UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA

Análise de Risco no GDPR

Pedro Alexandre Brandão Mendes

Mestrado em Segurança Informática

Trabalho de projeto orientado por:
Prof. Mário Calha
E coorientado pelo Mestre Sérgio Valentim Costa de Sá.

2018

Agradecimentos

Em primeiro lugar devo agradecer aos meus colegas de curso que me deram todo apoio que precisei para a realização deste trabalho o João Lopes, Gil Correia, Diogo Carou e João Calado, e que de uma forma ou outra também me foram dando motivação nas alturas mais complicadas para conseguir avançar.

Não quero deixar de agradecer à minha família, que sem o apoio deles, este trabalho não seria possível, e que me deram as condições para o conseguir fazer ajudando nas pequenas coisas que são também muito importantes.

Grande parte do trabalho também se deve aos meus colegas na EY, em particular ao Sérgio Sá que me apoiou mais diretamente na realização do trabalho, ao Gerson que me deu inspiração que levou o trabalho a ser o que é, ao Sérgio Martins por me ter ajudado a criar condições para conciliar o projeto da EY com este projeto, e quero agradecer ainda por todo o apoio dado para conseguir realizar o projeto ao Radu, Jorge, Rodrigo e João Stott.

Por último, mas não menos importante, muito obrigado ao Professor Mário Calha, cujo acompanhamento, dedicação e muita paciência foram importantes para tornar este trabalho no que é.

Obrigado.

À minha filha, Rosa.

Resumo

Nos dias de hoje com a crescente adesão da população aos sistemas virtuais, e com o aumento de recolha de dados pessoais por parte das organizações quer seja para sua utilização, quer para venda, o valor desses dados tem aumentado significativamente. Como tal, ataques direcionados para comprometer dados pessoais têm também vindo a aumentar, assim como os abusos da utilização desses mesmos dados. Estatísticas indicam que diariamente, cerca de 5 milhões de registos são perdidos ou roubados, sendo um grande número desses registos potencialmente pessoais.

Sendo os dados pessoais os que mais podem causar impacto na vida das pessoas, podendo condicionar as suas liberdades e direitos, a União Europeia decidiu criar um regulamento para obrigar as organizações que trabalham com dados pessoais de cidadãos Europeus a implementar medidas para proteger esses dados, obter consentimento legítimo para a recolha e processamento dos mesmos, e informar os cidadãos dos tratamentos efetuados e possíveis fugas de informação dos seus dados.

O novo Regulamento Geral de Proteção de Dados, obrigatório e aplicável em todos os estados membros da União Europeia a partir de 25 Maio de 2018, introduz algumas novidades importantes a nível organizacional, sendo uma novidade a destacar a Avaliação de Impacto de Proteção de Dados, uma medida obrigatória a tomar para todos os processos organizacionais que tratem dados pessoais e que possam originar um risco elevado para os direitos e liberdades dos cidadãos, para garantir que os riscos são identificados e que são aplicadas as medidas de mitigação necessárias.

Por forma a determinar se um processo organizacional irá originar num risco elevado, foi desenvolvida uma metodologia que permite efetuar uma análise de risco a processos organizacionais levando em conta o seu âmbito, contexto, propósitos do processamento de dados e criticidade das aplicações, tendo como base o nível de conformidade do processo com o regulamento. Para complementar a metodologia desenvolvida é proposto um conjunto de medidas a implementar pelas organizações, consoante os seus processos, para alcançar a conformidade com o regulamento e mitigar os riscos identificados que podem afetar os titulares dos dados.

Palavras-chave: RGPD, Risco, Dados Pessoais, Segurança dos Dados, Privacidade

Abstract

Nowadays with the growing adherence of the population to virtual systems, and with the increase in the personal data collection by the organizations for their own purpose, or for sale, the value of this data has been significantly increased. As such, abuse and direct attacks to compromise personal data have been increasing. Statistics indicate that every day, about 5 million records are lost or stolen, and potentially a large percentage is personal data.

Among all data, the personal data can cause the biggest impact in people's life, with the possibility to condition their rights and freedoms, the European Union decided to create a regulation to oblige organizations that work with European citizens' personal data to implement measures to protect those data, obtain legitimate consent to the collection and processing of data, and inform their citizens of the treatments in place and possible data leaks.

The new General Data Protection Regulation, mandatory and applicable in all European Union member states since 2018 May 25th, introduces some important novelties at the organizational level. It highlights the Data Protection Impact Assessments, a mandatory measure to take for every process that may originate a high risk to the rights and freedoms of the citizens, ensure that risks are identified and that the required mitigation measures are applied.

To determine if an organizational process will originate a high risk, a methodology has been developed, that allows a risk analysis to be made for organizational processes, considering their purpose, context, data processing contexts and applications critically, having as a base the process compliance level with the regulation. To complement the methodology, a set of measures is proposed to be implemented by the organizations in accordance with their processes, to achieve compliance with the regulation and mitigate the identified risks that may affect the data owners.

Keywords: GDPR, Risk, Personal Data, Data Security, Privacy

Conteúdo

Índice de figuras

Índice de tabelas

1 Introdução

Com a massificação da virtualização dos sistemas e adesão a novas tecnologias como *smartphones*, ambientes na *Cloud*, *Internet of Things*, entre outros, cada vez são recolhidos mais dados pessoais com o propósito de observar comportamentos e padrões e proporcionar uma melhor experiência para os utilizadores, permitindo em último caso gerar receita para as organizações. Como tal, cada vez mais os dados que as organizações recolhem, armazenam e processam são o seu bem mais valioso.

Alguns dos dados recolhidos sendo mais sensíveis (temos como exemplo dados relacionados com a saúde, registos criminais, opiniões políticas), levam a que os mesmos possam causar um maior impacto na vida de um indivíduo, e é necessário garantir que estão implementados os controlos e medidas necessários para garantir a privacidade e segurança desses dados. No entanto, mesmo com o grande crescimento na área da segurança da informação nos últimos anos, também tem havido um grande crescimento nas comunidades que procuram explorar vulnerabilidades de dispositivos de rede, sistemas e aplicações, reduzindo a eficácia das medidas de segurança existentes. Outro dos problemas relacionado com a recolha de dados pessoais é a utilização dos dados para tratamentos com fins para além daqueles para que os dados foram recolhidos e/ou autorizados inicialmente, ou a transmissão dos mesmos para outras entidades sem autorização dos titulares dos dados. Temos em Portugal vários casos do conhecimento do público, como o caso da EDP partilhar dados dos seus clientes à NOS e PT sem o consentimento dos clientes (Urquhart, 2017), que resulta em chamadas abusivas por parte das operadoras.

A privacidade dos dados dos cidadãos é um assunto que tem vindo a preocupar cada vez mais os cidadãos, nomeadamente depois das fugas de informação de Snowden em 2013 ao expor que a NSA espiava centenas de milhões de indivíduos de tal forma que poderia elaborar um perfil detalhado de grande parte deles (Ewen Macaskill, 2013). Em adição a isso podemos observar constantemente nas notícias grandes empresas a serem alvo de ataques informáticos que procuram comprometer os seus dados de negócio pelo valor que têm e que acabam por ser vendidos ou publicados na internet. Nesses dados muitas vezes encontram-se dados pessoais, que pela exposição que têm para os respetivos titulares dos dados deve-se ter um cuidado adicional. A publicação desses dados pode ter um grande impacto negativo na vida das pessoas, como aconteceu com muitos

utilizadores que foram expostos nas fugas de informação do Ashley Madison, e também para as organizações, que para além das elevadas indemnizações que têm que pagar, estão sujeitas a enormes perdas de reputação (Khandelwal, 2017), sendo depois muito difícil recuperá-la.

Para tentar reduzir as ameaças existentes é necessária uma regulamentação que especifique as medidas a levar em conta na recolha, processamento, armazenamento e transmissão de dados pessoais para que as organizações tomem ações de modo a tornar os seus sistemas mais seguros, tentar evitar que os dados pessoais sejam obtidos por entidades cujo propósito seja tratar os dados de forma diferente daquela para a qual os dados foram inicialmente recolhidos ou entidades maliciosas, e garantir que os titulares são informados e têm conhecimento do que acontece aos seus dados.

Por esse motivo tem sido desenvolvido nos últimos anos o Regulamento Geral de Proteção de Dados (RGPD, e de sigla internacional GDPR), que já se encontra em vigor desde 25 de Maio de 2016 e se tornou obrigatório em 25 de Maio de 2018, com o objetivo de colmatar as falhas da Diretiva Europeia De Proteção de Dados (Diretiva 95/46/CE). A conformidade com o RGPD é obrigatória para todas as organizações, dentro e fora da União Europeia, que processem ou armazenem dados de cidadãos Europeus. Ao contrário da Diretiva Europeia, o RGPD deverá ser implementado de igual forma em todos os países e aborda a questão da proteção dos dados de uma forma orientada à gestão do risco.

No RGPD procura-se, com base nos tipos de dados pessoais e nos processos que tratam esses dados, analisar o risco associado aos mesmos e às suas atividades de modo a determinar efetivamente o risco a que os mesmos estão sujeitos, permitindo aplicar as medidas e controlos de segurança da informação necessários para mitigar esses riscos e garantir que os dados pessoais e titulares dos mesmos estão protegidos de possíveis abusos da informação e ameaças.

Este trabalho foi proposto e desenvolvido para a EY Portugal, uma organização que fornece entre outros serviços, serviços de consultoria de segurança da informação tanto no mercado nacional como internacional, sendo o RGPD uma das áreas em que é especializada. Neste âmbito a EY apoia as organizações na implementação do regulamento e realiza auditorias a implementações. Neste contexto, surgiu uma oportunidade alinhada com as necessidades da organização que permitiu a identificação de uma área onde não existem métodos bem definidos para a sua realização, que é a identificação e gestão de processos de tratamento de dados pessoais que possam resultar em riscos elevados para os direitos e liberdades dos cidadãos.

1.1 Motivação

De acordo com o Artigo 35 (Avaliação de impacto sobre a proteção de dados) do RGPD, é obrigatório para qualquer processo de tratamento de dados pessoais que esteja sujeito a um risco elevado para os direitos e liberdades de um indivíduo, a realização de uma Avaliação de Impacto de Proteção de Dados (de sigla internacional DPIA) (Council of the European Union, 2016). Como tal surge a necessidade de uma metodologia que permita avaliar e identificar os riscos associados a esses processos por forma a poder-se determinar se os mesmos indicam um risco elevado para os direitos e liberdades dos cidadãos. Essa metodologia seria uma avaliação preliminar para se identificar os riscos de alto nível para os titulares dos dados nos tratamentos realizados pelo processo em questão, e, se identificado que o processo pode resultar num ou mais riscos elevados então aí complementar a realização de um DPIA.

Um DPIA é um processo interno de uma organização que deve ser desenvolvido para descrever os tratamentos, avaliar as necessidades e proporções desses tratamentos e ajudar a gerir os riscos para os direitos e liberdades dos titulares, avaliando e determinando as medidas a aplicar para mitigar os riscos. Os DPIAs permitem também definir um responsável pelo tratamento dos dados, e garantir que foram tomadas as medidas necessárias de mitigação de riscos para os titulares, e que a organização está em conformidade com o regulamento.

Quando após a realização de um DPIA se verifica que existiria um elevado risco para um processo de tratamento de dados na ausência das medidas tomadas pela organização para atenuar o risco, a organização deve consultar a Autoridade Supervisora (de sigla internacional DPA e que em Portugal será a CNPD), uma entidade reguladora pública que tem o propósito de ajudar a garantir a conformidade com o RGPD num estado membro, de acordo com o Artigo 36 (Consulta prévia) do regulamento. Nestes casos, a CNPD deverá aconselhar a organização sobre como proceder em tais casos, sugerindo medidas de mitigação de risco a implementar, ou até indicar que o processo de tratamento de dados em causa não deverá ser realizado, seguindo o Artigo 58 (Poderes), ponto 2 alínea f.

O regulamento refere um conjunto de tipos de atividade de tratamento de dados pessoais que devem ser considerados como risco elevado, mas em último caso depende de outros fatores relacionados com o tratamento em si. Ou seja, uma operação por si só, ainda que considerada de risco elevado, pode não implicar que efetivamente constitua um

risco. Por exemplo, o processamento de dados pessoais de um grande volume de titulares é indicado no regulamento como sendo um tratamento provável de resultar num risco elevado, no entanto se o processamento for de curta duração, onde é recolhido um conjunto de dados que não é considerado sensível, e se imediatamente após esse processamento forem aplicadas técnicas de minimização dos dados que não permitam identificar mais os titulares, este tratamento deixará de resultar num risco elevado para os titulares devido aos dados terem sido transformados num conjunto de dados que já não se encontram associados a ninguém em particular, logo deixando de se considerar dados pessoais. Atualmente não existe publicamente disponível uma metodologia para avaliar os riscos associados aos tipos de tratamento de dados que levem em conta os vários fatores associados ao tratamento e contexto em que vão processar os dados.

O RGPD afirma ainda que as Autoridades Supervisoras são obrigadas a definir e tornar pública uma lista de atividades de tratamento de dados que devem ser sujeitas obrigatoriamente a um DPIA. Nestes casos, um DPIA deverá ser efetuado de qualquer forma, e a metodologia de análise de risco proposta neste trabalho servirá para fazer uma avaliação dos riscos que será aproveitada na realização de um DPIA, nomeadamente para a alínea c) do ponto 7 do Artigo 35, caso o tratamento em causa constitua efetivamente um risco elevado para os direitos e liberdades dos titulares dos dados.

A subjetividade a que uma análise de risco de um processo de tratamento de dados está sujeito pode ser reduzida significativamente com uma metodologia que permita avaliar o risco com base no contexto, propósitos do tratamento de dados, criticidade dos dados pessoais e das aplicações envolvidas no tratamento, sendo assim mais fácil e direto propor soluções para mitigar os riscos associados. Para isso é necessário realizar, em primeiro lugar, uma avaliação de maturidade dos processos por forma a entender o seu estado em relação à conformidade com o regulamento e os controlos e medidas de segurança implementados. Dessa forma será possível calcular os riscos associados em função do RGPD e da segurança dos dados, e será mais simples de se sugerir controlos de segurança a aplicar em variadas situações, pela maior parte das organizações.

A necessidade de aplicar a metodologia proposta levou ainda à necessidade de se desenvolver uma ferramenta que permita efetuar uma avaliação de riscos específica para processos de tratamento de dados pessoais com base numa avaliação de maturidade, que simplifique todo este processo e permita à organização registar e mapear os seus processos organizacionais que envolvem dados pessoais, observar a maturidade e

conformidade com o RGPD, e ainda gerir os riscos inerentes aos processos, assim como os respetivos controlos de segurança implementados.

1.2 Objetivos

O objetivo principal deste trabalho é desenvolver um modelo de Análise de Risco para o RGPD, para ajudar a garantir a conformidade com o Artigo 35 através da realização de uma avaliação de criticidade do processo e da avaliação dos riscos para os dados pessoais dos titulares, com base numa avaliação de maturidade que permita determinar se se justifica a realização de um DPIA. Esta avaliação é orientada aos processos organizacionais que realizam tratamentos em dados pessoais e deve permitir não só identificar os riscos associados aos processos, como validar a conformidade desses processos com o RGPD em geral. Dessa forma o objetivo é fornecer uma metodologia, assim como validar a aplicabilidade da mesma, que permita às organizações:

- Ter os seus processos de tratamento de dados pessoais em conformidade com o RGPD, através da realização de uma avaliação de maturidade que permita entender o estado dos seus processos em relação à conformidade com os requisitos do regulamento;
- Melhorar os seus processos de gestão de risco, através da identificação e classificação de riscos a que os seus processos de tratamento de dados pessoais estão sujeitos, com base numa avaliação de maturidade;
- Através da identificação de tratamentos de risco elevado para os dados pessoais e do contexto dos processos, validar se os mesmos carecem da realização de um DPIA por forma a garantir a conformidade, mais concretamente com o Artigo 35 do RGPD;
- Assegurar com mais confiança a segurança dos seus dados pessoais, através da identificação de um conjunto de medidas e controlos de segurança da informação a implementar para mitigar os riscos associados, no que respeita às atividades de tratamento de dados pessoais;

Um objetivo paralelo aos pontos anteriores é ainda desenvolver um protótipo de uma ferramenta que permita colocar a metodologia proposta em prática e que seja passível de ser facilmente adaptado para se adequar à metodologia de gestão de risco e necessidades específicas de cada organização caso seja necessário.

1.3 Contribuições

A principal contribuição deste trabalho é a proposta de um modelo que servirá de base para realizar avaliações de maturidade dos processos organizacionais que contenham atividades de tratamento de dados pessoais, por forma a permitir a realização de análises de risco nesses processos, no âmbito do RGPD, que terá utilidade de imediato para apoiar as organizações a alcançar a conformidade com o Artigo 35 do regulamento, relativo a Análises de Impacto de Proteção de Dados (DPIAs) e a assegurar que os direitos e liberdades dos titulares são garantidos. Este modelo pretende contribuir para a uniformização de uma metodologia para a análise de risco, uma vez que o processo de análise de risco é algo que tende a ser muito característico de cada organização, e dessa forma de difícil adoção para organizações com diferentes modelos de negócio.

Para além do modelo proposto, é entregue um protótipo da ferramenta desenvolvida, que será a evidência mais concreta deste trabalho, e que permitirá observar a aplicação do modelo de forma clara e prática, permitindo às organizações terem uma noção dos tipos de controlos que devem implementar para reduzir os riscos associados aos seus processos que tratam dados pessoais e concluir se os tratamentos de dados em causa são viáveis.

1.4 Plano de trabalho

O plano de trabalho definido inicialmente incluía as seguintes etapas:

1. **Recolha de informação:** Levantamento de informação relacionada com o RGPD, motivações e respetivas barreiras/obstáculos à sua implementação (3 semanas);
2. **Identificação de riscos:** Identificar riscos / ameaças / danos relacionados com o RGPD, e determinar de que modo é que os mesmos podem ser classificados (5 semanas);
3. **Identificação do estado de organizações:** Definir conjuntos de questões que permitam avaliar o risco a que as atividades de tratamento de dados podem estar sujeitas (5 semanas);
4. **Modelo de Risco do RGPD:** Desenvolvimento de um modelo que permita classificar os riscos em função do tipo de atividade de tratamento, probabilidade de ocorrência e impacto dos mesmos para determinar que riscos são elevados e quais as medidas para os mitigar (5 semanas);

5. **RGPD numa organização:** Criação de uma lista de contexto de tratamento de dados para apoiar no ponto anterior, bem como uma lista de procedimentos para mitigar os riscos identificados durante a análise de risco (5 semanas);
6. **Aplicação do conhecimento:** Conclusões sobre o RGPD em relação à sua implementação na prática, quais as dificuldades que as organizações mais sentem em relação ao cumprimento com o regulamento, e aspetos mais relevantes do RGPD (3 semanas);
7. **Gestão de Risco em organizações:** Em que sentido é que o RGPD pode mudar a forma como se aborda a gestão de risco no contexto de uma organização (3 semanas);
8. **Escrita do relatório:** Desenvolvimento do relatório em paralelo com o projeto da EY e o trabalho no tema proposto (8 semanas);

O plano de trabalho apresentado com a proposta do mesmo foi sujeito a algumas alterações devido ao âmbito que tinha sido idealizado inicialmente ter sido mais aprofundado. A ideia inicial assentava no desenvolvimento de um modelo de análise de risco que permitisse identificar a maturidade das organizações em relação ao RGPD de uma forma mais geral, e que acabou por se direcionar para um artigo mais específico, o Artigo 35, após se ter identificado um défice de uma metodologia que permitisse analisar o risco no contexto desse artigo. No entanto o plano de trabalho manteve-se o mesmo quase na sua totalidade, tendo sido sujeito a algumas alterações de alto nível.

As primeiras duas etapas do plano de trabalho definido correram conforme expectável, permitindo o levantamento de informação relacionada com o RGPD, bem como um conjunto limitado de riscos relacionados com dados pessoais e informação relacionada esses riscos.

A terceira etapa atrasou-se cerca de duas semanas devido a ser uma tarefa mais complexa do que havia sido calculado inicialmente, e começou a ser desenvolvida já no contexto da quarta etapa, o modelo de risco. O resultado desta fase pretende permitir descrever a maturidade dos processos que tratam dados em relação ao RGPD, e como tal necessita de levar vários fatores em consideração, sendo necessária uma metodologia que permita identificar o estado desses fatores em relação aos processos em questão.

A quarta etapa também se atrasou umas semanas, apesar de uma das fases do modelo já ter sido desenvolvida na etapa anterior. O desenvolvimento do modelo necessitou de ser mais detalhado do que tinha sido identificado inicialmente. Começou-

se por se desenvolver um esboço do modelo, descrever de forma geral o que era esperado em cada fase, os *inputs* necessários e os resultados expectáveis, e posteriormente fase a fase foi-se começando a detalhar exatamente o que era suposto realizar em cada fase e como fazê-lo.

A quinta etapa descrita no plano de trabalho sofreu algumas alterações, não se identificando a necessidade de desenvolver uma lista de contextos de tratamento de dados, e os procedimentos para mitigar os riscos identificados foram traduzidos para controlos de segurança da informação de modo a mitigar os riscos identificados através do modelo de gestão de risco desenvolvido.

Para a sexta etapa, através da participação em projetos de auditoria de RGPD, foi possível obter conclusões relacionadas à sua implementação que permitiram começar a definir mais concretamente cada fase do modelo, assim como o protótipo para colocar o modelo em prática, tornando-os mais "amigáveis" do RGPD. Esta etapa acabou por ser desenvolvida em paralelo com a quinta e sétima etapas.

A sétima etapa, como dito anteriormente, foi realizada em paralelo com a sexta etapa, e foi uma etapa mais focada nas fases do modelo relacionadas com a gestão de risco, por forma a estarem mais alinhadas com o RGPD.

Por fim, a oitava etapa constituiu a escrita e composição do relatório, assim como a criação e desenvolvimento do protótipo. Nesta fase juntou-se o trabalho desenvolvido nas fases anteriores, melhorando a qualidade da informação e criando uma organização estruturada para a entrega final, afinando ainda alguns tópicos de acordo com a informação que ia sendo materializada no protótipo.

2 Conceitos e trabalho relacionado

2.1 Surgimento do RGPD

Apesar do conceito de privacidade datar da antiguidade, o que se entende pelo termo nos dias de hoje foi sendo alterado ao longo dos tempos, e tem influência da nossa realidade moderna orientada aos sistemas virtuais.

Já desde há muito tempo que existem preocupações com trocas de mensagens, havendo registos de na antiguidade se usarem cifras para evitar comprometer informações pessoais, existindo até atualmente uma técnica de cifra que recebeu o nome após um imperador romano, Júlio César, por este a utilizar nas suas mensagens privadas (Hal Abelson, 2008).

Nos EUA as preocupações com a privacidade surgiram cedo também, cerca do século XVIII, apesar dessas preocupações recentemente parecerem recentemente ter sido abandonadas devido a interesses. No século XIX nos EUA, o congresso decretou um estatuto em que quem interferisse com correspondência alheia seria multado ou preso. Anos mais tarde com o aparecimento do telégrafo, voltaram a surgir preocupações com a privacidade das comunicações, e quase 40 anos após a sua invenção foi também introduzido no congresso um projeto de lei para proteger a privacidade dos telegramas (Solove, 2006).

Em 1890 Warren e Brandeis publicaram um artigo intitulado "O Direito à Privacidade", que foi inspirado nas preocupações com a privacidade derivadas do grande crescimento dos jornais e do aparecimento das máquinas de fotografar. Neste artigo os autores comentam: "*A lei comum garante a cada indivíduo, o direito de determinar, a extensão com que devem ser comunicados os seus pensamentos, sentimentos e emoções a terceiros.*" (Solove, 2006).

Mais recentemente, a II guerra mundial causou um grande impacto, principalmente na Alemanha, sobre a forma como os cidadãos pensam na proteção dos dados e na privacidade. Durante o regime Nazi, foram utilizadas inúmeras formas para monitorizar o público, controlar e usar os cidadãos para reportarem comportamentos uns dos outros, ditando a vida pública e privada. Esta marca que ficou nos cidadãos levou à criação de uma secção na constituição específica para os direitos de proteção de dados e de liberdade pessoal (Freude).

Como tal, em 1970 no Estado de Hesse na Alemanha surgiu o primeiro ato de proteção de dados derivado do aumento da automação e do processamento de dados eletrónicos para colmatar preocupações com os dados tratados. Ainda que um bocado limitada comparada com legislações atuais, já tinha alguns dos elementos básicos que agora são usados, e após esse seguiram-se outros durante a mesma década (Jentzsch, 2007).

Em 1980 a Organização para a Cooperação e Desenvolvimento Económico, com a intenção de criar um sistema de proteção de dados em toda a Europa, publicou as "Recomendações do Conselho relativas às Diretrizes sobre a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais", que eram compostos por 8 princípios. No entanto estas diretrizes não eram obrigatórias e as leis de privacidade de dados variavam de acordo com os países. Estas variações acabaram por levar a que se propusesse uma diretiva a nível Europeu, a Diretiva de Proteção de dados 95/46/EC (Council of the European Union, 1980).

A diretiva 95/46/EC tinha o propósito de uniformizar as leis dos diferentes estados membros, mas sendo uma diretiva, ainda havia espaço para cada país fazer a sua interpretação e as organizações também nunca deram grande importância à mesma. Juntando a estes factos, o rápido crescimento dos dados *online* e da virtualização, surgiu a necessidade de uma atualização desta diretiva, agora sob a forma de um regulamento, o RGPD.

O RGPD já é de uma complexidade significante com grandes mudanças e impactos nos negócios, e como se trata de um regulamento, para além de ter que ser cumprido de igual forma em todos os países da União Europeia, a sua implementação é obrigatória também nos países membros. O cumprimento com este regulamento tem como princípio fundamental a gestão de riscos para os dados pessoais dos titulares dos dados, e implica que as organizações necessitem de realizar análises de risco aos seus processos que tratem dados pessoais e às suas atividades que os processam.

Em 1996 foi criado um órgão de aconselhamento Europeu em matéria de proteção e privacidade dos dados, Article 29 Working Party (ou Art 29 WP), resultante da diretiva 95/46/EC que é composto por representantes dos vários estados membros da União Europeia com o propósito de apoiar, aconselhar e criar recomendações relacionadas com a proteção e privacidade dos dados. Até ao momento a Art 29 WP já criou e publicou um conjunto de recomendações e diretrizes relacionadas com o RGPD (Article 29 Working Party, s.d.), das quais uma delas é relevante para este trabalho, as diretrizes para a

realização de DPIAs (Article 29 Data Protection Working Party, 2017) que será abordada mais à frente.

Atualmente está ainda para ser aprovada uma lei portuguesa para o regulamento de proteção de dados que visa traduzir o RGPD para a Português e transpor alguns dos tópicos, onde o regulamento deixa espaço para interpretação, para a lei Portuguesa. Em adição foi ainda aprovada a Resolução do Conselho de Ministros 41/2018 (Presidência do Conselho de Ministros, 2018), publicada a 28 de Março, que pretende especificar de forma mais técnica as medidas de segurança da informação a implementar para garantir a conformidade dos sistemas de informação com o regulamento por parte das entidades públicas.

2.2 Gestão de risco

Neste capítulo é descrito o ciclo de vida do risco, e como é que o mesmo deve ser abordado numa organização.

2.2.1 O que é o risco

O risco é considerado como o efeito da incerteza de um evento que pode ocorrer na persecução dos objetivos (International Organization for Standardization, 2009), sendo que no contexto deste trabalho serão apenas considerados riscos com impacto negativo. De acordo com o RGPD, na implicação (75), o risco é descrito da seguinte forma (Council of the European Union, 2016):

"O risco para os direitos e liberdades das pessoas singulares, [...], poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, …"

No contexto do RGPD, a probabilidade e impacto do risco dos direitos e liberdades dos titulares dos dados deve ser determinado com base na natureza, âmbito, contexto e propósito dos processos que envolvem tratamento dos dados pessoais. Como tal deve-se procurar identificar os riscos a que esses processos estão sujeitos e as vulnerabilidades que possam ser exploradas.

2.2.2 Processo de gestão do risco

O processo de gestão do risco é o processo da identificação e análise dos riscos, neste caso relacionados com processos que tratam dados pessoais, e os passos que se

tomam para reduzir o risco para um nível aceitável. De acordo com a ISO 27005 (International Organization for Standardization, 2011) o processo de gestão de risco, apresentado na Figura 1 - Fases do processo de gestão do risco, é composto pelas seguintes fases:

1. **Definição do contexto:** A fase de definição do contexto serve para definir o âmbito da realização da gestão do risco e ainda os critérios sobre os quais se vai avaliar o risco. O âmbito desta fase deve ser alinhado com o contexto e objetivos da organização;
2. **Análise de riscos:** Nesta fase determina-se o valor dos ativos, identifica-se as ameaças e vulnerabilidades, os controlos existentes e os seus efeitos nos riscos identificados, determina-se as suas potenciais consequências, e finalmente prioriza-se os riscos identificados. Esta fase divide-se em 3 subfases:
    a. **Identificação de riscos:** Aqui pretende-se determinar o que é que pode vir a ocorrer que possa causar potenciais perdas e tentar perceber como e porque é que essas perdas podem acontecer;
    b. **Estimativa de riscos:** Nesta atividade o objetivo é determinar o valor dos riscos através da análise das componentes que permitem determinar esse valor, como a probabilidade de ocorrência e o impacto dos riscos;
    c. **Avaliação de riscos:** Tendo como *input* os riscos estimados do passo anterior, são comparados os níveis de risco obtidos com os critérios de avaliação e aceitação de risco definidos durante o estabelecimento do contexto;
3. **Tratamento do risco:** Nesta fase são determinados os controlos para reduzir, manter, evitar ou partilhar os riscos e define-se um plano de implementação;
4. **Aceitação do risco:** Chegando à fase de aceitação do risco, toma-se a decisão de se aceitar ou não o plano de tratamento ao risco, com base nos riscos residuais que poderão subsistir;
5. **Comunicação do risco:** Na fase de comunicação e consulta essencialmente trocam-se informações sobre os riscos entre os responsáveis pelas tomadas de decisões e pelos *stakeholders* com o intuito de todas as partes envolvidas terem conhecimento dos riscos existentes e das tomadas de decisões;
6. **Monitorização e análise crítica de riscos:** Os riscos e respetivos fatores devem ser monitorizados e revistos por forma a dar continuidade ao ciclo de vida da gestão do risco.

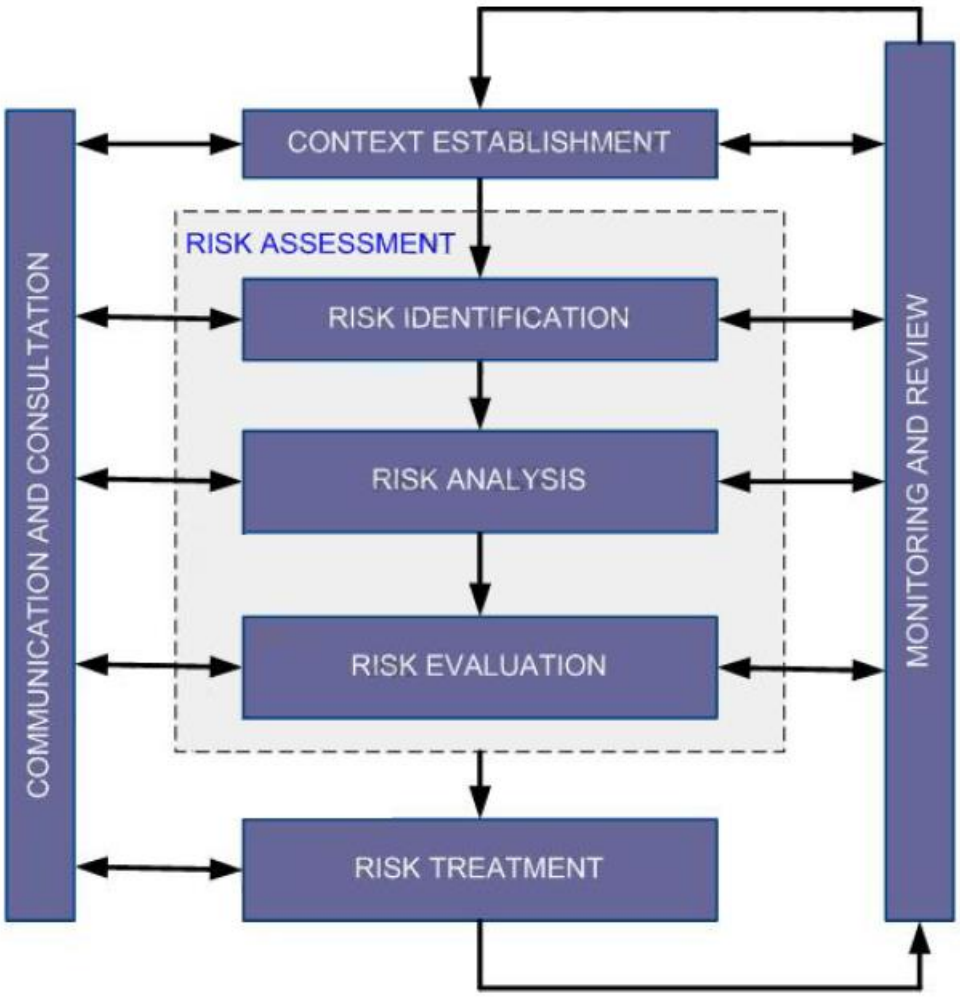


Figura 1 - Fases do processo de gestão do risco. Fonte: ISO 27005, figura 1.

A gestão do risco é um processo contínuo que deve fazer parte da estratégia da organização, endereçando os riscos relacionados com as atividades da mesma. Esta gestão deve ser integrada na cultura da organização com uma política e programa efetivos que traduzem a estratégia em objetivos táticos e operacionais, permitindo definir responsáveis pelos riscos. Esta gestão deve permitir às organizações minimizar o risco por forma a estar alinhado com o seu apetite ao risco, ou seja, a "quantidade" e natureza do risco que as organizações estão dispostas a aceitar.

Com uma gestão de risco já integrada na cultura de uma organização, torna mais fácil e transparente a implementação das Avaliações de Impacto de Proteção de Dados nas suas atividades de processamento de dados pessoais.

2.2.3 Fatores de risco

O risco é constituído por um conjunto de fatores que juntos podem dar origem a um evento inesperado que irá causar um impacto, sendo no contexto deste trabalho, o impacto nos titulares dos dados pessoais.

Um ativo, por exemplo dados pessoais na posse de uma organização, pode estar sujeito ao risco através de uma ou mais vulnerabilidades, que são exploradas através de ameaças (p.e., vírus) por agentes de ameaça (p.e., *hackers*). A partir deste ciclo é possível calcular o risco associado aos dados pessoais (ISACA, 2015).

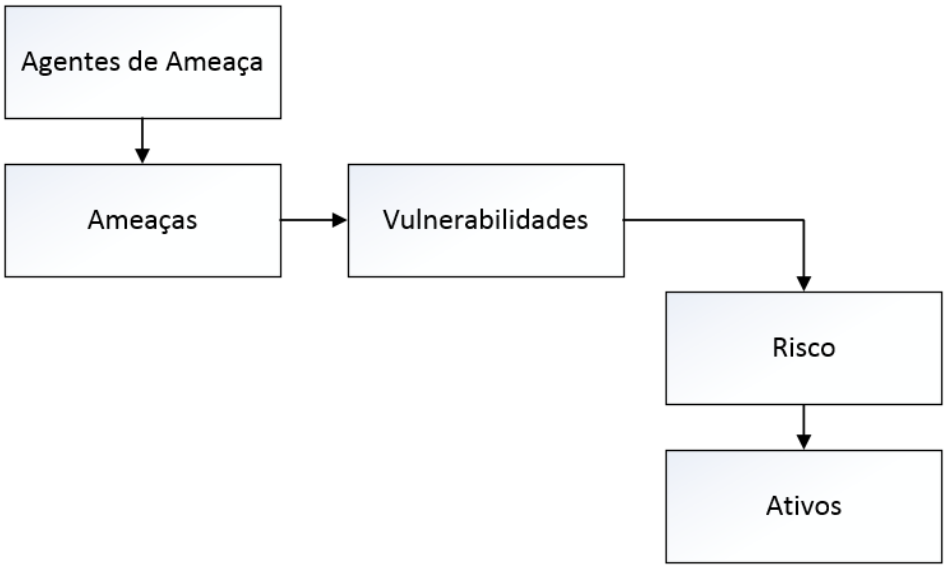


Figura 2 - Fatores de risco. Fonte: CRISC 2015, figura 1.15

Na figura 2 podemos observar a sequência dos fatores principais associados ao risco, sendo o risco consequência da possibilidade de ocorrência dos três primeiros fatores, permitindo desta forma a realização de uma análise de risco mais precisa.

Neste trabalho a abordagem face aos riscos é orientada aos processos de tratamento de dados, de acordo com as guias de orientação definidas pelo regulamento. Como tal na imagem descrita em cima, a caixa "Ativos" representa os processos que tratam dados pessoais e respetivos dados pessoais, para os quais serão identificados e classificados os riscos e vulnerabilidades em função desses tipos de processos.

2.2.4 Risco elevado

Risco elevado é um conceito que apesar de não estar claramente definido no RGPD, tem referências em alguns artigos e implicações.

Através de informação extraída ao longo do regulamento é possível indicar o risco elevado como resultado da consideração de um conjunto de critérios envolvendo a

segurança dos dados, potencial de uma fuga de informação, garantia de privacidade, limitação dos propósitos e motivos do processamento. Alguns exemplos de tipos de processamentos que podem ser considerados como risco elevado são descritos posteriormente neste capítulo.

Como tal o risco elevado no contexto deste trabalho irá ser definido como um risco que possa resultar em consequências significantes para um titular dos dados, em que este possa ter dificuldades sérias para superar essas consequências. Este tema será mais desenvolvido no capítulo 3, durante a avaliação dos riscos.

2.3 Processo de tratamento de dados

Um processo de tratamento de dados, abreviadamente um processo, é qualquer processo organizacional em que sejam tratados dados pessoais, ou seja, que está ao abrigo do RGPD. Um processo é um conjunto de atividades, e podem nem todas as atividades envolver tratamentos com dados pessoais, e como tal, as medidas impostas pelo regulamento são orientadas a essas atividades que envolvem dados pessoais.

Por forma a simplificar a análise dos processos, iremos abstrair-nos das atividades, e considerar os riscos dessas atividades como riscos do processo. Estes processos, quando possivelmente possam representar um risco elevado para os direitos e liberdades dos cidadãos, servirão como *input* para as Avaliações de Impacto de Proteção de Dados.

Temos como exemplo de um processo de tratamento de dados que costuma existir em todas as organizações, embora implementado de diferentes formas, o processo de recrutamento. Este processo é constituído por várias fases, como entrevistas, recolha de dados dos candidatos, consultas de médico, entre outras. Uma vez que este processo contém dados pessoais, está ao abrigo do RGPD, e como tal, deve ser alvo de uma análise de risco que poderá determinar se deve ser realizada uma Avaliação de Impacto de Proteção de dados.

2.3.1 Responsável do processo de tratamento de dados

O responsável do processo de tratamentos de dados pessoais é a pessoa (ou pessoas) que determine as finalidades e meios do tratamento dos dados. Caso dois ou mais responsáveis determinem de forma conjunta as finalidades e meios do tratamento, todos devem ser considerados corresponsáveis pelo tratamento. Neste caso devem ficar bem definidas as responsabilidades de cada corresponsável, na gestão dos pedidos de exercício

de direitos pelos titulares dos dados. De qualquer forma, os titulares podem exercer os seus direitos perante e contra cada um dos corresponsáveis.

2.4 Avaliação de Impacto de Proteção de Dados

De acordo com o Artigo 35 do regulamento, deve sempre ser realizada uma Avaliação de Impacto de Proteção de Dados (ou um DPIA), para todas atividades de tratamento de dados que possivelmente resultem num risco elevado para os direitos e liberdades dos titulares dos dados, tendo em conta a natureza, âmbito, contexto e propósitos do tratamento. Um DPIA é um processo usado para descrever uma atividade de tratamento de dados ou até todo um processo que contenha atividades de tratamento de dados, avaliar a necessidade e proporcionalidade dos tratamentos e para ajudar a gerir os riscos para os direitos e liberdades dos titulares resultantes do tratamento de dados pessoais.

Para além dos pontos descritos anteriormente, um DPIA deve também conter a avaliação de necessidade da operação e dos riscos a que está sujeita, assim como as medidas propostas para mitigar os riscos para um nível aceitável. Esta avaliação deve ser realizada com o apoio do Encarregado de Proteção de Dados, o responsável pela conformidade com o RGPD numa organização.

Sempre que um DPIA indique que o processo de tratamento de dados efetivamente possa resultar num risco elevado, se a organização não conseguir mitigar esse risco, a mesma deve consultar a CNPD para obter um parecer sobre se deverá avançar com o tratamento ou se deverá cessar essa atividade.

Na figura em baixo estão ilustrados os princípios básicos associados a um DPIA (Article 29 Data Protection Working Party, 2017):

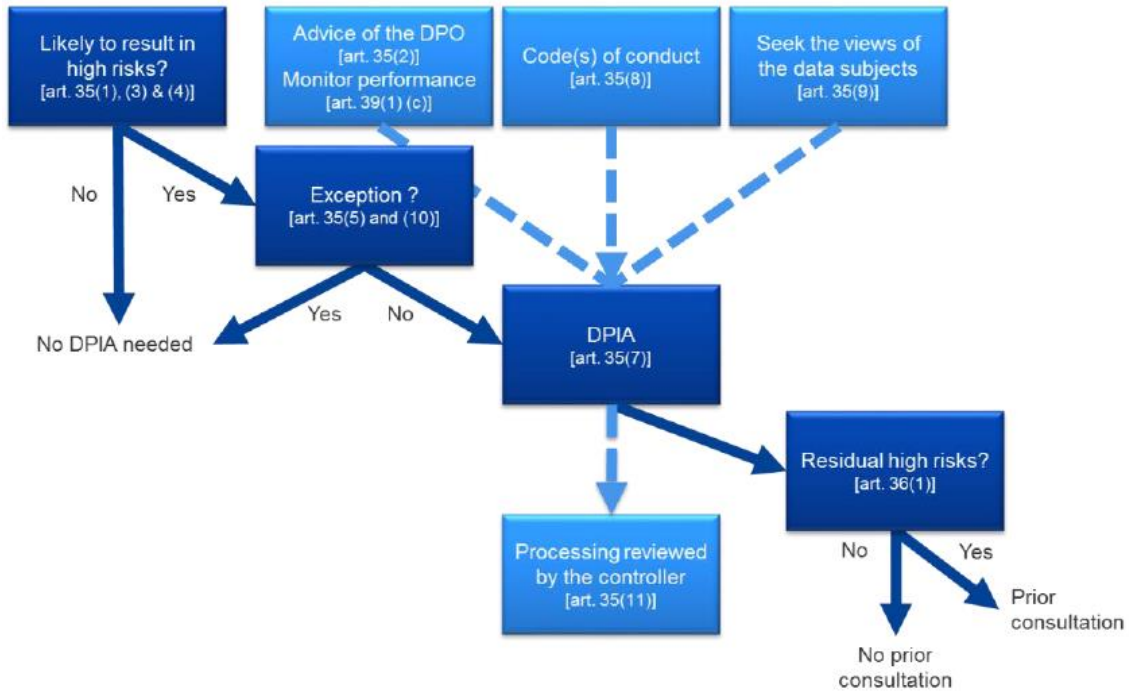


Figura 3 - Workflow de um DPIA. Fonte: Article 29 Data Protection Working Party, pág. 6

Na realização de um DPIA em si, segundo a alínea 7 do Artigo 35 do RGPD, o mesmo é constituído pelo menos pelo seguinte:

a) Uma descrição sistemática das operações de tratamento previstas e o propósito do tratamento, incluindo quando aplicável, o interesse legítimo da organização;
b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação ao propósito do tratamento;
c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados;
d) As medidas previstas para endereçar os riscos, incluindo proteções, medidas de segurança e mecanismos para garantir a proteção dos dados pessoais e demonstrar conformidade com o regulamento tendo em conta os interesses legítimos dos titulares.

Para além do DPIA ser um processo obrigatório para cumprir com o RGPD, serve também para demonstrar que foram tomadas as medidas necessárias para garantir a conformidade com os requisitos do regulamento, e para atribuir responsabilidades às atividades de tratamento de dados.

2.4.1 Casos em que é recomendada um DPIA

De acordo com as diretrizes para a realização de DPIAs pela Art 29 WP (Article 29 Data Protection Working Party, 2017), que têm como base o regulamento, uma atividade

de tratamento de dados pode estar sujeita a um risco elevado se se cumprirem pelo menos dois dos seguintes critérios:

1. Processamento automatizado de dados onde é traçado um perfil dos indivíduos (*profiling*), especialmente informação relacionada com o desempenho no trabalho, situação económica, saúde, preferências pessoais ou interesses, confiabilidade ou comportamento, localização ou deslocações;
2. Processamento automatizado de dados, em que sejam tomadas decisões legais para o indivíduo, ou decisões de efeito semelhante;
3. Processamento de dados utilizados para observar, monitorar ou controlar indivíduos, incluindo dados recolhidos através de monitoramento sistemático em locais públicos;
4. Processamento de dados sensíveis. No capítulo seguinte estão descritos os dados que se inserem nesta categoria;
5. Processamento de dados em grande escala. Ainda que no RGPD não exista uma definição do que é considerado grande escala, alguns fatores que podem impactar neste sentido são o número de indivíduos em questão, o volume de dados, a duração do processamento e a extensão geográfica da atividade de processamento.
6. Processamento sobre conjuntos de dados que tenham sido combinados, por exemplo resultantes de operações com diferentes propósitos;
7. Processamento de dados de indivíduos vulneráveis, como crianças e indivíduos com incapacidades;
8. Processamento de dados através do uso de novas tecnologias no mercado ou na organização;
9. Transferência de dados para fora da União Europeia;
10. Processamento de dados que possa impedir indivíduos de exercer algum direito ou usufruir de serviços ou contratos.

É importante ter em consideração que só por ter pelo menos dois dos critérios em cima não quer dizer que a atividade de tratamento de dados vá resultar num risco elevado. Quantos mais dos critérios se aplicarem mais provável é que o processamento contenha um risco elevado, no entanto essa atividade deve ser sujeita a uma análise de risco onde se leve em conta outros fatores descritos na secção 2.4 acima.

2.4.2 Dados sensíveis

No RGPD foi criada uma nomenclatura para dados pessoais de categorias especiais que são classificados como sendo dados sensíveis. Estes dados são considerados sensíveis por a sua exposição ser mais crítica, podendo colocar em causa os direitos e restringir as liberdades e opções dos titulares dos dados.

De acordo com o regulamento, os dados considerados sensíveis são os seguintes: Dados de raça, etnia, opiniões políticas, crenças religiosas ou filosóficas, dados de sindicatos, dados genéticos, dados de saúde, dados relacionados com a vida sexual, dados de registo criminal e ofensas.

2.5 Obrigações do RGPD

Para além do DPIA em processos de risco elevado que contêm tratamentos de dados pessoais, as organizações têm que cumprir com outros requisitos impostos no regulamento, para que os cidadãos da UE possam usufruir dos direitos e liberdades que o RGPD oferece. Esses requisitos visam não só reduzir os riscos associados ao processamento de dados pessoais como garantir que as organizações têm noção dos riscos a que estão sujeitos e dos controlos de mitigação que devem implementar, assim como as medidas a tomar em caso de uma fuga de informação que possa comprometer os dados processados.

2.5.1 Principais obrigações das organizações

Esta secção pretende descrever as principais obrigações que devem ser implementadas pelas organizações para que estejam em conformidade com o regulamento, e de que forma é que essas obrigações influenciam na gestão do risco.

2.5.1.1 Nomeação de um Encarregado de Proteção de Dados

No Artigo 37 (Designação do encarregado da proteção de dados) está especificado que uma organização deve designar um Encarregado de Proteção de dados em qualquer caso em que:

a) O processamento de dados pessoais é realizado por uma autoridade pública, à exceção de tribunais na realização de deveres jurídicos;
b) As atividades base da organização consistem em operações que necessitem de monitorização regular e sistemática de indivíduos em grande escala;

c) As atividades base da organização consistem no processamento em grande escala de dados sensíveis;

O Encarregado de Proteção de Dados é o responsável pela conformidade com o regulamento numa organização, servindo também como ponto de contacto com os titulares dos dados e a entidade reguladora.

2.5.1.2 Responsabilidade

De acordo com o Artigo 24 (Registos das atividades de tratamento) a organização deve ter documentadas as políticas, procedimentos e operações de processamento de dados que comprovam que a organização está em conformidade com o regulamento, e que devem ser disponibilizados à entidade reguladora caso seja requisitado.

2.5.1.3 Privacidade incorporada no desenho

No Artigo 25 (Proteção de dados desde a conceção e por defeito) está especificado que as organizações devem incorporar a proteção de dados apropriada por defeito, desde a conceção, no desenho e desenvolvimento dos processos, levando em conta os dados que tratam, o tipo de tratamento, e os riscos a que podem estar sujeitos de forma a estar em conformidade com o regulamento e a proteger os direitos dos indivíduos.

Devem ser implementadas medidas para garantir que apenas os dados necessários são recolhidos, processados, acedidos, e apenas durante o período de tempo necessário.

2.5.1.4 Consentimento

O Artigo 7 (Condições aplicáveis ao consentimento) indica que nos casos em que o processamento de dados é feito com base no consentimento, a organização deve ser capaz de provar que o indivíduo deu o seu consentimento. A organização deve esclarecer de forma clara e concisa o propósito para qual os dados irão ser processados, e deve ser possível aos indivíduos retirar o consentimento tão facilmente como foi dá-lo.

No Artigo 8 (Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação) é contemplado o consentimento aplicado aos menores, sendo que nestes casos o consentimento deve ser dado pelos encarregados de educação ou tutor do menor.

2.5.1.5 Notificação

No Artigo 33 (Notificação de uma violação de dados pessoais à autoridade de controlo) está definido que em caso de uma fuga de informação que afete dados pessoais,

a organização deve num período máximo de 72 horas, depois de se aperceber da fuga, notificar a entidade reguladora, informando a causa da fuga, potenciais consequências da mesma, o número aproximado de indivíduos afetados e o número de registos em causa, assim como os detalhes do Encarregado de Proteção de Dados, caso seja necessário pedir detalhes posteriormente.

A organização deve também, de acordo com o Artigo 34 (Comunicação de uma violação de dados pessoais ao titular dos dados), notificar os indivíduos afetados pela fuga de dados no caso de se verificar que pode resultar num risco elevado para os direitos e liberdades desses indivíduos. Esta notificação deve esclarecer como é que essa fuga pode ou irá afetar o indivíduo.

2.5.1.6 Dicionário de dados

Segundo o Artigo 30 (Registos de atividades de processamento) deve ser mantido um registo das atividades de processamento que deve conter essencialmente informação relacionada com os processos de tratamento de dados que permita identificar os propósitos e finalidades dos mesmos, os responsáveis pelos tratamentos e os fluxos dos dados pessoais.

2.5.1.7 Transferências de dados para terceiros

De acordo com Artigo 44 (Princípios gerais para transferências), transferências através de fronteiras podem apenas ser realizadas quando houverem garantias de que os terceiros cumprem com o regulamento e os motivos da transferência estão devidamente justificados.

2.5.2 Coimas associadas ao RGPD

O não cumprimento com um conjunto específico de artigos do RGPD pode levar à aplicação de coimas pela CNPD, de acordo com o Artigo 83 (Condições gerais para a aplicação de coimas) do regulamento. Essas coimas podem variar entre “baixas” ou elevadas.

As coimas categorizadas como baixas não são de todo baixas, apenas significa que têm um valor menor associado às mesmas, sendo esse valor passível de ir até 10 milhões de euros ou até 2% da faturação anual global da organização, enquanto que as coimas elevadas podem ir até aos 20 milhões de euros ou até 4% da faturação anual global da organização.

2.6 Riscos relacionados com o RGPD

Para se realizar uma análise de risco nas atividades de tratamento de dados pessoais, é necessário reunir primeiro um conjunto de tipos de tratamentos que sejam realizados pelas organizações, que possam estar sujeitos a riscos. Segundo, é necessário identificar os riscos em si que possam estar associados aos tratamentos de dados identificados.

2.6.1 Tratamentos de dados potencialmente sujeitos a risco

Com base principalmente na lista elaborada no capítulo 2.4.1, de atividades de processamento possíveis de resultar em riscos elevados extraídas de algumas implicações e artigos (como por exemplo das implicações 75, 89, 91, e dos Artigos 32 [Segurança do tratamento] e 35), definiu-se o conjunto de tipos de tratamentos considerados como possíveis de resultar num risco elevado que irá ser utilizado neste trabalho, e que possam implicar que um processo de dados pessoais seja sujeito à realização de um DPIA.

Tabela 1 - Tratamentos sujeitos a risco

Tratamentos sujeitos a risco	Descrição
Processamento automatizado de dados onde é traçado um perfil dos indivíduos (profiling)	Especialmente informação relacionada com o desempenho no trabalho, situação económica, saúde, preferências pessoais ou interesses, confiabilidade ou comportamento, localização ou deslocações.
Processamento automatizado de dados com consequências legais	Em que sejam tomadas decisões legais para o indivíduo, ou decisões de efeito semelhante.
Processamento de dados utilizados para observar, monitorar ou controlar indivíduos	Incluindo dados recolhidos através de monitoramento sistemático em locais públicos.
Processamento de dados sensíveis	Quando são processados dados sensíveis, de acordo com o especificado no RGPD.
Processamento de dados em grande escala	Processamento de dados de um número elevado de indivíduos, ou um elevado volume ou com uma grande extensão geográfica.

Processamento sobre conjuntos de dados que tenham sido combinados	Por exemplo dados com origem em diferentes fontes ou resultantes de operações com diferentes propósitos.
Processamento de dados de indivíduos considerados vulneráveis	Como crianças, idosos e indivíduos com incapacidades.
Processamento de dados através do uso de novas tecnologias	Quando são utilizadas novas tecnologias, seja no mercado, seja nova na organização.
Transferência de dados para fora da União Europeia	Quando dados processados ou por processar são transferidos para fora da UE.
Processamento de dados que possa impedir indivíduos de exercer direitos	Ou de usufruir de serviços ou contratos.
Processamento de novos tipos de dados pessoais	Quando é realizado o processamento de novos tipos de dados que não eram processados antes.
Novos tipos de processamento de dados	Quando são realizados novos tipos de processamento de dados que não eram realizados antes.

É importante realçar que esta lista não é exclusiva e que podem haver outros tratamentos que possam ser considerados como resultando num risco elevado, dependendo de vários fatores. No âmbito deste trabalho será utilizado este conjunto mas outros poderão ser acrescentados se se verificar necessário.

2.6.2 Riscos relacionados com tratamentos de dados pessoais

O Centro de Informação de Políticas de Liderança (CIPL) (CIPL, 2016) com a sua vasta experiência no desenvolvimento de matrizes de risco e projetos anteriores, desenvolveu um documento com umas linhas orientadoras para o desenvolvimento de um modelo de risco no RGPD, onde juntamente com o conjunto de tratamentos possíveis de resultar num risco elevado descrito no capítulo anterior identificado pela Art 29 WP (Article 29 Data Protection Working Party, 2017), fez ainda o levantamento de potenciais riscos relacionados com o tratamento de dados pessoais que podem levar à causa de dano nos titulares dos dados e por consequente ter um impacto negativo nos mesmos.

Tabela 2 - Riscos relacionados com tratamentos de dados pessoais

Risco
Recolha de dados não justificada
Recolha de dados excessiva
Acesso não autorizado aos dados
Destruição ou alteração acidental/ilegal de dados
Divulgação não autorizada de dados
Roubo de dados
Uso/Armazenamento de dados desatualizados
Utilização dos dados para além do que é expectável
Utilização dos dados para além do que é socialmente aceitável
Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar

Existem outros tipos de riscos ainda que podem ser relevantes no contexto dos dados pessoais por poderem afetar sistemas de informação que contenham este tipo de dados, no entanto no contexto deste trabalho vamos limitar a este conjunto de riscos, e tal como nos tratamentos de dados potencialmente sujeitos a um risco elevado, aqui também se poderão acrescentar outros riscos caso se verifique a sua necessidade.

2.7 Trabalho relacionado

No âmbito deste trabalho foi feita uma pesquisa sobre as opções existentes no mercado relacionadas com o tema de Avaliação de Impacto de Proteção de Dados de onde foram aproveitados e explorados alguns conceitos.

Para além da pesquisa realizada, surgiu a oportunidade de analisar algumas metodologias de Avaliação de Impacto de Privacidade (ou PIAs, do inglês *Privacy Impact Assessments*) de um conjunto de organizações em Portugal, principalmente no setor financeiro, o que permitiu aproveitar e trabalhar alguns conceitos, principalmente ao nível da gestão de risco num contexto geral, ou seja sem ser direcionado especificamente para dados pessoais, e ainda de analisar resultados de projetos de auditoria de conformidade com o RGPD e de participar num, noutras organizações, o que ajudou a reunir alguma informação relevante para o projeto.

Em relação à pesquisa feita, existe ainda relativamente pouco trabalho realizado disponível neste âmbito, e é difícil encontrar trabalhos mais concretos desenvolvidos. Isto acontece principalmente porque as organizações que desenvolvem estas metodologias usam-nas como parte do seu negócio e como tal não é do seu interesse ter as mesmas disponíveis publicamente.

Apesar disso, ao longo dos últimos dois anos após a publicação do RGPD, algumas organizações com o propósito de apoiar na proteção e privacidade dos dados têm vindo a publicar documentos com linhas orientadoras para o desenvolvimento de DPIAs e modelos de avaliação do risco no contexto de privacidade dos dados, sendo alguns deles referidos no presente trabalho, como a ICO (ICO, s.d.) e a CNIL (CNIL, 2018), e ainda da Art 29 WP (Article 29 Data Protection Working Party, 2017) e do CIPL (CIPL, 2016).

2.7.1 Autoavaliação de proteção de dados

A ICO, entidade reguladora do Reino Unido, desenvolveu um conjunto de questionários com temas distintos (ICO, s.d.), relacionados com a privacidade dos dados para permitir avaliar a maturidade das organizações em relação a esses temas. Estes questionários estão orientados para pequenas e médias empresas, mais na ótica de garantir que as organizações cumprem os requisitos de privacidade dos dados, não estando focados nos riscos para os direitos e liberdades dos titulares. Não existe um mapeamento com os artigos do RGPD, dificultando um pouco depois a perceção do estado de conformidade das organizações com o regulamento, e são utilizados 4 níveis de classificação de maturidade que permitem após o término do questionário a definição de um conjunto de medidas que constituem um plano de ação. O plano de ação final não contempla aspetos mais técnicos, nem está direcionado para a definição de medidas de segurança da informação, estando mais orientado a definir medidas processuais.

2.7.2 Realização de avaliação de impactos de privacidade

Este é um documento desenvolvido pela ICO que tem como propósito ajudar as organizações a entender o que é uma avaliação de impacto de privacidade (ICO, 2014), quando é que estas devem ser realizadas, quais os critérios para a sua realização, os riscos que podem existir para os cidadãos e como é que as organizações devem integrar estas avaliações nos seus processos.

2.7.3 Bases de conhecimento

Um dos documentos da CNIL relacionados com o tema de DPIAs (CNIL, 2018), de Fevereiro de 2018, que fornece um conjunto de informações relacionadas com o RGPD, mais concretamente relacionadas com o risco e a sua classificação, e com segurança da informação. A informação relacionada com o risco serve como introdução para os restantes capítulos, em que em cada um se pretende abordar um tema específico

de segurança da informação, onde tem descritas as boas práticas relacionadas com o tema e como é que o mesmo deve ser tratado no RGPD.

2.7.4 PIA

Para além dos documentos relacionados com o tema, a CNIL lançou ainda no fim de janeiro do presente ano a versão beta de um *software open source*, intitulado de PIA, para apoiar no desenvolvimento dos DPIAs (CIPL, 2016). O PIA tem como objetivo permitir a uma organização realizar e gerir os DPIAs dos seus processos num só local.

Este *software* tem uma secção para preencher os detalhes de um DPIA, orientado com o que está descrito no capítulo 2.3, no entanto não leva depois esses fatores em conta na apresentação dos resultados finais ou para uma análise de maturidade do processo, servindo apenas para registo e posterior revisão. Tem também uma secção direcionada para os riscos relacionados com o processo, divididos em três categorias, acesso ilegítimo aos dados, modificações não pretendidas nos dados e desaparecimento dos dados, que possibilita a introdução dos impactos, ameaças, fontes de riscos e de controlos de mitigação, e também estimar o impacto e probabilidade dos riscos ocorrerem.

De certa forma, este *software* fornece uma avaliação de risco que pretende ser dinâmica, mas que não leva em conta a maturidade do processo, ao contrário do modelo proposto que apesar da análise de risco ser mais estática, utiliza a maturidade do processo de tratamento de dados como base para a análise de risco o que permite obter resultados mais alinhados com o RGPD.

No final, após preenchidas as secções do DPIA e de avaliação de risco, é apresentado um resumo dos riscos e tem uma secção para se definirem planos de ação, não sugerindo medidas concretas, que é um dos objetivos propostos do trabalho apresentado neste documento, apresentar algumas soluções para resolver as inconformidades com o RGPD e mitigar os riscos identificados, cabendo depois à organização definir a sua estratégia de implementação.

2.7.5 Linhas orientadoras para um DPIA

Um dos documentos desenvolvidos pela Art 29 WP, tem como foco a realização dos DPIAs, assim como em que situações é que um DPIA deverá ser realizado. De certa forma este documento acaba por ser uma interpretação do RGPD mas com exemplos mais concretos, e alguns conceitos melhor definidos, permitindo obter uma visão de um lado

mais prático do regulamento, uma vez que este por vezes é um bocado abstrato e tem lugar para muita interpretação.

No fundo o objetivo acaba por ser fazer uma tradução do que está definido no RGPD sobre os DPIAs para que as organizações possam mais facilmente definir os seus processos de realização de DPIAs.

2.7.6 Avaliações de Risco e DPIAs no âmbito do RGPD

No fim do ano de 2016, a CIPL escreveu um artigo interpretando o conceito de risco e das Avaliações de Impacto de Proteção de Dados através dos artigos e implicações do RGPD, relacionando com a sua própria abordagem ao risco, propondo dessa forma um conjunto de riscos que devem ser levados em conta relacionados com privacidade dos dados, assim como uma sugestão de como é que o desenvolvimento de uma metodologia para a realização dos DPIAs deve ser abordado.

Este documento abrange vários aspetos a considerar na definição de uma metodologia baseada numa avaliação de risco e consegue extrair do regulamento os pontos relevantes que devem ser considerados neste âmbito. Devido à abrangência dos conceitos abordados o documento acaba por fazer sugestões de alto nível, definindo no entanto umas linhas orientadoras em sincronia com o RGPD.

3 Modelo para análise de risco

O trabalho consiste na proposta de uma metodologia, assim como um protótipo de uma ferramenta que permita aplicar essa metodologia, no âmbito do Artigo 35 do RGPD. Esta metodologia pretende servir como uma pré-avaliação dos riscos em processos de tratamento de dados pessoais, com base numa avaliação de maturidade que permita validar se esses processos podem constituir um risco elevado para os titulares, e como tal, se os processos devem ser sujeitos a um DPIA. Adicionalmente pretende-se ainda validar a conformidade dos processos com o regulamento e identificar um conjunto de medidas e controlos de segurança adequados para garantir a conformidade e mitigar os riscos identificados.

Sendo o RGPD um regulamento aplicável a todas as organizações, este deixa espaço para interpretação em alguns artigos, por forma a dar mais liberdade de aplicação do regulamento, e por vezes descreve os artigos com algum nível de abstração deixando espaço para interpretação de acordo com o contexto em que os tratamentos são efetuados. Como tal, neste trabalho podem ser feitas algumas suposições que procuram ser justificadas, mas que em último caso podem sempre ser adaptadas de acordo com as necessidades das organizações.

Para este trabalho é importante definir-se como podemos fazer uma análise dos riscos associados a um processo de tratamento de dados, e para isso vai ser necessário uma abordagem faseada, que permita identificar os riscos, neste caso através de uma avaliação de maturidade, avaliar os riscos associados aos dados pessoais tratados, e posteriormente identificar formas de mitigar esses riscos. Esta necessidade levou ao desenvolvimento de um modelo de Análise de Risco orientado à privacidade dos dados pessoais que procura ser útil, e que facilite as organizações tanto a alcançar a conformidade com o RGPD, como a avaliar e garantir a maturidade dos controlos de segurança que procuram proteger e garantir a privacidade dos dados, em função dos riscos a que os mesmos podem estar sujeitos. Para permitir cumprir com estes objetivos é importante que o modelo cumpra com alguns requisitos.

3.1 Identificação e análise de requisitos

Como foi dito anteriormente é importante que o modelo cumpra com um conjunto de requisitos, nomeadamente relacionados com o RGPD, com a gestão de risco e com a aplicabilidade do modelo.

O RGPD estabelece um conjunto de normas que constituem requisitos obrigatórios para o modelo a desenvolver. Estes são:

- Deve existir uma forma de verificar a conformidade dos processos com o RGPD por forma a permitir uma identificação dos riscos eficaz;
- Como resultado da aplicação do modelo deve ser possível identificar as medidas a realizar para mitigar as falhas de conformidade com o RGPD;
- O resultado da aplicação do modelo deverá ainda ser útil para cumprir com o Artigo 35, caso durante a sua aplicação se verifique a necessidade da realização de um DPIA;

Derivado da análise de resultados de projetos de auditoria de RGPD, e do contexto da organização em que o trabalho está a ser desenvolvido, surgiram os seguintes requisitos:

- O modelo deve facilitar a gestão do risco para os processos organizacionais, permitindo a este tornar-se uma componente do ciclo de vida dos processos que não seja mais um obstáculo ou impedimento para a realização de um processo;
- Deve ser genérico o suficiente para permitir adaptar-se a diferentes modelos de negócio, uma vez que todas as organizações potencialmente tratam dados pessoais, tendo objetivos e realidades diferentes;

Para se poder desenvolver um modelo de gestão de risco alinhado com o RGPD, uma vez que não se encontrou nenhum modelo do género disponível publicamente, surge a necessidade de se especificar de raiz um conjunto de requisitos que permita integrar a proteção e privacidade dos dados como foco do modelo e garantir que a gestão de risco é seguida de acordo com as melhores práticas. Como tal, e levando em conta os requisitos anteriores, é especificado um conjunto de requisitos que permite desenvolver um modelo de gestão de risco integrado com o RGPD:

- Deve ser identificado um conjunto de riscos que sejam relevantes para uma análise de risco orientada à privacidade dos dados pessoais;
- Deve ser feito um mapeamento realista com os riscos identificados e os artigos do regulamento, por forma a permitir associar o não cumprimento de um determinado artigo com um ou mais riscos.
- As fases de gestão do risco devem estar alinhadas com as melhores práticas no mercado, nomeadamente práticas relacionadas com a gestão de risco no contexto da segurança da informação;
- O modelo deve ser desenvolvido tendo em conta que será acompanhado pelos responsáveis dos processos, juntamente o apoio de técnicos de segurança da informação, para garantir que são tomadas as melhores decisões para proteger a privacidade dos dados pessoais.

3.2 Arquitetura do modelo

O objetivo deste modelo é descrever o ciclo de vida da análise de riscos de um processo de tratamento de dados pessoais, desde a identificação do processo em si e avaliação do nível de maturidade em relação ao RGPD, até à definição dos passos a realizar e controlos de segurança a implementar para alcançar a conformidade com o RGPD e garantir a segurança e privacidade dos dados pessoais, incluindo a realização de 4 fases relacionadas com gestão do risco, relacionadas com o ciclo de vida dos riscos descrito no capítulo 2.2.2 deste documento. Estas fases da gestão do risco foram usadas como base para o modelo desenvolvido neste trabalho.

De acordo com os requisitos propostos existe a necessidade de se alinhar o modelo com o RGPD, e como tal, antes da gestão do risco foram acrescentadas duas fases que permitem validar a conformidade dos processos organizacionais com o regulamento, que deverão produzir um resultado que se irá apoiar na gestão do risco.

Na gestão do risco foi destacada uma fase, em que se pretende validar se é necessário proceder à mitigação dos riscos, e por consequência, proceder à revisão do processo. O resultado desta fase é importante para se poder demonstrar que o processo em questão está em conformidade tanto com o regulamento, como com a organização em termos de apetite ao risco.

Em baixo podemos observar na imagem uma representação de alto nível da arquitetura do modelo e das fases que o constituem.

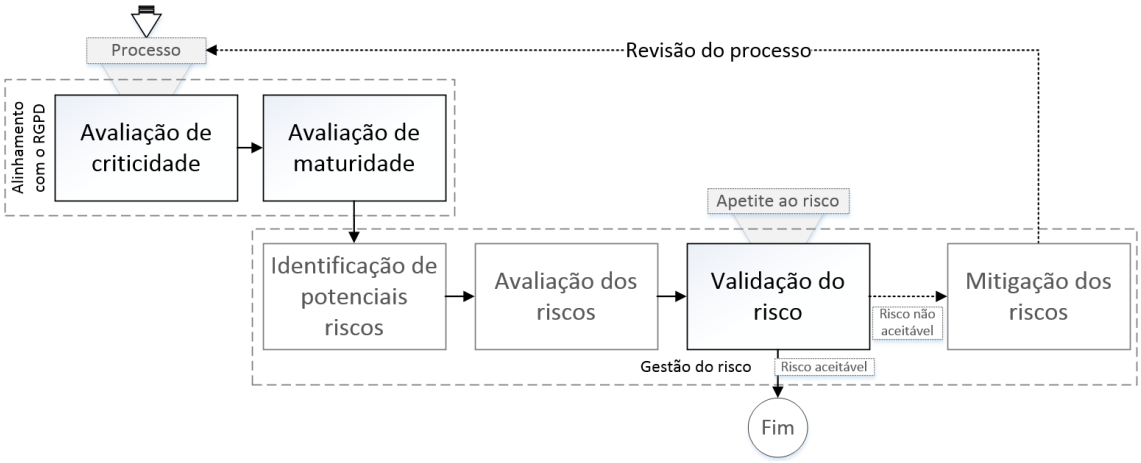


Figura 4 - Integração de componentes do modelo de risco

O ponto de entrada no modelo é a fase de avaliação de criticidade, em que temos um processo de tratamento de dados pessoais como *input*. Para esse processo vai ser identificado um conjunto de dados relevantes no âmbito do RGPD, como os tipos de dados pessoais tratados, os tratamentos efetuados, os tipos de aplicações no processo e transferências de dados, que irão permitir efetuar uma análise da criticidade do processo. Esta fase é essencial para se permitir fazer uma avaliação da maturidade do processo, e é também considerada como a identificação do contexto de um processo de tratamento de dados no âmbito do RGPD.

Com a avaliação de criticidade realizada, é necessário então realizar a avaliação de maturidade orientada à conformidade com o RGPD, tanto em relação à componente processual, como aos controlos de segurança associados aos artigos relevantes para o tratamento de dados pessoais.

Após a avaliação de maturidade, sabendo mais concretamente o que está em falta implementar ou que não está de acordo com as imposições e recomendações do regulamento, é possível identificar os riscos para os titulares dos dados pessoais associados à falta de maturidade e conformidade com os artigos do RGPD identificados, permitindo de seguida proceder à avaliação dos riscos através da caracterização da sua probabilidade de ocorrência e impacto para os titulares dos dados.

Após a identificação e avaliação dos riscos, segue-se a fase de validação do risco, em que de acordo com o *input* "apetite ao risco" da organização se determina quais os riscos que são necessários mitigar. Chegando a esta fase existem duas alternativas:

1. Temos como resultado um risco aceitável onde não são identificados riscos relevantes para se mitigar e o processo chega ao fim.

2. Temos como resultado um risco não aceitável e é identificado um ou mais riscos que requerem atenção, e procedemos então à fase de mitigação do risco.

No caso da segunda alternativa, passamos à fase de mitigação do risco como já foi dito, onde temos uma base sólida para se poder determinar os controlos de segurança a implementar para mitigar os riscos identificados e ainda garantir a conformidade com o regulamento. Os controlos a implementar deverão ser priorizados pela organização de acordo com a sua estratégia face ao risco.

Com a fase de mitigação dos riscos concluída, é necessário rever o processo. Isto implica atualizar a avaliação de criticidade, se se aplicar, atualizar a avaliação de maturidade, e reavaliar os riscos e validar novamente o risco aceitável que irá subsistir após a implementação das medidas e controlos identificados, onde se validará se o risco está alinhado com o apetite de risco da organização. Caso isso não se verifique é necessário revisitar a fase de mitigação do risco e voltar novamente ao início do modelo.

Depois de alinhados os riscos com o apetite de risco da organização, é necessário definir-se um período para a revisão dos riscos, que poderá também ser despoletado se forem realizadas alterações significantes no processo ou se surgirem novas ameaças que o possam afetar.

3.3 Descrição das fases

Tendo já sido descrito o fluxo das fases do modelo iremos então entrar em detalhe nas mesmas e entender os *inputs* necessários para cada fase, como é que a fase se processa, e os resultados expectáveis.

3.3.1 Avaliação de criticidade

O objetivo desta primeira fase é permitir identificar o contexto de um processo de tratamento de dados por forma a poder classificar o mesmo em relação à sua criticidade de acordo com um conjunto de parâmetros recolhidos.

Como tal, esta fase passa por documentar os detalhes de um processo, definir o seu propósito e finalidades, identificar as categorias de dados pessoais tratados, os tipos de tratamentos efetuados, os responsáveis pelo processo e tratamento dos dados, a forma de recolha dos dados, que tipos de aplicações são usadas para os tratamentos e o fluxo dos dados pessoais ao longo do processo. No preenchimento dos tipos de tratamentos de

dados pessoais que são realizados no processo deve-se levar em conta se é efetuado algum dos tratamentos identificados como possíveis de resultar num risco elevado de acordo com o capítulo 2.6.1 deste documento.

Com base na recolha dos dados descritos acima, será possível validar se o processo deve estar sujeito a um DPIA ou não, por forma a garantir conformidade com o Artigo 35. Este cálculo deve ser feito com base nas categorias de dados pessoais tratados, tipos de tratamentos efetuados, tipos de aplicações usadas para o processamento e se são ou não realizadas transferências de dados pessoais. Pode-se observar mais em detalhe como é feita esta ponderação no capítulo 4.2.

Consoante o nível de detalhe a que a organização pretende ir, e as suas necessidades, pode ser recolhida ainda mais informação que a organização ache relevante. No âmbito deste trabalho, estes dados são suficientes para completar esta fase, sendo alguma informação mais específica recolhida na próxima fase.

Organizações com maior maturidade têm o hábito de ter os seus processos identificados e documentados, no entanto se esse não for o caso, deve-se proceder ao levantamento dos dados necessários juntamente do dono do processo. Um exemplo de uma ficha de levantamento de informação de um processo de tratamento de dados pessoais pode ser encontrado no Anexo A. O preenchimento dessa ficha irá também contribuir para o registo das atividades de tratamento requerido pelo Artigo 30 descrito no capítulo 2.5.1.6, e assim garantir conformidade com o mesmo.

3.3.1.1 Criticidade dos ativos

Na identificação do processo é importante a definição da criticidade de ativos para posteriormente se poder estimar o nível de risco a que um processo pode estar sujeito levando em conta os seus ativos. No contexto deste trabalho irá trabalhar-se com dois tipos de ativos, dados pessoais e aplicações. Para classificar a sua criticidade definiu-se uma escala que leva em conta o impacto que a sua má utilização ou comprometimento pode causar aos titulares dos dados. Devido à importância e relevância que o regulamento procura atribuir aos dados pessoais, optou-se por se classificar os mesmos numa escala contemplando apenas os níveis de criticidade média, alta e elevada.

Tabela 3 - Critérios de criticidade dos dados pessoais

Criticidade	Racional
Média	Dados pessoais identificativos, muitas vezes publicados por livre vontade dos titulares, e que numa situação normal, sem a presença de dados sensíveis, o seu comprometimento por si só não deve causar um grande impacto.
Alta	Dados pessoais que podem permitir chegar fisicamente perto do titular, identificar hábitos ou padrões dos mesmos, ou efetuar transações e/ou danos financeiros em nome dos/aos titulares.
Elevada	Dados pessoais classificados como sensíveis pelo próprio regulamento por poderem conter informação que pode colocar a integridade física e/ou moral do titular em causa.

No contexto deste trabalho assume-se que a criticidade e impacto do comprometimento dos dados pessoais dos titulares podem variar conforme o contexto do processamento e a situação dos titulares. Como tal esta escala será usada como base, mas pode ser adaptada para cada processo caso surja a necessidade.

A criticidade das aplicações utilizadas nos processos deve levar em conta o tipo de tratamentos que a aplicação realiza e/ou a sua exposição e maturidade, de acordo com os tratamentos que possam resultar num risco elevado identificados na tabela 1 – Tratamentos sujeitos a risco.

Na tabela seguinte está um exemplo de classificação de criticidade que procura abranger as categorias de dados pessoais mais comuns. As categorias de dados descritas foram identificadas e classificadas seguindo as linhas orientadoras de um documento da ENISA de recomendações de uma metodologia para a avaliação do impacto dos dados pessoais em fugas de informação (ENISA, 2013).

Tabela 4 - Categorias de dados pessoais identificados e respetivas criticidades

Ativo	Tipo	Racional	Criticidade
Dados identificativos	Dado pessoal	Dados pessoais que permitem identificar o titular e que não permitem identificar padrões comportamentais, nem a sua localização ou causar danos financeiros.	Média
Dados demográficos			
Experiência profissional			
Características físicas			
Perfilagem e dados comportamentais	Dado pessoal	Dados que permitem identificar padrões comportamentais, a localização e paradeiro atual e/ou causar danos ou fraude financeira aos titulares.	Alta
Dados de contas, transações ou créditos			
Propriedades			
Outros dados financeiros / preferências / localização			
Origem racial ou étnica	Dado pessoal sensível	Dados pessoais sensíveis, de acordo com o regulamento, que podem mais severamente condicionar as liberdades e direitos do titular e resultar num risco elevado para o mesmo.	Elevada
Opiniões políticas			
Convicções religiosas ou filosóficas			
Filiação sindical			
Dados genéticos			
Dados biométricos			
Dados relativos à saúde			
Dados relativos à vida sexual ou orientação sexual			
Dados da vida privada			

Na próxima tabela, são apresentados os tipos de aplicações identificados como sendo possíveis de ser usados para o tratamento de dados pessoais que se encontram nas organizações. A lista de aplicações apresentada foi desenvolvida com base nos tratamentos de dados potencialmente sujeitos a risco descritos no capítulo 2.5.1, procurando perceber que tipos de aplicações é que poderiam realizar estes tratamentos, e complementando também com alguma experiência relacionada com o assunto obtida noutros projetos.

Tabela 5 - Tipos de aplicações identificadas e respetivas criticidades

Ativo	Tipo	Racional	Criticidade
Aplicação que combina dados de várias fontes	Aplicação	Aplicação que combina dados de titulares provenientes de 2 ou mais fontes de dados.	Alta
Aplicação exposta na web		Aplicação que está exposta na web e mais facilmente é acedida por agentes maliciosos.	Alta
Nova aplicação no mercado (menos de 1 ano)		Nova aplicação no mercado de baixa maturidade, possivelmente com mais bugs e/ou vulnerabilidades.	Alta
Nova aplicação na organização (menos de 2 meses)		Nova aplicação na organização, tendo a mesma uma baixa maturidade na utilização e/ou configuração da tecnologia.	Alta
Aplicação na *cloud*		Aplicação na *cloud*, ou *SaaS* (*Software as a Service*). Apesar dos dados se encontrarem for a da organização este tipo de aplicações já costuma ter alguma maturidade, dependendo também dos fornecedores.	Média
Outros tipos de aplicação para processamento de dados		Aplicações simplesmente utilizadas no processamento de dados.	Baixa

3.3.2 Avaliação de maturidade

Antes de se poder fazer uma identificação e análise dos riscos associados ao processo de tratamento de dados pessoais é necessário primeiro avaliar a maturidade do mesmo. Para isso procurou-se definir uma forma de realizar uma avaliação de maturidade orientada à conformidade com o RGPD. Inicialmente investigou-se que ferramentas e *frameworks* estariam disponíveis para realizar esta avaliação de maturidade, no entanto não se encontrou nenhuma que corresponda ao que se pretende. Os resultados da pesquisa retornaram apenas avaliações de maturidade superficiais, orientadas para garantir a conformidade das organizações com o regulamento em geral, em vez de ser orientada a atividades de processamento de dados e a garantir as liberdades e direitos dos cidadãos, não contemplando muitas das vezes critérios importantes do regulamento.

Como tal surgiu a necessidade de desenhar um questionário de raiz que permita avaliar a maturidade de um processo de tratamento de dados, por forma a identificar *GAPs* conformidade com o regulamento, mais concretamente, de artigos que possam estar mais relacionados com a segurança da informação. Para este fim foram analisados todos os

artigos do regulamento, foram identificados os artigos relacionados com o tratamento de dados pessoais e foi desenvolvida uma lista de perguntas para avaliar essa conformidade. O conjunto dos artigos identificados encontra-se no Anexo B, juntamente com uma breve descrição desses artigos e o tipo de coima associado a cada um.

O objetivo desta avaliação de maturidade não é ser muito intensivo mas sim conter um conjunto de questões que permitir validar a conformidade do processo com o regulamento, assim como identificar possíveis falhas de segurança que possam resultar em riscos para os direitos e liberdades dos titulares dos dados. Como tal esta avaliação está mais orientada numa perspetiva de controlos de segurança da informação nos processos, não descurando também a conformidade com os artigos que são mais relevantes para garantir que os mesmos estão em conformidade com o RGPD.

A avaliação de maturidade proposta está dividida por áreas, onde cada área contém um conjunto de questões relacionadas entre si, extraídas de artigos do regulamento, e no caso da área dos controlos de segurança foram identificadas ainda outras questões que procuram complementar o questionário de forma a permitir identificar possíveis falhas de segurança e os riscos do processo em relação à segurança da informação. Estas questões que procuram complementar a avaliação de maturidade foram extraídas com base num conjunto de requisitos técnicos de alto nível relevantes, classificados como obrigatórios na Resolução do Conselho de Ministros 41/2018 (Presidência do Conselho de Ministros, 2018) e de algumas das boas práticas recomendadas no documento Knowledge Bases da CNIL (CNIL, 2018).

As áreas da avaliação de maturidade definidas são as seguintes:

Tabela 6 - Descrição das áreas de avaliação de maturidade

Áreas	Breve descrição
Recolha e informação	Artigos relacionados com a recolha de dados dos titulares e a informação dada aos mesmos sobre o propósito da recolha.
Consentimento e direitos dos titulares	Artigos relacionados com a possibilidade de demonstrar e/ou retirar o consentimento por parte de um titular e com a possibilidade de um titular exercer os seus direitos sobre os seus dados pessoais.
Documentação e requisitos legais	Artigos relacionados com a documentação do processo por forma a permitir a realização de análises de risco, e com requisitos legais e contratuais que devem ser cumpridos e garantidos.
Controlos de segurança lógica	Artigos relacionados com os controlos de segurança implementados para garantir a segurança e privacidade dos dados pessoais de um ponto de vista dos sistemas de informação.
Controlos de segurança física	Artigos relacionados com os controlos de segurança implementados para garantir a segurança e privacidade dos dados pessoais de um ponto de vista físico.
Transferências de dados internacionais	Artigos relacionados com a transferência de dados pessoais, nomeadamente para outros países e para fora da União Europeia.

No Anexo C é apresentado o conjunto de questões que compõem a avaliação de maturidade proposta para processos organizacionais que tratem dados pessoais. Para se responder às questões identificadas deve estar definida uma forma de classificação que permita identificar a maturidade do processo em relação a cada questão. Como tal é necessário definir-se os critérios para a classificação da maturidade dos controlos.

3.3.2.1 Classificação de maturidade

Para a classificação dos controlos numa avaliação de maturidade é necessário a utilização de uma escala que permita identificar o estado atual dos controlos em relação ao estado da sua implementação. Com este objetivo em mente, foram analisados e comparados os níveis de maturidade de três *frameworks* de organizações com impacto na área da segurança da informação por forma a se escolher a mais apropriada para este trabalho, os níveis da ISO/IEC 21827 (International Organization for Standardization, 2008), do COBIT 5 (ISACA, 2012) e de segurança da informação do NIST (NIST, 2017).

As duas primeiras *frameworks* têm 6 níveis de classificação da maturidade e a terceira 5 níveis. Estas permitem identificar não só se os controlos estão implementados mas também se estão implementadas medidas de otimização e melhoria contínua.

- Os níveis do NIST têm a descrição por tópicos e é claro o que está definido em cada nível mas os próprios níveis de classificação não estão alinhados com o que se pretende, sendo a sua classificação de maturidade um pouco confusa.
- No COBIT 5 os níveis de classificação já estão mais alinhados com o que se pretende, no entanto não estão tão orientados à segurança da informação.
- Na ISO/IEC 21827 os níveis estão também alinhados com o que se pretende, a *framework* foi desenhada a pensar na segurança da informação como base e tem as descrições de cada nível bem detalhadas e organizadas, no entanto podem ser um bocado confusas e ir até a um nível de maturidade excessivo.

Como tal, optou-se por escolher a última *framework*, a ISO/IEC 21827, para classificar os níveis de maturidade dos processos de tratamento de dados, tendo sido no entanto, a mesma adaptada por forma a simplificar a sua implementação e estar alinhada com os objetivos da metodologia proposta. Dos 5 níveis originais foi removido o terceiro nível de classificação "Planeado e rastreado", por introduzir alguma redundância com o quarto, e foi acrescentado também um nível para se permitir identificar se uma questão em particular não é aplicável ao processo a ser avaliado.

Tabela 7 - Níveis de classificação de maturidade adaptados da ISO/IEC21827

Nível de maturidade	**Definição**
Não implementado	O controlo não está ainda implementado.
Executado informalmente	O controlo está implementado mas informalmente, podendo não estar bem definido. Pode não se encontrar documentado, pode não ser executado da melhor forma ou de forma adequada, e pode não ser prática a sua execução em situações semelhantes.
Bem definido	O controlo está documentado e aprovado, sendo prática comum utilizar-se em situações semelhantes.
Controlado quantitativamente	Os resultados do controlo são analisados continuamente com o objetivo de se melhorar a performance e obter melhores resultados.
Melhorado continuamente	Em adição aos anteriores, o controlo é revisto periodicamente e adaptado conforme as necessidades da realidade da organização.
Não aplicável	Em algumas situações determinado controlo pode não ser aplicável por não fazer sentido tendo em conta o contexto do processamento.

3.3.3 Identificação de potenciais riscos

Esta fase é contemplada na fase análise/avaliação de riscos descrita no capítulo 2.2.2. Para o desenvolvimento desta fase recorreu-se ao manual da certificação CRISC da ISACA de 2015 (ISACA, 2015) para apoiar no processo de identificação dos riscos, que foi depois adaptado de acordo com o contexto do presente trabalho tendo em conta a integração com o RGPD.

De acordo com o manual, para a identificação de potenciais riscos deve ser realizada uma abordagem sistemática. Isso é alcançado através do exame detalhado dos resultados da avaliação de maturidade por forma a encontrar os possíveis pontos de falha que possam originar em riscos. A imagem em baixo descreve como é realizado este processo, adaptado para o modelo desenvolvido.

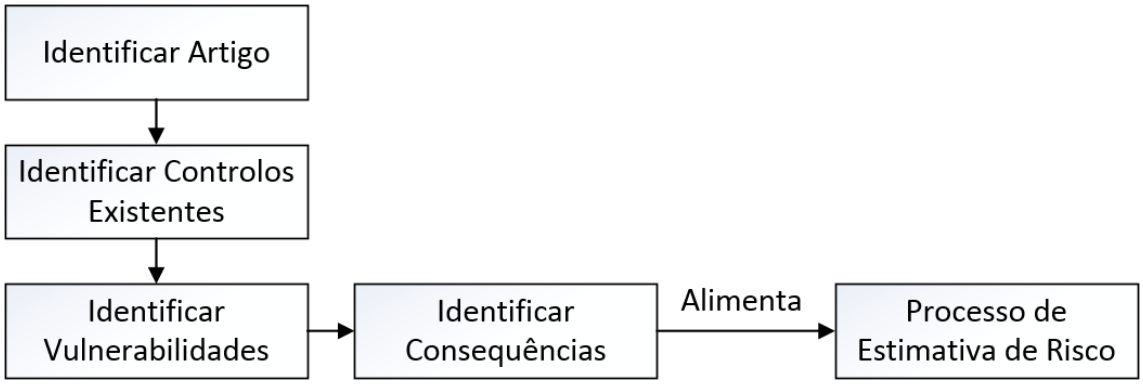


Figura 5 - Processo adaptado de identificação do risco. Fonte: CRISC 2015, figura 1.5

Tendo sido identificados os artigos da fase de avaliação de maturidade, e realizada essa avaliação que permite identificar os controlos existentes, é necessário ter como base um conjunto de vulnerabilidades resultantes do possível não cumprimento de determinado artigo, para que se possa identificar as consequências que podem advir da exploração dessas vulnerabilidades, e, posteriormente mapear com os riscos relacionados com tratamentos de dados pessoais identificados no capítulo 2.6.2.

Existem diferentes tipos de ameaças que se podem aplicar em diferentes contextos, podendo ser ameaças originadas por humanos, tendo como exemplo *hackers* ou danos acidentais nos dados, ou ser originadas por *malware*, como vírus, e assume-se que estão presentes enquanto existir um risco, no entanto para este trabalho vamos limitar-nos a não especificar o tipo de ameaças e assumir um valor neutro para o cálculo do risco por forma a contemplar a sua presença. Caso seja relevante ou surja a necessidade é sempre possível descrever os tipos de ameaças aplicáveis e atribuir um valor às mesmas.

A identificação das vulnerabilidades foi realizada com o apoio da norma ISO 27005 (International Organization for Standardization, 2011), tendo sido analisado para cada questão da avaliação de maturidade as vulnerabilidades que podem estar associadas à mesma, ou seja, que possam advir pelo não cumprimento de determinado artigo e que faça com que um risco possa ser efetivo, e com que as respetivas consequências das vulnerabilidades possam ser exploradas. Essas vulnerabilidades irão servir para alimentar o processo de avaliação de risco descrito no próximo capítulo. Mais vulnerabilidades também podem ser associadas às várias questões da avaliação de maturidade caso se identifique que faça sentido.

Tendo sido identificadas as vulnerabilidades, assim como as possíveis consequências, para cada questão foram mapeados os riscos identificados no capítulo 2.6.2 que podem afetar a mesma. Este mapeamento vai-nos permitir identificar com base na avaliação de maturidade a presença dos riscos a que os dados pessoais do processo em questão podem estar sujeitos.

A lista de vulnerabilidades identificadas para cada questão, assim como as consequências que podem advir das mesmas e respetivos riscos estão enumeradas no Anexo D, associadas ao ID de cada questão da avaliação de maturidade.

Uma consequência que não está mapeada com as questões de maturidade, mas que está sempre implícita, é a aplicação de coimas no caso de incumprimento dos artigos a que as questões estão associadas, uma vez que todas as questões identificadas têm como base artigos que podem sujeitar a aplicação de coimas às organizações em caso de não cumprimento.

3.3.4 Avaliação dos riscos

Esta fase está também contemplada na fase análise/avaliação de riscos descrita no capítulo 2.2.2. Com os potenciais riscos identificados, é necessário avaliar cada risco com base na probabilidade de ocorrência e impacto das vulnerabilidades dos dados pessoais para os titulares, para que a organização possa definir uma estratégia de priorização e definição de implementação de controlos mitigatórios.

Devido a este trabalho procurar ser genérico, ao ponto de se adaptar à realidade de organizações com diferentes modelos de negócio, escolheu-se uma abordagem de estimativa de risco qualitativa. Com a abrangência que se procura ter, a definição de uma abordagem quantitativa é impraticável, uma vez que o processo de atribuição de valores concretos associados a perdas leva em conta imensos fatores, e é algo muito característico

das organizações que varia bastante dependendo do modelo de negócio de cada organização.

Levando em conta as escalas de classificação de probabilidade de ocorrência e impacto descritos nas próximas secções abaixo, obtemos o valor do risco através da seguinte tabela:

Tabela 8 - Classificação do risco

Impacto Ocorrência	Insignificante	Limitado	Significante	Máximo
Insignificante				
Limitada				
Significante				
Máxima				

Baixo	Médio	Alto	Elevado

Tanto para a classificação de probabilidade de ocorrência como para a classificação de impacto dos riscos optou-se por se seguir a abordagem e escalas definidos no documento Knowledge Bases da CNIL (CNIL, 2018). Esta escolha deve-se à CNIL, a entidade reguladora em matéria de proteção de dados em França, ser uma organização com um grande historial neste assunto e ter peritos com uma vasta experiência de privacidade dos dados, assim como vários documentos e ferramentas publicadas com o intuito de apoiar as organizações Francesas a cumprir com o RGPD.

Os riscos referidos como elevados pelo regulamento irão mapear-se com os riscos altos resultantes da fase de análise de risco, uma vez que de acordo com a definição do capítulo 2.2.4 Risco elevado, estes riscos poderão resultar em consequências significantes para os titular dos dados, podendo existir dificuldades sérias para superar essas consequências.

No preenchimento destes dois parâmetros do cálculo do risco deve-se levar em conta os vários fatores que têm influência no processo, encontrando-se alguns exemplos descritos abaixo.

3.3.4.1 Classificação de probabilidade de ocorrência dos riscos

Os valores apresentados são orientados para a realização de estimativas de probabilidade de ocorrência das vulnerabilidades apresentadas para cada questão da avaliação de maturidade tendo em conta os riscos associados.

Tabela 9 - Classificação de probabilidade de ocorrência dos riscos

Ocorrência	Definição	Racional
Insignificante	Não parece possível que os riscos se materializem através da exploração das vulnerabilidades.	Roubo de documentação armazenada num espaço protegido por leitor de cartões e um pin de acesso.
Limitada	Parece difícil que os riscos se materializem através da exploração das vulnerabilidades.	Roubo de documentação armazenada num espaço protegido por leitor de cartões.
Significante	Parece possível que os riscos se materializem através da exploração das vulnerabilidades.	Roubo de documentação armazenada num espaço que não pode ser acedido sem antes se fazer *check-in* na receção.
Máxima	É quase certo que os riscos se materializem através da exploração das vulnerabilidades.	Roubo de documentação armazenada num espaço público.

Esta classificação pode variar de acordo com o contexto do processo de tratamento de dados e ainda tendo outros critérios em consideração, como se existem aplicações no processo expostas na *web*, se são transferidos dados para países estrangeiros, a existência ou não de transferências de dados entre aplicações, a heterogeneidade ou homogeneidade do sistema, a estabilidade do sistema, a reputação da organização, o valor da informação, entre outros (CNIL, 2018).

3.3.4.2 Classificação de impacto dos riscos

O impacto dos riscos no contexto do RGPD deve ser classificado na ótica do impacto que a exposição dos dados pessoais pode causar para os titulares dos dados, através da exploração de uma vulnerabilidade, levando em conta os controlos mitigatórios existentes.

Tabela 10 - Classificação de impacto dos riscos

Impacto	Definição	Definição
Insignificante	Os titulares não são afetados ou poderão encontrar uns pequenos inconvenientes que conseguem superar sem problema.	Perda de tempo a repetir procedimentos, receção de SPAM, alvo de campanhas de publicidade para produtos de consumo comuns.
Limitado	Os titulares podem encontrar inconvenientes significantes que conseguem superar apesar de algumas dificuldades.	Pagamentos imprevistos (multas impostas erroneamente), custos adicionais, negação de acesso a serviços, perda de oportunidade para progressão na carreira, receção de *email* não solicitado propenso a denegrir a reputação dos titulares, processamento de dados incorretos levando a resultados não desejados.
Significante	Os titulares podem enfrentar consequências significantes que devem conseguir superar, embora com dificuldades sérias e reais.	Desvios de fundos não compensados, dificuldades financeiras não temporárias (obrigação a um empréstimo), danos em propriedades, perda de emprego, perda de casa, separação ou divórcio.
Máximo	Os titulares podem enfrentar consequências significantes ou até irreversíveis que podem não conseguir superar.	Risco financeiro, dívidas substanciais, incapacidade de trabalhar, incapacidade de realocar, perda de acesso a estrutura vital (água, eletricidade).

Esta classificação pode variar de acordo com o contexto do processo de tratamento de dados e ainda levando em conta outros critérios como a criticidade dos dados pessoais em causa, a natureza das origens do risco, a quantidade de ligações para transferências de dados (especialmente entre aplicações externas), o número de entidades envolvidas no processo, entre outros (CNIL, 2018).

3.3.5 Validação do risco aceitável

Nesta fase temos como *input* os resultados da fase anterior, a fase de avaliação de risco, e o apetite ao risco da organização. Com base no apetite ao risco, deve-se validar para cada risco identificado na fase anterior se existe a necessidade de se realizar alguma ação para se mitigar o risco, e como tal, tomar a decisão de se passar à fase de mitigação dos riscos, ou, caso não exista nenhum risco em que seja necessário realizar alguma ação, pode-se decidir concluir o processo.

3.3.5.1 Notificação à entidade reguladora

Antes de se proceder à fase de mitigação dos riscos, no caso de se verificar que o processo contenha riscos elevados para os titulares dos dados, na ausência de medidas tomadas pela organização para atenuar o risco, a entidade reguladora, CNPD, deve ser consultada de acordo com o Artigo 36 do RGPD.

3.3.6 Mitigação dos riscos

Esta fase está relacionada com a fase de tratamento do risco descrita no capítulo 2.2.2, e é a fase em que serão identificadas as decisões a tomar face a cada risco, definindo a estratégia para cada risco. A sua implementação será numa fase posterior.

Nesta fase já temos classificados os riscos associados ao processo em causa, e com base nisso podemos identificar as áreas que necessitam de maior foco e onde é que se deve priorizar a definição de medidas e a implementação de controlos de segurança.

Para cada questão da avaliação de maturidade deve-se identificar a estratégia ao risco a tomar. Para os riscos classificados como baixos pode-se eventualmente escolher a opção de aceitar o risco, no entanto isso não deve ser aceitável dos riscos médios para cima. Para a mitigação de cada risco deve-se identificar se efetivamente é necessário a implementação de controlos de segurança ou se basta definir um controlo a nível processual, como um procedimento ou uma política interna, para poder garantir a conformidade com o regulamento e mitigar o risco.

Como tal, para cada questão da avaliação de maturidade foi identificado um ou mais controlos para mitigar os riscos associados às vulnerabilidades tanto com base em controlos de segurança como na definição de políticas ou procedimentos para acomodar a conformidade com o RGPD. Para a implementação de cada controlo, deve-se ainda estimar o esforço envolvido, permitindo dessa forma detalhar um plano de implementação de medidas para mitigar os riscos, e identificar os riscos que podem ser mitigados com menor esforço e trazer benefícios imediatos para o negócio.

O resultado desta fase deve ser alinhado com o DPO, e permite posteriormente ao mesmo provar que os riscos são conhecidos na organização, e que foram tomadas as medidas necessárias para a organização estar alinhada com os mesmos, permitindo dessa forma demonstrar a conformidade com os requisitos de segurança do regulamento.

No Anexo E é apresentado o conjunto de sugestões de controlos desenvolvido para as questões classificadas na avaliação de maturidade e de risco. Os controlos apresentados

são meramente sugestões, podendo as organizações optar por outra forma de mitigar os riscos.

3.3.6.1 Estratégias de mitigação do risco

De acordo com o livro dos princípios da segurança da informação (Michael E. Whitman, 2012), que foi usado para se retirar as fases de gestão do risco descritas no capítulo 2.2.2, existem 5 estratégias de mitigação do risco:

- Proteger: quando se pretende proteger um ativo da exploração de uma vulnerabilidade através da remoção da mesma, podendo ser através da aplicação de políticas, formação e treino dos utilizadores e/ou da aplicação de tecnologias;
- Transferir: quando se pretende transferir a responsabilidade para outros ativos, processos ou organizações. Um exemplo de transferência de risco é a aquisição de um seguro para determinado ativo;
- Mitigar: esta estratégia pretende reduzir o impacto causado pela exploração de vulnerabilidades através de planeamento e preparação. Esta abordagem requer a criação de três tipos de planos: plano de resposta a incidentes, plano de recuperação de desastres e plano de continuidade de negócio;
- Aceitar: esta estratégia consiste na opção de não se fazer nada em relação ao risco e de se aceitar os resultados da exploração de uma vulnerabilidade;
- Terminar: a estratégia de terminar o risco consiste em desistir de se utilizar determinado ativo que possa estar vulnerável, de se realizar um tratamento de dados que possa significar esse risco, ou no limite desistir da realização de um processo.

Das estratégias descritas em cima pretende-se apenas considerar a proteção e aceitação dos riscos, devido às outras três estratégias não fazerem tanto sentido.

A estratégia da transferência do risco não se aplica no RGPD uma vez a organização que é responsável pelos dados pessoais não pode delegar essa responsabilidade a terceiras partes. Quando é contratada uma terceira parte essa também passa a ter responsabilidades sobre os dados, mas a organização que a contratou não é menos responsável pelos dados.

A estratégia de mitigação do risco não se aplica a todas as questões da avaliação de maturidade, e é contemplada nas questões 4.17 e 4.18.

A estratégia de terminar os riscos não se enquadra pela forma como foi desenvolvida a avaliação de maturidade. Caso se pretenda optar por terminar algum risco, o processo em si deve ser revisto, atualizando os detalhes da criticidade do processo, e/ou a avaliação de maturidade onde se aplicar e a avaliação do risco, ou até no limite optando por se desistir do processo.

Para os riscos que se pretenderem aceitar, deve-se documentar esses riscos, deve ser definida uma data para revisão e reavaliação dos riscos, e deve haver um responsável que assuma esses riscos e as suas possíveis consequências.

3.3.7 Revisão do processo

Após implementação de controlos mitigatórios para os riscos, deve ser revista a criticidade do processo, se aplicável, e devem ser revistas a maturidade e a análise de risco do processo, atualizando os valores de acordo com os benefícios dos controlos implementados, chegando novamente à fase de validação do risco aceitável onde se irá obter o risco residual. O risco residual é o valor do risco que irá subsistir após a implementação das medidas de mitigação. Nesta fase novamente se toma a decisão de se aceitar o risco residual e concluir o processo, ou de se avançar novamente para a fase de mitigação dos riscos.

3.3.8 Conclusão do processo

Após a aceitação do risco residual, de acordo com a criticidade do processo e os riscos residuais aceites, devem ser definidos os critérios para revisão e reavaliação do processo, assim como da sua maturidade e avaliação de riscos. Idealmente as revisões seriam realizadas com uma periodicidade bem definida, por exemplo anualmente, ou aquando a realização de alterações maiores no processo, como a introdução de uma nova aplicação, ou a inclusão de uma nova terceira parte no tratamento dos dados.

Nesta revisão devem-se rever todas as componentes do modelo proposto, passando por todas as fases, começando por identificar as alterações que possam existir na fase de avaliação de criticidade e atualizar a matriz de avaliação de maturidade em função dessas alterações e/ou evolução do processo.

É muito importante que o processo de gestão de risco seja um processo contínuo, uma vez que estão sempre a surgir novas ameaças e que também podem ainda ocorrer eventos que possam levar a que se alterem as condições iniciais em que o processo de

tratamento de dados foi avaliado inicialmente, levando a que surjam novos riscos que possam pôr em causa as liberdades e direitos dos titulares dos dados.

3.4 Resultados da aplicação do modelo

Após a aplicação do modelo num determinado processo, iremos ter um conjunto de resultados, através da realização das diferentes fases, que irá contribuir para a conformidade com o RGPD:

- Indicação se o processo deve ser sujeito a um DPIA, contribuindo para a conformidade com o Artigo 35, resultante da fase de Avaliação de criticidade;
- Indicação se o processo deve ser comunicado à CNPD, contribuindo para a conformidade com o Artigo 36, resultante da fase Validação do risco aceitável;
- Uma avaliação dos riscos para os direitos e liberdades dos titulares, um dos quatro requisitos para a realização de DPIAs, de acordo com o Artigo 35, alínea c) do ponto 7, resultante da fase de Avaliação dos riscos;
- As medidas previstas para fazer face aos riscos, um dos quatro requisitos para a realização de DPIAs, de acordo com o Artigo 35, alínea d) do ponto 7, resultante da fase de Mitigação dos riscos;
- Informações para cumprir com as alíneas a), b), c), e) do ponto 1 do Artigo 30, resultante da fase de Avaliação de criticidade;
- Informações para cumprir com as alíneas g) do ponto 1 do Artigo 30, resultante da fase de Avaliação de maturidade;
- Motivação para se arranjar evidência de conformidade do processo com os artigos 5, 6, 7, 9, 13, 14, 15, 16, 17, 18, 19, 20, 21, 25, 28, 30, 32, 44, 45, 46 do RGPD, resultante da fase de Avaliação de maturidade;
- Evidências de que o processo está em conformidade com o RGPD, permitindo ao DPO demonstrar essa conformidade, cumprindo com o Artigo 24, resultante da aplicação das várias fases do modelo.

Para alguns dos artigos descritos em cima a implementação do modelo só por si não irá garantir a conformidade desses artigos, apenas contribuir para a mesma, uma vez que para garantir a conformidade se podem envolver outros fatores a nível da organização em

si e não apenas a nível dos processos de tratamento de dados, como por exemplo os artigos 24, 30 e 35.

4 Protótipo funcional do modelo

Por forma a demonstrar a aplicabilidade e eficácia do modelo, foi desenvolvido um protótipo funcional, utilizando o *Excel* do conjunto de ferramentas da Microsoft Office, que permite pôr em prática as diferentes fases do modelo de análise de risco proposto no presente trabalho.

O protótipo desenvolvido é uma adaptação de uma *framework* já publicada, cujo contexto é a maturidade na *Cloud*, tendo sido para este trabalho desenvolvida uma metodologia semelhante para a avaliação de maturidade orientada ao RGPD (Ferreira, 2017). Ainda, outro fator relevante na escolha do Excel para a implementação do protótipo foi o facto de ser uma ferramenta diária de trabalho na maioria das organizações, o que facilita o entendimento do seu funcionamento. Deste modo também é possível a adaptação do modelo e a realização de alterações ao protótipo, caso as organizações decidam posteriormente afiná-lo de acordo com as suas necessidades.

O protótipo divide-se essencialmente em 4 partes principais. A primeira parte é composta por um enquadramento inicial com a informação essencial para o utilizador realizar as fases do modelo descritas no capítulo anterior, a segunda parte pelos formulários para preencher a avaliação de criticidade e de maturidade, seguida pela terceira parte com a classificação dos riscos identificados e a quarta parte terminando com a mitigação dos riscos.

Este capítulo foca-se na segunda, terceira e quarta componentes do protótipo por forma a descrever o seu funcionamento e demonstrar exemplos do preenchimento do mesmo. No anexo F podem-se observar as várias componentes do protótipo.

O protótipo encontra-se disponível na web para aplicação através do seguinte link: https://drive.google.com/drive/folders/1HV83R2BgJZ7QXVu-YYgYAtDpNuL5irN2?usp=sharing.

4.1 Mapeamento com o modelo

O protótipo é constituído por 14 folhas com diferentes propósitos. Algumas pretendem apenas fornecer informação para o preenchimento dos formulários, enquanto outras contêm os formulários a ser preenchidos e temos ainda outras para demonstrar os resultados do preenchimento dos formulários. Neste capítulo pretende-se abordar como

se preenchem os formulários e como se devem interpretar os respetivos resultados. Como tal temos mapeado neste capítulo as fases:

- Avaliação de criticidade: Esta fase está contemplada na folha "04 Criticidade", e é preenchido o formulário apresentado no Anexo A. No caso desta fase, os resultados do preenchimento do formulário são disponibilizados na própria folha;
- Avaliação de maturidade: Esta fase é realizada na folha "05 Maturidade", onde é classificada cada uma das questões descritas no Anexo C, que por sua vez estão associadas a artigos do RGPD. Os resultados desta fase são apresentados na folha seguinte;
- Identificação de potenciais riscos: Para esta fase não existe necessidade de interação. Os riscos já foram identificados previamente e mapeados com as questões de maturidade no desenvolvimento do modelo, e inseridos no protótipo. Como tal podemos observar os riscos presentes associados a cada questão na folha "08 Riscos";
- Avaliação dos riscos: Esta fase acontece também na folha "08 Riscos", onde para cada questão da avaliação de maturidade, que já tem os riscos mapeados, podemos classificar a probabilidade de ocorrência e impacto dos mesmos;
- Validação do risco aceitável: Esta fase é ser realizada através da observação dos resultados da fase anterior, na folha "09 Resumo riscos";
- Mitigação dos riscos: Nesta fase são escolhidas as estratégias face ao risco de cada questão da avaliação de maturidade, que decorre na folha "10 Mitigação";
- Revisão: Esta fase passa por rever algumas das fases anteriores, conforme descrito no capítulo 3.3.7, e deve basear-se nos resultados da fase anterior disponíveis na folha "11 Resumo mitigação".

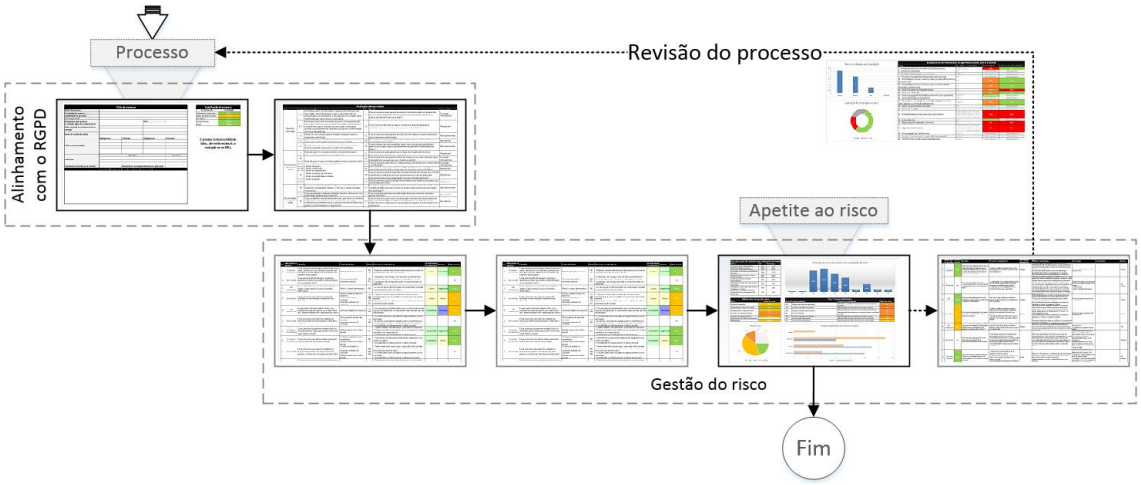


Figura 6 - Mapeamento protótipo com o modelo

A mitigação dos riscos deve ser realizada com base nos resultados da aplicação do protótipo. Na fase de mitigação dos riscos, na folha "10 Mitigação" estão descritas possíveis soluções a implementar que podem ser aplicadas para a mitigação dos riscos. Após essa fase poderá então ser realizada a revisão do processo.

4.2 Avaliação de criticidade

Este é o primeiro passo do modelo de análise de risco, descrito no capítulo 3.3.1. Antes do preenchimento do formulário temos a folha "03 Classificação criticidade" com a legenda da criticidade que nos deverá apoiar no preenchimento do formulário. Na folha do preenchimento em si, "04 Criticidade", encontramos o formulário de identificação e contexto do processo, que após preenchida irá resultar na avaliação de criticidade do processo. A avaliação de criticidade está dividida em 5 componentes que variam automaticamente de acordo com o preenchimento dos campos da ficha do processo.

Classificação do processo	
Em termos de	**Criticidade**
Tratamentos efetuados	Baixa
Dados pessoais tratados	Média
Aplicações	Baixa
Transferências	Baixa
Geral	Baixa

Figura 7 - Componentes de classificação de criticidade de um processo

O primeiro critério, tratamentos efetuados, é calculado com base no campo "É realizado algum dos tratamentos de dados possíveis de resultar num risco elevado"? Neste campo estão listados os tratamentos de dados potencialmente sujeitos a risco identificados

no capítulo 2.6.1. Se não for efetuado nenhum destes tratamentos no processo então este critério é considerado como tendo criticidade baixa, enquanto se for selecionado apenas um dos tratamentos passa a ter uma criticidade alta, e com dois ou mais tratamentos passa a ter uma criticidade elevada. É importante notar que a não seleção deste parâmetro não quer dizer que não sejam efetuados tratamentos, mas sim que não é efetuados nenhum dos tratamentos identificados como possíveis de resultar num risco elevado.

O segundo critério, dados pessoais tratados, vai ter sempre o valor de criticidade associado ao tipo de dados selecionado com a criticidade mais elevada, de acordo com o capítulo 3.3.1.1. Este critério tem como valor por omissão a criticidade média, devido ao tipo de dados pessoais com menor criticidade ser sempre considerados de criticidade média no âmbito deste trabalho. Se for selecionado da lista um tipo dado de pessoal de criticidade superior, este critério assume esse valor.

O terceiro critério funciona à semelhança do segundo, mas com os tipos de aplicações utilizadas no processo, também de acordo com o capítulo 3.3.1.1, mas se não for selecionado nenhum tipo de aplicação dos listados a criticidade por defeito é baixa, devido ao tipo de aplicação com a criticidade mais baixa ter a criticidade baixa.

O quarto critério está relacionado com as transferências de dados pessoais realizadas no processo, tendo como base dois parâmetros. Se forem realizadas apenas transferências para outros departamentos e/ou aplicações, ou seja os dados estão a ser transferidos dentro da organização, a criticidade deste parâmetro é média, enquanto que se forem realizadas transferências para terceiros, ou seja outras entidades, a média é alta por serem transferidos dados para fora da organização deixando a mesma de ter controlo sobre os dados transferidos, enquanto que se não forem realizadas transferências nem para departamentos, aplicações ou terceiros a criticidade é baixa. A transferência de dados para organizações fora da União Europeia está contemplada nos tratamentos possíveis de resultar num risco elevado.

O quinto critério, geral, é uma média dos critérios descritos anteriormente. Com base neste quinto critério é apresentada uma mensagem ao utilizador que indica se deve ou não realizar uma Avaliação de Impacto de Dados Pessoais. As mensagens apresentadas variam com a criticidade da seguinte forma:

- **Elevada:** "O processo tem uma criticidade Elevada, sendo obrigatória a realização de um DPIA.";
- **Alta:** "O processo tem uma criticidade alta, sendo que deve ser realizado um DPIA.";

- **Média:** "O processo tem uma criticidade média, o que indica uma baixa probabilidade de necessidade de um DPIA.";
- **Baixa:** "O processo tem uma criticidade baixa, não sendo necessária a realização de um DPIA.".

4.3 Avaliação de maturidade

Como já foi descrito no capítulo 0, a avaliação de maturidade divide-se em seis áreas principais diretamente relacionadas com os artigos retirados do RGPD. Cada uma dessas áreas contém um conjunto de questões onde está indicado o artigo ou artigos relacionados com cada questão, assim como uma breve justificação do porque é que deve existir um controlo para garantir a conformidade com essa questão. Nesta folha deve apenas ser preenchida a coluna "Maturidade", de acordo com o estado atual do processo permitindo validar a conformidade com a questão a ser preenchida. A maturidade deve ser preenchida seguindo as orientações das classificações de maturidade descritas no capítulo 3.3.1.1.

Avaliação de maturidade					
Área	**Artigo**	**Justificação**	**Id**	**Questão**	**Maturidade**
Consentimento e direitos dos titulares	7	Deve ser possível os titulares retirarem o consentimento para o	2.1	Existe um processo para garantir que os dados dos titulares deixem de ser processados caso o titular assim o	Não aplicável
	15	Deve ser possível para os titulares poderem exercer os direitos sobre os seus dados pessoais, caso seja aplicável: - Direito de acesso; - Direito à retificação; - Direito ao esquecimento; - Direito à restrição de tratamento; - Direito à portabilidade dos dados; - Direito à objeção.	2.2	Existe um processo que permita mostrar aos titulares os seus dados pessoais que a organização tem na sua posse caso o mesmo os solicite?	Executado informalmente
	16, 19		2.3	Existe um processo para retificar os dados pessoais dos titulares caso o titular solicite a sua retificação?	Executado informalmente
	17, 19		2.4	Existe um processo para garantir que os dados dos titulares sejam apagados caso seja solicitado pelos próprios, ou não seja mais necessário tratar esses dados?	Não aplicável
	20		2.5	Existe um processo para a exportação dos dados pessoais de um titular num formato interpretável por máquinas por forma a que os mesmos sejam enviados para processamento para outras organizações caso seja	Não aplicável
	18, 21		2.6	Existe um processo para limitar e/ou terminar determinado tratamento de dados caso seja solicitado	Não aplicável

Figura 8 - Extrato da avaliação de maturidade

4.3.1 Resumo da avaliação de maturidade

Posteriormente ao preenchimento da avaliação de maturidade temos uma folha com um resumo da conformidade do processo de tratamento de dados com o RGPD e das classificações de maturidade atribuídas.

No resumo da avaliação de maturidade é apresentada a média da classificação por área, e usa-se a classificação "Bem definido" como classificação aceitável para a área estar em conformidade.

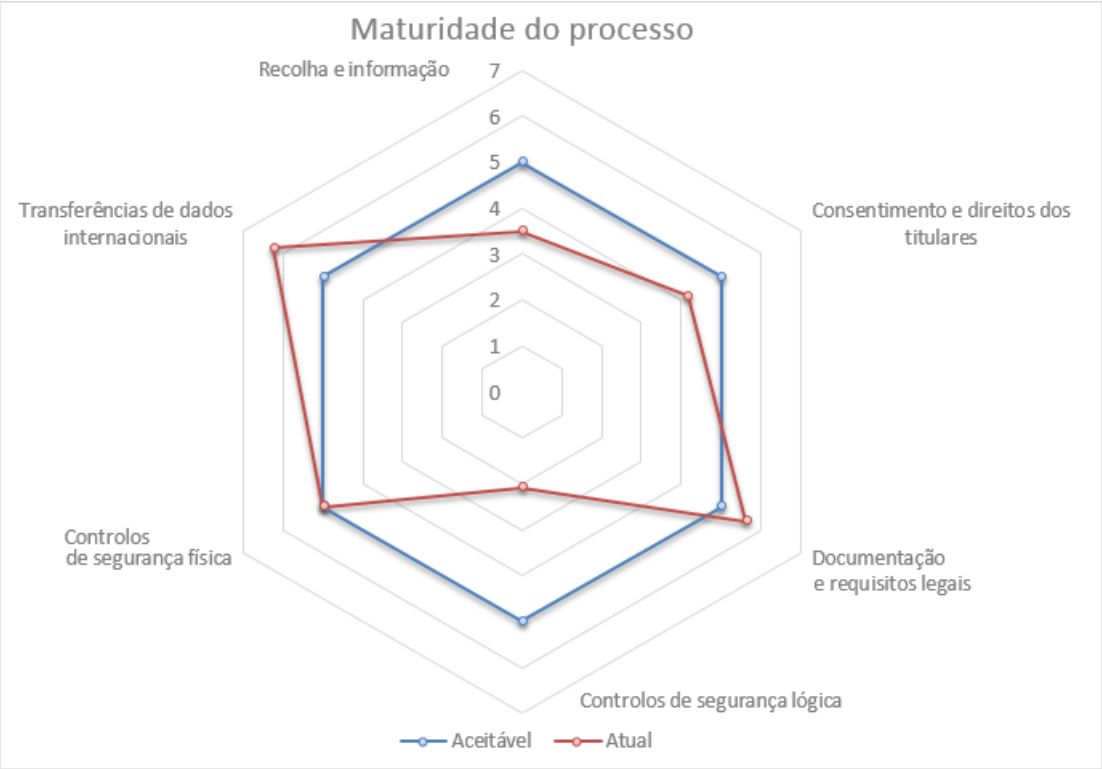


Figura 9 - Resumo de maturidade do processo

Este gráfico dá-nos uma visão geral do processo, e permite-nos identificar imediatamente as áreas em que será necessário mais esforço para alinhar o processo com o RGPD.

4.4 Avaliação dos riscos

A seguir entramos na componente de avaliação dos riscos. Antes da avaliação em si temos a folha "07 Classificação risco" onde estão apresentadas as descrições dos impactos e probabilidades, assim como a matriz de risco.

A folha de avaliação de riscos, "08 Riscos", mostra os riscos associados a cada questão da avaliação de maturidade. Para cada questão está indicada a classificação de maturidade preenchida anteriormente, a questão de maturidade em si, as vulnerabilidades a que a questão potencialmente está sujeita e os riscos que podem advir assim das consequências da exploração dessas vulnerabilidades. Estes riscos estão mapeados com a lista apresentada no capítulo 2.6.2, e o mapeamento pode encontrar-se no Anexo D.

Nas duas colunas seguintes preenche-se a probabilidade de ocorrência das vulnerabilidades e o impacto que a exploração das mesmas e o comprometimento dos

dados pessoais podem ter nos titulares dos dados. Após o preenchimento destes dois parâmetros a coluna do risco deverá ficar preenchida.

Id	Maturidade da questão	Questão	Vulnerabilidades	Riscos	Possíveis consequências	Probabilidade de ocorrência	Impacto	Valor do risco
4.15	Bem definido	Caso sejam transmitidos dados pessoais para fora da organização, estas transferências são feitas através de canais seguros garantido por métodos de cifra?	- Canais de comunicação inseguros	- R03 - R04 - R05	- Fuga de informação dos dados transferidos - Perda ou destruição dos dados em trânsito	Significante	Significante	Alto
4.16	Bem definido	Os sistemas estão protegidos do exterior das suas redes por firewalls e estão bloqueados todos os portos que não são usados?	- Sistemas mal protegidos	- R03 - R04 - R05 - R06	- Comprometimento da rede interna - Fuga de informação	Insignificante	Limitado	Baixo

Figura 10 - Exemplo de classificação do risco

Nas questões que foram identificadas como "Não aplicável", não será necessário classificar o risco para essas questões, uma vez que não se aplicam no processo em questão, e o valor do risco vem já preenchido como "n/a", não aplicável.

4.4.1 Resumo da avaliação dos riscos

A folha seguinte, "09 Resumo riscos", contém um resumo da classificação dos riscos, onde se pode observar de forma geral o processo em termos dos riscos presentes e da sua classificação. Pode-se observar a presença dos riscos no processo de acordo com o seu risco, o valor médio do risco por área de avaliação de maturidade, a relação da probabilidade de ocorrência e impacto preenchidas para as questões, e o top 7 de vulnerabilidades com o risco mais elevado assim como controlos de mitigação sugeridos e níveis de risco associados a cada vulnerabilidade.

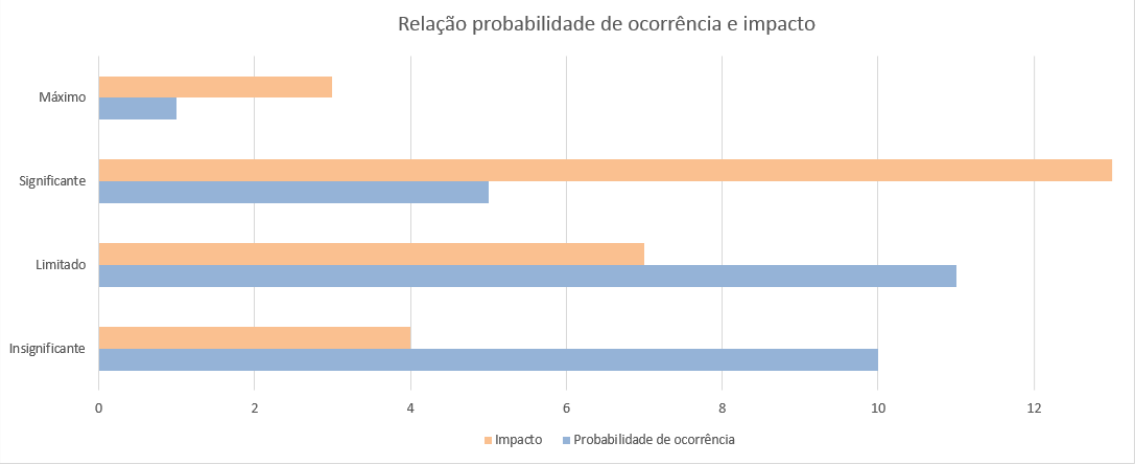


Figura 11 - Gráfico de relação probabilidade de ocorrência e impacto num processo

4.4.1.1 Validação do risco aceitável

Como foi dito em cima, no resumo da avaliação de riscos podemos observar a presença dos riscos no processo, através do gráfico em baixo. Com base na percentagem das presenças de cada risco no processo, é possível avaliar se essa percentagem é mais elevada do que o que se pretende aceitar, e como tal decidir se se deve tomar alguma decisão em relação ao risco.

Figura 12 - Presença dos riscos num processo

Para validar o risco aceitável num processo em termos de classificação (baixo, médio, etc.), podemos observar o gráfico em baixo. Neste gráfico estão contemplados todos os riscos do processo, incluindo os que não se aplicam. Idealmente deveria tomar-se alguma decisão pelo menos em relação a riscos elevados, altos e médios.

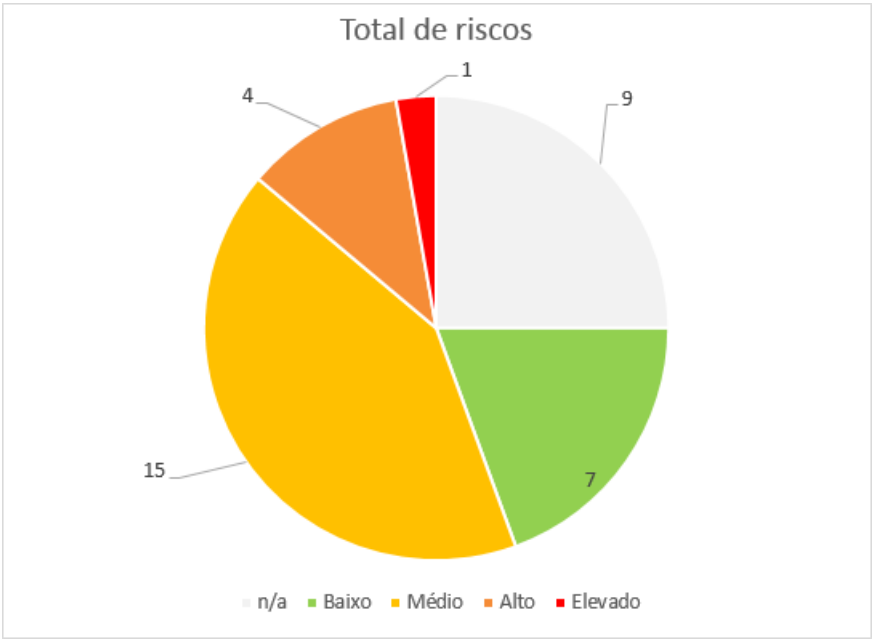


Figura 13 - Riscos subsistentes num processo

Após a validação do risco aceitável, se se pretender mitigar alguns dos riscos identificados deve-se proceder à seguinte folha "10 Mitigação" para se decidir a abordagem a tomar em relação aos riscos. Se se achar que os riscos identificados são aceitáveis, o processo de análise de risco pode terminar nesta fase.

4.5 Mitigação dos riscos

Na folha da mitigação dos riscos temos uma lista com as questões da avaliação de maturidade, com a respetiva classificação de maturidade e de risco e as possíveis consequências da exploração das vulnerabilidades identificadas na folha anterior. Para além disso, foi acrescentada uma coluna para se identificar a estratégia a tomar face ao risco para cada questão onde se pode escolher uma de duas opções:

- Proteger: Decisão de mitigar o risco, através da implementação de políticas/procedimentos ou medidas tecnológicas;
- Aceitar: Decisão de aceitar o risco e não fazer nada em relação ao mesmo.

Para os riscos em que se toma a decisão de proteger, são apresentadas sugestões de medidas recomendadas para a mitigação dos riscos, assim como as tecnologias associadas às sugestões, e uma estimativa pré-preenchida da implementação das sugestões. Tanto as sugestões como as tecnologias e estimativas servem apenas como base para a tomada de decisões, mas podem/devem ser alteradas sempre que uma organização optar por tomar outra decisão, por forma a ficar registada a sua ação face ao risco. Existe também uma coluna para comentários, para se acrescentar notas que possam fazer sentido aquando da mitigação dos riscos.

Id	Maturidade	Risco	Questão	Possíveis consequências	Estratégia de mitigação	Medidas recomendadas	Tecnologias	Comentários	Esforço
4.9	Não implementado	Alto	Ficheiros com dados pessoais que sejam armazenados pelas aplicações têm algoritmos de cifra aplicados nos mesmos?	- Acesso a dados pessoais não autorizados diretamente dos ficheiros por administradores com acesso aos sistemas - Destruição e/ou modificação acidental dos dados	Proteger	Ficheiros que contenham dados pessoais devem ser cifrados para impedir a leitura dos dados por utilizadores do sistema que não devem aceder a esses dados e para dificultar a divulgação dos dados em caso de fuga de informação.	Aplicação de algoritmos de cifra em ficheiros que contenham dados pessoais.		1 a 2 meses
4.10	Não implementado	Alto	São realizados testes de segurança periódicos, pelo menos anualmente?	- Existência de vulnerabilidades conhecidas nas aplicações - Possibilidade de exploração de vulnerabilidades por agentes maliciosos	Proteger	Definição e execução de um plano de testes de segurança periódicos, de preferência por uma entidade externa ou por testers que não tenham estado envolvidos no desenvolvimento do sistema, para garantir que não existem vulnerabilidades conhecidas nas aplicações.	N/A		2 semanas

Figura 14 - Exemplo da fase de mitigação dos riscos

4.5.1 Resumo da mitigação dos riscos

A folha de resumo da mitigação dos riscos permite-nos observar os riscos por categoria, que irão subsistir após a implementação de controlos de mitigação, também a relação de riscos em que foi tomada a decisão de se aceitar ou mitigar, e uma tabela com um resumo da conformidade do processo com os artigos do RGPD, com base nos resultados da avaliação de maturidade, da avaliação de risco, e das tomadas de decisão face ao risco.

Figura 15 - Exemplo de presença de riscos após decisão de aceitação de riscos

Em relação à tabela apresentada temos 4 colunas, uma com a descrição do artigo, outra onde estão indicadas as questões de avaliação de maturidade em que o artigo está presente, a terceira coluna que indica o nível de conformidade do processo com o artigo, e a quarta coluna que indica se o processo vai ficar em conformidade com o artigo.

Estado de conformidade dos artigos relacionados com o processo			
Artigo	**Questões de maturidade**	**Conformidade**	**Vai ficar em conformidade?**
5 - Princípios relativos ao tratamento de dados pessoais	1.1, 1.3, 1.4, 1.5	38%	Sim
6 - Licitude do tratamento	1.2	Não aplicável	Não aplicável
7 - Condições aplicáveis ao consentimento	1.2, 2.1	Não aplicável	Não aplicável
9 - Tratamento de categorias especiais de dados pessoais	3.2	Não aplicável	Não aplicável
13 - Informações a facultar quando os dados pessoais são recolhidos junto do titular	1.1	50%	Sim
14 - Informações a facultar quando os dados pessoais não são recolhidos junto do titular	1.1	50%	Sim
15 - Direito de acesso do titular dos dados	2.2	50%	Não
16 - Direito de retificação	2.3	50%	Sim
17 - Direito ao apagamento dos dados («direito a ser esquecido»)	2.4, 3.4	Em conformidade	Não aplicável
18 - Direito à limitação do tratamento	2.6	Não aplicável	Não aplicável
19 - Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento	2.3, 2.4	50%	Sim
20 - Direito de portabilidade dos dados	2.5	Não aplicável	Não aplicável
21 - Direito de oposição	2.6	Não aplicável	Não aplicável
25 - Proteção de dados desde a conceção e por defeito	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 4.15, 4.16, 4.17, 4.18,	33%	Não
28 - Subcontratante	3.3	Em conformidade	Não aplicável
30 - Registos das atividades de tratamento	3.1	0%	Não
32 - Segurança do tratamento	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 4.15, 4.16, 4.17, 4.18,	33%	Não
44 - Princípio geral das transferências	6.1, 6.2	Não aplicável	Não aplicável
45 - Transferências com base numa decisão de adequação	6.1, 6.2	Não aplicável	Não aplicável
46 - Transferências sujeitas a garantias adequadas	6.1, 6.2	Não aplicável	Não aplicável

Figura 16 - Exemplo da tabela de resumo da conformidade do processo

O valor da terceira coluna é calculado com base na avaliação de maturidade preenchida inicialmente, sendo feita uma média da conformidade das várias questões em que o artigo pode estar presente, e em que se consideram os seguintes valores para cada classificação:

- Não implementado: 0%;
- Executado informalmente: 50%;
- Bem definido ou superior: 100%.

O valor da quarta coluna varia conforme a decisão tomada face ao risco para as questões em que o artigo está presente. Ou seja, se uma questão tiver sido classificada como "Não implementado", e tiver um risco que se for mitigado irá alinhar a conformidade da questão com os artigos associados, com base no valor da coluna de estratégia da mitigação na folha anterior, o valor irá ser "Sim" ou "Não", conforme a decisão de mitigar, ou aceitar o risco.

5 Avaliação do modelo e protótipo

Para garantir a qualidade do modelo proposto e do protótipo desenvolvido, assim como para perceber o valor que efetivamente irão trazer para as organizações, ao apoiar as mesmas a alcançar a conformidade com o regulamento, aplicou-se o modelo em diferentes projetos de implementação e auditoria de RGPD.

5.1 Modelo de avaliação

Foi desenvolvido um questionário, que está dividido em dois grupos principais, um grupo para avaliar o modelo em si e para entender a sua importância na contribuição de uma metodologia para apoiar as organizações a alcançar a conformidade com o RGPD, e outro grupo para avaliar o protótipo, entender se mapeia o que está descrito no modelo e a sua facilidade de utilização e adaptação à necessidade das organizações.

Cada uma das secções é constituída por 6 perguntas para classificação de 1 a 4 e uma pergunta de texto livre. Optou-se por escolher uma classificação entre 1 a 4 para evitar que fosse atribuída uma avaliação "intermédia", e assegurar que a avaliação é positiva ou negativa.

Por forma a se obterem resultados de confiança deve ser cumprido um conjunto de requisitos para ajudar a garantir a qualidade da avaliação:

- Os participantes têm que ter experiência prévia em projetos de auditoria ou implementação de RGPD, e conhecimentos sólidos do regulamento;
- Os participantes têm que estar integrados atualmente num projeto de RGPD. Os projetos devem em diferentes organizações, com diferentes áreas no mercado;
- Os participantes têm que ter conhecimentos e experiência na área de segurança da informação.

5.1.1 Participantes

Como tal, de acordo com os critérios em cima, foram selecionados dois participantes, consultores na EY, que tiveram a oportunidade de pôr em prática o modelo e o protótipo nos projetos em que estão inseridos.

Um dos participantes estava envolvido num projeto para uma organização no setor bancário, enquanto que o outro participante estava envolvido num projeto para uma organização no setor da saúde.

5.2 Resultados da avaliação

Após os participantes terem posto o protótipo em prática, para um conjunto dos processos identificados como críticos nos projetos em que estavam envolvidos, por forma a identificar se o protótipo indicava também os mesmos processos como sendo críticos e a comparar os resultados face à metodologia atual, procederam à resposta dos questionários. Os resultados da avaliação foram positivos de forma geral, e são descritos com mais detalhe em baixo.

5.2.1 Avaliação do modelo de risco

As questões relacionadas com o modelo de risco dividem-se em duas componentes principais, a avaliação da importância do modelo enquanto contribuição para o RGPD e a avaliação do modelo de risco em si.

5.2.1.1 Importância do modelo enquanto contribuição para o RGPD

Tabela 11 - Avaliação de importância do modelo enquanto contribuição para o RGPD

Importância do modelo enquanto contribuição	P1	P2
A metodologia representa uma contribuição importante para ajudar as organizações a alcançar a conformidade com o RGPD.	4	4
A metodologia representa uma contribuição importante para validar a maturidade em termos de segurança dos processos organizacionais.	3	4
Total	7	8
Percentagem	87,50%	100,00%

5.2.1.2 Modelo de risco

Tabela 12 - Avaliação do modelo de risco

Modelo de risco	P1	P2
A metodologia facilita o ciclo de vida da gestão do risco à volta dos processos organizacionais.	3	4
A metodologia é genérica o suficiente para permitir adaptar-se a diferentes modelos de negócio.	4	4
Os riscos identificados são relevantes para uma análise de risco relacionada com o RGPD.	3	4
O mapeamento de riscos e vulnerabilidades com a avaliação de maturidade permite identificar os riscos a que um processo organizacional pode estar sujeito de forma precisa.	3	3
Total	13	15
Percentagem	81,25%	93,75%

5.2.1.3 Comentários

As avaliações dadas pelos participantes foram positivas, e foram dadas ainda algumas sugestões com o âmbito de melhorar o modelo:

- Uma das sugestões foi que nas fases finais do modelo, tentar não focar tanto no risco, e dar uma maior visibilidade à conformidade dos artigos, procurando identificar por exemplo os artigos nos quais se deve procurar dar mais foco;
- Outra sugestão foi que seria interessante que o modelo permitisse classificar especificamente diferentes tipos de impacto para os titulares dos dados (p.ex., impacto financeiro, impacto reputacional, impacto na vida humana);
- Sugeriu-se ainda que a análise de maturidade não se focasse apenas a nível de segurança, mas também a nível processual/operacional, ou seja, contemplar a análise de maturidade noutras perspetivas para a organização.

5.2.2 Avaliação do protótipo

A avaliação do protótipo permite avaliar a congruência com o modelo de risco desenvolvido e também a sua usabilidade e aplicabilidade.

5.2.2.1 Congruência com o modelo de risco

Tabela 13 - Avaliação de congruência com o modelo de risco

Congruência com o modelo de risco	P1	P2
O protótipo consegue mapear e aplicar o que está descrito na metodologia.	4	4
O protótipo é útil na realização de uma análise de risco de um processo organizacional.	4	4
O protótipo é útil na identificação de controlos para a mitigação de riscos de um processo organizacional.	3	4
Os outputs gerados pelo protótipo são uteis para compreender os resultados da análise de risco.	3	4
Total	14	16
Percentagem	87,50%	100,00%

5.2.2.2 Usabilidade e aplicabilidade do protótipo

Tabela 14 - Avaliação de usabilidade e aplicabilidade do protótipo

Usabilidade e aplicabilidade do protótipo	P1	P2
O protótipo é intuitivo e de fácil utilização.	3	3
O protótipo tem flexibilidade suficiente para permitir a adaptação dos parâmetros para se ajustar com diferentes modelos de negócio.	4	4
Total	7	7
Percentagem	87,50%	87,50%

5.2.2.3 Comentários

Como se pode observar pelos resultados as avaliações dadas pelos participantes continuam positivas, e foram sobressaídos alguns pontos positivos do protótipo:

- O facto de permitir centralizar todo o ciclo de vida de gestão de maturidade e dos riscos do processo é um ponto bastante positivo, facilitando a organização e gestão do ciclo de vida dos processos;
- Ainda devido a estar tudo centrado num ficheiro de *Excel*, pode-se evitar custos, sendo necessária apenas uma primeira formação com os responsáveis dos processos, permitindo entregar depois o modelo aos clientes que poderão de forma autónoma classificar os processos com mais calma e detalhe, evitando a necessidade de várias entrevistas.

Para além disso foram também dadas algumas sugestões com o âmbito de melhorar o protótipo:

- Uma sugestão foi na folha de resumo de mitigação dos riscos, colocar o top de riscos a mitigar de acordo com o esforço, permitindo identificar de imediato as mais valias;
- Outra sugestão foi que poderia haver uma forma mais fácil/intuitiva de se introduzir/modificar os riscos e/ou vulnerabilidades associadas às questões;
- Sugeriu-se ainda que se podia detalhar melhor as instruções de preenchimento no próprio protótipo, que numa primeira vista pode ser confuso se não se tiver uma "formação" de utilização.

6 Conclusões e trabalho futuro

O objetivo deste capítulo é descrever as conclusões obtidas do modelo desenvolvido, assim como como identificar alguns possíveis pontos de melhoria para se introduzirem no modelo de futuro.

6.1 Validação de requisitos do modelo

No início do desenvolvimento do modelo foi especificado um conjunto de requisitos para ajudar o modelo a cumprir com os seus objetivos. Esses requisitos estavam divididos em três grupos com propósitos específicos.

O primeiro grupo de requisitos estava relacionado com o RGPD, especificando que deve ser possível verificar a conformidade dos processos com o regulamento, que deve ser possível identificar medidas para colmatar as falhas de conformidade, e os resultados do modelo devem ser úteis na realização de um DPIA. Estes requisitos foram cumpridos, através da avaliação de maturidade, que permitiu alcançar os dois primeiros, e o último foi alcançado através do alinhamento do Artigo 35 ponto 7 da alínea c) com os resultados da fase de avaliação do risco e da alínea d) com os resultados da fase da mitigação do risco.

O segundo grupo de requisitos que surgiu no contexto da EY, para permitir usar o modelo desenvolvido em organizações com diferentes modelos de negócios, e também para facilitar a gestão do risco para não ser mais um obstáculo no ciclo de vida dos processos. O cumprimento destes requisitos é demonstrado através do protótipo, que para além de ser genérico para permitir abranger vários modelos, facilita a gestão do risco através dos mecanismos implementados e dos resultados gerados.

O terceiro grupo de requisitos tem como objetivo garantir a integração da gestão de risco com o RGPD. A identificação dos riscos e das fases da gestão do risco devem estar alinhadas com a proteção de dados. Este processo está descrito no capítulo 2, onde se aborda o trabalho relacionado, e através da metodologia de avaliação do modelo foi possível validar a harmonia entre a gestão do risco e o regulamento.

6.1.1 Cumprimento dos objetivos propostos

Durante a fase de planeamento do presente trabalho foi definido um conjunto de objetivos a alcançar por forma a garantir a qualidade e aplicabilidade do modelo que se pretendia desenvolver.

O primeiro objetivo prendia-se com a definição de uma metodologia para avaliar a conformidade de processos de tratamento de dados pessoais com o RGPD, permitindo dessa forma identificar os passos a realizar para alcançar a conformidade. Este objetivo foi alcançado através da fase de avaliação de maturidade descrita no capítulo 0 do modelo desenvolvido.

O segundo objetivo, melhorar os processos de gestão de risco numa perspetiva do RGPD, atingiu-se através da integração da fase de avaliação de maturidade proposta no primeiro objetivo com um conjunto de fases de gestão de risco, permitindo assim harmonizar o RGPD com a gestão de risco.

O terceiro objetivo estava orientado a um artigo em concreto, o Artigo 35, e pretendia-se validar se determinado processo deveria ser sujeito a um DPIA. Este objetivo foi alcançado através da primeira fase do modelo, a avaliação de criticidade, onde com base no contexto do processo se calcula a criticidade e se determina se o processo deve ser sujeito a um DPIA ou não.

Com o quarto objetivo pretendia-se assegurar com mais confiança a segurança dos dados pessoais, objetivo que foi alcançado através da proposta de um conjunto de controlos a ser aplicados de acordo com a maturidade de cada processo e com os riscos identificados.

Concluindo, não só os objetivos foram cumpridos, como permitiram orientar o desenvolvimento do modelo garantindo a interligação entre o RGPD e a segurança da informação para os processos das organizações. Esta interligação é essencial uma vez que o regulamento tem como principal objetivo garantir a privacidade e proteção dos dados pessoais, alinhando sempre com uma avaliação de risco por forma a aplicar os controlos mais adequados em cada situação.

6.2 Conclusões

O modelo desenvolvido tem como objetivo principal propor uma metodologia que ajude as organizações a identificar e avaliar os riscos para os dados pessoais que trata nos seus processos organizacionais, permitindo assim garantir a conformidade de processos

organizacionais com o RGPD, através da validação da maturidade do processo e da gestão de risco orientada ao RGPD e aos princípios de segurança da informação. O modelo ajuda posteriormente na mitigação dos possíveis riscos para as liberdades e direitos dos cidadãos através da proposta de um conjunto de controlos mitigatórios que permitem alcançar a conformidade com o regulamento de acordo com as melhores práticas de segurança da informação.

Apesar do modelo desenvolvido propor uma metodologia para facilitar a análise e avaliação dos riscos de processos de tratamento, a realização de algumas fases do modelo ainda que com o apoio do protótipo da ferramenta, carecem sempre de acompanhamento e validação de um técnico com conhecimentos em segurança da informação e conhecimentos do regulamento para garantir que a conformidade com o RGPD é garantida e que são aplicadas as medidas mitigatórias mais apropriadas para cada risco, tendo em conta o seu contexto.

Através de uma metodologia de avaliação, foi possível validar a aplicabilidade não só do modelo, mas também do protótipo, e chegar à conclusão de que para além de ser uma ferramenta útil no apoio à conformidade com o regulamento, também é uma contribuição para a gestão do risco nas organizações, que facilita a abordagem ao risco do ponto de vista dos dados pessoais.

6.3 Trabalho futuro

Em termos de trabalho a desenvolver no futuro podemos identificar pontos de melhoria tanto no modelo como no protótipo.

Em termos do modelo, de acordo com o que foi sugerido na avaliação do trabalho, temos os seguintes pontos de melhoria:

- Poderia levar-se mais em conta os impactos para os titulares dos dados por forma a se realizar uma avaliação de risco mais focada nos titulares;
- Identificou-se ainda que o modelo podia abordar mais o RGPD não só do ponto de vista de segurança, mas também de um ponto de vista processual e operacional.

O modelo poderia também estar alinhado com um modelo de atribuição de responsabilidades, permitindo definir quem seriam os intervenientes que deveriam

realizar cada fase, quem deveria ser consultado, sendo que o Encarregado de Proteção de Dados seria sempre ser o responsável por garantir que o modelo é seguido.

Um fator que poderia também ser levado em conta na ponderação da gestão dos riscos seria os benefícios que os tratamentos poderiam trazer. Tendo em conta os benefícios de cada tratamento teríamos mais informação para fazer uma avaliação de risco mais precisa. No entanto este é um fator difícil de prever por variar de processo para processo e de organização para organização. Uma abordagem seria começar-se por uma lista genérica de benefícios que pudesse ser personalizada por cada organização.

Também se poderia enriquecer o trabalho com um conjunto de controlos de segurança propostos mais exaustivo por forma a permitir entregar soluções viáveis mais facilmente a organizações com diferentes realidades.

Uma vez que este trabalho está orientado aos processos de tratamento de dados, poderia ser feita uma versão para gerir a conformidade da organização em si, orientada a artigos mais genéricos que não são abordados a nível processual.

Quanto à usabilidade do protótipo, temos um ponto claro a melhorar de acordo com as avaliações. Poderia ser desenvolvido através de tecnologias *web*, que poderia trazer várias vantagens como permitir parametrizar níveis de classificação, facilitar a utilização, permitir a utilização por parte de diferentes utilizadores num repositório central, permitir atribuir diferentes responsabilidades a diferentes utilizadores e fazer exportações de métricas relevantes para o negócio e para o Encarregado de Proteção de Dados.

Glossário

RGPD

O regulamento em si que é constituído pelos artigos e definições necessários para a implementação e conformidade do mesmo.

Tratamento de Dados Pessoais

Qualquer operação ou conjunto de operações efetuados sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, comparação ou interconexão, bem como a limitação, apagamento ou destruição.

Atividade de tratamento de dados pessoais

Uma atividade em que seja efetuado um ou mais tratamentos de dados pessoais de acordo com a definição anterior.

Elaboração de perfis

Toda a forma de tratamento automatizado de dados pessoais consistente para utilizar dados pessoais para avaliar determinados aspetos pessoais de uma pessoa singular, em particular para analisar ou prever aspetos relacionados com o rendimento profissional, situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou movimentos da pessoa singular.

Processo de tratamento de dados

Um conjunto de atividades de tratamento de dados pessoais com um propósito final específico.

Indivíduos / Titulares dos dados

Pessoas que podem ser identificadas direta ou indiretamente, sobre quem os dados pessoais são tratados.

DPIA

Avaliação de impacto de uma atividade de tratamento de dados pessoais que é provável que resulte num risco elevado para os direitos e liberdades dos indivíduos, levando em conta a natureza, âmbito, contexto e propósito do processamento dos dados. Nesta avaliação deve também determinar-se como é que se pretende mitigar os riscos, sendo obrigatória a consulta da entidade reguladora no caso de não ser possível mitigar os riscos para um nível aceitável.

Controlador

Entidade, pessoa, agência ou autoridade pública responsável por determinar os propósitos e forma de processar os dados pessoais. No contexto deste documento assume-se que o controlador faz parte da mesma organização que o processador.

Processador

Entidade, pessoa, agência ou autoridade pública que processa os dados em nome do controlador. No contexto deste documento assume-se que o processador faz parte da mesma organização que o controlador.

Pseudonimização

É uma forma de processar dados pessoais, aplicando a minimização de dados, um conceito dos princípios de proteção de dados, de tal forma que os mesmos não possam ser atribuídos a um indivíduo em específico.

Fugas de informação

Uma falha na segurança que pode levar ao comprometimento dos princípios da segurança, nomeadamente à destruição, perda, alteração, divulgação e/ou acesso não autorizados de dados pessoais.

Autoridade Supervisora

Data Protection Authority no seu termo original, em Português Autoridade de Proteção de Dados, a entidade reguladora pública que é estabelecida pelo estado membro que ajuda a garantir a conformidade do RGPD nesse estado membro.

CNPD

Comissão Nacional de Proteção de Dados, a Autoridade de Proteção de Dados em Portugal.

Encarregado de Proteção de Dados

Data Protection Officer no seu termo original, em Português Encarregado de Proteção de Dados, uma pessoa nomeada pelo controlador e o processador para apoiar nas atividades base do RGPD e garantir que a organização está em conformidade com o regulamento. Uma organização não é obrigada a nomear um encarregado, apenas em casos específicos de acordo com a implicação (97) do RGPD.

Bibliografia

Article 29 Data Protection Working Party. (2017). *Guidelines on Data Protection Impact Assessment.*

Article 29 Working Party. (s.d.). *Guidelines*. Obtido de Justice and Consumers: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360&tpa_id=6936

CIPL. (2016). *Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR.*

CNIL. (2018). *PIA, knowledge bases.*

CNIL. (31 de Maio de 2018). *The open source PIA software helps to carry out data protection impact assesment*. Obtido de CNIL: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

Council of the European Union. (1980). *Organisation for Economic Cooperation and Development guidelines.*

Council of the European Union. (2016). *General Data Protection Regulation.* Bruxelas.

ENISA. (2013). *Recommendations for a methodology of the assessment of severity of personal data breaches.*

Ewen Macaskill, G. D. (1 de Novembro de 2013). *NSA Files: decoded*. Obtido de The Guardian: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/4

Ferreira, L. P. (2017). Cloud Security Risk and Readiness. Em *Dissertação de Mestrado em Segurança Informática.* Faculdade de Ciências da Universidade de Lisboa. Obtido em Dezembro de 2017, de http://repositorio.ul.pt/handle/10451/31251

Freude, A. C. (s.d.). Echoes of History: Understanding German Data Protection. *Newpolitik.*

Gemalto. (2018). *Breach Level Index*. Obtido de Breach Level Index: http://breachlevelindex.com

Hal Abelson, K. L. (2008). *Secret Bits: How Codes Became Unbreakable.*

ICO. (2014). *Conducting privacy impact assessments code of practice.*

ICO. (s.d.). *Data protection self assessment*. Obtido de ICO: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

International Organization for Standardization. (2008). *ISO/IEC 21827 Systems Security Engineering - Capability Maturity Model (SSE-CMM).*

International Organization for Standardization. (2011). *ISO/IEC 27005 Security techniques - Information security risk management.*

ISACA. (2012). *COBIT 5.*

ISACA. (2015). *CRISC Review Manual.*

Jentzsch, N. (2007). *The Economics and Regulation of Financial Privacy: An International Comparison of Credit Reporting Systems.*

Khandelwal, S. (16 de Julho de 2017). *Ashley Madison to Pay $11.2 Million to Data Breach Victims*. Obtido de The Hacker News: https://thehackernews.com/2017/07/ashley-madison-data-breach.html

Michael E. Whitman, H. J. (2012). *Principles of Information Security 4th Edition.*

NIST. (31 de Julho de 2017). *Program Review for Information Security Assistance*. Obtido de National Institute of Standards and Technology: https://csrc.nist.gov/Projects/Program-Review-for-Information-Security-Assistance/Security-Maturity-Levels

Presidência do Conselho de Ministros. (2018). *Resolução do Conselho de Ministros 41/2018.*

Solove, D. J. (2006). *A Brief History of Information Privacy Law.* Washington.

Standardization, I. O. (2009). *ISO/IEC 31000 Risk management - Principles and guidelines.*

Urquhart, J. (16 de Setembro de 2017). *EDP, NOS e PT partilham dados de clientes ilegalmente*. Obtido de Sic Notícias: http://sicnoticias.sapo.pt/pais/2017-09-16-EDP-NOS-e-PT-partilham-dados-de-clientes-ilegalmente

Anexo A

Ficha do processo				
Nome do processo				
Finalidades do processo				
Legitimidade do processo				
Dono do processo				
Responsável pelo processo			DPO	
É realizado algum dos tratamentos de dados possível de resultar num risco elevado?				
Meios de recolha dos dados				
Dados pessoais tratados	Dado pessoal	Criticidade	Dado pessoal	Criticidade
Aplicações	Aplicação			Criticidade
Transferência de dados para terceiros		Transferências entre departamentos ou aplicações		
Fluxos de dados pessoais (por onde circulam os dados pessoais)				

Figura 17 - Ficha de levantamento de processo

Nome do processo: Nome pelo qual o processo é conhecido.

Finalidades do processo: Quais as finalidades para os tratamentos dos dados pessoais.

Dono do processo: Quem é responsável pelos dados e resultados do processo.

Responsável pelo processo: Quem é responsável para que o processo seja executado.

DPO: Encarregado de Proteção de Dados da organização.

É realizado algum dos tratamentos de dados possível de resultar num risco elevado: Selecionar da lista de tratamentos identificados como possíveis de resultar num risco elevado de acordo com o capítulo 2.6.1.

Meios de recolha dos dados: Como é que os dados são recolhidos, pessoalmente, via formulário web, aplicação mobile, etc.

Dados pessoais tratados: Categorias de dados pessoais tratados no processo, de acordo com o capítulo 3.3.1.1.

Aplicações: Se é utilizado algum tipo de aplicação de acordo com os tipos descritos no capítulo 3.3.1.1.

Transferências de dados para terceiros: Se é feita alguma transferência de dados para alguma terceira parte que não seja parte da organização.

Transferências entre departamentos ou aplicações: Se é feita alguma transferência de dados entre aplicações ou departamentos dentro da organização.

Fluxos de dados pessoais: Fluxos por onde circulam os dados pessoais no processo.

Anexo B

A tabela em baixo contém os artigos que se consideraram relevantes para a gestão do risco relacionada com os processos, que têm implicação a nível dos processos de forma geral.

Tabela 15 - Artigos identificados relacionados com processos organizacionais

Artigo	Coima associada
5 - Princípios relativos ao tratamento de dados pessoais	Elevada
6 - Licitude do tratamento	Elevada
7 - Condições aplicáveis ao consentimento	Elevada
9 - Tratamento de categorias especiais de dados pessoais	Elevada
13 - Informações a facultar quando os dados pessoais são recolhidos junto do titular	Elevada
14 - Informações a facultar quando os dados pessoais não são recolhidos junto do titular	Elevada
15 - Direito de acesso do titular dos dados	Elevada
16 - Direito de retificação	Elevada
17 - Direito ao apagamento dos dados («direito a ser esquecido»)	Elevada
18 - Direito à limitação do tratamento	Elevada
19 - Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento	Elevada
20 - Direito de portabilidade dos dados	Elevada
21 - Direito de oposição	Elevada
25 - Proteção de dados desde a conceção e por defeito	Baixa
28 - Subcontratante	Baixa
30 - Registos das atividades de tratamento	Baixa
32 - Segurança do tratamento	Baixa
35 - Avaliação de impacto sobre a proteção de dados	Baixa
36 - Consulta prévia	Baixa
44 - Princípio geral das transferências	Elevada
45 - Transferências com base numa decisão de adequação	Elevada
46 - Transferências sujeitas a garantias adequadas	Elevada

Anexo C

Abaixo são descritas as questões para a realização de avaliação de maturidade de um processo de contém atividades de tratamento de dados pessoais, separados pelas respetivas áreas.

Área	Artigo	Justificação	Id	Questão
Recolha e informação	5, 13, 14	Os titulares devem ser informados do propósito do tratamento dos seus dados, do período durante o qual os seus dados irão ser armazenados, dos seus direitos, e caso aplicável, se os dados serão transferidos para outros países ou instituições.	1.1	Existe um processo para garantir que antes da recolha dos dados, os titulares têm uma informação atualizada e clara do propósito dos seus dados pessoais e do processo de tratamento dos seus dados?
	6, 7	Os titulares devem dar o consentimento para o processamento dos seus dados e deve ser possível demonstrar que os titulares deram o consentimento para o tratamento dos seus dados, excetuando quando o processamento for necessário para garantir conformidade com uma obrigação legal.	1.2	Existe uma forma definida de registar, armazenar e disponibilizar quando requisitado o consentimento para o processamento dos dados?
	5	Devem ser ser recolhidos apenas os dados necessários para os tratamentos identificados.	1.3	Existe um processo para garantir que são recolhidos apenas os dados necessários para os tratamentos identificados?
	5	Apenas devem ser realizados os tratamentos aos dados pessoais que foram identificados para os titulares na recolha dos dados.	1.4	Existe um processo para garantir que apenas são realizados os tratamentos que foram propostos aos titulares?
	5	Os dados pessoais devem apenas permitir identificar os titulares durante o propósito para o qual os dados foram recolhidos.	1.5	Existem medidas de minimização dos dados, como pseudoanonimização para garantir que os dados depois dos tratamentos não permitem a identificação dos titulares?

Área	Artigo	Justificação	Id	Questão
Consentimento e direitos dos titulares	7	Deve ser possível os titulares retirarem o consentimento para o tratamento dos seus dados, caso seja aplicável.	2.1	Existe um processo para garantir que os dados dos titulares deixem de ser processados caso o titular assim o requisite?
	15	Deve ser possível para os titulares poderem exercer os direitos sobre os seus dados pessoais, caso seja aplicável: - Direito de acesso; - Direito à retificação; - Direito ao esquecimento; - Direito à restrição de tratamento; - Direito à portabilidade dos dados; - Direito à objeção.	2.2	Existe um processo que permita mostrar aos titulares os seus dados pessoais que a organização tem na sua posse caso o mesmo os solicite?
	16, 19		2.3	Existe um processo para retificar os dados pessoais dos titulares caso o titular solicite a sua retificação?
	17, 19		2.4	Existe um processo para garantir que os dados dos titulares sejam apagados caso seja solicitado pelos próprios, ou não seja mais necessário tratar esses dados?
	20		2.5	Existe um processo para a exportação dos dados pessoais de um titular num formato interpretável por máquinas por forma a que os mesmos sejam enviados para processamento para outras organizações caso seja solicitado pelo titular?
	18, 21		2.6	Existe um processo para limitar e/ou terminar determinado tratamento de dados caso seja solicitado pelo titular?

Área	Artigo	Justificação	Id	Questão
Documentação e requisitos legais	30	Deve ser mantido e atualizado um registo com os detalhes do tratamento, tipos de dados tratados e o flow de circulação de dados no processo.	3.1	É mantido um registo com os detalhes do tratamento, os tipos de dados, os fluxos de circulação de dados pessoais e existe um processo para garantir que esses dados estão atualizados?
	9	Caso seja efetuado o tratamento de dados sensíveis, deve existir uma justificação válida para esse tratamento.	3.2	Existe, e está documentada uma justificação válida para o tratamento de dados pessoais sensíveis?
	28	Caso o tratamento seja efetuado por terceiros, deve existir um contrato estabelecido entre as partes onde o processador assume que implementa as medidas técnicas e organizacionais apropriadas para garantir a conformidade com o regulamento.	3.3	Existe um processo para incluir uma cláusula em contratos com processadores de dados externos, para garantir que os mesmos assumem os riscos e tomam as medidas técnicas e organizacionais apropriadas para garantir a conformidade com o regulamento?
	17	O direito ao esquecimento aplica-se apenas quando o processamento não for obrigatório para cumprir com uma obrigação legal ou for do interesse público o registo dos dados como para fins científicos.	3.4	Caso seja obrigatório manter os dados pessoais após o processamento, devido a alguma obrigação legal, existe um processo para garantir que os dados são apagados após o prazo de retenção definido por lei?

Área	Artigo	Justificação	Id	Questão
Controlos de segurança físicos	25, 32	No armazenamento de documentos com dados pessoais devem ser garantidas as medidas de segurança apropriadas para proteger os dados contra acessos indevidos.	5.1	O acesso a documentos físicos está protegido contra acessos indevidos?

Área	Artigo	Justificação	Id	Questão
Transferências de dados internacionais	44, 45, 46	Caso sejam transferidos dados para outros países ou organizações internacionais, devem ser tomadas as medidas necessárias para garantir a segurança dos dados e privacidade dos titulares.	6.1	Existe um processo para garantir que os dados pessoais apenas são transferidos para entidades que cumpram com o regulamento?
			6.2	Estão implementadas medidas técnicas para garantir que os dados pessoais em trânsito para fora da organização não são comprometidos, como criptografia utilizando chaves apropriadas?

Área	Artigo	Justificação	Id	Questão
Controlos de segurança lógicos	25, 32	No tratamento de dados pessoais devem ser garantidas as medidas de segurança apropriadas para proteger os dados contra processamentos ilegais, perda acidental, destruição, dano, e colocar os dados disponíveis em caso de incidente.	4.1	Estão implementados controlos de autenticação antes de se aceder a qualquer dado pessoal do processo?
			4.2	As aplicações têm implementada autenticação multi-factor para utilizadores priveligiados?
			4.3	Caso as aplicações contenham dados pessoais sensíveis, têm implementada autenticação multi-factor para utilizadores com acesso a esses dados?
			4.4	Estão implementados mecanismos de modificação de passwords periódica?
			4.5	Está definida e em prática uma política de revisão de acessos periódica?
			4.6	Está implementado o princípio de previlégios mínimos na atribuição de acessos a novos utilizadores?
			4.7	Têm um procedimento definido e implementado para garantir que não são carregados dados pessoais em ambientes de qualidade?
			4.8	Tabelas de base de dados com dados pessoais, têm algoritmos de cifra aplicados nos mesmos?
			4.9	Ficheiros com dados pessoais que sejam armazenados pelas aplicações têm algoritmos de cifra aplicados nos mesmos?
			4.10	São realizados testes de segurança periódicos, pelo menos anualmente?
			4.11	Estão implementados mecanismos técnicos que permitam fazer tracking de todas as ações realizadas relacionadas com dados pessoais?
			4.12	Estão implementados mecanismos técnicos que permitam fazer tracking de todas as ações realizadas relacionadas com gestão de acessos?
			4.13	Estão implementados mecanismos técnicos para garantir a integridade dos logs?
			4.14	Caso sejam transmitidos dados sensíveis entre aplicações, estas transferências são feitas através de canais seguros garantido por métodos de cifra?
			4.15	Caso sejam transmitidos dados pessoais para fora da organização, estas transferências são feitas através de canais seguros garantido por métodos de cifra?
			4.16	Os sistemas estão protegidos do exterior das suas redes por firewalls e estão bloqueados todos os portos que não são usados?
			4.17	Está definida e em prática uma política de backups regular?
			4.18	Está implementado um sistema para garantir a restauração dos dados pessoais em caso de desastre, dano ou perda dos mesmos?

Anexo D

Id	Vulnerabilidades	Riscos	Possíveis consequências
1.1	- Falta de informação aos titulares	- R01 - R08	- Podem ser realizados tratamentos aos dados pessoais que o titular não tenha autorizado e que não esteja de acordo
1.2	- O consentimento não fica devidamente registado	- R08 - R10	- A organização não consegue validar que está a efetuar tratamentos apenas para titulares que autorizaram o tratamento dos seus dados - A organização não consegue demonstrar o consentimento dado caso requisitado
1.3	- Recolha de dados desnecessários	- R02	- Em caso de fuga de informação podem ser comprometidos mais dados que permitam causar dano aos titulares
1.4	- Especificações incompletas dos tratamentos - Tratamentos de dados não autorizados - Acesso por entidades não autorizadas	- R03 - R05 - R08 - R09 - R10	- Podem ser realizados tratamentos que não foram identificados inicialmente e que possam resultar em riscos imprevistos para os dados pessoais - Os dados podem ser acedidos por pessoas ou entidades que não estão autorizados para lhes aceder
1.5	- Informação identificativa disponível	- R05 - R06	- Caso seja necessário manter os dados para fins estatísticos, em caso de fuga de informação podem ser comprometidos dados pessoais que já não são utilizados
2.1	- Processamentos de dados não autorizados - Acesso por entidades não autorizadas	- R05 - R08	- Os titulares podem sofrer consequências de processamentos que não autorizaram - No contexto do processamento os dados podem ser transferidos para entidades que já não devem ter autorização para processar os dados - Impossibilidade dos titulares exercerem o direito à oposição
2.2	- Falta de controlo sobre os dados pessoais	- R07	- Titulares não sabem que dados é que a organização tem na sua posse - Titulares podem não conseguir retificar os seus dados se não souberem que dados é que a organização tem - Impossibilidade dos titulares exercerem o direito de acesso
2.3	- Tratamentos de dados pessoais desatualizados - Falta de controlo sobre os dados pessoais	- R07 - R10	- Processamento de dados pessoais desatualizados que podem causar impacto nos titulares - Impossibilidade dos titulares exercerem o direito à retificação

2.4	- Tratamentos de dados não autorizados - Acesso por entidades não autorizadas - Falta de controlo sobre os dados pessoais	- R03 - R04 - R08	- Tratamentos de dados pessoais para os quais já não estão autorizados - Os dados podem ser acedidos por pessoas ou entidades que já não estão autorizados para lhes aceder - Os titulares podem sofrer consequências de processamentos que não autorizaram - Impossibilidade dos titulares exercerem o direito ao esquecimento
2.5	- Falta de controlo sobre os dados pessoais - Retenção indevida dos dados	- R09 - R10	- Titulares podem querer que os seus dados passem a ser processados por outra entidade e dessa forma podem ser "obrigados" a continuar a usar serviços indesejados - Impossibilidade dos titulares exercerem o direito à portabilidade dos dados
2.6	- Falta de controlo sobre os dados pessoais - Tratamentos de dados indevidos	- R08 - R09 - R10	- Tratamentos nos dados ilegais/não autorizados pelos titulares - Impossibilidade dos titulares exercerem o direito à limitação ou objeção
3.1	- Falta de controlo sobre os dados pessoais - Falta de controlo sobre os tratamentos de dados	- R05 - R08	- Podem ser tratados dados pessoais que não deviam ser tratados - Tratamentos de dados pessoais para os quais não estão autorizados
3.2	- Falta de controlo sobre os dados pessoais - Processamento de dados sem justificação	- R08 - R09 - R10	- Tratamentos de dados de pessoas sensíveis sem necessidade - Tratamentos de dados pessoais que não deviam ser efetuados - Possíveis consequências para os titulares das quais eles não se consigam proteger
3.3	- Processamentos realizados por entidade em não conformidade	- R04 - R05 - R06 - R08 - R09 - R10	- Os processadores podem não assumir a responsabilidade pelos dados em caso de perda ou fuga de informação - Os processadores podem não ter implementadas medidas para garantir que os dados não são perdidos ou alvo de fugas de informação
3.4	- Conservação de dados pessoais para além do que é expectável	- R06 - R07	- Conservação de dados pessoais não autorizados - Em caso de fuga de informação podem ser comprometidos dados que não deviam estar na posse da organização
4.1	- Acessos indevidos	- R03 - R04 - R05 - R06	- Acesso a dados pessoais por utilizadores não autorizados - Fuga de informação dos dados acedidos - Destruição e/ou modificação indevida dos dados

4.2	- Autenticação inapropriada	- R03 - R04 - R06	- Contas de utilizador privilegiadas podem ser comprometidas mais facilmente - Acesso a dados pessoais por utilizadores não autorizados - Fuga de informação dos dados acedidos - Destruição e/ou modificação indevida dos dados
4.3	- Autenticação inapropriada	- R03 - R04 - R06	- Contas de utilizador com acesso a dados sensíveis podem ser comprometidas mais facilmente - Acesso a dados pessoais por utilizadores não autorizados - Fuga de informação dos dados acedidos - Destruição e/ou modificação indevida dos dados
4.4	- Má gestão de *passwords*	- R03 - R04 - R06	- *Passwords* eventualmente comprometidas podem nunca ser substituídas - Acesso a dados pessoais por utilizadores não autorizados - Fuga de informação dos dados acedidos - Destruição e/ou modificação indevida dos dados
4.5	- Acessos indevidos	- R03 - R04 - R05 - R06	- Acesso aos dados pessoais por utilizadores que já não deviam ter acesso aos mesmos - Fuga de informação dos dados acedidos - Destruição e/ou modificação indevida dos dados
4.6	- Acessos indevidos	- A03 - A04 - A05 - A06	- Novos utilizadores com acesso a funcionalidades que não devem ter - Fuga de informação dos dados acedidos - Destruição e/ou modificação indevida dos dados
4.7	- Carregamento de dados pessoais em ambientes de qualidade	- A03 - A05 - A08 - A09	- Acesso a dados pessoais por utilizadores apenas com permissão para testes que não deviam aceder aos dados pessoais - Dados são divulgados para utilizadores que não deveriam ter acesso
4.8	- Acessos indevidos	- A03 - A04	- Acesso a dados pessoais não autorizados diretamente das tabelas por administradores com acesso às bases de dados - Destruição e/ou modificação acidental dos dados
4.9	- Acessos indevidos	- A03 - A04	- Acesso a dados pessoais não autorizados diretamente dos ficheiros por administradores com acesso aos sistemas - Destruição e/ou modificação acidental dos dados
4.10	- Falhas conhecidas nas aplicações	- A03 - A04 - A05 - A06	- Existência de vulnerabilidades conhecidas nas aplicações - Possibilidade de exploração de vulnerabilidades por agentes maliciosos

4.11	- Uso não controlado dos sistemas	- A04 - A05 - A08	- Falta de controlo sobre as ações realizadas nos dados pessoais - Alterações de dados que não são possíveis de confirmar - Exportações de dados que não são possíveis de detetar
4.12	- Uso não controlado dos sistemas	- A03 - A04 - A05 - A08	- Falta de controlo na atribuição de acessos a utilizadores com acesso a dados pessoais - Acesso aos dados pessoais por utilizadores que não deviam ter acesso aos mesmos
4.13	- Uso não controlado dos sistemas	- A04 - A05 - A08	- Possibilidade de se modificar os *logs* não permitindo controlar as ações realizadas nos dados pessoais - Alterações de dados que não são possíveis de confirmar - Exportações de dados que não são possíveis de detetar
4.14	- Canais de comunicação inseguros	- A03 - A04 - A05	- Fuga de informação dos dados transferidos - Perda ou destruição dos dados em trânsito
4.15	- Canais de comunicação inseguros	- A03 - A04 - A05	- Fuga de informação dos dados transferidos - Perda ou destruição dos dados em trânsito
4.16	- Sistemas mal protegidos	- A03 - A04 - A05 - A06	- Comprometimento da rede interna - Fuga de informação
4.17	- Falta de *backups*	- A04	- Impossibilidade de recuperar dados pessoais em caso de acidente ou perda de dados
4.18	- Falta de um procedimento de recuperação de desastres	- A04	- Impossibilidade de recuperar dados pessoais em caso de desastre, acidente ou perda de dados
5.1	- Acessos indevidos	- R03 - R04 - R06	- Acesso a dados pessoais não autorizados diretamente dos ficheiros - Destruição dos dados - Roubo dos dados
6.1	- Processamentos realizados por entidade em não conformidade	- R04 - R05 - R06 - R08 - R09 - R10	- Os processadores podem não ter implementadas medidas para garantir que os dados não são perdidos ou alvo de fugas de informação
6.2	- Canais de comunicação inseguros	- R03 - R04 - R05 - R06	- Fuga de informação dos dados transferidos - Perda ou destruição dos dados em trânsito

Anexo E

Id	Medidas recomendadas	Tecnologias
1.1	Criar um documento onde estejam descritos os motivos e finalidades da recolha dos dados pessoais, ou seja o propósito do processo identificado na aba "Processo", e os tratamentos a que os dados vão ser sujeitos. Este documento deve ser claro e de fácil leitura, e sempre disponibilizado aos titulares previamente à recolha de dados. Esta documentação deve ser revista sempre que se efetuarem alterações no processo de tratamento de dados.	Ferramenta de processamento de texto, ex: *Word*.
1.2	Definir um procedimento de gestão de consentimentos onde esteja definido que deve ficar registado, previamente à recolha dos dados do titular, algo que torne possível a verificação do consentimento do utilizador, seja o registo de uma ação efetuada numa página web, um documento assinado digitalmente ou presencialmente, ou um *email* recebido pelo titular, e ter um sistema que permita à organização pesquisar pelo consentimento quando necessário, seja uma base de dados, um sistema de ficheiros ou um arquivo onde estejam implementadas medidas para garantir a integridade do consentimento.	Sistema onde seja possível armazenar documentos digitais e pesquisar pelos mesmos: - Base de dados; - Sistema de gestão de ficheiros.
1.3	Identificar e documentar que dados são necessários para cada tratamento que é efetuado no processo, identificados na aba "Processo" e o motivo do seu tratamento por forma a serem recolhidos apenas os dados necessários. Esta documentação deve ser revista sempre que se efetuarem alterações no processo de tratamento de dados.	Ferramenta de processamento de texto, ex: *Word*.
1.4	Ter documentados os tratamentos efetuados no processo no documento que é disponibilizado aos titulares previamente à recolha de dados pessoais, quer sejam tratamentos realizados através das aplicações identificadas na aba "Processo", quer sejam tratamentos manuais. Esta documentação deve ser revista sempre que se efetuarem alterações no processo de tratamento de dados. Em caso de serem acrescentados novos tipos de tratamentos o titular deve ser notificado e deve ser recolhido o seu consentimento para os novos tratamentos.	Ferramenta de processamento de texto, ex: *Word*.

1.5	Devem estar documentados os sistemas onde estão armazenados dados dos titulares (sistemas produtivos, sistemas de backups, entre outros) por forma a poder executar-se uma ferramenta para remover os dados que permitam identificar os titulares nos sistemas identificados.	- Ferramenta de processamento de texto, ex: *Word*; - Ferramenta para minimização de dados.
2.1	Deve estar implementado um mecanismo nos sistemas de armazenamento dos dados pessoais que permita verificar os dados dos titulares podem ser processados ou não, como um campo numa tabela de base de dados ou num ficheiro que indique se os dados pessoais de cada titular devem ser processados ou não, e antes de cada processamento deve-se verificar o valor desse campo.	Funcionalidade para verificar se os dados de cada titular podem ser processados ou não, de forma a que seja possível de se verificar previamente à realização de um tratamento. Exemplos de sistemas onde seja possível definir se os dados de um titular podem ser processados ou não: - Base de dados; - Sistema de gestão de ficheiros.
2.2	Devem estar documentados os sistemas onde estão armazenados os dados dos titulares e ter ferramentas que permitam extrair os dados desses sistemas a pedido dos titulares. Idealmente de forma a manter a confidencialidade dos dados pessoais.	Ferramenta que permita extrair os dados pessoais dos titulares, ex: - Página web autenticada para acesso do titular aos seus dados; - Ferramenta de *reporting* que permita apenas a um conjunto de utilizadores autorizados extrair os dados de determinado titular a pedido do mesmo.
2.3	Devem estar documentados os sistemas onde estão armazenados os dados dos titulares (sistemas produtivos, sistemas de backups, entre outros) e ter ferramentas que permitam modificar os dados desses sistemas a pedido do titular. Idealmente de forma a manter a confidencialidade dos dados pessoais.	Ferramenta que permita modificar os dados pessoais do titular, ex: - Página web autenticada para acesso do titular aos seus dados e opção para modificar os mesmos; - Ferramenta que permita apenas a um conjunto de utilizadores autorizados modificar os dados de determinado titular a pedido do mesmo.
2.4	Devem estar documentados os sistemas onde estão armazenados os dados dos titulares (sistemas produtivos, sistemas de backups, entre outros) e ter ferramentas que permitam apagar os dados desses sistemas a pedido do titular.	Ferramenta que permita apagar os dados pessoais do titular e que seja refletido em todos os sistemas incluindo *backups*, ex: - Página web autenticada para acesso do titular aos seus dados e opção para apagar os mesmos; - Ferramenta que permita apenas a um conjunto de utilizadores autorizados apagar os dados de determinado titular a pedido do mesmo.
2.5	Devem estar documentados os sistemas onde estão armazenados os dados dos titulares e ter ferramentas que permitam extrair os dados desses sistemas a pedido do titular, e numa forma possível de ser interpretável por máquinas. Idealmente de forma a manter a confidencialidade dos dados pessoais.	Ferramenta que permita extrair os dados pessoais do titular, ex: - Página web autenticada para acesso do titular aos seus dados; - Ferramenta de *reporting* que permita apenas a um conjunto de utilizadores autorizados extrair os dados de determinado titular a pedido do mesmo.

		Os dados devem estar num formato possível de ser importado por outros *softwares*, ex: XML, JSON, CSV.
2.6	Devem estar documentados os tratamentos que são realizados para cada titular e ter um mecanismo para ativar/desativar tratamentos para cada titular.	Ferramenta que permita limitar os tratamentos efetuados ao titular, ex: - Página web autenticada para o titular consultar os tratamentos a que está afeto e poder mudar a sua decisão; - Ferramenta que permita apenas a um conjunto de utilizadores autorizados limitar os tratamentos de determinado titular a pedido do mesmo.
3.1	Criar um documento onde estejam descritos os tratamentos efetuados, a justificação de cada tratamento, os tipos de dados pessoais tratados, qual o *flow* de circulação dos dados, quais as aplicações por onde os dados circulam e as entidades com acesso aos mesmos. Esta documentação deve ser revista sempre que se efetuarem alterações no processo de tratamento de dados.	Ferramenta de processamento de texto, ex: *Word*.
3.2	Dados pessoais sensíveis apenas devem ser tratados se existir uma justificação válida para a realização desses tratamentos. Por justificação válida entenda-se que os dados são essenciais para atingir o objetivo do processamento identificado no processo. Caso exista essa justificação a mesma deve estar documentada, senão esses dados devem deixar de ser recolhidos e tratados.	Ferramenta de processamento de texto, ex: *Word*.
3.3	Deve-se validar para cada entidade externa interveniente no processo se existe um contrato com a mesma e se nesse contrato existem cláusulas onde esteja contemplada a conformidade com o GDPR e a responsabilização. Caso não exista deve-se negociar uma alteração ao contrato. Em novos contratos essas cláusulas devem estar sempre presentes.	Sistema que permita armazenar e gerir os contratos, ex: sistema de gestão de ficheiros.

3.4	Quando os dados de um titular deixam de ser processados deve ser atribuída a data do último processamento a esses dados e deve estar incorporado nos sistemas de gestão desses dados pessoais um mecanismo que periodicamente valida o período de armazenamento atual dos dados com o que é imposto por lei e apagar os mesmos ou deve existir um sistema independente com a capacidade de fazer essa validação e apagar os dados caso aplicável.	- Funcionalidade para verificar o período de armazenamento atual dos dados e apagar os mesmos, incorporada na tecnologia de gestão/armazenamento dos dados; - *Scheduler* que corre um serviço de verificação do período dos dados que permita apagar os mesmos caso aplicável.
4.1	Qualquer acesso a dados pessoais deve ser restringido por mecanismos de autenticação que permitam apenas o acesso por pessoas autorizadas e posteriormente se poder identificar quem realizou que ações sobre os dados pessoais.	- Interface de login; - Mecanismo de proteção de acessos não autenticados aos dados.
4.2	Deve existir um meio adicional de autenticação para além de uma *password* para acessos privilegiados a funcionalidades mais críticas para reduzir os riscos no caso de comprometimento de passwords.	Utilização de *tokens* ou de mensagens com códigos gerados no momento de autenticação.
4.3	Deve existir um meio adicional de autenticação para além de uma *password* para acessos a dados sensíveis para reduzir os riscos no caso de comprometimento de passwords.	Utilização de *tokens* ou de mensagens com códigos gerados no momento de autenticação.
4.4	Deve existir uma política onde esteja especificado o tempo de vida de uma *password*, e devem estar implementados mecanismos técnicos para forçar essa alteração.	*Scheduler* que corre um serviço de verificação do período de vida das *passwords* e que obriga os utilizadores a modificarem a mesma caso aplicável.
4.5	Deve existir uma política onde esteja especificado quando é efetuada uma recertificação de acessos, e essa política deve ser cumprida, podendo recorrer-se a notificações para os administradores de sistemas.	*Scheduler* para notificar os administradores quando devem realizar a recertificação de acessos.
4.6	Quando é inserido um novo utilizador no sistema, o mesmo não deve ter acessos concedidos por defeito, e devem ser dados à medida que for surgindo a necessidade.	Configuração dos acessos atribuídos por defeito a novos utilizadores
4.7	Não devem ser utilizados dados produtivos em ambientes de qualidade ou testes, mas em caso de haver necessidade de utilizar dados produtivos nesses ambientes devem estar implementadas medidas técnicas para mascarar/remover dados pessoais quando os dados forem transitados de um ambiente para outro.	Tecnologia para mascarar dados pessoais ou apagar os mesmos em passagens de dados entre ambientes.
4.8	Bases de dados que contenham dados pessoais devem ser cifradas para impedir a leitura dos dados por utilizadores do sistema que não devem aceder a esses dados e para dificultar a divulgação dos dados em caso de fuga de informação.	Mecanismos de cifra nas bases de dados, podendo aplicar-se apenas nos valores, em tabelas inteiras ou na base de dados em si dependendo da criticidade dos dados e da base de dados. Ex: TDE em bases de dados de MSSQL superiores a 2008

4.9	Ficheiros que contenham dados pessoais devem ser cifrados para impedir a leitura dos dados por utilizadores do sistema que não devem aceder a esses dados e para dificultar a divulgação dos dados em caso de fuga de informação.	Aplicação de algoritmos de cifra em ficheiros que contenham dados pessoais.
4.10	Definição e execução de um plano de testes de segurança periódicos, de preferência por uma entidade externa ou por *testers* que não tenham estado envolvidos no desenvolvimento do sistema, para garantir que não existem vulnerabilidades conhecidas nas aplicações.	N/A
4.11	Implementação de um mecanismo de registo de ações, que guarde esses registos num sistema distinto do sistema a ser auditado por forma a garantir a integridade dos mesmos em caso de comprometimento do sistema.	Sistema de *logs* centralizado.
4.12	Implementação de um mecanismo de registo de ações, que guarde esses registos num sistema distinto do sistema a ser auditado por forma a garantir a integridade dos mesmos em caso de comprometimento do sistema.	Sistema de *logs* centralizado.
4.13	Os *logs* devem ter implementados mecanismos para garantir a integridade dos mesmos, como armazenamento dos *logs* num sistema distinto e aplicação de *hashs* ou *MACs*.	- Sistema de *logs* centralizado; - Mecanismo para assinar os *logs*.
4.14	Devem estar implementados mecanismos de cifra para transferências entre aplicações quando são transmitidos dados sensíveis para reduzir o risco de comprometimento dos mesmos.	Canais de comunicação seguros.
4.15	Devem estar implementados mecanismos de cifra em transferências de dados pessoais para fora da organização para evitar o risco de comprometimento dos mesmos.	- Canais de comunicação seguros; - Cifra de ficheiros; - Cifra de *emails*.
4.16	Para evitar o comprometimento da rede interna, a mesma deve estar separada da rede externa por pelo menos uma *firewall*, e essa firewall deve ter bloqueados todos os portos que não são usados.	*Firewall*.
4.17	Deve estar em prática uma medida para garantir que são realizados *backups* aos dados ou sistemas de acordo com a sua criticidade.	Sistema de *backups*.
4.18	Devem ser mantidos backups dos sistemas numa localização física distinta da localização dos sistemas para o caso de acontecimento de desastre que danifique os sistemas de *backups* local	Sistema de *backups*.
5.1	Implementação de um mecanismo de proteção físico, adequado aos dados a proteger: - Cadeado	N/a

	- Leitor de cartões - Leitor de código pin	
6.1	Previamente a se transferir os dados para uma entidade, deve-se garantir que essa entidade cumpre com os requisitos do GDPR. Esta validação deve ser feita periodicamente.	N/a
6.2	Devem ser usados meios seguros ou estar implementados canais seguros para transporte dos dados com algoritmos de criptografia apropriados para transmitir os dados para sistemas que tenham mecanismos de acesso controlado por *password*.	- *Email* com ficheiros cifrados; - Canal com SFTP ou FTPS implementados; - Aplicação web com HTTPS implementado.

Anexo F

Prints de um exemplo do protótipo preenchido com dados anonimizados e ligeiramente modificados por forma a garantir a confidencialidade.

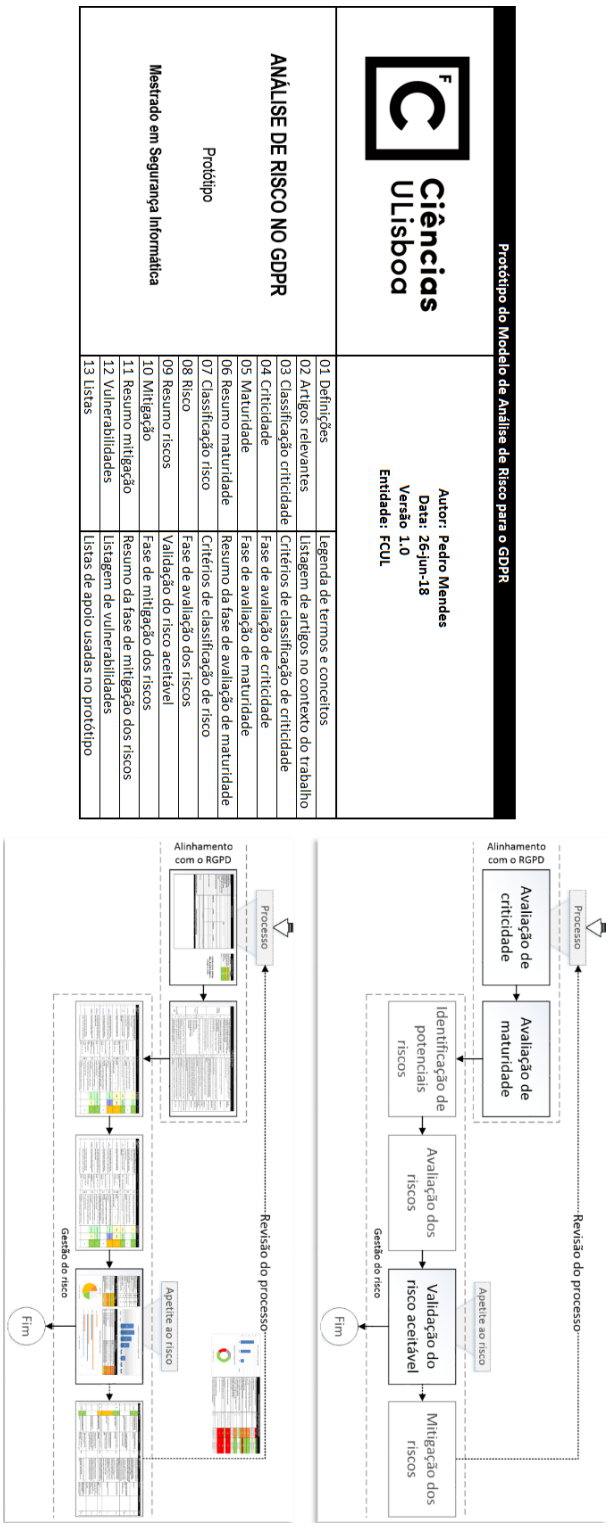


Figura 18 - Ecrã de introdução

Termo	Definição
RGPD	O regulamento em si que é constituído pelos artigos e definições necessários para a implementação e conformidade do mesmo.
Tratamento de Dados Pessoais	Qualquer operação ou conjunto de operações efetuados sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, comparação ou interconexão, bem como a limitação, apagamento ou destruição.
Atividade de tratamento de dados pessoais	Uma atividade em que seja efetuado um ou mais tratamentos de dados pessoais de acordo com a definição anterior.
Processo de tratamento de dados	Um conjunto de atividades de tratamento de dados pessoais com um propósito final específico.
Indivíduos / Titulares dos dados	Pessoas que podem ser identificadas direta ou indiretamente, sobre quem os dados pessoais são tratados.
DPIA	Avaliação de impacto de uma atividade de tratamento de dados pessoais que é provável que resulte num risco elevado para os direitos e liberdades dos indivíduos, levando em conta a natureza, âmbito, contexto e propósito do processamento dos dados. Nesta avaliação deve também determinar-se como é que se pretende mitigar os riscos, sendo obrigatória a consulta da entidade reguladora no caso de não ser possível mitigar os riscos para um nível aceitável.
Controlador	Entidade, pessoa, agência ou autoridade pública responsável por determinar os propósitos e forma de processar os dados pessoais. No contexto deste documento assume-se que o controlador faz parte da mesma organização que o processador.
Processador	Entidade, pessoa, agência ou autoridade pública que processa os dados em nome do controlador. No contexto deste documento assume-se que o processador faz parte da mesma organização que o controlador.
Pseudonimização	É uma forma de processar dados pessoais, aplicando a minimização de dados, um conceito dos princípios de proteção de dados, de tal forma que os mesmos não possam ser atribuídos a um indivíduo em específico.
Fugas de informação	Uma falha na segurança que pode levar ao comprometimento dos princípios da segurança, nomeadamente à destruição, perda, alteração, divulgação e/ou acesso não autorizados de dados pessoais.
Autoridade Supervisora	Data Protection Authority no seu termo original, em Português Autoridade de Proteção de Dados, a entidade reguladora pública que é estabelecida pelo estado membro que ajuda a garantir a conformidade do RGPD nesse estado membro. Em Portugal é a Comissão Nacional de Proteção de Dados (CNPD).
Encarregado de Proteção de Dados	Data Protection Officer no seu termo original, em Português Encarregado de Proteção de Dados, uma pessoa nomeada pelo controlador e o processador para apoiar nas atividades base do RGPD e garantir que a organização está em conformidade com o regulamento. Uma organização não é obrigada a nomear um encarregado, apenas em casos específicos de acordo com a implicação (97) do RGPD.

Nível de maturidade	Definição
Não implementado	O controlo não está ainda implementado.
Executado informalmente	O controlo está implementado mas informalmente, podendo não estar bem definido. Pode não se encontrar documentado, pode não ser executado da melhor forma ou de forma adequada, e pode não ser prática a sua execução em situações semelhantes.
Bem definido	O controlo está documentado e aprovado, sendo prática comum utilizar-se em situações semelhantes.
Controlado quantitativamente	Os resultados do controlo são analisados continuamente com o objetivo de se melhorar a performance e obter melhores resultados.
Melhorado continuamente	Em adição aos anteriores, o controlo é revisto periódicamente e adaptado conforme as necessidades da realidade da organização.
Não aplicável	Em algumas situações determinado controlo pode não ser aplicável por não fazer sentido tendo em conta o contexto do processamento.

Tratamentos sujeitos a risco	Descrição
Processamento automatizado de dados onde é traçado um perfil dos indivíduos	Especialmente informação relacionada com o desempenho no trabalho, situação económica, saúde, preferências pessoais ou interesses, confiabilidade ou comportamento, localização ou deslocações.
Processamento automatizado de dados	Em que sejam tomadas decisões legais para o indivíduo, ou decisões de efeito semelhante.
Processamento de dados utilizados para observar, monitorar ou controlar indivíduos	Incluindo dados recolhidos através de monitoramento sistemático em locais públicos.
Processamento de dados sensíveis	Quando são processados dados sensíveis, de acordo com o especificado no GDPR.
Processamento de dados em grande	Processamento de dados de um número elevado de indivíduos, ou um elevado volume ou com uma grande extensão geográfica.
Processamento sobre conjuntos de dados que tenham sido combinados	Por exemplo dados com origem em diferentes fontes ou resultantes de operações com diferentes propósitos.
Processamento de dados de indivíduos considerados vulneráveis	Como crianças, idosos e indivíduos com incapacidades.
Processamento de dados através do uso de novas tecnologias	Quando são utilizadas novas tecnologias, seja no mercado, seja nova na organização.
Transferência de dados para fora da União Europeia	Quando dados processados ou por processar são transferidos para fora da UE.
Processamento de dados que possa impedir indivíduos de exercer direitos	Ou de usufruir de serviços ou contratos.
Processamento de novos tipos de dados	Quando é realizado o processamento de novos tipos de dados que não eram processados antes.
Novos tipos de processamento de dados	Quando são realizados novos tipos de processamento de dados que não eram realizados antes.

Identificador	Risco
R01	Recolha de dados não justificada
R02	Recolha de dados excessiva
R03	Acesso não autorizado aos dados
R04	Destruição ou alteração acidental/ilegal de dados
R05	Divulgação não autorizada de dados
R06	Roubo de dados
R07	Uso/Armazenamento de dados desatualizados
R08	Utilização dos dados para além do que é expectável
R09	Utilização dos dados para além do que é socialmente aceitável
R10	Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar

Figura 19 - Ecrã de definições

Área	Breve descrição
Recolha e informação	Artigos relacionados com a recolha de dados dos titulares e a informação dada aos mesmos sobre a própria da recolha.
Consentimento e direitos dos titulares	Artigos relacionados com a possibilidade de demonstrar o fato e retirar o consentimento por parte de um titular e com a possibilidade de um titular exercer os seus direitos sobre os seus dados pessoais.
Documentação e requisitos legais	Artigos relacionados com a documentação do processo para forma a permitir a realização de análises de risco, e com requisitos legais e contratuais que devem ser cumpridos e garantidos.
Controlos de segurança lógica	Artigos relacionados com os controlos de segurança implementados para garantir a segurança e privacidade dos dados pessoais de um ponto de vista dos sistemas de informação.
Controlos de segurança física	Artigos relacionados com os controlos de segurança implementados para garantir a segurança e privacidade dos dados pessoais de um ponto de vista física.
Transferências de dados internacionais	Artigos relacionados com a transferência de dados pessoais, nomeadamente para outros países e para fora da União Europeia.

Artigo	Breve descrição	Crimes associados
5 - Princípios relativos ao tratamento de dados pessoais	Os dados pessoais são: a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados (<licitude, lealdade e transparência>); b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 (<limitação das finalidades>); c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (<minimização dos dados>); d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para as quais são tratados, sejam apagados ou retificados sem demora (<exatidão>); e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados (<limitação da conservação>); f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou	Elevada
6 - Licitude do tratamento	O tratamento é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) O tratamento for necessário ao exercício de função de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os	Elevada
7 - Condições aplicáveis ao consentimento	Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.	Elevada
9 - Tratamento de categorias especiais de dados pessoais	É proibido o tratamento de 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.	Elevada
13 - Informações a facultar quando os dados pessoais são recolhidos junto do titular	Quando os dados pessoais forem recolhidos junto do titular, o responsável pelo tratamento faculta-lhe, aquando da recolha destes dados pessoais, as seguintes informações: a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante; b) Os contactos do encarregado da proteção de dados, se for caso disso; c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento; d) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro; e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver; f) Se for caso disso, a fato de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.º ou 47.º, ou no artigo 49.º, n.º	Elevada
14 - Informações a facultar quando os dados pessoais não são recolhidos junto do titular	Quando os dados pessoais não forem recolhidos junto do titular, o responsável pelo tratamento fornece-lhe os seguintes informações: a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante; b) Os contactos do encarregado da proteção de dados, se for caso disso; c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento; d) As categorias dos dados pessoais em questão; e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver; f) Se for caso disso, a fato de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.º ou 47.º, ou no artigo 49.º, n.º 1, segunda parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia dos mesmos, ou onde foram disponibilizados;	Elevada
15 - Direito de acesso do titular dos dados	O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações: a) As finalidades do tratamento dos dados; b) As categorias dos dados pessoais em questão; c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais; d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo; e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento; f) O direito de apresentar reclamação a uma autoridade de controlo; g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem destes dados; h) A existência de decisões automatizados, incluindo a definição de perfis, referida nos artigos 22.º, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.	Elevada
16 - Direito de retificação	O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.	Elevada
17 - Direito ao apagamento dos dados («direito a ser esquecido»)	O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento; c) O titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2; d) Os dados pessoais foram tratados ilicitamente; e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou dos Estados-Membros a que o responsável pelo tratamento esteja sujeito; f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1.	Elevada

Figura 20 - Ecrã com a listagem de artigos, parte 1

18 - Direito à limitação do tratamento	O titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, nos seguintes situações: a) Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização; c) O responsável pelo tratamento já não precisar dos dados pessoais para fins do tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial; d) Se tiver oposto ao tratamento nos termos do artigo 21.º, n.º 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.	Elevada
19 - Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento	O responsável pelo tratamento comunica a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento a que se tenha procedido em conformidade com o artigo 16.º, o artigo 17.º, n.º 1, e o artigo 18.º, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado. Se o titular dos dados o solicitar, o responsável pelo tratamento fornece-lhe informações sobre os referidos destinatários.	Elevada
20 - Direito de portabilidade dos dados	O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se: a) O tratamento se basear no consentimento dado nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a), ou num contrato referido no artigo 6.º, n.º 1, alínea b); e b) O tratamento for realizado por meios automatizados.	Elevada
21 - Direito de oposição	O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.º, n.º 1, alínea e) ou f), ou no artigo 6.º, n.º 4, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.	Elevada
25 - Proteção de dados desde a conceção e por defeito	Tendo em conta o estado da técnica, os custos da aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.	Baixa
28 - Subcontratante	Quando o tratamento dos dados for efetuado por sua conta, 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.	Baixa
30 - Registos das atividades de tratamento	Cada responsável pelo tratamento e, sendo caso disso, o seu representante conservam um registo de todas as atividades de tratamento sob a sua responsabilidade. Esse registo contem todas as seguintes informações: a) O nome e os contactos do responsável pelo tratamento e, sendo caso disso, de qualquer responsável conjunto pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados; b) As finalidades do tratamento dos dados; c) A descrição das categorias de titulares de dados e das categorias de dados pessoais; d) As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais; e) Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 49.º, n.º 1, segundo parágrafo, a documentação que comprove a existência das garantias adequadas; f) Se possível, os prazos previstos para o apagamento das diferentes categorias de dados; g) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32.º, n.º 1.	Baixa
32 - Segurança do tratamento	Tendo em conta as técnicas mais avançadas, os custos da aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado: a) A pseudonimização e a cifragem dos dados pessoais; b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.	Baixa
35 - Avaliação de impacto sobre a proteção de dados	Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação do impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes puder ser analisado numa única avaliação.	Baixa
36 - Consulta prévia	O responsável pelo tratamento consulta a autoridade de controlo antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados nos termos do artigo 35.º indicar que o tratamento resultaria num elevado risco na ausência de medidas tomadas pelo responsável pelo tratamento para atenuar o	Baixa
44 - Princípio geral das transferências	Qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional. Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento.	Elevada
45 - Transferências com base numa decisão de adequação	Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.	Elevada
46 - Transferências sujeitas a garantias adequadas	Não tendo sido tomada qualquer decisão nos termos do artigo 45.º, n.º 3, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.	Elevada

Figura 21 - Ecrã com a listagem de artigos, parte 2

Racional	Criticidade
Os impactos nos titulares são tendencialmente pouco significativos e não existe uma grande exposição ao risco.	Baixa
Os impactos nos titulares são mais significativos e existe uma maior exposição ao risco.	Média
Existe uma exposição ao risco alta e o comprometimento dos dados possívelmente terá impactos significativos nos titulares.	Alta
Existe uma exposição elevada ao risco e o comprometimento dos dados pode comprometer os direitos e liberdades dos titulares.	Elevada

Racional - No contexto dos dados pessoais	Criticidade
Dados pessoais identificativos, muitas vezes publicados por livre vontade dos titulares, e que numa situação normal, sem a presença de dados sensíveis, o seu comprometimento por si só não deve causar um grande impacto.	Média
Dados pessoais que podem permitir chegar fisicamente perto do titular, identificar hábitos ou padrões dos mesmos, ou efetuar transações e/ou danos financeiros em nome dos/aos titulares.	Alta
Dados pessoais classificados como sensíveis pelo próprio regulamento por poderem conter informação que pode colocar a integridade física e/ou moral do titular em causa.	Elevada

Ativo	Tipo	Racional	Criticidade
Dados identificativos	Dado pessoal	Dados pessoais que permitem identificar o titular e que não permitem identificar padrões comportamentais, nem a sua localização ou causar danos financeiros.	Média
Dados demográficos			
Experiência profissional			
Características físicas			
Perfilagem e dados comportamentais	Dado pessoal	Dados que permitem identificar padrões comportamentais, a localização e paradeiro atual e/ou causar danos ou fraude financeira aos titulares.	Alta
Dados de contas, transações ou créditos			
Propriedades			
Outros dados financeiros / preferências / localização			
Origem racial ou étnica	Dado pessoal sensível	Dados pessoais sensíveis, de acordo com o regulamento, que podem mais severamente condicionar as liberdades e direitos do titular e resultar num risco elevado para o mesmo.	Elevada
Opiniões políticas			
Convicções religiosas ou filosóficas			
Filiação sindical			
Dados genéticos			
Dados biométricos			
Dados relativos à saúde			
Dados relativos à vida sexual ou orientação sexual			
Dados da vida privada			
Aplicação que combina dados de várias fontes	Aplicação	Aplicação que combina dados de titulares provenientes de 2 ou mais fontes de dados.	Alta
Aplicação exposta na web		Aplicação que está exposta na web e mais facilmente é acedida por agentes maliciosos.	Alta
Nova aplicação no mercado (menos de 1 ano)		Nova aplicação no mercado de baixa maturidade, possivelmente com mais bugs e/ou vulnerabilidades.	Alta
Nova aplicação na organização (menos de 2 meses)		Nova aplicação na organização, tendo a mesma uma baixa maturidade na utilização e/ou configuração da tecnologia.	Alta
Aplicação na cloud		Aplicação na cloud, ou SaaS (Software as a Service). Apesar dos dados se encontrarem for a da organização este tipo de aplicações já costuma ter alguma maturidade, dependendo também dos fornecedores.	Média
Outros tipos de aplicação para processamento de dados		Aplicações simplesmente utilizadas no processamento de dados.	Baixa

Figura 22 - Ecrã de definições de classificação de criticidade

Ficha do processo				
Nome do processo	Processo de Recrutamento			
Finalidades do processo	Avaliação e seleção de possíveis candidatos para a organização			
Legitimidade do processo	Ao abrigo da legislação			
Dono do processo	Sr. Silva			
Responsável pelo processo	Eng. Silva		**DPO**	Dr. Silva
É realizado algum dos tratamentos de dados possível de resultar num risco elevado?	Processamento de dados sensíveis			
Meios de recolha dos dados	Presencial		Formulário web	
Dados pessoais tratados	**Dado pessoal**	**Criticidade**	**Dado pessoal**	**Criticidade**
	Dados identificativos	Média	Dados relativos à saúde	Elevada
	Dados demográficos	Média		
	Experiência profissional	Média		
	Dados de contas, transaçõ	Alta		
	Filiação sindical	Elevada		
Aplicações	**Aplicação**			**Criticidade**
	Aplicação que combina dados de várias fontes			Alta
Transferência de dados para terceiros	Não	**Transferências entre departamentos ou aplicações**		Sim
Fluxos de dados pessoais (por onde circulam os dados pessoais)				

Classificação do processo	
Em termos de	**Criticidade**
Tratamentos efetuados	Alta
Dados pessoais tratados	Elevada
Aplicações	Alta
Transferências	Média
Geral	Alta

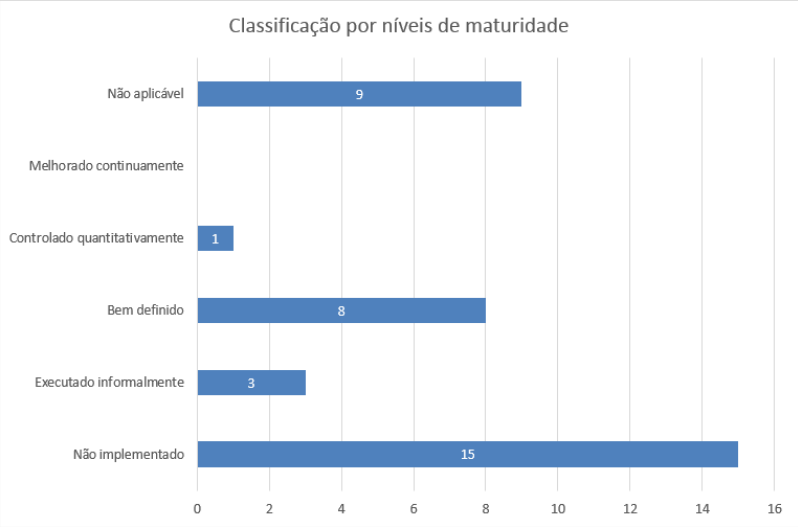
O processo tem uma criticidade alta, sendo que deve ser realizado um DPIA.

Figura 23 - Ecrã da fase de avaliação de criticidade

Avaliação de maturidade					
Área	Artig	Justificação	Id	Questão	Maturidade
Recolha e informação	5, 13, 14	Os titulares devem ser informados da propósito do tratamento dos seus dados, do período durante o qual os seus dados irão ser armazenados, dos seus direitos, e caso aplicável, se os dados serão transferidos para outros países ou instituições.	1.1	Existe um processo para garantir que antes da recolha dos dados, os titulares têm uma informação atualizada e clara do propósito dos seus dados posse a do processo de tratamento dos seus dados?	Executada informalmente
	6, 7	Os titulares devem dar o consentimento para o processamento dos seus dados e deve ser possível demonstrar que os titulares deram o consentimento para o tratamento dos seus dados, excetuando quando o processamento for necessário para garantir conformidade com uma obrigação legal.	1.2	Existe uma forma definida de recolher, armazenar e disponibilizar quando requisitada o consentimento para o processamento dos dados?	Não aplicável
	5	Devem ser recolhidos apenas os dados necessários para os tratamentos identificados.	1.3	Existe um processo para garantir que são recolhidos apenas os dados necessários para os tratamentos identificados?	Não implementada
	5	Apenas devem ser realizados os tratamentos aos dados posse que foram identificados para os titulares na recolha dos dados.	1.4	Existe um processo para garantir que apenas são realizados os tratamentos que foram propostos aos titulares?	Bem definida
	5	Os dados posse devem apenas permitir identificar os titulares durante o propósito para o qual os dados foram recolhidos.	1.5	Existem medidas de minimização dos dados, como pseudo anonimização para garantir que os dados depois dos tratamentos não permitem a identificação dos titulares?	Não implementada
Consentimento e direitos dos titulares	7	Deve ser possível aos titulares retirarem o consentimento para o tratamento dos seus dados, caso seja aplicável.	2.1	Existe um processo para garantir que os dados dos titulares deixem de ser processados caso o titular assim o requisite?	Não aplicável
	15	Deve ser possível para os titulares poderem exercer os direitos sobre os seus dados posse, caso seja aplicável: - Direito de acesso; - Direito à retificação; - Direito ao esquecimento; - Direito à restrição do tratamento; - Direito à portabilidade dos dados; - Direito à objeção.	2.2	Existe um processo que permita mostrar aos titulares os seus dados posse que a organização tem nos seus pose caso a mesma assim o solicite?	Executada informalmente
	16, 19		2.3	Existe um processo para retificar os dados posse aos titulares caso a titular solicite a sua retificação?	Executada informalmente
	17, 19		2.4	Existe um processo para garantir que os dados dos titulares sejam apagados caso seja solicitado pelos mesmos, ou não seja mais necessário tratar esses	Não aplicável
	20		2.5	Existe um processo para a exportação dos dados posse a um titular num formato interpretável por máquinas para forma a que os mesmos sejam enviados para o processamento para outras organizações caso seja solicitado pelo titular?	Não aplicável
	18, 21		2.6	Existe um processo para limitar ou autorizar determinado tratamento de dados caso seja solicitado pelo titular?	Não aplicável
Documentação requisitos legais	30	Deve ser mantido e atualizado um registo com os detalhes do tratamento, tipos de dados tratados e o fluxo de circulação do dados na organização.	3.1	É mantido um registo com os detalhes do tratamento, os tipos de dados, os fluxos de circulação de dados posse e existe um processo para garantir que esses dados estão atualizados?	Não implementada
	9	Caso seja efetuado o tratamento de dados sensíveis, deve existir uma justificação válida para esse tratamento.	3.2	Existe, e está documentada uma justificação válida para o tratamento de dados posse sejam sensíveis?	Não aplicável
	28	Caso o tratamento seja efetuado por terceiros, deve existir um contrato estabelecido entre as partes onde o processador assume que implementa as medidas técnicas e organizacionais apropriadas para garantir a conformidade com a regulamento.	3.3	Existe um processo para incluir uma cláusula em contratos com processadores de dados externos, para garantir que os mesmos assumem os riscos e tomam as medidas técnicas e organizacionais apropriadas para garantir a conformidade com a regulamento?	Bem definida
	17	O direito ao esquecimento aplica-se apenas quando a processamento não for obrigatória para cumprir com uma obrigação legal ou for de interesse público a registo dos dados como para fins científicos.	3.4	Caso seja obrigatória manter os dados posse após a processamento, devido a alguma obrigação legal, existe um processo para garantir que os dados são apagados após a prazo de retenção definido por lei?	Bem definida
Controlar de segurança lógicas	25, 32	Nos tratamentos de dados posse devem ser garantidas as medidas de segurança apropriadas para proteger os dados contra processamentos ilegais, perda acidental, destruição, dano, e colocar os dados disponíveis em caso de incidente.	4.1	Estão implementados controlos de autenticação antes de se aceder a qualquer dado pessoal do processo?	Bem definida
			4.2	As aplicações têm implementada autenticação multi-factor para utilizadores privilegiados?	Não implementada
			4.3	Caso as aplicações contenham dados posse sensíveis, têm implementada autenticação multi-factor para utilizadores com acesso a esses dados?	Não implementada
			4.4	Estão implementados mecanismos de modificação de passwords periódicas?	Bem definida
			4.5	Está definida e em prática uma política de revisão de acessos periódica?	Não
			4.6	Está implementado o princípio de privilégios mínimos na atribuição de acessos a novos utilizadores?	Não implementada
			4.7	Têm um procedimento definido e implementado para garantir que não são carregados dados posse em ambientes de qualidade?	Não implementada
			4.8	Tabelas de bases de dados com dados posse, têm algoritmos de cifra aplicados nos mesmos?	Não implementada
			4.9	Ficheiros com dados posse que sejam armazenados pelas aplicações têm algoritmos de cifra aplicados nos mesmos?	Não implementada
			4.10	São realizados testes de segurança periódicos, pelo menos anualmente?	Não
			4.11	Estão implementados mecanismos técnicos que permitam fazer tracking de todas as ações realizadas relacionadas com dados posse?	Não implementada
			4.12	Estão implementados mecanismos técnicos que permitam fazer tracking de todas as ações realizadas relacionadas com portais de acesso?	Não implementada
			4.13	Estão implementados mecanismos técnicos para garantir a integridade dos	Não aplicável
			4.14	Caso sejam transmitidos dados sensíveis entre aplicações, estas transferências são feitas através de canais seguros garantidos por métodos de	Não implementada
			4.15	Caso sejam transmitidos dados posse para fora da organização, estas transferências são feitas através de canais seguros garantidos por métodos de cifra?	Bem definida
			4.16	Os sistemas estão protegidos do exterior das suas redes por firewalls e estão bloqueados todos os portos que não são usados?	Centralizada quantitativamente
			4.17	Está definida e em prática uma política de backups regulares?	Bem definida
			4.18	Está implementado um sistema para garantir a restauração dos dados posse em caso de desastre, dano ou perda dos mesmos?	Bem definida
Controlar de segurança física	25, 32	Nos armazenamentos de documentos com dados posse devem ser garantidas as medidas de segurança apropriadas para proteger os dados contra acessos indevidos.	5.1	O acesso a documentos físicos está protegido contra acessos indevidos?	Não implementada
Transferências de dados internacionais	44, 45, 46	Caso sejam transferidos dados para outros países ou organizações internacionais, devem estes ser tomadas as medidas necessárias para garantir a segurança dos dados e privacidade dos titulares.	6.1	Existe um processo para garantir que os dados posse são apenas transferidos para entidades que cumpram com a regulamento?	Não aplicável
			6.2	Estão implementadas medidas técnicas para garantir que os dados posse em trânsito para fora da organização não são comprometidos, como criptografia utilizando chaves apropriadas?	Não aplicável

Figura 24 - Ecrã da fase de avaliação de maturidade

Resultados da avaliação de maturidade (de 0 a 10) (5 = Bem definido)		
Área	**Aceitável**	**Atual**
Recolha e informação	5	3,5
Consentimento e direitos dos titulares	5	5,8
Documentação e requisitos legais	5	5,0
Controlos de segurança lógica	5	2,4
Controlos de segurança física	5	0,0
Transferências de dados internacionais	5	10,0



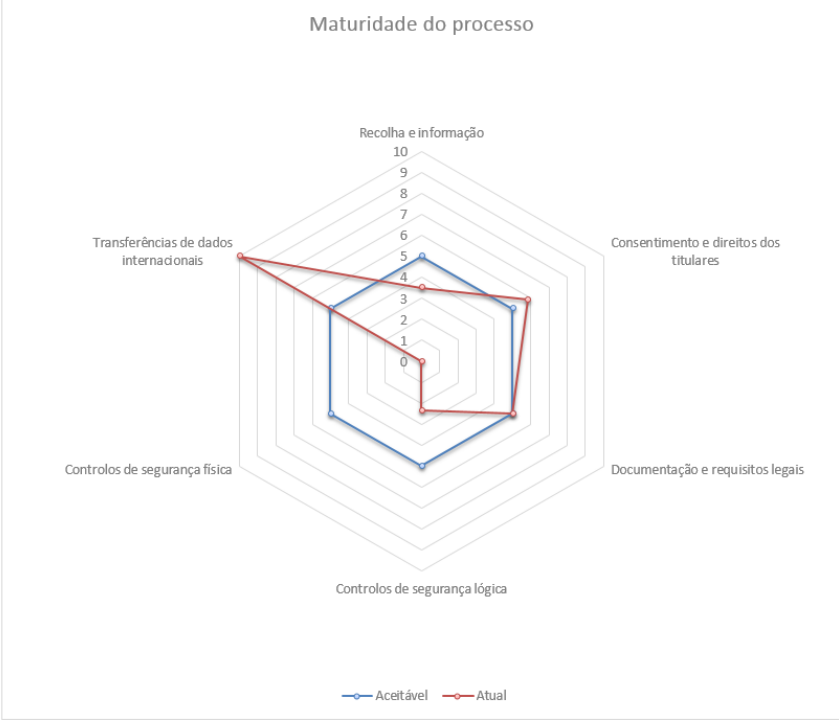


Figura 25 - Ecrã de resumo da fase de avaliação de maturidade

Ocorrência	Definição	Racional
Insignificante	Não parece possível que os riscos se materializem através da exploração das vulnerabilidades.	Roubo de documentação armazenada num espaço protegido por leitor de cartões e um pin de acesso.
Limitada	Parece difícil que os riscos se materializem através da exploração das vulnerabilidades.	Roubo de documentação armazenada num espaço protegido por leitor de cartões.
Significante	Parece possível que os riscos se materializem através da exploração das	Roubo de documentação armazenada num espaço que não pode ser acedido sem antes se fazer check-in na receção.
Máxima	É quase certo que os riscos se materializem através da exploração das vulnerabilidades.	Roubo de documentação armazenada num espaço público.

Impacto	Definição	Racional
Insignificante	Os titulares não são afetados ou poderão encontrar uns pequenos inconvenientes que conseguem superar sem problema.	Perda de tempo a repetir procedimentos, receção de SPAM, alvo de campanhas de publicidade para produtos de consumo comuns.
Limitado	Os titulares podem encontrar inconvenientes significantes que conseguem superar apesar de algumas dificuldades.	Pagamentos imprevistos (multas impostas erroneamente), custos adicionais, negação de acesso a serviços, perda de oportunidade para progressão na carreira, receção de email não solicitado propenso a denegrir a reputação dos titulares, processamento de dados incorretos levando a resultados não desejados.
Significante	Os titulares podem enfrentar consequências significantes que devem conseguir superar, embora com	Desvios de fundos não compensados, dificuldades financeiras não temporárias (obrigação a um empréstimo), danos em propriedades, perda de emprego, perda de casa, separação ou divórcio.
Máximo	Os titulares podem enfrentar consequências significantes ou até irreversíveis que podem não conseguir	Risco financeiro, dívidas substanciais, incapacidade de trabalhar, incapacidade de re-alocar, perda de acesso a estrutura vital (água, eletricidade).

Figura 26 - Ecrã de definições de classificação de risco

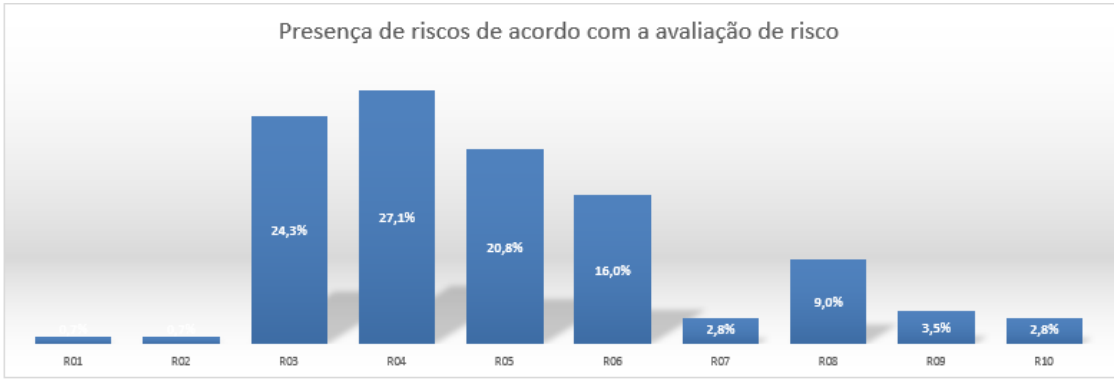
Id	Maturidade da questão	Questão	Vulnerabilidades	Riscos	Possíveis consequências	Probabilidade de	Impacto	Valor do risco
1.1	Executado informalmente	Existe um processo para garantir que antes da recolha dos dados, os titulares têm uma informação atualizada e clara do propósito dos seus dados pessoais e do processo de tratamento dos seus dados?	- Falta de informação aos titulares	- R01 - R08	- Podem ser realizados tratamentos aos dados pessoais que o titular não tenha autorizado e que não esteja de acordo	Limitada	Insignificante	Baixo
1.2	Não aplicável	Existe uma forma definida de registar, armazenar e disponibilizar quando requisitado o consentimento para o processamento dos dados?	- O consentimento não fica devidamente registado	- R08 - R10	- A organização não consegue validar que está a efetuar tratamentos apenas para titulares que autorizaram o tratamento dos seus dados - A organização não consegue demonstrar o consentimento dado caso requisitado			n/a
1.3	Não implementado	Existe um processo para garantir que são recolhidos apenas os dados necessários para os tratamentos identificados?	- Recolha de dados desnecessários	- R02	- Em caso de fuga de informação podem ser comprometidos mais dados que permitam causar dano aos titulares	Limitada	Insignificante	Baixo
1.4	Bem definido	Existe um processo para garantir que apenas são realizados os tratamentos que foram propostos aos titulares?	- Especificações incompletas dos tratamentos - Tratamentos de dados não autorizados - Acesso por entidades não autorizadas	- R03 - R05 - R08 - R09 - R10	- Podem ser realizados tratamentos que não foram identificados inicialmente e que possam resultar em riscos imprevistos para os dados pessoais - Os dados podem ser acedidos por pessoas ou entidades que não estão autorizados para lhes aceder	Limitada	Limitado	Médio
1.5	Não implementado	Existem medidas de minimização dos dados, como pseudoanonimização para garantir que os dados depois dos tratamentos não permitem a identificação dos titulares?	- Informação identificativa disponível	- R05 - R06	- Caso seja necessário manter os dados para fins estatísticos, em caso de fuga de informação podem ser comprometidos dados pessoais que já não são utilizados	Insignificante	Significante	Médio
2.1	Não aplicável	Existe um processo para garantir que os dados dos titulares deixem de ser processados caso o titular assim o requisite?	- Processamentos de dados não autorizados - Acesso por entidades não autorizadas	- R05 - R08	- Os titulares podem sofrer consequências de processamentos que não autorizaram - No contexto do processamento os dados podem ser transferidos para entidades que já não devem ter autorização para processar os dados - Impossibilidade dos titulares exercerem o direito à oposição			n/a
2.2	Executado informalmente	Existe um processo que permita mostrar aos titulares os seus dados pessoais que a organização tem na sua posse caso o mesmo os solicite?	- Falta de controlo sobre os dados pessoais	- R07	- Titulares não sabem que dados é que a organização tem na sua posse - Titulares podem não conseguir retificar os seus dados se não souberem que dados é que a organização tem	Insignificante	Insignificante	Baixo
2.3	Executado informalmente	Existe um processo para retificar os dados pessoais dos titulares caso o titular solicite a sua retificação?	- Tratamentos de dados pessoais desatualizados - Falta de controlo sobre os dados pessoais	- R07 - R10	- Processamento de dados pessoais desatualizados que podem causar impacto nos titulares - Impossibilidade dos titulares exercerem o direito à retificação	Insignificante	Limitado	Baixo
2.4	Não aplicável	Existe um processo para garantir que os dados dos titulares sejam apagados caso seja solicitado pelos próprios, ou não seja mais necessário tratar esses dados?	- Tratamentos de dados não autorizados - Acesso por entidades não autorizadas - Falta de controlo sobre os dados pessoais	- R03 - R04 - R08	- Tratamentos de dados pessoais para os quais já não estão autorizados - Os dados podem ser acedidos por pessoas ou entidades que já não estão autorizados para lhes aceder - Os titulares podem sofrer consequências de processamentos que não autorizaram			n/a
2.5	Não aplicável	Existe um processo para a exportação dos dados pessoais de um titular num formato interpretável por máquinas por forma a que os mesmos sejam enviados para processamento para outras organizações caso seja solicitado pelo titular?	- Falta de controlo sobre os dados pessoais - Retenção indevida dos dados	- R09 - R10	- Titulares podem querer que os seus dados passem a ser processados por outra entidade e dessa forma podem ser "obrigados" a continuar a usar serviços indesejados - Impossibilidade dos titulares exercerem o direito à portabilidade dos dados			n/a
2.6	Não aplicável	Existe um processo para limitar e/ou terminar determinado tratamento de dados caso seja solicitado pelo titular?	- Falta de controlo sobre os dados pessoais - Tratamentos de dados indevidos	- R08 - R09 - R10	- Tratamentos nos dados ilegais/não autorizados pelos titulares - Impossibilidade dos titulares exercerem o direito à limitação ou objeção			n/a
3.1	Não implementado	É mantido um registo com os detalhes do tratamento, os tipos de dados, os fluxos de circulação de dados pessoais e existe um processo para garantir que esses dados estão atualizados?	- Falta de controlo sobre os dados pessoais - Falta de controlo sobre os tratamentos de dados	- R05 - R08	- Podem ser tratados dados pessoais que não devem ser tratados - Tratamentos de dados pessoais para os quais não estão autorizados	Limitada	Insignificante	Baixo
3.2	Não aplicável	Existe, e está documentada uma justificação válida para o tratamento de dados pessoais sensíveis?	- Falta de controlo sobre os dados pessoais - Processamento de dados sem justificação	- R08 - R09 - R10	- Tratamentos de dados de pessoas sensíveis sem necessidade - Tratamentos de dados pessoais que não devem ser efetuados - Possíveis consequências para os titulares das quais eles não se consigam proteger			n/a
3.3	Bem definido	Existe um processo para incluir uma cláusula em contratos com processadores de dados externos, para garantir que os mesmos assumem os riscos e tomam as medidas técnicas e organizacionais apropriadas para garantir a conformidade com o regulamento?	- Processamentos realizados por entidade em não conformidade	- R04 - R05 - R06 - R08 - R09 - R10	- Os processadores podem não assumir a responsabilidade pelos dados em caso de perda ou fuga de informação - Os processadores podem não ter implementadas medidas para garantir que os dados não são perdidos ou alvo de fugas de informação	Insignificante	Limitado	Baixo
3.4	Bem definido	Caso seja obrigatório manter os dados pessoais após o processamento, devido a alguma obrigação legal, existe um processo para garantir que os dados são apagados após o prazo de retenção definido por lei?	- Conservação de dados pessoais para além do que é expectável	- R06 - R07	- Conservação de dados pessoais não autorizados - Em caso de fuga de informação podem ser comprometidos dados que não devem estar na posse da organização	Insignificante	Significante	Médio

Figura 27 - Ecrã da fase de classificação do risco, parte 1

Id	Maturidade da questão	Questão	Vulnerabilidades	Riscos	Possível consequência	Probabilidade	Impacto	Valor do risco
4.1	Bem definida	Estão implementadas contrales de autenticação antes do seu acesso a qualquer dado pessoal da processa?	- Acessar indevidamente	- R03 - R04 - R05 - R06	- Acesso a dados pessoais por utilizadores não autorizados - Fuga de informação dos dados acedidos - Destruição ou modificação indevida dos dados	Insignificante	Significante	Média
4.2	Não implementada	As aplicações têm implementada autenticação multi-factor para utilizadores privilegiados?	- Autenticação inapropriada	- R03 - R04 - R06	- Contas de utilizador privilegiadas podem ser comprometidas mais facilmente - Acesso a dados pessoais por utilizadores não autorizados - Fuga de informação dos dados acedidos - Destruição ou modificação indevida dos dados	Limitada	Significante	Média
4.3	Não implementada	Caso as aplicações contenham dados pessoais sensíveis, têm implementada autenticação multi-factor para utilizadores com acesso a esses dados?	- Autenticação inapropriada	- R03 - R04 - R06	- Contas de utilizador com acesso a dados sensíveis podem ser comprometidas mais facilmente - Acesso a dados pessoais por utilizadores não autorizados - Fuga de informação dos dados acedidos - Destruição ou modificação indevida dos dados	Limitada	Significante	Média
4.4	Bem definida	Estão implementadas mecanismos de modificação de password periódica?	- Má gestão de password	- R03 - R04 - R06	- Password eventualmente comprometidas podem nunca ser substituídas - Acesso a dados pessoais por utilizadores não autorizados - Fuga de informação dos dados acedidos - Destruição ou modificação indevida dos dados	Insignificante	Limitada	Baixa
4.5	Não implementada	Está definido e em prática uma política de revisão de acessos periódica?	- Acessar indevidamente	- R03 - R04 - R05 - R06	- Acesso aos dados pessoais por utilizadores que já não deviam ter acesso aos mesmos - Fuga de informação dos dados acedidos - Destruição ou modificação indevida dos dados	Limitada	Limitada	Média
4.6	Não implementada	Está implementado o princípio de previlégios mínimos na atribuição de acessos a novos utilizadores?	- Acessar indevidamente	- R03 - R04 - R05 - R06	- Novos utilizadores com acesso a funcionalidades que não devem ter - Fuga de informação dos dados acedidos - Destruição ou modificação indevida dos dados	Significante	Limitada	Média
4.7	Não implementada	Têm um procedimento definido e implementado para garantir que não são carregados dados pessoais em ambientes de qualidade?	- Carregamento de dados pessoais em ambientes de qualidade	- R03 - R05 - R08 - R09	- Acesso a dados pessoais por utilizadores apenas com permissão para tratar que não deviam aceder aos dados pessoais - Dados são divulgados para utilizadores que não deveriam ter acesso	Limitada	Limitada	Média
4.8	Não implementada	Tabelas de bases de dados com dados pessoais, têm algoritmos de cifra aplicados nos mesmos?	- Acessar indevidamente	- R03 - R04	- Acesso a dados pessoais não autorizados diretamente das tabelas por administradores com acesso às bases de dados - Destruição ou modificação acidental dos dados	Limitada	Significante	Média
4.9	Não implementada	Ficheiros com dados pessoais que sejam armazenados pelas aplicações têm algoritmos de cifra aplicados nos mesmos?	- Acessar indevidamente	- R03 - R04	- Acesso a dados pessoais não autorizados diretamente dos ficheiros por administradores com acesso aos sistemas - Destruição ou modificação acidental dos dados	Significante	Significante	Alta
4.10	Não implementada	São realizados testes de segurança periódicos, pelo menos anualmente?	- Falhas conhecidas nas aplicações	- R03 - R04 - R05 - R06	- Existência de vulnerabilidades conhecidas nas aplicações - Possibilidade de exploração de vulnerabilidades por agentes maliciosos	Significante	Máxima	Alta
4.11	Não implementada	Estão implementados mecanismos técnicos que permitam fazer tracking de todas as ações realizadas relacionadas com dados pessoais?	- Uma não centralização dos sistemas	- R04 - R05 - R08	- Falta de centralização das ações realizadas nos dados pessoais - Alterações de dados que não são possíveis de confirmar - Exportações de dados que não são possíveis de detetar	Significante	Máxima	Alta
4.12	Não implementada	Estão implementados mecanismos técnicos que permitam fazer tracking de todas as ações realizadas relacionadas com gestão de acessos?	- Uma não centralização dos sistemas	- R03 - R04 - R05 - R08	- Falta de centralização na atribuição de acessos a utilizadores com acesso a dados pessoais - Acesso aos dados pessoais por utilizadores que não deviam ter acesso aos mesmos	Significante	Significante	Alta
4.13	Não aplicável	Estão implementados mecanismos técnicos para garantir a integridade dos logs?	- Uma não centralização dos sistemas	- R04 - R05 - R08	- Possibilidade de se modificar os logs não permitindo centralização das ações realizadas nos dados pessoais - Alterações de dados que não são possíveis de confirmar - Exportações de dados que não são possíveis de detetar			n/a
4.14	Não implementada	Caso sejam transmitidos dados sensíveis entre aplicações, estas transferências são feitas através de canais seguros garantidos por métodos de cifra?	- Canais de comunicação inseguros	- R03 - R04 - R05	- Fuga de informação dos dados transferidos - Perda ou destruição dos dados em trânsito	Significante	Máxima	Alta
4.15	Bem definida	Caso sejam transmitidos dados pessoais para fora da organização, estas transferências são feitas através de canais seguros garantidos por métodos de cifra?	- Canais de comunicação inseguros	- R03 - R04 - R05	- Fuga de informação dos dados transferidos - Perda ou destruição dos dados em trânsito	Limitada	Significante	Média
4.16	Centralização quantitativamente	Os sistemas estão protegidos do exterior das suas redes por firewalls e estão bloqueados todos os portos que não são usados?	- Sistemas mal protegidos	- R03 - R04 - R05 - R06	- Comprometimento da rede interna - Fuga de informação	Insignificante	Significante	Média
4.17	Bem definida	Está definido e em prática uma política de backups regulares?	- Falta de backups	- R04	- Impossibilidade de recuperar dados pessoais em caso de acidente ou perda de dados	Insignificante	Significante	Média
4.18	Bem definida	Está implementado um sistema para garantir a restauração dos dados pessoais em caso de desastres, danos ou perda dos mesmos?	- Falta de um procedimento de recuperação de desastres	- R04	- Impossibilidade de recuperar dados pessoais em caso de desastres, acidentes ou perda de dados	Insignificante	Significante	Média
5.1	Não implementada	O acesso a documentos físicos está protegido contra acessos indevidos?	- Acessar indevidamente	- R03 - R04 - R06	- Acesso a dados pessoais não autorizados diretamente dos ficheiros - Destruição dos dados - Roubo dos dados	Limitada	Significante	Média
6.1	Não aplicável	Existe um processo para garantir que os dados pessoais apenas são transferidos para entidades que cumpram com a regulamento?	- Processamentos realizados por entidades em não conformidade	- R04 - R05 - R06 - R08 - R09 - R10	- Os processadores podem não ter implementadas medidas para garantir que os dados não são perdidos ou alvo de fugas de informação			n/a
6.2	Não aplicável	Estão implementadas medidas técnicas para garantir que os dados pessoais em trânsito para fora da organização não são comprometidos, como criptografia utilizando chaves apropriadas?	- Canais de comunicação inseguros	- R03 - R04 - R05 - R06	- Fuga de informação dos dados transferidos - Perda ou destruição dos dados em trânsito			n/a

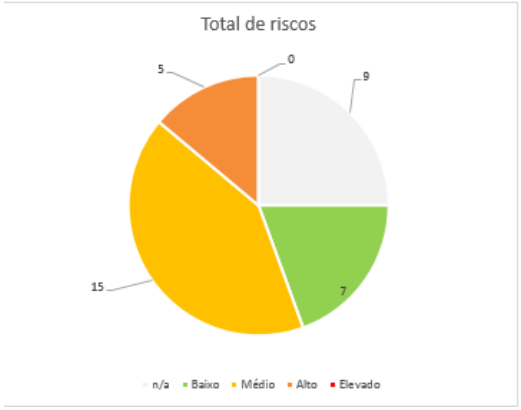
Figura 28 - Ecrã da fase de classificação do risco, parte 2

Presença de riscos de acordo com avaliação de maturidade		
Risco	**ID**	**Presença**
Recolha de dados não justificada	R01	0,7%
Recolha de dados excessiva	R02	0,7%
Acesso não autorizado aos dados	R03	24,3%
Destruição ou alteração acidental/ilegal de dados	R04	27,1%
Divulgação não autorizada de dados	R05	20,8%
Roubo de dados	R06	16,0%
Uso/Armazenamento de dados desatualizados	R07	2,8%
Utilização dos dados para além do que é expectável	R08	9,0%
Utilização dos dados para além do que é socialmente aceitável	R09	3,5%
Inferências ou tomadas de decisões injustificáveis que a organização não pode tomar	R10	2,8%



Média dos riscos por área	
Área	**Nível de risco**
Recolha e informação	Médio
Consentimento e direitos dos dados	Baixo
Documentação e requisitos legais	Médio
Controlos de segurança lógicos	Alto
Controlos de segurança físicos	Médio
Transferências de dados	...
Processo	**Médio**

Top 7 vulnerabilidades			
Questã	**Vulnerabilidade**	**Controlo de mitigação**	**Nível de risco**
4.10	Falhas conhecidas nas aplicações	Definição e execução de um plano de testes de segurança periódico	Alto
4.11	Uso não controlado dos sistemas	Implementação de um mecanismo de registo de ações	Alto
4.14	Canais de comunicação inseguros	Implementação de mecanismos de cifra para transferências entre aplicações	Alto
4.9	Acessos indevidos	Implementação de mecanismos de cifra em ficheiros com dados pessoais	Alto
4.12	Uso não controlado dos sistemas	Implementação de um mecanismo de registo de ações	Alto
4.2	Autenticação inapropriada	Implementação de login com 2 fatores de autenticação	Médio
4.3	Autenticação inapropriada	Implementação de login com 2 fatores de autenticação	Médio



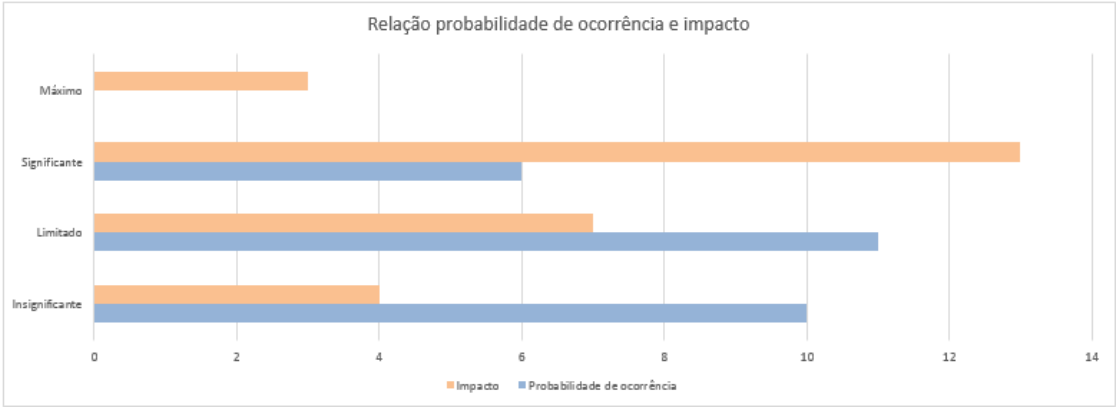


Figura 29 - Ecrã de resumo da fase de classificação do risco

Id	Maturidade da questão	Risco da questão	Questão	Possíveis consequências	Estratégia de mitigação do	Medidas recomendadas	Tecnologias	Comentários	Esforço
1.1	Executado informalmente	Básico	Existe um processo para garantir que antes da recolha dos dados, os titulares têm uma informação atualizada e clara do propósito dos seus dados pessoais e do processo de tratamento dos seus dados?	- Podem ser realizados tratamentos aos dados pessoais que o titular não tenha autorizado e que não esteja de acordo	Proteger	Criar um documento onde estejam descritos os motivos e finalidades da recolha dos dados pessoais, ou seja o propósito do processo identificado na aba "Processo", e os tratamentos a que os dados vão ser sujeitos. Este documento deve ser claro e de fácil leitura, e sempre disponibilizado aos titulares previamente à recolha de dados. Esta documentação deve ser revista sempre que se efetuarem.	Ferramenta de processamento de texto, ex: Word.		1 semana
1.2	Não aplicável	n/a	Existe uma forma definida de registar, armazenar e disponibilizar quando requisitado o consentimento para o processamento dos dados?	- A organização não consegue validar que está a efetuar tratamentos apenas para titulares que autorizaram o tratamento dos seus dados - A organização não consegue demonstrar o consentimento dado caso requisitado		Definir um procedimento de gestão de consentimentos onde esteja definido que deve ficar registado, previamente à recolha dos dados do titular, algo que torne possível a verificação do consentimento do utilizador, seja o registo de uma ação efetuada numa página web, um documento assinado digitalmente ou presencialmente, ou um email recebido pelo titular, e ter um sistema que permita à organização pesquisar pelo consentimento quando necessário, seja uma base de dados, um sistema de ficheiros ou um arquivo onde estejam implementadas medidas para garantir a integridade do consentimento.	Sistema onde seja possível armazenar documentos digitais e pesquisar pelos mesmos: - Base de dados; - Sistema de gestão de ficheiros.		2 a 3 semanas
1.3	Não implementado	Básico	Existe um processo para garantir que são recolhidos apenas os dados necessários para os tratamentos identificados?	- Em caso de fuga de informação podem ser comprometidos mais dados que permitam causar dano aos titulares	Proteger	Identificar e documentar que dados são necessários para cada tratamento que é efetuado no processo, identificados na aba "Processo" e o motivo do seu tratamento por forma a serem recolhidos apenas os dados necessários. Esta documentação deve ser revista sempre que se efetuarem alterações no processo de tratamento de dados.	Ferramenta de processamento de texto, ex: Word.		1 semana
1.4	Bem definido	Médio	Existe um processo para garantir que apenas são realizados os tratamentos que foram propostos aos titulares?	- Podem ser realizados tratamentos que não foram identificados inicialmente e que possam resultar em riscos imprevistos para os dados pessoais - Os dados podem ser acedidos por pessoas ou entidades que não estão autorizados para lhes aceder	Proteger	Ter documentados os tratamentos efetuados no processo no documento que é disponibilizado aos titulares previamente à recolha de dados pessoais, quer sejam tratamentos realizados através das aplicações identificadas na aba "Processo", quer sejam tratamentos manuais. Esta documentação deve ser revista sempre que se efetuarem alterações no processo de tratamento de dados. Em caso de serem acrescentados novos tipos de tratamentos o titular deve ser notificado e deve ser recolhido o seu consentimento para os	Ferramenta de processamento de texto, ex: Word.		1 semana
1.5	Não implementado	Médio	Existem medidas de minimização dos dados, como pseudonomização para garantir que os dados depois dos tratamentos não permitem a identificação dos titulares?	- Caso seja necessário manter os dados para fins estatísticos, em caso de fuga de informação podem ser comprometidos dados pessoais que já não são utilizados	Proteger	Devem estar documentados os sistemas onde estão armazenados dados dos titulares (sistemas produtivos, sistemas de backups, entre outros) por forma a poder executar-se uma ferramenta para remover os dados que permitam identificar os titulares nos sistemas identificados.	- Ferramenta de processamento de texto, ex: Word; - Ferramenta para minimização de dados.		1 mês
2.1	Não aplicável	n/a	Existe um processo para garantir que os dados dos titulares deixem de ser processados caso o titular assim o requisite?	- Os titulares podem sofrer consequências de processamentos que não autorizaram - No contexto do processamento os dados podem ser transferidos para entidades que já não devem ter autorização para processar os dados - Impossibilidade dos titulares exercerem o direito à oposição		Deve estar implementado um mecanismo nos sistemas de armazenamento dos dados pessoais que permita verificar os dados dos titulares podem ser processados ou não, como um campo numa tabela de base de dados ou num ficheiro que indique se os dados pessoais de cada titular devem ser processados ou não, e antes de cada processamento deve-se verificar o valor desse campo.	Funcionalidade para verificar se os dados de cada titular podem ser processados ou não, de forma a que seja possível de se verificar previamente à realização de um tratamento. Exemplos de sistemas onde seja possível definir se os dados de um titular podem ser processados ou não: - Base de dados; - Sistema de gestão de ficheiros.		1 a 2 meses
2.2	Executado informalmente	Básico	Existe um processo que permita mostrar aos titulares os seus dados pessoais que a organização tem na sua posse caso o mesmo os solicite?	- Titulares não sabem que dados é que a organização tem na sua posse - Titulares podem não conseguir retificar os seus dados se não souberem que dados é que a organização tem - Impossibilidade dos titulares exercerem o direito de acesso	Aceitar	Devem estar documentados os sistemas onde estão armazenados os dados dos titulares e ter ferramentas que permitam extrair os dados desses sistemas a pedido dos titulares. Idealmente deforma a manter a confidencialidade dos dados pessoais.	Ferramenta que permita extrair os dados pessoais dos titulares, ex: - Página web autenticada para acesso do titular aos seus dados; - Ferramenta de reporting que permita apenas a um conjunto de utilizadores autorizados extrair os dados de determinado titular a pedido do mesmo.		2 a 3 semanas
2.3	Executado informalmente	Básico	Existe um processo para retificar os dados pessoais dos titulares caso o titular solicite a sua retificação?	- Processamento de dados pessoais desatualizados que podem causar impacto nos titulares - Impossibilidade dos titulares exercerem o direito à retificação	Proteger	Devem estar documentados os sistemas onde estão armazenados os dados dos titulares (sistemas produtivos, sistemas de backups, entre outros) e ter ferramentas que permitam modificar os dados desses sistemas a pedido do titular. Idealmente deforma a manter a confidencialidade dos dados pessoais.	Ferramenta que permita modificar os dados pessoais do titular, ex: - Página web autenticada para acesso do titular aos seus dados e opção para modificar os mesmos; - Ferramenta que permita apenas a um conjunto de utilizadores autorizados modificar os dados de determinado titular a pedido do mesmo.		1 mês
2.4	Não aplicável	n/a	Existe um processo para garantir que os dados dos titulares sejam apagados caso seja solicitado pelos próprios, ou não seja mais necessário tratar esses dados?	- Tratamentos de dados pessoais para os quais já não estão autorizados - Os dados podem ser acedidos por pessoas ou entidades que já não estão autorizados para lhes aceder - Os titulares podem sofrer consequências de processamentos que não autorizaram - Impossibilidade dos titulares exercerem o direito ao esquecimento		Devem estar documentados os sistemas onde estão armazenados os dados dos titulares (sistemas produtivos, sistemas de backups, entre outros) e ter ferramentas que permitam apagar os dados desses sistemas a pedido do titular.	Ferramenta que permita apagar os dados pessoais do titular e que seja refletido em todos os sistemas incluindo backups, ex: - Página web autenticada para acesso do titular aos seus dados e opção para apagar os mesmos; - Ferramenta que permita apenas a um conjunto de utilizadores autorizados apagar os dados de determinado titular a pedido do mesmo.		2 a 3 meses

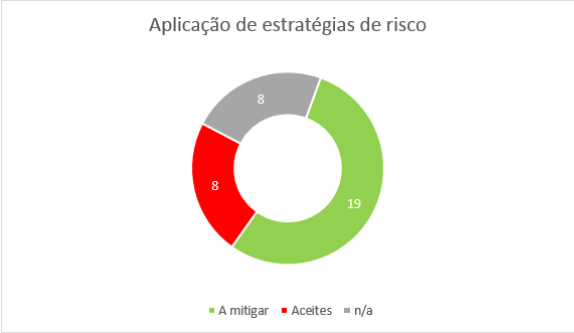
Figura 30 - Ecrã da fase de mitigação dos riscos, parte 1

Id	Maturidade da questão	Risco da questão	Questão	Possíveis consequências	Estratégia de mitigação do	Medidas recomendadas	Tecnologias	Comentários	Esforço
2.5	Não aplicável	n/a	Existe um processo para a exportação dos dados pessoais de um titular num formato interpretável por máquinas por forma a que os mesmos sejam enviados para processamento para outras organizações caso seja solicitado pelo titular?	- Titulares podem querer que os seus dados passem a ser processados por outra entidade e desse forma podem ser "obrigados" a continuar a usar serviços indesejados - Impossibilidade dos titulares exercerem o direito à portabilidade dos dados		Devem estar documentados os sistemas onde estão armazenados os dados dos titulares e ter ferramentas que permitam extrair os dados desses sistemas a pedido do titular, e num forma possível de ser interpretável por máquinas. Idealmente deforma a manter a confidencialidade dos dados pessoais.	Ferramenta que permita extrair os dados pessoais do titular, ex: - Página web autenticada para acesso do titular aos seus dados; - Ferramenta de reporting que permita apenas a um conjunto de utilizadores autorizados extrair os dados de determinado titular a pedido do mesmo. Os dados devem estar num formato possível de ser importado por outros softwares, ex: XML, JSON, CSV.		2 meses
2.6	Não aplicável	n/a	Existe um processo para limitar e/ou terminar determinado tratamento de dados caso seja solicitado pelo titular?	- Tratamentos nos dados ilegalmão autorizados pelos titulares - Impossibilidade dos titulares exercerem o direito à limitação ou objeção		Devem estar documentados os tratamentos que são realizados para cada titular e ter um mecanismo para ativar/desativar tratamentos para cada titular.	Ferramenta que permita limitar os tratamentos efetuados ao titular, ex: - Página web autenticada para o titular consultar os tratamentos a que está sujeito e poder mudar a sua decisão; - Ferramenta que permita apenas a um conjunto de utilizadores autorizados limitar os tratamentos de determinado titular a pedido do mesmo.		
3.1	Não implementado	Básico	É mantido um registo com os detalhes do tratamento, os tipos de dados, os fluxos de circulação de dados pessoais e existe um processo para garantir que esses dados estão atualizados?	- Podem ser tratados dados pessoais que não devam ser tratados - Tratamentos de dados pessoais para os quais não estão autorizados	Aceitar	Criar um documento onde estejam descritos os tratamentos efetuados, a justificação de cada tratamento, os tipos de dados pessoais tratados, qual o flow de circulação dos dados, quais as aplicações por onde os dados circulam e as entidades com acesso aos mesmos. Esta documentação deve ser revista sempre que se efetuarem alterações no processo de tratamento de dados.	Ferramenta de processamento de texto, ex: Word.		1 semana
3.2	Não aplicável	n/a	Existe, e está documentada uma justificação válida para o tratamento de dados pessoais sensíveis?	- Tratamentos de dados de pessoas sensíveis sem necessidade - Tratamentos de dados pessoais que não devam ser efetuados - Possíveis consequências para os titulares dos quais eles não se consigam proteger		Dados pessoais sensíveis apenas devem ser tratados se existir uma justificação válida para a realização desses tratamentos. Por justificação válida entenda-se que os dados são essenciais para atingir o objetivo do processamento identificado no processo. Caso exista essa justificação a mesma deve estar documentada, senão esses dados devem deixar de ser recolhidos e tratados.	Ferramenta de processamento de texto, ex: Word.		1 semana
3.3	Bem definido	Básico	Existe um processo para incluir uma cláusula em contratos com processadores de dados externos, para garantir que os mesmos assumem os riscos e tomam as medidas técnicas e organizacionais apropriadas para garantir a conformidade com o regulamento?	- Os processadores podem não assumir a responsabilidade pelos dados em caso de perda ou fuga de informação - Os processadores podem não ter implementadas medidas para garantir que os dados não são perdidos ou alvo de fuga de informação	Aceitar	Deve-se validar para cada entidade externa interveniente no processo se existe um contrato com a mesma e se nesse contrato existem cláusulas onde esteja contemplada a conformidade com o GDPR e a responsabilização. Caso não exista deve-se negociar uma alteração ao contrato. Em novos contratos essas cláusulas devem estar sempre presentes.	Sistema que permita armazenar e gerir os contratos, ex: sistema de gestão de ficheiros.		2 a 3 meses
3.4	Bem definido	Médio	Caso seja obrigatório manter os dados pessoais após o processamento, devido a alguma obrigação legal, existe um processo para garantir que os dados são apagados após o prazo de retenção definido por lei?	- Conservação de dados pessoais não autorizados - Em caso de fuga de informação podem ser comprometidos dados que não deviam estar na posse da organização	Proteger	Quando os dados de um titular deixam de ser processados deve ser atribuída a data do último processamento a esses dados e deve estar incorporado nos sistemas de gestão desses dados pessoais um mecanismo que periodicamente valida o período de armazenamento atual dos dados com o que é imposto por lei e apagar os mesmos ou deve existir um sistema independente com a capacidade de fazer essa validação e apagar os dados caso aplicável.	- Funcionalidade para verificar o período de armazenamento atual dos dados e apagar os mesmos, incorporada na tecnologia de gestão/armazenamento dos dados; - Scheduler que corre um serviço de verificação do período dos dados que		2 a 3 meses
4.1	Bem definido	Médio	Estão implementados controlos de autenticação antes de se aceder a qualquer dado pessoal do processo?	- Acesso a dados pessoais por utilizadores não autorizados - Fuga de informação dos dados acedidos - Destruição e/ou modificação indevida dos dados	Proteger	Qualquer acesso a dados pessoais deve ser restringindo por mecanismos de autenticação que permitam apenas o acesso por pessoas autorizadas e posteriormente se poder identificar quem realizou que ações sobre os dados pessoais.	- Interface de login; - Mecanismo de proteção de acessos não autenticados aos dados.		2 a 4 semanas
4.2	Não implementado	Médio	As aplicações têm implementada autenticação multi-factor para utilizadores privilegiados?	- Contas de utilizador privilegiadas podem ser comprometidas maisfacilmente - Acesso a dados pessoais por utilizadores não autorizados - Fuga de informação dos dados acedidos - Destruição e/ou modificação indevida dos dados	Proteger	Deve existir um meio adicional de autenticação para além de uma password para acessos privilegiados a funcionalidades mais críticas para reduzir ao risco no caso de comprometimento de passwords.	Utilização de tokens ou de mensagens com códigos gerados no momento de autenticação.		2 a 4 semanas
4.3	Não implementado	Médio	Caso as aplicações contenham dados pessoais sensíveis, têm implementada autenticação multi-factor para utilizadores com acesso a esses dados?	- Contas de utilizador com acesso a dados sensíveis podem ser comprometidas maisfacilmente - Acesso a dados pessoais por utilizadores não autorizados - Fuga de informação dos dados acedidos - Destruição e/ou modificação indevida dos dados	Aceitar	Deve existir um meio adicional de autenticação para além de uma password para acessos a dados sensíveis para reduzir ao risco no caso de comprometimento de passwords.	Utilização de tokens ou de mensagens com códigos gerados no momento de autenticação.		2 a 4 semanas
4.4	Bem definido	Básico	Estão implementados mecanismos de modificação de password periódica?	- Passwords eventualmente comprometidas podem nunca ser substituídas - Acesso a dados pessoais por utilizadores não autorizados - Fuga de informação dos dados acedidos - Destruição e/ou modificação indevida dos dados	Aceitar	Deve existir uma política onde esteja especificado o tempo de vida de uma password, e devem estar implementados mecanismos técnicos para forçar essa alteração.	Scheduler que corre um serviço de verificação do período de vida das passwords e que obriga os utilizadores a modificarem a mesma caso aplicável.		1 semana
4.5	Não implementado	Médio	Está definido e em prática uma política de revisão de acessos periódica?	- Acesso aos dados pessoais por utilizadores que já não devian ter acesso aos mesmos - Fuga de informação dos dados acedidos - Destruição e/ou modificação indevida dos dados	Aceitar	Deve existir uma política onde esteja especificado quando é efetuada uma recertificação de acessos, e essa política deve ser cumprida, podendo recorrer-se a notificações para os administradores de sistemas.	Scheduler para notificar os administradores quando devem realizar a recertificação de acessos.		1 semana

Figura 31 - Ecrã da fase de mitigação dos riscos, parte 2

Id	Maturidade da questão	Risco da questão	Questão	Possíveis consequências	Estratégia de mitigação do	Medidas recomendadas	Tecnologias	Comentários	Esforço
4.6	Não implementado	Médio	Está implementado o princípio de previlégios mínimos na atribuição de acessos a novos utilizadores?	- Novos utilizadores com acesso a funcionalidades que não devem ter - Fuga de informação dos dados acedidos - Destruição e/ou modificação indevida dos dados	Proteger	Quando é inserido um novo utilizador no sistema, o mesmo não deve ter acessos concedidos por defeito, e devem ser dados à medida que for surgindo a necessidade.	Configuração dos acessos atribuídos por defeito a novos utilizadores		1 semana
4.7	Não implementado	Médio	Têm um procedimento definido e implementado para garantir que não são carregados dados pessoais em ambientes de qualidade?	- Acesso a dados pessoais por utilizadores apenas com permissão para testes que não deviam aceder aos dados pessoais - Dados são divulgados para utilizadores que não deveriam ter acesso	Proteger	Não devem ser utilizados dados produtivos em ambientes de qualidade ou testes, mas em caso de haver necessidade de utilizar dados produtivos nesses ambientes devem estar implementadas medidas técnicas para mascarar/remover dados pessoais quando os dados forem transitados de um ambiente para outro.	Tecnologia para mascarar dados pessoais ou apagar ao mesmo em passagens de dados entre ambientes.		2 a 3 semanas
4.8	Não implementado	Médio	Tabelas de base de dados com dados pessoais, têm algoritmos de cifra aplicados nos mesmos?	- Acesso a dados pessoais não autorizados diretamente das tabelas por administradores com acesso às bases de dados - Destruição e/ou modificação acidental dos dados	Aceitar	Bases de dados que contenham dados pessoais devem ser cifradas para impedir a leitura dos dados por utilizadores do sistema que não devem aceder a esses dados e para dificultar a divulgação dos dados em caso de fuga de informação.	Mecanismos de cifra nas bases de dados, podendo aplicar-se apenas nos valores, em tabelas inteiras ou na base de dados em si dependendo da criticidade dos dados e da base de dados. Ex: TDE em bases de dados de MSSQL superiores a 2008		1 a 2 meses
4.9	Não implementado	Alto	Ficheiros com dados pessoais que sejam armazenados pelas aplicações têm algoritmos de cifra aplicados nos mesmos?	- Acesso a dados pessoais não autorizados diretamente dos ficheiros por administradores com acesso aos sistemas - Destruição e/ou modificação acidental dos dados	Proteger	Ficheiros que contenham dados pessoais devem ser cifrados para impedir a leitura dos dados por utilizadores do sistema que não devem aceder a esses dados e para dificultar a divulgação dos dados em caso de fuga de informação.	Aplicação de algoritmos de cifra em ficheiros que contenham dados pessoais.		1 a 2 meses
4.10	Não implementado	Alto	São realizados testes de segurança periódicos, pelo menos anualmente?	- Existência de vulnerabilidades conhecidas nas aplicações - Possibilidade de exploração de vulnerabilidades por agentes maliciosos	Proteger	Definição e execução de um plano de testes de segurança periódicos, de preferência por uma entidade externa ou por testers que não tenham estado envolvidos no desenvolvimento do sistema, para garantir que não existem vulnerabilidades conhecidas nas aplicações.	N/A		N/A
4.11	Não implementado	Alto	Estão implementados mecanismos técnicos que permitam fazer tracking de todas as ações realizadas relacionadas com dados pessoais?	- Falta de controlo sobre as ações realizadas nos dados pessoais - Alterações de dados que não são possíveis de confirmar -Exportações de dados que não são possíveis de detetar	Proteger	Implementação de um mecanismo de registo de ações, que guarde esses registos num sistema distinto do sistema a ser auditado por forma a garantir a integridade dos mesmos em caso de comprometimento do sistema.	Sistema de logs centralizado.		2 meses
4.12	Não implementado	Alto	Estão implementados mecanismos técnicos que permitam fazer tracking de todas as ações realizadas relacionadas com gestão de acessos?	- Falta de controlo na atribuição de acessos a utilizadores com acesso a dados pessoais - Acesso aos dados pessoais por utilizadores que não deviam ter acesso aos mesmos	Aceitar	Implementação de um mecanismo de registo de ações, que guarde esses registos num sistema distinto do sistema a ser auditado por forma a garantir a integridade dos mesmos em caso de comprometimento do sistema.	Sistema de logs centralizado.		2 meses
4.13	Não aplicável	n/a	Estão implementados mecanismos técnicos para garantir a integridade dos logs?	- Possibilidade de se modificar os logs não permitindo controlar as ações realizadas nos dados pessoais - Alterações de dados que não são possíveis de confirmar - Exportações de dados que não são possíveis de detetar		Os logs devem ter implementados mecanismos para garantir a integridade dos mesmos, como armazenamento dos logs num sistema distinto e aplicação de hashs ou MACs.	- Sistema de logs centralizado; - Mecanismo para assinar os logs.		1 a 2 meses
4.14	Não implementado	Alto	Caso sejam transmitidos dados sensíveis entre aplicações, estas transferências são feitas através de canais seguros garantido por	- Fuga de informação dos dados transferidos - Perda ou destruição dos dados em trânsito	Proteger	Devem estar implementados mecanismos de cifra para transferências entre aplicações quando são transmitidos dados sensíveis para reduzir o risco de comprometimento dos mesmos.	Canais de comunicação seguros.		1 a 2 meses
4.15	Bem definido	Médio	Caso sejam transmitidos dados pessoais para fora da organização, estas transferências são feitas através de canais seguros garantido por métodos de cifra?	- Fuga de informação dos dados transferidos - Perda ou destruição dos dados em trânsito	Proteger	Devem estar implementados mecanismos de cifra em transferências de dados pessoais para fora da organização para evitar o risco de comprometimento dos mesmos.	- Canais de comunicação seguros; - Cifra de ficheiros; - Cifra de emails.		1 a 2 meses
4.16	Controlado quantitativamente	Médio	Os sistemas estão protegidos do exterior das suas redes por firewalls e estão bloqueados todos os portos que não são usados?	- Comprometimento da rede interna - Fuga de informação	Proteger	Para evitar o comprometimento da rede interna, a mesma deve estar separada da rede externa por pelo menos uma firewall, e essa firewall deve ter bloqueados todos os portos que não são usados.	Firewall.		1 mês
4.17	Bem definido	Médio	Está definido e em prática uma política de backups regular?	- Impossibilidade de recuperar dados pessoais em caso de acidente ou perda de dados	Proteger	Deve estar em prática uma medida para garantir que são realizados backups aos dados ou sistemas de acordo com a sua criticidade.	Sistema de backups.		1 mês
4.18	Bem definido	Médio	Está implementado um sistema para garantir a restauração dos dados pessoais em caso de desastre, dano ou perda dos mesmos?	- Impossibilidade de recuperar dados pessoais em caso de desastre, acidente ou perda de dados	Proteger	Devem ser mantidos backups dos sistemas numa localização física distinta da localização dos sistemas para o caso de acontecimento de desastre que danifique os sistemas de backups local	Sistema de backups.		2 a 3 meses
5.1	Não implementado	Médio	O acesso a documentos físicos está protegido contra acessos indevidos?	- Acesso a dados pessoais não autorizados diretamente dos ficheiros - Destruição dos dados - Roubo dos dados	Proteger	Implementação de um mecanismo de proteção físico, adequado aos dados a proteger: - Cadeado - Leitor de cartões - Leitor de código pin	N/a		1 a 3 semanas
6.1	Não aplicável	n/a	Existe um processo para garantir que os dados pessoais apenas são transferidos para entidades que cumprem com o regulamento?	- Os processadores podem não ter implementadas medidas para garantir que os dados não são perdidos ou alvo de fugas de informação		Previamente a ce transferir os dados para uma entidade, deve-se garantir que essa entidade cumpre com os requisitos do GDPR. Esta validação deve ser feita periodicamente.	N/a		N/a
6.2	Não aplicável	n/a	Estão implementadas medidas técnicas para garantir que os dados pessoais em trânsito para fora da organização não são comprometidos, como criptografia utilizando chaves	- Fuga de informação dos dados transferidos - Perda ou destruição dos dados em trânsito		Devem ser usados meios seguros ou estar implementados canais seguros para transporte dos dados com algoritmos de criptografia apropriados para transmitir os dados para sistemas que tenham mecanismos de acesso controlado por password.	- Email com ficheiros cifrados; - Canal com SFTP ou FTPS implementados; - Aplicação web com HTTPS		2 a 3 meses

Figura 32 - Ecrã da fase de mitigação dos riscos, parte 3



Estado de conformidade dos artigos relacionados com o processo			
Artigo	**Questões de maturidade**	**Conformidade**	**Vai ficar em conformidade?**
5 - Princípios relativos ao tratamento de dados pessoais	1.1, 1.3, 1.4, 1.5	38%	Sim
6 - Licitude do tratamento	1.2	Não aplicável	Não aplicável
7 - Condições aplicáveis ao consentimento	1.2, 2.1	Não aplicável	Não aplicável
9 - Tratamento de categorias especiais de dados pessoais	3.2	Não aplicável	Não aplicável
13 - Informações a facultar quando os dados pessoais são recolhidos junto do titular	1.1	50%	Sim
14 - Informações a facultar quando os dados pessoais não são recolhidos junto do titular	1.1	50%	Sim
15 - Direito de acesso do titular dos dados	2.2	50%	Não
16 - Direito de retificação	2.3	50%	Sim
17 - Direito ao apagamento dos dados («direito a ser esquecido»)	2.4, 3.4	Em conformidade	Não aplicável
18 - Direito à limitação do tratamento	2.6	Não aplicável	Não aplicável
19 - Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento	2.3, 2.4	50%	Sim
20 - Direito de portabilidade dos dados	2.5	Não aplicável	Não aplicável
21 - Direito de oposição	2.6	Não aplicável	Não aplicável
25 - Proteção de dados desde a conceção e por defeito	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 4.15, 4.16, 4.17, 4.18,	33%	Não
28 - Subcontratante	3.3	Em conformidade	Não aplicável
30 - Registos das atividades de tratamento	3.1	0%	Não
32 - Segurança do tratamento	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 4.15, 4.16, 4.17, 4.18,	33%	Não
44 - Princípio geral das transferências	6.1, 6.2	Não aplicável	Não aplicável
45 - Transferências com base numa decisão de adequação	6.1, 6.2	Não aplicável	Não aplicável
46 - Transferências sujeitas a garantias adequadas	6.1, 6.2	Não aplicável	Não aplicável

Figura 33 - Ecrã de resumo da fase de mitigação dos riscos

Id	Vulnerabilidades	Controlos de mitigação	Valor risc	Risco
1.1	Falta de informação aos titulares	Documento onde estejam descritos os motivos e finalidades da recolha dos dados pessoais	2	Baixo
1.2	O consentimento não fica devidamente registado	Definir procedimento para a gestão de consentimentos	0	n/a
1.3	Recolha de dados desnecessários	Identificação dos dados pessoais a recolher	2	Baixo
1.4	Especificações incompletas dos tratamentos	Documentar devidamente os tratamentos efetuados	4	Médio
1.4	Tratamentos de dados não autorizados	Efetuar apenas os tratamentos para os quais o titular deu consentimento	4	Médio
1.4	Acesso por entidades não autorizadas	Restringir o acesso dos dados apenas para as finalidades identificadas e consentidas	4	Médio
1.5	Informação identificativa disponível	Mascaramento ou pseudonimização dos dados pessoais	3	Médio
2.1	Processamentos de dados não autorizados	Implementar sistema de remoção de consentimento por parte dos titulares	0	n/a
2.1	Acesso por entidades não autorizadas	Implementar sistema de remoção de consentimento por parte dos titulares	0	n/a
2.2	Falta de controlo sobre os dados pessoais	Definir um procedimento para disponibilizar os dados dos titulares quando requisitado	1	Baixo
2.3	Tratamentos de dados pessoais desatualizados	Definir um procedimento para atualizar os dados dos titulares quando requisitado	2	Baixo
2.3	Falta de controlo sobre os dados pessoais	Definir um procedimento para atualizar os dados dos titulares quando requisitado	2	Baixo
2.4	Tratamentos de dados não autorizados	Definir um procedimento para apagar os dados dos titulares quando não são mais necessários	0	n/a
2.4	Acesso por entidades não autorizadas	Definir um procedimento para apagar os dados dos titulares quando não são mais necessários	0	n/a
2.4	Falta de controlo sobre os dados pessoais	Definir um procedimento para apagar os dados dos titulares quando não são mais necessários	0	n/a
2.5	Falta de controlo sobre os dados pessoais	Definir um procedimento para exportar os dados dos titulares quando requisitado	0	n/a
2.5	Retenção indevida dos dados	Definir um procedimento para exportar os dados dos titulares quando requisitado	0	n/a
2.6	Falta de controlo sobre os dados pessoais	Definir um procedimento para limitar/terminar tratamentos específicos aos dados pessoais	0	n/a
2.6	Tratamentos de dados indevidos	Definir um procedimento para limitar/terminar tratamentos específicos aos dados pessoais	0	n/a
3.1	Falta de controlo sobre os dados pessoais	Desenvolver um dicionário com as localizações dos dados pessoais	2	Baixo
3.1	Falta de controlo sobre os tratamentos de dados	Desenvolver um dicionário com as finalidades dos dados pessoais	2	Baixo
3.2	Falta de controlo sobre os dados pessoais	Recolher dados pessoais sensíveis apenas quando necessário e com uma justificação	0	n/a
3.2	Processamento de dados sem justificação	Recolher dados pessoais sensíveis apenas quando necessário e com uma justificação	0	n/a
3.3	Processamentos realizados por entidade em não conformidade	Validação de contratos com entidade externa e de cláusulas referentes ao RGPD	2	Baixo
3.4	Conservação de dados pessoais para além do que é expectável	Implementação de mecanismo para validar e apagar registos após período de retenção	3	Médio
4.1	Acessos indevidos	Implementação de mecanismo de login	3	Médio
4.2	Autenticação inapropriada	Implementação de login com 2 fatores de autenticação	6	Médio
4.3	Autenticação inapropriada	Implementação de login com 2 fatores de autenticação	6	Médio
4.4	Má gestão de passwords	Implementação de mecanismos para força a troca periódica de password	2	Baixo
4.5	Acessos indevidos	Definição de política de recertificação de acessos	4	Médio
4.6	Acessos indevidos	Definição de política de atribuição de acessos mínimos	6	Médio
4.7	Carregamento de dados pessoais em ambientes de qualidade	Implementação de mecanismo para mascarar dados em passagens de produção para testes	4	Médio
4.8	Acessos indevidos	Implementação de mecanismos de cifra nas bases de dados	6	Médio
4.9	Acessos indevidos	Implementação de mecanismos de cifra em ficheiros com dados pessoais	9	Alto
4.10	Falhas conhecidas nas aplicações	Definição e execução de um plano de testes de segurança periódico	12	Alto
4.11	Uso não controlado dos sistemas	Implementação de um mecanismo de registo de ações	12	Alto
4.12	Uso não controlado dos sistemas	Implementação de um mecanismo de registo de ações	9	Alto
4.13	Uso não controlado dos sistemas	Implementação de um mecanismo de verificação de integridade no registo de ações	0	n/a
4.14	Canais de comunicação inseguros	Implementação de mecanismos de cifra para transferências entre aplicações	12	Alto
4.15	Canais de comunicação inseguros	Implementação de mecanismos de cifra para transferências para fora da organização	6	Médio
4.16	Sistemas mal protegidos	Implementação de firewalls entre a rede interna e a rede externa	3	Médio
4.17	Falta de backups	Implementação de um sistema de backups	3	Médio
4.18	Falta de um procedimento de recuperação de desastres	Definição de um procedimento de recuperação de desastres	3	Médio
5.1	Acessos indevidos	Implementação de um mecanismo de proteção física	6	Médio
6.1	Processamentos realizados por entidade em não conformidade	Validação de contratos com entidade externa e de cláusulas referentes ao RGPD	0	n/a
6.2	Canais de comunicação inseguros	Implementação de mecanismos de cifra para transferências para fora da organização	0	n/a

Figura 34 - Ecrã de listagem de vulnerabilidades

Níveis de maturidade	Valor	Sim/não	Ativos	Criticidade	Valor	Tratamentos	Dados pessoais	Criticidade	Aplicações	Criticidade	Ocorrênci	Valor	Impacto	Valor	Mitigação risco
Não implementado	0	Sim	Dado pessoal	Baixa	1	Processamento automatizado de da	Dados identificati	Média	Aplicação qu	Alta	Insignifica	1	Insignifica	1	Proteger
Executado informalmer	1	Não	Dado pessoal sens	Média	2	Processamento automatizado de da	Dados demográfi	Média	Aplicação ex	Alta	Limitada	2	Limitado	2	Aceitar
Bem definido	2		Aplicação	Alta	3	Processamento de dados utilizados	Experiência profis	Média	Nova aplicaç	Alta	Significant	3	Significant	3	
Controlado quantitativ	3		Infraestrutura	Elevada	4	Processamento de dados sensíveis	Características fís	Média	Nova aplicaç	Alta	Máxima	4	Máximo	4	
Melhorado continuame	4					Processamento de dados em grande	Perfilagem e dadi	Alta	Aplicação na	Média					
Não aplicável	n/a					Processamento sobre conjuntos de	Dados de contas,	Alta	Outros tipos	Baixa					
						Processamento de dados de indivíd	Propriedades	Alta							
						Processamento de dados através do	Outros dados fin	Alta							
						Transferência de dados para fora da	Origem racial ou	Elevada							
						Processamento de dados que possa	Opiniões política	Elevada							
						Processamento de novos tipos de d	Convicções religi	Elevada							
						Novos tipos de processamento de d	Filiação sindical	Elevada							
							Dados genéticos	Elevada							
							Dados biométrico	Elevada							
							Dados relativos à	Elevada							
							Dados relativos à	Elevada							
							Dados da vida pri	Elevada							

Figura 35 - Ecrã de listas de apoio ao protótipo