para cumprir as obrigações do RGPD;Inexistência de avaliação regular da conformidade com o RGPD;Incapacidade em identificar se os dados são alvo de um tratamento lícito;Falta de Recursos Humanos;Falta de orientações práticas ou de normas de aplicação;	Identificação, classificação e gestão dos dados;Formação dos/as colaboradores/as;
21	Sem dificuldades;	Identificação, classificação e gestão dos dados;
22	Falta de conhecimento sobre o tema (RGPD);Falta de formação (contínua) sobre o tema (RGPD);	Formação dos/as colaboradores/as;Abordagem baseada em risco;
23	Incapacidade em identificar se os dados são alvo de um tratamento lícito;Desconhecimento quanto aos contratos com prestadores de serviços relativamente à conformidade com o RGPD;Falta de orientações práticas ou de normas de aplicação;	Definição de processos;

24	Falta de formação (contínua) sobre o tema (RGPD);	Formação dos/as colaboradores/as;
25	Falta de orientações práticas ou de normas de aplicação;	Gestão do consentimento;Abordagem baseada em risco;
26	Falta de formação (contínua) sobre o tema (RGPD);	Gestão do consentimento;Identificação, classificação e gestão dos dados;
27	Falta de formação (contínua) sobre o tema (RGPD);Falta de Recursos Humanos;Falta de orientações práticas ou de normas de aplicação;Inexistência de avaliação regular da conformidade com o RGPD;	Identificação, classificação e gestão dos dados;Formação dos/as colaboradores/as;Definição de processos;Estabelecimento de medidas de segurança;
28	Falta de formação (contínua) sobre o tema (RGPD);Incapacidade em identificar se os dados são alvo de um tratamento lícito;Falta de orientações práticas ou de normas de aplicação;	Definição de processos;Identificação, classificação e gestão dos dados;
29	Necessidade de definir uma metodologia para cumprir as obrigações do RGPD;Falta de Recursos Humanos;	Formação dos/as colaboradores/as;
30	Falta de orientações práticas ou de normas de aplicação;Incapacidade em identificar se os dados são alvo de um tratamento lícito;Desconhecimento dos direitos dos titulares dos dados;	Gestão do consentimento;Estabelecimento de medidas de segurança;
31	Falta de orientações práticas ou de normas de aplicação;Falta de Recursos Informáticos / Tecnologia;Falta de formação (contínua) sobre o tema (RGPD);	Definição de processos;Formação dos/as colaboradores/as;Estabelecimento de medidas de segurança;
32	Falta de conhecimento sobre o tema (RGPD);Falta de formação (contínua) sobre o tema (RGPD);Falta de Recursos Humanos;Desconhecimento dos direitos dos titulares dos dados;Falta de orientações práticas ou de normas de aplicação;Desconhecimento da obrigação de notificação de uma violação de dados pessoais à autoridade de controlo;	Definição de processos;Identificação, classificação e gestão dos dados;Estabelecimento de medidas de segurança;
33	Falta de formação (contínua) sobre o tema (RGPD);	Gestão do consentimento;
34	Sem dificuldades;	Definição de processos;Gestão do consentimento;Abordagem baseada em risco;Estabelecimento de medidas de segurança;

ID	Quais os principais benefícios do RGPD para a sua empresa?	Conhece a ENISA – Agência da União Europeia para a Segurança de Redes e Informações, e as suas orientações para as PME, no sentido de ajudá-las a avaliar os riscos de segurança e, consequentemente...
1	Melhoria da imagem pública e reputação da organização;	Não
2	Garantia da confiança dos clientes;	Sim
3	Melhoria da gestão da informação;Garantia da confiança dos clientes;Melhoria da segurança e privacidade da informação;	Não
4	Redução do risco sancionatório;	Não
5	Garantia da confiança dos clientes;	Não
6	Garantia da confiança dos clientes;Redução do risco sancionatório;	Não
7	Melhoria da gestão da informação;Garantia da confiança dos clientes;Redução do risco sancionatório;	Sim
8	Garantia da confiança dos clientes;	Não
9	Garantia da confiança dos clientes;Redução do risco sancionatório;	Não
10	Melhoria da segurança e privacidade da informação;	Não
11	Garantia da confiança dos clientes;	Não
12	Garantia da confiança dos clientes;	Não
13	Garantia da confiança dos clientes;Redução do risco sancionatório;	Sim
14	Garantia da confiança dos clientes;	Não
15	Garantia da confiança dos clientes;	Não
16	Melhoria da gestão da informação;Garantia da confiança dos clientes;Melhoria da segurança e privacidade da informação;	Sim
17	Garantia da confiança dos clientes;	Não
18	Melhoria da segurança e privacidade da informação;	Não

19	Garantia da confiança dos clientes;Melhoria da segurança e privacidade da informação;	Não
20	Melhoria da segurança e privacidade da informação;Garantia da confiança dos clientes;Melhoria da gestão da informação;	Não
21	Melhoria da segurança e privacidade da informação;	Não
22	Melhoria da segurança e privacidade da informação;Melhoria da gestão da informação;Garantia da confiança dos clientes;	Não
23	Garantia da confiança dos clientes;Redução do risco sancionatório;Melhoria da imagem pública e reputação da organização;Melhoria da segurança e privacidade da informação;	Sim
24	Melhoria da segurança e privacidade da informação;	Não
25	Redução do risco sancionatório;	Não
26	Garantia da confiança dos clientes;Redução do risco sancionatório;	Não
27	Redução do risco sancionatório;	Não
28	Melhoria da segurança e privacidade da informação;Melhoria da gestão da informação;Garantia da confiança dos clientes;	Sim
29	Garantia da confiança dos clientes;Redução do risco sancionatório;Melhoria da imagem pública e reputação da organização;	Sim
30	Garantia da confiança dos clientes;Redução do risco sancionatório;	Não
31	Nenhum;	Não
32	Melhoria da segurança e privacidade da informação;Melhoria da gestão da informação;Garantia da confiança dos clientes;Redução do risco sancionatório;	Não
33	Garantia da confiança dos clientes;	Não
34	Garantia da confiança dos clientes;Redução do risco sancionatório;Melhoria da imagem pública e reputação da organização;	Não

ID	Conhece os controlos de segurança da ISO/IEC 27001:2013?	Conhece a extensão da ISO/IEC 27001 para a gestão de informações de privacidade – ISO/IEC 27701:2019?	Deseja realizar uma Prova de Conceito da solução proposta para Conformidade, Proteção e Privacidade dos dados pessoais, no âmbito deste trabalho de investigação?
1	Não	Não	Não
2	Sim	Sim	Não
3	Sim	Sim	Não
4	Não	Não	Sim
5	Não	Não	Não
6	Não	Não	Não
7	Não	Não	Sim
8	Não	Não	Não
9	Sim	Sim	Não
10	Não	Não	Sim
11	Não	Não	Sim
12	Sim	Sim	Não
13	Não	Não	Não
14	Não	Não	Não
15	Não	Não	Não
16	Não	Não	Não
17	Não	Não	Sim
18	Não	Não	Não

19	Não	Não	Não
20	Não	Não	Não
21	Não	Não	Não
22	Sim	Sim	Não
23	Sim	Sim	Não
24	Sim	Sim	Não
25	Não	Não	Não
26	Não	Não	Não
27	Não	Não	Não
28	Não	Não	Sim
29	Não	Não	Sim
30	Não	Não	Não
31	Não	Não	Não
32	Não	Não	Sim
33	Não	Não	Não
34	Não	Não	Não

Anexo 14 – Respostas da "Prova de Conceito junto das PME"

Respostas da "Prova de Conceito junto das PME"

FASE I - Iniciação

ID	Morada	Função dentro da empresa	O responsável da PME é também responsável pela implementação do RGPD?	Se a resposta anterior foi afirmativa, qual o cargo?	Proposta de data para reunião	Modo de apresentação
1	Lisboa	Proprietário/a	Sim	Outro	4/16/2021	Remoto
2	Porto	Proprietário/a	Sim	Outro	4/21/2021	Remoto
3	Porto	Proprietário/a	Sim	Outro	4/21/2021	Remoto
4	Lisboa	Gestor/a	Sim	Outro	4/23/2021	Remoto
5	Lisboa	Proprietário/a	Sim	Encarregado/a de Proteção de Dados (DPO)	4/27/2021	Remoto
6	Lisboa	Proprietário/a	Sim	Outro	5/5/2021	Remoto

FASE II – Planeamento e Análise

ID	Definição do âmbito (ex: máximo 2 tratamentos de dados pessoais)	Entregas previstas (ex: preenchimento integral de uma proposta de solução)	Função dentro da organização do/a gestor/a do projeto
1	Realização de certificados de participação em eventos / Ação de receção de funcionários - evento, com molduras e fotografias (subcontratante; com sub-subcontratados)	Concretizar a gestão do risco para 2 tratamentos	Proprietário/a
2	Gestão de clientes individuais	preenchimento de uma proposta para o tratamento gestão de clientes individuais	Proprietário/a
3	Envio de marketing para clientes	exemplo de preenchimento de uma proposta	Proprietário/a
4	Recrutamento e seleção de RH	preenchimento de uma proposta para o tratamento de recrutamento e seleção	Gestor/a
5	1 tratamento - mailling para clientes - marketing / prospeção	preenchimento de uma proposta	Proprietário/a
6	Campanha de marketing	pré-preenchimento do ficheiro proposta	Proprietário/a

ID	Definição da equipa de projeto (ex: pessoa responsável pelo tratamento de dados; diretor/a responsável; responsável TI; responsável jurídico; Encarregado de Proteção de Dados, etc.)	Partes interessadas no PoC (ex: prestadores de serviços, fornecedores, instituições públicas, etc.)	Definição das sessões	Declaro que concordo em não utilizar de forma alguma a informação confidencial no âmbito deste PoC, fabricar ou testar qualquer produto que incorpore esta informação confidencial, exceto para os fins autorizados pelos seus autores
1	Equipa composta por 2 elementos: Proprietário e responsável RH	Parceiro de negócio	Remoto	Aceito as condições do PoC
2	A própria	para já não se aplica	Remoto	Aceito as condições do PoC
3	A própria	N/A	Remoto	Aceito as condições do PoC
4	O próprio	entrevistados e os clientes finais alvo do recrutamento	Remoto	Aceito as condições do PoC
5	Equipa composta por 3 elementos: Proprietário, Responsável de Estratégia, CFO	Clientes	Remoto	Aceito as condições do PoC
6	O próprio	Clientes	Remoto	Aceito as condições do PoC

FASE III – Fecho do Projeto

ID	A proposta de apresentação do PoC à PME foi satisfatória?	Comentários sobre a pergunta anterior (apresentação do PoC):	Que lições foram aprendidas com o PoC?	A definição do âmbito foi ajustada ao PoC?	Comentários sobre a pergunta anterior (definição do âmbito):
1	Sim	sem aplicação concreta em empresas deste setor de negócio, com poucos dados pessoais	Pode ser útil para empresas que tenham mais dados pessoais	Sim	N/A
2	Sim	Capacidade de transmitir conhecimento	Deu condições para encarar o RGPD como uma forma de encarar o serviço	Não	Fomos bastante ambiciosos face ao nosso nível de conhecimento
3	Sim	Todas as questões foram fundamentadas e com conteúdo. Sempre foi mostrado onde se encontra a informação e o porquê de pedir a informação	Conclui que a minha empresa tem o processo de RGPD bastante bem organizado.	Sim	Foi uma boa aposta definir o âmbito deste PoC numa atividade bastante importante da organização
4	Sim	N/A	Perceber que posso aplicar o RGPD de modo faseado.	Sim	N/A
5	Sim	Cumpre com o pretendido	Acrescentou valor na medida em que ajudou a tomar consciência sobre alguns pontos que, no dia-a-dia, ficam renegados para segundo plano.	Sim	Sem aplicação
6	Sim	Assertiva	A nossa estrutura terá de fazer várias melhorias para cumprir os requisitos.	Sim	N/A

ID	Os prazos definidos foram cumpridos?	Comentários sobre a pergunta anterior (prazos):	A duração do PoC foi satisfatória?	Comentários sobre a pergunta anterior (duração):
1	Sim	N/A	Sim	N/A
2	Não	Resvalou visto terem aparecido várias questões de entendimento	Sim	N/A
3	Sim	N/A	Sim	O tempo necessário
4	Sim	N/A	Sim	N/A
5	Sim	Sem aplicação	Sim	Sem aplicação
6	Sim	Imprimimos uma tónica de urgência à melhoria da realidade da nossa empresa	Sim	N/A

ID	A alocação de recursos foi ajustada às necessidades?	Comentários sobre a pergunta anterior (alocação de recursos):	As entregas previstas foram cumpridas?	Comentários sobre a pergunta anterior (entregas):	Gostava de ter esta solução implementada em toda a organização?	Comentários sobre a pergunta anterior (implementação):
1	Sim	N/A	Não	sem aplicação a empresas com poucos dados pessoais	Não	Não se aplica a organizações com poucos dados pessoais
2	Sim	N/A	Sim	N/A	Sim	É uma implementação trabalhosa.
3	Sim	Foi bom. Se o PoC fosse relativo ao marketing seria diferente. Relativamente ao processo de vendas correu bem	Sim	N/A	Sim	Faria sentido porque a organização tem outros aspetos que preocupa em relação ao RGPD, nomeadamente relacionado com o marketing
4	Sim	Em contexto do PoC foi ajustado. Contudo, num exercício mais completo de conformidade, seria bom aumentar a equipa	Sim	N/A	Sim	Sim, mas seria complicado pelo tempo de implementação
5	Sim	O desafio teve mais a ver com a dimensão da empresa do que na	Sim	Sem aplicação	Sim	Contudo, a manutenção operacional é exigente -

		alocação de recursos, por ser PME com pouco colaboradores				é um processo bastante exigente e complexo
6	Sim	Como teve de ser praticamente adaptada de raiz, a sua alocação foi ajustada ao que é a realidade da nossa empresa	Sim	N/A	Sim	Assumimos como mais um dos factores diferenciadores a sua implementação

ID	Etapa de Avaliação do risco	Etapa de Tratamento do risco	Etapa de Aceitação do risco	Etapa de Comunicação do risco
1	não	não	parece bem	não
2	Há perguntas formuladas na negativa que tornam difícil o preenchimento	Sem propostas	Impecável. Sem dúvidas de interpretação	Tudo óbvio - ligado aos procedimentos a aplicar em caso de risco efetivo
3	Muito bem explicado	Muito bem explicado	Muito bem explicado. O Ranking faz sentido na medida em que ajuda a começar a trabalhar	Muito bem explicado
4	sem observações	A componente visual deveria estar mais simplificada - tem muita informação - a informação deveria ser apresentada apenas quando é necessária	A componente visual deveria estar mais simplificada - tem muita informação - a informação deveria ser apresentada apenas quando é necessária. A componente de aceitação poderia ter uma vertente financeira associada às opções de melhoria, para além do ranking das multas	Também a componente visual mas não tão relevante como referido anteriormente.
5	Sem sugestão de melhoria	Está bem conseguido - está simples e concreto. Relaciona-se diretamente com os artigos do RGPD.	Está bem conseguido - ajuda a tomar decisões e apresenta propostas de solução. As medidas estão associadas ao RGPD - dá segurança/conforto a quem toma decisões, perante as questões que surgem na organização. E ajuda a priorizar/tomar decisões de acordo com os diferentes níveis de risco.	Sem comentários. Numa PME a comunicação é algo intrínseco visto haver poucos recursos e haver comunicação fluida.
6	sem observações	sem observações	sem observações	sem observações

ID	Nível global de satisfação do PoC	Outras recomendações sobre como proceder numa implementação completa no contexto da organização	Comentários finais	Data de submissão
1	Bom	Sem recomendações	N/A	4/21/2021
2	Muito bom	Envolver todos os decisores no processo de implementação	Faz falta este tipo de iniciativa	4/26/2021
3	Muito bom	implementação faseada para os vários tratamentos existentes	N/A	4/26/2021
4	Muito bom	Implementar a proposta num sistema de informação web-based que vai facilitar todos os utilizadores com acesso à mesma	Transformar este PoC em produto Web/APP	5/5/2021
5	Bom	Sem recomendações	Para empresas que não estão por dentro deste tema, é um processo complexo.	5/6/2021
6	Muito bom	Poderemos fazer num futuro próximo	Foi enriquecedor participar neste estudo e perceber que mesmo baixos os riscos que enfrentávamos é fundamental garantir a sua resolução e prevenção.	5/10/2021