LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

MESTRADO

GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO

TRABALHO DE PROJETO

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS – O IMPACTO CAUSADO NUMA ORGANIZAÇÃO

ECATERINA CORENI

OUTUBRO - 2018

LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

MESTRADO EM
GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO
TRABALHO DE PROJETO

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS – O IMPACTO CAUSADO NUMA ORGANIZAÇÃO

ECATERINA CORENI

ORIENTAÇÃO:

PROFESSORA DOUTORA WINNIE NG PICOTO

Agradecimentos

Em primeiro lugar gostaria de agradecer aos meus colegas de trabalho, pela oportunidade única de fazer parte deste projeto e por tudo o que me ensinaram.

A todos os professores que me acompanharam ao longo destes dois anos. Em especial, claro, à professora Winnie Picoto que sempre esclareceu todas as minhas dúvidas em tempo *record*.

Um grande obrigado à turma de GSI, especialmente aos Random, por partilharem o vosso ponto de situação que me fazia sentir melhor. À Andreia, por ter tolerado o meu mau feitio desde os tempos em que eramos caloiras.

Tenho ainda a agradecer aos meus pais e avós, pela paciência, apoio, motivação e, mais que tudo, por me estarem sempre a relembrar que tenho uma tese por acabar.

A ti, Marçal, por seres quem és e estares sempre comigo.

Resumo

A entrada em vigor do Regulamento Geral de Proteção de Dados (RGPD), em maio de 2018, acarreta vários impactos no mundo empresarial. O objetivo deste trabalho consiste na realização de um projeto para uma dada organização, de modo a perceber quais são as inconformidades entre a sua situação atual e as novas exigências regulamentares e identificar as alterações que terão de ser implementadas.

Em primeiro lugar, será revista a literatura existente relacionada com os temas do ciclo de vida dos dados, segurança de informação e gestão da mudança das organizações, bem como os aspetos inovadores constantes no RGPD.

Posteriormente, serão apresentadas as etapas do projeto realizado, nomeadamente o conhecimento dos processos de negócio, a avaliação da situação atual e identificação das inconsistências com as exigências regulamentares e, por último, a apresentação das recomendações e do plano de ação de modo a atingir a conformidade com o RGPD.

Para finalizar, serão enumeradas as principais conclusões do projeto, as lições aprendidas e, ainda, oportunidades de melhoria em projetos futuros.

Palavras-chave: regulamento geral de proteção de dados, privacidade dos dados, ciclo de vida dos dados, segurança de informação.

Abstract

The entry into force of the General Data Protection Regulation, in May 2018, has several impacts in the business world. The aim of this work is to carry out a project for a given organization in order to understand the nonconformities between its existing situation and the regulatory requirements and to identify the changes that will have to be implemented.

Firstly, there will be a review of existing literature related to data life cycle issues, information security and organizational change management, as well as the innovative aspects of the Regulation.

Subsequently, the stages of the project will be presented, specifically the understanding of the business processes, the evaluation of the existing situation and identification of inconsistencies with the regulatory requirements, and finally, the presentation of the recommendations and the action that should be made in order to achieve compliance with the General Data Protection Regulation.

Finally, will be listed the main conclusions of the project, the lessons learned and opportunities for improvement in future projects.

Keywords: general data protection regulation, data privacy, data life cycle, information security.

Lista de Siglas e Acrónimos

TI – Tecnologias de Informação

SGBD – Sistema de Gestão de Bases de Dados

RGPD – Regulamento Geral de Proteção de Dados

DPIA – *Data Protection Impact Analysis*

DPO – *Data Protection Officer*

Índice

AGRADECIMENTOS I

RESUMO II

ABSTRACT III

LISTA DE SIGLAS E ACRÓNIMOS IV

ÍNDICE V

ÍNDICE TABELAS VII

CAPÍTULO 1 – INTRODUÇÃO 1

1.1 Regulamento Geral de Proteção de Dados 1

1.2 Relevância do estudo e objetivos do projeto 1

1.3 Metodologia utilizada e identificação atividades do projeto 2

CAPÍTULO 2 – REVISÃO DE LITERATURA 2

2.1 As novas tendências e a importância crescente de regularizar a utilização dos dados 2

2.2 O ciclo de vida dos dados 4
2.2.1 Recolha e controlo de acesso 4
2.2.2 Armazenamento e classificação 5
2.2.3 Segurança: os impactos de um data breach 6

2.3 O impacto do RGPD nas organizações 8

2.4 Gestão da mudança nas organizações 13

CAPÍTULO 3 – PROJETO: ASSESSMENT REALIZADO NUMA ORGANIZAÇÃO 15

3.1 Conhecimento da organização 15

3. 2 Avaliação da situação atual 17
3.2.1 Matriz de Risco 17
3.2.2 Data Protection Impact Analysis (DPIA) 20
3.2.3 Dicionário de Dados 23

3.3 Análise de maturidade e identificação dos gaps 24

3.4 Recomendações e plano de ação 27

CAPÍTULO 4 – DISCUSSÃO 28

4.1 Teoria & Prática 28

4.2 Reflexão – Qual o verdadeiro impacto causado pelo RGPD? 29

CAPÍTULO 5 – CONCLUSÕES 31

5.1 Principais conclusões 31

5.2 Lições aprendidas 32

5.3 Oportunidades de melhoria em projetos futuros 33

5.4 Questões de investigação futura 33

CAPÍTULO 6 – REFERÊNCIAS BIBLIOGRÁFICAS 35

ANEXOS 37

Anexo 1.1 – Matriz de Risco para sistemas de informação, recursos humanos e operações 37

Anexo 1.2 – Data Protection Impact Analysis para sistemas de informação 40

Anexo 1.3 – Exemplos de Gaps Identificados por Domínio de Maturidade 43

Anexo 1.4 – Exemplos de Recomendações 47

Índice Tabelas

Tabela 1 – Variáveis analisadas na Matriz de Risco

Tabela 2 – Matriz de Risco para sistemas de informação, recursos humanos e operações

Tabela 3 – *Data Protection Impact Analysis* para sistemas de informação

Capítulo 1 – Introdução

1.1 Regulamento Geral de Proteção de Dados

Em maio de 2016, foi publicado no Jornal Oficial da União Europeia, o Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral de Proteção de Dados – RGPD). Este regulamento introduz novas exigências regulamentares em matéria de proteção das pessoas singulares e no que diz respeito ao tratamento de dados pessoais e à livre circulação dos mesmos. O RGPD dá corpo a um novo quadro jurídico, tornando-se aplicável aos 28 Estados-Membros. Ocorreu um período de transição de 2 anos até à implementação total, com entrada em vigor a 25 de maio de 2018.

Esta legislação é aplicada aos responsáveis pelo tratamento de dados (controladores) e aos subcontratantes a que recorram para efetuar esse tratamento (processadores). É, também, aplicada às operações de processamento que se focam nos assuntos de dados pessoais europeus, independentemente se o controlador (processador) esteja ou não localizado na União Europeia (Jordan A. & Sowerby M., 2016; RGPD).

1.2 Relevância do estudo e objetivos do projeto

A introdução do novo regulamento geral de proteção de dados origina um vasto leque de implicações e oportunidades para as organizações de todo o mundo. O RGPD coloca o ónus da proteção da privacidade dos cidadãos nas entidades que recolhem, armazenam, analisam e gerem informações que permitem identificar univocamente um determinado indivíduo. Neste sentido, as organizações que falharem na proteção adequada dos dados pessoais, para além de se sujeitarem às elevadas penalizações previstas no novo regulamento, arriscam-se também a perder a confiança dos seus *stakeholders*, que é considerada como crítica para o sucesso de qualquer organização (Jordan A. & Sowerby M., 2016; RGPD).

O assunto abordado é relativamente recente e, por isso, existe pouca informação estando muitas vezes dispersa. Assim, este projeto tem como objetivos reunir a informação relevante sobre o RGPD de várias fontes, fornecendo uma visão teórica do que é o Regulamento Geral de Proteção de Dados e quais as implicações causadas ao nível das organizações; demonstrar as principais alterações na recolha, armazenamento,

tratamento, divulgação, partilha e destruição de dados pessoais; e ainda fornecer uma visão geral sobre os principais conceitos, direitos e responsabilidades com as quais as organizações terão de lidar.

Por outro lado, este projeto desenvolve uma *framework* básica de quais são os passos iniciais que as empresas devem seguir de modo a estar em conformidade com regulamento. Esta *framework* consolida o conhecimento adquirido e as lições aprendidas num projeto em concreto, podendo uma fonte de conhecimento para outras organizações.

1.3 Metodologia utilizada e identificação atividades do projeto

É objetivo deste trabalho avaliar o cumprimento dos requisitos regulamentares por uma determinada organização e definir um conjunto de iniciativas sob a forma de um plano de ação que permitam colmatar as lacunas identificadas. Deste modo, será feita uma pesquisa bibliográfica nas áreas de gestão do ciclo de vida dos dados e gestão de mudança e impacto do RGPD nas organizações. Posteriormente, será descrito o projeto, do qual fiz parte, composto pelas seguintes atividades:

- Conhecimento da organização: identificação dos processos de negócio existentes.
- Avaliação da situação atual: análise dos macroprocessos e definição dos que são considerados críticos.
- Análise de maturidade e identificação dos *gaps.*
- Apresentação das recomendações e do plano de ação.

Capítulo 2 – Revisão de Literatura

2.1 As novas tendências e a importância crescente de regularizar a utilização dos dados

Um fluxo contínuo de inovações no campo de tecnologias da informação está a transformar o mundo comercial. Os exemplos incluem o *cloud computing*, o crescimento de plataformas de negócios digitais móveis baseadas em *smartphones*, *tablets* e *ultrabooks*, e não menos importante, a utilização de redes sociais por gestores de forma a atingir os objetivos de negócio. Estas inovações possibilitam a criação de novos

produtos e serviços, o desenvolvimento de novos modelos de negócios e a transformação do quotidiano empresarial (Laudon & Laudon, 2014). Assim, as organizações estão interessadas em recolher cada vez mais informação sobre os seus clientes, por vezes sem o seu conhecimento e / ou consentimento. Deste modo, segundo Weber (2010), torna-se crucial garantir a segurança e a privacidade dos dados, através da definição de processos de negócios com um alto grau de fiabilidade. Para tal, é importante ter em conta requisitos como a resiliência aos ataques direcionados aos sistemas, a autenticação de dados, o controlo de acessos e a privacidade do cliente.

De acordo com Bertino (2015), garantir a fiabilidade dos dados pode exigir um controlo rigoroso dos processos de gestão de dados. Estes devem garantir certas condições de segurança, nomeadamente:

- Confidencialidade - proteção de dados contra divulgação não autorizada;
- Integridade - prevenção de modificação não autorizada ou imprópria de dados;
- Disponibilidade - prevenção e recuperação de erros de *hardware* e *software*, bem como negação de acesso a dados maliciosos.

A importância das tecnologias de informação cresceu ao longo dos anos e a sua utilização sofreu alterações relevantes. De acordo com Thomson e Solms (1998), passamos de uma situação em que existiam poucos utilizadores com um perfil altamente especialista, para um elevado número de utilizadores com pouco conhecimento informático.

O regulamento geral de proteção de dados representa, assim, uma forma de sensibilizar as organizações quanto à importância de garantir a segurança de informação, uniformizar o ciclo de vida dos dados e evitar a sua utilização excessiva.

Nos subcapítulos seguintes serão abordados o ciclo de vida dos dados, as principais alterações que o RGPD acarreta, bem como a gestão de mudança nas organizações.

2.2 O ciclo de vida dos dados

2.2.1 Recolha e controlo de acesso

No mundo empresarial contemporâneo, existe uma interdependência crescente entre a capacidade de negócio e os sistemas de informação. Assim, as mudanças ao nível da estratégia e das regras ou processos de negócios exigem cada vez mais alterações nas bases de dados, *hardware*, *software* e telecomunicações, ou seja, nos sistemas de informação. De um modo geral, as ações que uma determinada empresa poderá realizar estão diretamente relacionadas com a capacidade dos seus sistemas de informação (Laudon & Laudon, 2014).

De acordo com Bertino (2015), duas fases relevantes do ciclo de vida dos dados são:

- Aquisição – são necessários mecanismos e ferramentas capazes (i) de impedir que os dispositivos (como por exemplo, telemóveis) adquiram dados sobre outros indivíduos, (ii) de bloquear automaticamente os dispositivos de aquisição de dados e / ou notificar os indivíduos que num determinado local encontram-se dispositivos capazes de recolher dados e (iii) de técnicas pelas quais cada sujeito registado possa expressar as suas preferências sobre a utilização dos dados.
- Transferência – é necessário informar os utilizadores sobre a partilha dos seus dados com terceiros. No entanto, tal atividade nem sempre é possível devido à, por exemplo, questão de confidencialidade da organização.

Outro aspeto relevante consiste em determinar quem é o proprietário dos dados. Pois, de uma forma geral, é quem controla os dados e tem o poder de decidir quem possui o direito de acesso aos mesmos e com que finalidade (Bertino, 2015).

Dada a natureza intangível da informação, bem como de muitos serviços *online*, por exemplo, a *cloud*, deve ser assegurado o correto acesso à informação. Deste modo, torna-se crucial a gestão eficaz do armazenamento de dados, de modo a garantir a acessibilidade contínua da informação. Existe a necessidade, por parte das empresas, de garantir que os dados são armazenados em áreas específicas (por exemplo, *data centers*), que tenham procedimentos de controlo de acesso físico, sejam

ambientalmente apropriado e asseguradas por meio de planos adequados de gestão de desastres (Baškarada & Koronios, 2014).

De acordo com o artigo 5º do Regulamento Geral de Proteção de Dados, os dados pessoais devem ser "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."

2.2.2 Armazenamento e classificação

Uma base de dados consiste numa coleção organizada de dados logicamente relacionados, pode ser de qualquer tamanho e complexidade. Um sistema de gestão de bases de dados (SGBD) é um *software* que permite o uso de uma abordagem de base de dados, cujo objetivo principal é fornecer um método sistemático de criação, atualização, armazenamento e recuperação de dados armazenados. Um SGBD permite aos utilizadores partilhar os dados entre si e entre várias aplicações e fornece recursos para controlar o acesso, impor a integridade e restaurar uma base de dados (Hoffer et al., 2016).

Segundo a definição apresentada no Cobit 5, os dados podem ser definidos como algo que é ou representa um facto. Por exemplo, texto, números, gráficos, som, vídeo. Por sua vez, a informação consiste num conjunto de dados num determinado contexto. O contexto implica fornecer um significado aos dados, defendendo o formato no qual estes são apresentados e a relevância dos mesmos. Os dados são representações armazenadas de objetos e eventos que possuem significado e importância para o utilizador. Por sua vez, a informação é composta por dados que foram processados de forma a aumentar o conhecimento do utilizador (Cobit 5).

O artigo 4º do Regulamento Geral de Proteção de Dados apresenta as seguintes definições de dados, que serão relevantes no decorrer do presente trabalho:

- Dados pessoais: "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por

referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular" (artigo 4º, RGPD).

- Dados genéticos: "dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa" (artigo 4º, RGPD).
- Dados biométricos: "dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos" (artigo 4º, RGPD).
- Dados relativos à saúde: "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde" (artigo 4º, RGPD).

2.2.3 Segurança: os impactos de um *data breach*

Segundo Givens (2000), *data breaches* ocorrem quando os dados pessoais, capazes de identificar um ser humano, como nome, números de segurança ou de cartão de crédito são acidentalmente perdidos ou maliciosamente roubados. Estas violações podem resultar num número elevado de registos comprometidos e levar ao roubo de identidade e outros crimes relacionados.

De acordo com Laudon e Laudon (2014), o roubo de identidade é um crime em que um impostor obtém informações pessoais importantes, como números de identificação social ou números de cartão de crédito, para se passar por outra pessoa. Esta informação poderá ser utilizada de diversas formas. Por exemplo, para incorrer em cobranças fraudulentas em contas existentes ou para solicitar novas contas de serviços públicos, como telefone, eletricidade, televisão, internet, e financeiras, como cartões de crédito e empréstimos (Romanosky et al., 2011).

A violação de dados pessoais, consiste numa "violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (artigo 4º, RGPD).

De acordo com Weber (2010), o direito à privacidade pode ser considerado um direito humano básico e intransmissível. A privacidade inclui a ocultação de informação pessoal, bem como a capacidade de controlar o que acontece com esta informação.

Segundo Hoffer (2016), quando se trata da privacidade, é importante considerar os seguintes aspetos:

- Quem está a recolher os dados?
- Que tipo de informação está a ser recolhida e com que finalidade?
- Que informação será partilhada com terceiras partes e quem são eles?
- Os utilizadores podem alterar a forma como os seus dados são usados?
- Como é que são resolvidos os conflitos de interesses?
- Quais são as políticas de retenção de dados e onde estas podem ser consultadas?

Adicionalmente, de acordo com Hoffer (2016), para garantir a segurança dos dados, as empresas adotam algumas técnicas, nomeadamente:

- Utilização de *passwords* – que representam a primeira linha de defesa. No entanto, estas não conseguem, por si só, garantir a segurança de acesso a um sistema e respetiva base de dados, pois não verificam quem é o utilizador que está a tentar aceder. Assim, por exemplo, devem ser guardados os *logs* de acesso, com a posterior análise das tentativas de *login* falhadas.
- Limitações de acesso – são controlos incorporados nos sistemas que restringem o acesso aos dados e, também, as ações que podem ser executadas sobre os mesmos.
- Procedimentos definidos pelo utilizador – alguns sistemas de gestão de bases de dados fornecem interfaces que permitem que os utilizadores criem seus próprios procedimentos de segurança, além das regras de autenticação básicas.
- Encriptação de dados – pode ser usada para proteger dados altamente confidenciais. Consiste na codificação de dados, de modo a que estes sejam

ilegíveis para um ser humano. Adicionalmente, é possível recorrer à anonimização dos dados.

O objetivo da segurança das bases de dados é proteger a integridade e o acesso aos dados contra as ameaças, que podem ser acidentais ou intencionais. No entanto, o foco exclusivo na segurança das bases de dados não é suficiente. Assim, a segurança deve ser garantida por todas as componentes do sistema empresarial, nomeadamente base de dados, redes, sistemas operacionais, infraestruturas e formação e sensibilização adequada de todos os colaboradores. A obtenção deste nível de segurança requer uma revisão cautelosa do sistema atual, estabelecimento de procedimentos e políticas de segurança, bem como a sua divulgação e aplicação prática pelos intervenientes diretos ou indiretos, sem excluir a necessidade de compromisso por parte de todos os colaboradores. (Hoffer et al., 2016).

2.3 O impacto do RGPD nas organizações

De seguida, são apresentadas as dez principais alterações causadas pelo RGPD, de acordo com Fazendeiro A. (2017).

1. Coimas por incumprimento

   A encabeçar a lista de novidades do Regulamento está o aumento substancial das coimas por incumprimento. As coimas podem ir até "20.000.000 ou, no caso de uma empresa, até 4% do seu volume de negócios anual, a nível mundial, correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado". (artigo 83º, RGPD)

2. Encarregado de proteção de dados

   O artigo 37º do RGPD torna obrigatória a nomeação do encarregado de proteção de dados para:

   - As autoridades e organismos públicos;
   - As entidades que procedam a tratamentos em larga escala de dados pessoais sensíveis;

- As entidades que efetuem tratamento de dados pessoais, também em larga escala, que exijam um controlo regular e sistemático dos titulares de dados.

O Regulamento permite que esta função possa ser desempenhada por um trabalhador da empresa ou ser externalizada com recurso a prestadores de serviços.

3. Registo de atividades de tratamento

A obrigação de proceder ao registo de tratamento dos dados pessoais é referida logo no nº2 do artigo 5º. O artigo 24º, nº 1, ajuda preencher melhor o conceito quando prevê que o responsável pelo tratamento de dados pessoais deve "poder comprovar que o tratamento é realizado em conformidade com o presente regulamento".

4. Avaliação de impacto sobre a proteção de dados (DPIA)

Estas avaliações devem ser levadas a cabo antes de serem iniciadas as operações de tratamento de dados que utilizem novas tecnologias e que possam implicar elevado risco para os direitos e liberdades dos titulares dos dados.

A autoridade de proteção de dados deve ser consultada antes de se iniciar qualquer tipo de tratamento quando a avaliação de impacto indicar que existe risco elevado, não mitigado pela tomada de medidas, devendo comunicar-lhe, nessa consulta, as informações previstas no artigo 36º, nº 3, do Regulamento.

5. Segurança e notificação de violação de dados pessoais

A segurança dos dados apresenta-se como fundamental no Regulamento que, em termos gerais, impõe regras mais exigentes para a segurança dos dados. O artigo 32º define o protótipo a seguir no que respeita à segurança do tratamento e obriga responsáveis pelo tratamento de dados e subcontratantes a implementar "medidas técnicas e organizativas adequadas" tendo em conta as "técnicas mais avançadas", os "custos de aplicação" e "a natureza, o âmbito, o contexto e as finalidades de tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares" (artigo 32º, RGPD).

Este artigo aponta sugestões específicas de medidas de segurança adequadas ao risco, como por exemplo a pseudonimização (conceito novo no Regulamento) e cifragem dos dados pessoais.

6. Consentimento

O consentimento no Regulamento continua a ser um dos fundamentos para a legitimidade do tratamento de dados pessoais.

O consentimento, de acordo com o artigo 4º, nº 11, consiste numa "manifestação de vontade, livre, específica, informada e explicita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".

Sempre que se considere o consentimento como base para o tratamento lícito dos dados, deve ser assegurado que este é:

- Ativo, ou seja, não se baseia na ausência de resposta, inatividade ou caixas pré-selecionadas;
- Explícito, no caso de dados pessoais sensíveis ou de fluxos de dados transfronteiriços;
- Distinto, claro e não associado com outros acordos escritos ou declarações.

Isto é, para cada atividade que implique o uso de dados pessoais fora do âmbito de contrato, o titular dos dados deve exprimir o seu consentimento por livre vontade, sem caixas pré-selecionadas. A finalidade com que serão usados os dados deve ser descrita de forma clara, explícita e desagrupada. Assim, o titular dos dados deve conseguir dar o consentimento por atividade e terá a opção de concordar com certas finalidades e outras não.

Deve-se ainda garantir que:

- A prestação de serviços não é condicionada ao consentimento quando não é necessária para que o serviço seja prestado;
- Os detentores da informação sejam informados do direito de retirar o consentimento em qualquer momento (através de métodos simples);

- São obtidos consentimentos separados para operações de processamento distintas.

7. Direito dos Titulares

O direito de ser esquecido - o direito de pedir aos responsáveis pelo tratamento de dados que apaguem todos os dados pessoais sem demora injustificada.

O direito à portabilidade de dados - quando os indivíduos forneceram dados pessoais a um prestador de serviços, podem exigir que o prestador "transfira" os dados para outro fornecedor, desde que tal seja tecnicamente viável.

O direito de se opor ao estabelecimento de perfil - o direito de não ser sujeito a uma decisão de perfil baseada unicamente em processamento automatizado.

O direito de proteção específica para pessoas vulneráveis, nomeadamente das crianças, onde a informação e proteção que lhes é providenciada deve ser especialmente cuidada, bem como o processo de obtenção de consentimento dos seus responsáveis/representantes.

8. Profiling

O artigo 4º, nº 4, define *profiling* como "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações".

São elementos essenciais desta definição:

- O tratamento automatizado dos dados;
- O uso destes para avaliar aspetos pessoais relativos a uma pessoa singular.

Assim, ficam excluídos tratamentos não automatizados de dados.

Embora por principio o titular dos dados tenha o direito de não ficar sujeito a decisões baseadas em tratamentos automatizados de dados, incluindo o *profiling*, estas serão possíveis, nos termos do artigo 22º, quando:

a) “necessárias para a celebração de um contrato ou execução do mesmo entre o titular dos dados e o responsável pelo tratamento”;

b) ”autorizadas pela lei de um estado membro”;

c) “existir consentimento explicito do titular”.

De acordo com o artigo 13º, nº 2, (f), devem ser facultadas ao titular dos dados informações relativas à “logica subjacente” no caso de *profiling*, “bem como a importância e as consequências previstas de tal tratamento para o titular dos dados”.

Se o tratamento tiver como finalidade o marketing direto, em caso de oposição o responsável pelo tratamento deve cessar o tratamento.

A existência de *profiling* é um dos motivos que levam à obrigatoriedade de realização de avaliações de impacto previstas no artigo 35º.

9. Responsável pelo tratamento e subcontratantes

O regulamento define o responsável pelo tratamento no seu artigo 4º, nº7, desta forma:

“«Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro”.

E o subcontratante no seu artigo 4º, nº 8, nos seguintes termos:

“«Subcontratante», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes”.

10. Outras novidades a assinalar

Código de conduta e selos de certificação – O Regulamento prevê que a adesão a estes códigos, elaborados por associações ou entidades representativas de

determinados sectores e submetidos às autoridades de proteção de dados, possa demonstrar o cumprimento das regras de proteção de dados. Os selos de certificação serão também uma prova de conformidade com estas regras (arts. 40º, 41º, 42º e 43º). (Ana Fazendeiro, Regulamento Geral sobre a Proteção de Dados, 2017)

Conceito de pseudonimização – "o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável" (artigo 4º, nº 5, RGPD).

Proteção de dados desde a conceção e por defeito – De acordo com estes princípios, as organizações devem implementar medidas técnicas e organizativas de forma a demonstrarem que consideram e integraram medidas de conformidade com as regras de proteção de dados nos tratamentos de dados que levam acabo, que apenas devem incidir sobre os dados que sejam realmente necessários para a prossecução das finalidades específicas do tratamento (artigo 25º, RGPD,). Deste modo, as empresas devem garantir que o uso de dados pessoais está de acordo com as normas do RGPD desde o momento da recolha, durante todas as fazes de tratamento e até à sua destruição, isto é, durante todo o seu ciclo de vida. Adicionalmente, deve ser garantido que os dados são utilizados somente para as finalidades para que foram recolhidos.

2.4 Gestão da mudança nas organizações

A implementação do RGPD nas empresas implica várias alterações em diferentes níveis organizacionais. Assim, um dos fatores de sucesso da sua implementação consiste na correta gestão da mudança organizacional.

Segundo Kettinger e Grover (1995), um processo de negócios é um conjunto de tarefas logicamente relacionadas, que utilizam os recursos de uma organização para alcançar um resultado de negócios definido. *Business process reengineering*, melhoria de processos, inovação de processos e redesenho de processos de negócios são termos

frequentemente usados para representar o fenómeno da mudança do processo de negócios. A mudança de processos de negócio pode ser definida como:

- Um processo metodológico que utiliza a tecnologia da informação para rever radicalmente os processos de modo a atingir os principais objetivos de negócios (Alter, 1990).
- Inclui a revisão de processos de negócios e estruturas de organização que limitam a competitividade, a eficácia e a eficiência da organização (Senn, 1991).
- Consiste num repensar fundamental e num redesenho radical dos processos de negócios para alcançar melhorias drásticas em medidas de desempenho críticas e contemporâneas, como custo, qualidade, serviço e velocidade (Hammer & Champy, 1993).
- Combina a adoção de uma visão de processo do negócio com a aplicação da inovação aos principais processos, a fim de alcançar melhorias significativas nos objetivos de negócios (Davenport, 1993).

O desenvolvimento organizacional permite implementar mudanças planeadas e, de igual modo, engloba a transferência de conhecimento para as organizações, para que estas tenham igualmente a capacidade de gerir a mudança no futuro.

O desenvolvimento organizacional abrange um sistema inteiro, isto é, uma equipa, um departamento ou uma organização na sua totalidade. Lida, também, com relacionamentos entre um sistema e o seu ambiente, bem como entre os diferentes recursos que compõem o este sistema.

O desenvolvimento organizacional representa a mudança como um processo, não como um evento ou estado final, e envolve uma série contínua de ações, bem como, o seu planeamento, implementação e avaliação. Consequentemente, este processo é altamente adaptável e altera-se à medida que torna-se conhecida nova informação (Cummings, 2004).

No que concerne à mudança nas organização, de acordo com Mathieson (1991), um aspeto crucial a ser considerado é *information security awareness,* que se refere a um estado em que os colaboradores estão cientes do seu compromisso com a segurança de informação. Os sistemas de informação podem ser úteis somente se as pessoas os

usarem. Da mesma forma, *information security awareness* é de extrema importância, à medida que as técnicas ou procedimentos de segurança da informação podem ser utilizados e / ou interpretados de forma errada, perdendo, assim, a sua utilidade. O aumento da consciencialização deve minimizar os erros relacionados com a falha humana, anulá-las em teoria e maximizar a eficiência das técnicas e procedimentos de segurança. Para implementar isto a um nível de organização, é importante, por exemplo, identificar, quantificar e entender o contexto e as razões subjacentes aos erros humanos. Isto deve ser feito sistematicamente, estabelecendo um programa baseado em identificar o âmbito, metas e objetivos do programa, identificar o público-alvo, motivar a administração e os funcionários, gerir o programa e, finalmente, avaliar o programa, devem ser desenvolvidas e implementadas diferentes atividades de *feedback* em cada etapa como uma fonte de avaliação e melhoria contínua (Siponen, 2000).

Capítulo 3 – Projeto: *Assessment* realizado numa organização

O projeto foi realizado numa organização que, por questões de confidencialidade, não poderá ser identificada. Assim, no decorrer do presente capítulo:

- A organização será designada por Entidade *Random*;
- A informação é anonimizada, havendo lugar à remoção de todas as menções e resultados que possam identificar direta ou indiretamente a organização.

Trata-se de um projeto de *assessment*, isto é, validação do nível de conformidade com as normas do RGPD da Entidade *Random*, identificação dos aspetos a serem melhorados e apresentação das respetivas recomendações e plano de ação. Deste modo, o projeto é constituído pelas seguintes etapas:

1. Conhecimento da organização: identificação dos processos de negócio existentes.
2. Avaliação da situação atual: análise dos macroprocessos e definição dos que são considerados críticos.
3. Análise de maturidade e identificação dos *gaps.*
4. Apresentação das recomendações e do plano de ação.

3.1 Conhecimento da organização

Em primeiro lugar, de modo a obter uma visão global da Entidade *Random*, foram realizadas 28 entrevistas *top-down* e *bottom-up.* Nestas sessões de trabalho, cuja duração era cerca de uma hora, participavam os responsáveis por cada área de negócio e a equipa que responsável por realizar este projeto, da qual eu fazia parte. O principal objetivo consistia em identificar os processos organizacionais existentes, bem como os possíveis problemas. As perguntas realizadas durante as reuniões, para cada macroprocesso de negócio, procuravam perceber:

- Qual a estrutura do departamento e as principais atividades.
- Quais os sistemas de informação aos quais os colaboradores têm acesso, quer utilizem-nos quer não.
- Quais os dados pessoais de clientes e colaboradores a que se tem acesso e, se entre estes constam dados sensíveis, nomeadamente dados genéticos, biométricos e relativos à saúde (ver capítulo 2.2.2 para definições detalhadas).
- Existe partilha de informação com terceiras partes (internas ou externas) e de que forma esta transmissão é feita (pen, e-mail, sistemas, *cloud*, etc.).
- Quais os locais de armazenamento dos dados pessoais (pastas de rede, computador pessoal, pen, etc.).
- Existe eliminação de dados após término das atividades para os quais estes eram necessários.

No total foram entrevistados 55 colaboradores e identificados 32 macroprocessos de negócio.

Adicionalmente, de modo a completar a informação obtida nas entrevistas, foram analisados os questionários de *Business Impact Analysis* (trata-se de uma descrição das atividades fundamentais para a continuidade do negócio e análise do impacto que uma disrupção poderá ter sobre essas atividades), preenchidos para cada macroprocesso da organização pelo seu responsável. Bem como, as políticas e procedimentos definidos na organização, entre as quais o organograma, a política de segurança da informação, política de privacidade do *site*, políticas de tratamento da informação nos vários canais, arquitetura técnica dos sistemas de informação e as respetivas matrizes de acesso e modelos de dados.

Com estes procedimentos foi possível obter uma visão geral da Entidade *Random*, entender os seus processos de negócio e a utilização que faz dos dados pessoais de clientes e colaboradores, bem como os sistemas de informação responsáveis pelo seu tratamento e armazenamento.

3. 2 Avaliação da situação atual

3.2.1 Matriz de Risco

Após a identificação e análise de alto nível dos macroprocesso da Entidade *Random*, procedeu-se a uma avaliação mais profunda dos mesmos. O foco desta avaliação consistia em determinar quais são os processos críticos da organização. Neste sentido, foi utilizada a matriz de risco, estruturada de forma a avaliar a (1) probabilidade de ocorrência de riscos associados ao ciclo de vida dos dados, bem como da (2) ocorrência de impactos resultantes de uma *breach* de segurança. No quadro abaixo constam as variáveis que foram alvo de análise e a respetiva descrição. Estas variáveis foram identificadas com base na análise do RGPD, por elementos mais seniores da equipa a nível global.

Variáveis em análise	Descrição
1. Riscos associados ao ciclo de vida dos dados	Agrupa os riscos associados às quatro fases do ciclo de vida
I. Recolha de dados	Agrupa os riscos associados à fase de recolha dos dados
I. Sem justificação para a recolha	Processos que detêm ou processam dados em que a empresa não consegue justificar a sua recolha
II. Excesso de volume de dados recolhidos	Processos que detêm ou processam um volume bastante significativo de dados
III. Excesso de volume de pessoas envolvidas	Processos que detêm ou processam dados sobre um volume bastante significativo de pessoas
II. Utilização de dados	Agrupa os riscos associados à fase de utilização dos dados
I. Utilização dos dados com erros	Processos que detêm ou processam dados de forma incoerente, transmitindo informações erradas
II. Utilização dos dados para além das expectativas do indivíduo	Processos que detêm ou processam dados para além do intuito autorizado pelo indivíduo a quem pertence os dados

III. Utilização que não é razoável de acordo com as normas sociais	Processos que detêm ou processam dados com objetivos que não são aceitáveis de acordo com as normas sociais
IV. Utilização dos dados sem justificação	Processos que detêm ou processam dados sem que a empresa tenha uma justificação plausível para a sua utilização
V. Processamento de dados sensíveis	Processos que detêm ou processam dados sensíveis (p.e., dados de saúde, dados com segredo profissional, dados de opiniões políticas, etc.)
VI. Processamento de dados de pessoas vulneráveis	Processos que detêm ou processam dados de pessoas vulneráveis (p.e., de crianças)
VII. Processamento automatizado de dados/ *profiling*	Processos que detêm ou processam dados com o objetivo de realizar *profilings* (p.e., pessoas entre 18 a 20 anos recebem publicidade de escolas de condução)
VIII. Processamento de dados que originem transferências internacionais	Processos que detêm ou processam dados em que estes são transferidos para entidades noutros países, que podem ter outras regulações para gerir dados
IX. Volume de terceiras partes que acedem aos dados	Processos que detêm ou processam dados através de terceiras partes onde existe um menor controlo, logo maior risco, no processamento dos dados
X. Processamento de dados com novas tecnologias	Processos que detêm ou processam dados através de novas tecnologias no mercado que podem não ter um estado de maturidade de segurança adequado, ou uma nova tecnologia para a empresa, cuja parametrização de segurança pode, ainda, não estar o suficientemente madura para gerir dados pessoais
XI. Novo processamento de dados	Processos que detêm ou processam dados de uma forma nova e que, por isso, podem ainda não ter os mecanismos de controlos e DPIAs associados
III. Gestão da divulgação de dados	Agrupa os riscos associados à fase de gestão da divulgação de dados
I. Perda de dados	Processos que detêm ou processam dados que foram perdidos
II. Alteração de dados	Processos que detêm ou processam dados que foram alterados
III. Roubo de dados	Processos que detêm ou processam dados que foram roubados
IV. Comunicação ou acesso não autorizado de dados	Processos que detêm ou processam dados que foram comunicados ou acedidos sem que tivesse sido dado autorização para o efeito
IV. Retenção e eliminação de dados	Agrupa os riscos associados à fase de retenção e eliminação de dados

I. Armazenamento de informação inadequada, desnecessária ou desatualizada	Processos que detêm ou processam dados que estão armazenados contendo informação que não é adequada, que não serve um propósito, ou que se encontra desatualizada
II. Armazenamento de informação sem mecanismos de segurança adequados	Processos que detêm ou processam dados que estão armazenados sem os mecanismos de segurança adequados (p.e., *disaster recovery*, *backups*, *logs*, etc.)
III. Destruição acidental dos dados	Processos que detêm ou processam dados que foram destruídos de forma acidental, sem que estivesse previsto
2. Impactos de um *breach* no manuseamento dos dados	Agrupa os impactos associados ao incorreto manuseamento dos dados
I. Dano tangível	Agrupa os impactos que são tangíveis e mensuráveis
I. Dano físico	Processos que detêm ou processam dados cujo incorreto manuseamento deu origem a danos físicos para o indivíduo (p.e., um dos seus ativos foi danificado)
II. Dano de propriedade intelectual	Processos que detêm ou processam dados cujo incorreto manuseamento deu origem a danos na propriedade intelectual detida pelo indivíduo
III. Perda financeira/ económica	Processos que detêm ou processam dados cujo incorreto manuseamento deu origem a uma perda financeiro ou económica para o indivíduo
IV. Perda de liberdade de circulação	Processos que detêm ou processam dados cujo incorreto manuseamento deu origem a que o indivíduo não pudesse circular livremente (p.e., a sua reputação foi denegrida e o indivíduo sente-se inibido a circular em determinado local)
II. Dano intangível	Agrupa os impactos que são intangíveis e que não são, por isso, mensuráveis de forma exata
I. Roubo de identidade/Fraude	Processos que detêm ou processam dados cujo incorreto manuseamento deu origem a roubos de identidade e possíveis fraudes em nome do indivíduo
II. Perda de controlo sobre os próprios dados	Processos que detêm ou processam dados cujo incorreto manuseamento deu origem a que o indivíduo não possa controlar os seus dados, bem como a sua utilização
III. Intrusão inaceitável na vida pessoal (vigilância excessiva)	Processos que detêm ou processam dados que são considerados intrusivos na vida pessoal do indivíduo e que não são aceitavas, pois revelam excesso de vigilância da vida do indivíduo)

IV. Dano que reprima Ação/ cause discriminação	Processos que detêm ou processam dados cujo incorreto manuseamento limita a liberdade de expressão de um determinado indivíduo, causa discriminação e/ou embaraço e ansiedade

Tabela 1 – Variáveis analisadas na Matriz de Risco

Para cada uma das variáveis descritas na Tabela 1 e por cada macroprocesso de negócio identificado, foi atribuída, pela equipa que realizou o projeto, uma pontuação das atividades com base na probabilidade de ocorrência. Esta pontuação é baseada numa escala de 1 a 4, em que 1 representa uma probabilidade muito baixa que um determinado processo esteja exposto a um determinado risco ou provoque determinado impacto no caso de uma *breach* de segurança, 2 representa uma probabilidade baixa, 3 – alta e 4 – muito alta.

Em anexo (anexo 1.1) encontra-se a matriz de risco preenchida para três macroprocessos de negócio a título de exemplo, nomeadamente sistemas de informação, recursos humanos e operações. Após a análise efetuada, é possível verificar que a probabilidade de riscos associados ao ciclo de vida dos dados é 52%, 50% e 30%, respetivamente. Por sua vez, os impactos de um *breach* no manuseamento dos dados são de 75%, 33% e 25%, respetivamente.

Um processo é considerado como crítico quando a probabilidade de riscos associados ao ciclo de vida dos dados e os impactos de um *breach* no manuseamento dos dados são superiores a 50%. Assim, conclui-se que dos macroprocessos supramencionados, apenas o de sistemas de informação é considerado crítico. No total, foram identificados dez macroprocessos críticos.

3.2.2 Data Protection Impact Analysis (DPIA)

A matriz de risco permite avaliar o risco associado ao processo e dessa forma definir a necessidade de realização de um DPIA.

O DPIA é uma ferramenta desenhada para descrever o processamento, avaliar a necessidade e proporcionalidade do mesmo, determinar a conformidade com os requisitos do RGPD, ajudar a gerir os riscos para os direitos e liberdades de pessoas singulares que resultam do processamento de dados pessoais e determinar as medidas apropriadas para abordar esses riscos (artigo 35º, nº7, RGPD). O RGPD recomenda a

realização de DPIA por parte do responsável pelo tratamento de dados ou subcontratantes, quando determinado 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 (artigo 35º, nº 1, RGPD). Esta recomendação passa a obrigatoriedade quando se verificar uma "avaliação sistemática e completa dos aspetos pessoais de pessoas singulares", "operações de tratamento em grande escala de categorias especiais de dados" e "controlo sistemático de zonas acessíveis ao público em grande escala" (artigo 35º, nº3, RGPD).

O RGPD indica que a avaliação de impacto de privacidade deve incluir:

- "A descrição sistemática das operações de tratamento previstas e a finalidade do tratamento";
- "A avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos";
- "Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos";
- "As medidas previstas para fazer face aos riscos, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o RGPD" (artigo35º, nº 7, RGPD).

Adicionalmente, o cumprimento dos códigos de conduta aprovados, referidos no artigo 40º do RGPD, devem ser devidamente tidos em consideração na avaliação do impacto das operações de processamento, por parte dos responsáveis de dados ou subcontratantes.

Assim, de forma a garantir o cumprimento dos pontos acima descritos a elaboração do DPIA e do respetivo relatório deve seguir cinco fases distintas:

1. Identificar necessidade do DPIA - Nesta primeira fase, o principal objetivo é a sistematização das razões pelo qual um determinado tratamento de dados é considerado de alto risco. Para tal, devem ser descritos os objetivos do tratamento, natureza, âmbito, contexto e finalidades bem como os benefícios

esperados para a organização, para os indivíduos e para as restantes partes envolvidas. Para tal, foi preenchida a matriz de risco.

2. Descrever fluxos de informação – De forma a fornecer uma descrição sistemática do processamento (artigo 35º, nº 7 (a), RGPD) deve ser feita a inventariação dos fluxos de informação. O fluxo tem de comtemplar uma visão abrangente sobre os dados pessoais desde do momento da recolha, utilização, período de armazenamento e destruição, bem como os destinatários, os recursos utilizados e gerados (*hardware*, *software*, redes, pessoas, papel ou canais de transmissão de papel) ao longo dos processos.
3. Identificar riscos de privacidade - Independentemente da sua forma, um DPIA deve ser uma avaliação genuína dos riscos nos diferentes domínios, nomeadamente circularização de dados; licitude e lealdade do tratamento de dados pessoais; finalidade; minimização e exatidão; direitos e transferências; segurança; conformidade; conservação; terceiros; transferências de dados pessoais; categorias especiais de dados pessoais; definição de perfis; análise alargada de dados e gestão de incidentes. Esta avaliação permitirá identificar as medidas a serem adotadas para mitigação dos riscos. Posteriormente, cada domínio deve ser avaliado e classificado em termos do seu impacto, como elevado, médio ou baixo, tendo em conta a probabilidade e gravidade do mesmo (artigo 35º, nº7 (c) e considerando 84, RGPD).
4. Identificar soluções de privacidade – Esta fase consiste em descrever as medidas previstas para mitigação dos riscos já identificados por domínios e dessa forma contribuir para o cumprimento do regulamento (artigo 35º, nº7 (d) e o considerando 90, RGPD).
5. Integrar resultados do DPIA – Após a elaboração das fases acima descritas é necessário compilar a informação num relatório e garantir que as medidas propostas são implementadas. A publicação dos relatórios do DPIA não é um requisito legal mas, em caso de consulta prévia o relatório deve ser comunicado à autoridade de supervisão. Contudo, a publicação do DPIA pode ser vista como uma demostração de transparência e boa prática, podendo ser publicado apenas

um resumo sem informação comercial que possa ser considerada sensível (Data Protection Working Party, 2017).

No total, foram realizados seis DPIAs para os macroprocessos críticos, ficando a Entidade *Random* responsável por realizar os restantes quatro. Em anexo 1.2 encontra-se o relatório de *Data Protection Impact Analysis* preenchido para o macroprocesso de Sistemas de Informação. Por questões de confidencialidade, foi omitida a fase 2 – descrição dos fluxos de informação.

3.2.3 Dicionário de Dados

De modo a ter uma visão geral do fluxo de dados pessoais da Entidade *Random*, foi desenvolvido o dicionário de dados, que consiste numa ferramenta de gestão robusta que garante à organização uma visão alargada dos dados que detêm e onde estes se encontram. Para a sua elaboração foram consultadas 30 fontes de informação, entre as quais as aplicações que suportam os macroprocessos críticos e os formulários de recolha de informação.

Por questões de confidencialidade, este documento não poderá ser divulgado no presente trabalho, apenas serão indicados os campos que o compõem, nomeadamente:

- Os dados pessoais que estão a ser utilizados (nome, número do cartão de identificação, morada, etc.).
- A categoria dos dados, ou seja, se são de clientes, colaboradores, fornecedores, etc.
- O macroprocesso associado.
- A fonte de informação, isto é, o meio de recolha dos dados.
- A sua categorização, se se trata de dados de identificação ou dados sensíveis.
- O tipo de identificação, se é direta ou indireta.
- A finalidade de tratamento.
- O fundamento regulamentar para o tratamento.
- O período de retenção dos dados.

O dicionário de dados sistematizou todos os dados pessoais identificados na fase de conhecimento da organização, com especial foco nos dados dos processos críticos. No

final, foram analisados 538 dados pessoais, dos quais 112 são de identificação e 3 são dados considerados sensíveis. Adicionalmente, foram identificados 6 fundamentos que permitem justificar o tratamento dos dados.

3.3 Análise de maturidade e identificação dos *gaps*

Foram identificados 20 domínios de maturidade, com base na análise do RGPD, por elementos mais seniores da equipa a nível global, relacionados com o tema da privacidade e proteção dos dados pessoais, que permitiram avaliar o nível de maturidade da Entidade *Random* face ao cumprimento do RGPD. Estes domínios são:

- Estratégia de privacidade – concentra-se na proteção de dados e na forma como os objetivos relacionados com o tema estão alinhados com os objetivos organizacionais, de modo a alcançar as prioridades estratégicas.
- Política de privacidade – exige que processos e controlos estejam implementados para proteger as informações pessoais processadas pela organização. Neste sentido, é necessário o desenvolvimento formal de documentação, mecanismos de revisão e aprovação de padrões e diretrizes no âmbito da privacidade de dados.
- Formação e sensibilização – informação relacionada com programas de consciencialização, incluindo formações obrigatórias de privacidade para todos os colaboradores da organização e certificações em privacidade para os principais responsáveis, o que implica o envolvimento de responsáveis de primeira linha associados aos temas de privacidade.
- Reporte regulamentar – os mecanismos e processos de reporte regulamentar devem definir claramente quem, dentro da organização, deve ser responsável por reportar ao regulador, o que deve ser reportado e quando deve ser reportado.
- Gestão da perceção pública – explora a forma como a organização lida com questões de violação de privacidade e / ou que tenham cobertura dos media.
- *Privacy by design and by default* - este domínio procura averiguar se a organização aplica a proteção de dados desde a conceção e por defeito, nomeadamente se possui iniciativas que exijam uma avaliação de impacto de

privacidade no início ou durante o processamento dos dados explorando, em particular, se este resulta num risco elevado para os indivíduos.

- Gestão de risco – considera a forma como a organização avalia os seus riscos de privacidade e os mitiga através da implementação de controlos-chave.
- Gestão da violação da segurança dos dados – foca-se no modo como a organização lida com uma violação de privacidade, nomeadamente na análise dos processos e procedimentos de monitorização, gestão, remediação e, quando apropriado, reporte de incidentes de privacidade.
- *Due diligence* a terceiros – inclui a avaliação dos requisitos de privacidade e proteção de dados que precisam de ser considerados nos contratos e obrigações com terceiros, bem como a monitorização dos processos em vigor para proteger os dados pessoais e garantir que estão implementadas as obrigações de privacidade apropriadas.
- Reclamações / pedidos do consumidor – as organizações devem ter um processo implementado para lidar com pedidos relacionados com os direitos dos indivíduos, analisar até que ponto as reclamações de privacidade são efetivamente tratadas, bem como de ser capazes de investigar e resolvê-las num prazo estabelecido.
- Classificação de dados – baseia-se no impacto para os indivíduos na eventualidade dos seus dados pessoais serem perdidos, roubados, divulgados inapropriadamente, alterados ou destruídos e tem como objetivo o estabelecimento de medidas de segurança adequadas de acordo com esse mesmo impacto.
- Gestão de dados externos – deve incluir mecanismos de controlo e proteção de dados pessoais acrescidos nos casos em que estes são transmitidos e armazenados entre diferentes países, o que engloba transferências intragrupo e, também, transferências com terceiros ou outras autoridades de controlo.
- Recolha de dados adequados – o processo de recolha de dados tem de ser justificável e devem ser solicitados os respetivos consentimentos (positivos e

distintos), bem como partilhada a informação exigida pelo regulamento para garantir a transparência e equidade na recolha dos dados.

- Uso relevante dos dados – aquando da recolha de dados pessoais a organização deve informar o titular sobre o propósito da recolha, garantir que os dados serão usados para fins específicos e averiguar se o posterior processamento de dados é válido, caso este seja necessário.
- Gestão de divulgação – as organizações devem ter procedimentos implementados para lidar com a divulgação de dados pessoais e garantir que esta é feita de forma legal.
- Retenção e eliminação apropriada – as organizações devem ter uma política adequada para gerir a retenção de dados e para proceder à sua eliminação de forma segura e adequada, garantindo que estes são mantidos durante o tempo estritamente necessário.
- Revisão das exigências de privacidade – explora como a organização avalia o impacto e atualiza as políticas, os procedimentos internos e de gestão de privacidade e diretrizes existentes, face às mudanças nas leis e exigências regulatórias.
- Exigências regulamentares – as organizações devem criar as estruturas internas e os mecanismos adequados que garantam o alinhamento da sua estratégia e do seu modelo de negócio com o RGPD.
- Auditoria à privacidade – verifica se a organização executou ou planeou uma auditoria sobre privacidade de modo a identificar áreas de risco ou potenciais inconformidades, para que estas possam ser geridas e resolvidas adequadamente.
- Gestão de fluxo de dados – concentra-se nos processos associados ao ciclo de vida dos dados pessoais e envolve a autenticação de identidade, criação de fluxos de informação, alteração de dados e a capacidade de auditar e reportar informações ao titular dos dados.

Com a informação recolhida na fase do conhecimento da organização, foi possível efetuar uma análise detalhada de cada um dos domínios e identificar os *gaps* entre o

que é feito atualmente pela Entidade *Random* e o que deveria ser feito de acordo com o RGPD.

Por exemplo, no que concerne ao domínio de gestão da violação da segurança dos dados, os requisitos regulamentares são: (i) notificação de uma violação de dados pessoais à autoridade de controlo e (ii) comunicação de uma violação de dados pessoais ao titular dos dados (artigos 33º e 34º, RGPD). No entanto, a situação atual da Entidade *Random* não está totalmente em conformidade com o RGPD, pois:

- A política e procedimentos formais de gestão de incidentes de violação de privacidade não descrevem à necessidade de cumprimento dos prazos estipulados (72h) de notificação à autoridade de controlo após o responsável pelo tratamento ter tido conhecimento de uma violação de dados pessoais.
- Os contratos estabelecidos com entidades externas não descrevem procedimentos para imputar responsabilidades a terceiros se a violação da privacidade ocorrer durante o tratamento realizado por estes.
- Inexistência de mecanismos que garantam a sensibilização dos *stakeholders,* quanto às suas responsabilidades e possíveis repercussões da violação das exigências relacionadas com a privacidade e a proteção dos dados pessoais.

No Anexo 1.3, encontram-se apresentados exemplos de outros *gaps* identificados por domínio de maturidade.

3.4 Recomendações e plano de ação

De modo a colmatar todas as inconformidades (*gaps*) identificadas,foram sugeridas recomendações que endereçam as necessidades específicas da Entidade *Random* para o tema da privacidade e da proteção de dados pessoais tendo em conta o RGPD. Abaixo encontra-se especificada uma das recomendações e respetivo plano de ação.

Recomendação:

Nomear o Encarregado de Proteção de Dados (*Data Protection Officer* – DPO) e definir o modelo de governo da função de DPO, nomeadamente a articulação entre a função e a restante organização. Definir uma estratégia que permita cumprir com o descrito no RGPD. Trata-se de uma recomendação cuja prioridade é considerada elevada e que irá abranger os *gaps* identificados nos domínios de (i) estratégia de privacidade, (ii) reporte

regulamentar e (iii) gestão da violação da segurança dos dados (descrito no subcapítulo anterior).

Plano de ação (ações de curto prazo):

1. Nomeação do DPO;
2. Publicação e comunicação de contactos do DPO à autoridade de controlo;
3. Definição de uma base de articulação da função de DPO com a restante organização;
4. Formação do DPO e respetiva equipa.

No anexo 1.4, a título de exemplo estão apresentadas, sucintamente, outras recomendações. De modo a salvaguardar a confidencialidade da Entidade Random, não é possível apresentar uma versão mais alargada e descritiva de todas as recomendações.

Capítulo 4 – Discussão

4.1 Teoria & Prática

Durante a redação deste trabalho deparei-me com algumas dificuldades. A principal consistia em fundamentar o trabalho prático com conceitos teóricos. Visto tratar-se de um tema relativamente recente, ainda não existem muitas pesquisas e artigos relacionados linearmente com o RGPD e o respetivo impacto. Assim, a revisão de literatura encontra-se estruturada da seguinte forma:

- 2.1 – As novas tendências e a importância crescente de regularizar a utilização dos dados. É um subcapítulo introdutório, cujo objetivo é apresentar os riscos associados à excessiva utilização dos sistemas de informação por parte das empresas e os motivos que levaram ao aparecimento do RGPD. Este subcapítulo não tem mapeamento direto com o projeto realizado.
- 2.2 – O ciclo de vida dos dados. O RGPD tem como ideia principal proteger os dados pessoais. Assim, considerei relevante abordar o ciclo de vida dos dados numa organização, para que os principais conceitos, artigos e fases do projeto se tornem mais percetíveis. Este subcapítulo mapeia com as fases iniciais do projeto, nomeadamente de conhecimento da organização e avaliação da sua situação atual.

- 2.3 – O impacto do RGPD nas organizações. Este subcapítulo é baseado no livro de Fazendeiro, A., que sistematiza e clarifica as principais ideias abordadas no RGPD. A leitura deste livro foi-me sugerida pelo elemento sénior da equipa, antes do início do projeto. A organização do livro mapeia, de forma indireta, com as questões colocadas durante as entrevistas, na fase de conhecimento da organização, com os documentos criados na avaliação da situação atual e algumas recomendações apresentadas.
- Capítulo 2.4 – Gestão da mudança nas organizações. Trata-se de um subcapítulo de conclusão, cujo objetivo é mostrar ao leitor que o conhecimento da sua organização e do ciclo dos dados não é suficiente para a correta implementação do RGPD. É necessário formar os colaboradores e gerir todas as fases da mudança que esta implementação acarreta. Este subcapítulo não mapeia com nenhuma das fases do projeto realizado, pois trata-se de um projeto de *assessment* e a gestão da mudança será relevante em projetos posteriores de implementação do RGPD.

Esta análise permite perceber que as duas últimas fases do projeto, nomeadamente a análise de maturidade e identificação dos *gaps* e apresentação das recomendações e do plano de ação, não estão devidamente suportadas pela revisão de literatura. Tal acontece, devido à escassez de pesquisas e artigos científicos relacionados com o impacto do RGPD. Os documentos que suportaram a realização destas fases são baseados nos trabalhos desenvolvidos pelo Grupo de Trabalho do Artigo 29º, trata-se de um grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de aplicação do RGPD).

4.2 Reflexão – Qual o verdadeiro impacto causado pelo RGPD?

A entrada em vigor do RGPD levou à realização de projetos semelhantes em larga escala tanto em Portugal como na União Europeia. Os projetos de *assesment* representam uma forma de mostrar ao Regulador que a empresa tem *awareness* da importância do Regulamento e da sua implementação. No entanto, a avaliação da situação atual é

apenas o primeiro passo para o cumprimento das normas. Para implementar na prática todas as recomendações resultantes desta avaliação são necessários grandes investimentos económicos, tecnológicos e de capital humano com conhecimento necessário. Assim, o RGPD apresenta várias oportunidades para o mundo empresarial (ver capítulo 2.3 – O impacto do RGPD nas organizações), entre as quais:

- A criação de novos cargos – por exemplo, o DPO que deve ter conhecimentos de legislação e também de tecnologia de informação.
- O desenvolvimento dos sistemas de informação empresariais, que podem não só ajudar a cumprir os requisitos regulamentares, mas também inovar, simplificar e melhorar os processos de negócio existentes.
- Otimização dos processos de negócio. Um dos fatores críticos de sucesso na implementação do RGPD é o conhecimento do fluxo dos dados pessoais dentro da organização (ver capítulo 2.2 – O ciclo de vida dos dados). Para obter a visão geral do ciclo de vida dos dados, é necessário rever todos os processos de negócio existentes, de modo a perceber se existe ou não a utilização de dados pessoais. Assim, as empresas podem alargar esta revisão de processos, de modo a otimizar os processos de negócio já existentes e melhorar a integração entre eles.
- Aumento de vendas, mais concretamente de projetos de *assessment* do cumprimento do RGPD e, posteriormente, de implementação das recomendações.

Não obstante ao supramencionado, a implementação total do RGPD na maioria das organizações em Portugal não foi efetuada até 25 de Maio de 2018. Da minha experiência pessoal, deparei-me com formulários de abertura de conta onde me era indicado que “De acordo com o RGPD devia preencher o consentimento para o uso dos dados pessoais ”. Este consentimento, resumia-se a uma ou duas folhas A4 onde eram descritas as finalidades para as quais os meus dados pessoas iam ser utilizados e no final deveria deixar a minha assinatura. Vamos então analisar esta situação:

1. Não é necessário o consentimento para a recolha e utilização de dados pessoais para finalidades abrangidas pelo contrato. Isto é, se pretendo abrir uma conta

numa companhia de seguros, presumo a partida que irão solicitar os meus dados pessoais como nome, número de identificação, morada, etc. Para as restantes finalidades, não relacionadas com o cumprimento do contrato, eu não "devia" dar o meu consentimento, pois este é uma manifestação de vontade livre.

2. As finalidades de tratamento de dados pessoais são apresentadas de forma agrupada. Assim, não é possível definir as atividades para os quais eu pretendo dar o meu consentimento e para as quais não. Não é cumprido o requisito que indica que o consentimento deve ser distinto, claro e não associado com outros acordos escritos ou declarações.
3. A assinatura que deve ser colocada no final não cumpre o requisito que indica que o consentimento deve ser ativo, ou seja, não se baseia na ausência de resposta, inatividade ou caixas pré-selecionadas.

Esta situação faz-nos perceber que as organizações que implementaram mecanismos de recolha de consentimento, não estão a fazê-lo de acor do comos requisitos regulamentares. Por outro lado, o impacto do RGPD não se resume apenas ao mundo empresarial. Acima de tudo, esta regulamentação pretende proteger os direitos do consumidor final. Na minha opinião, em Portugal existe pouca *awareness* por parte dos consumidores dos direitos que o RGPD lhes oferece. Muitos apenas interpretam o regulamento como "Agora as empresas não podem usar os meus dados pessoais" ou "Já não vou receber mais publicidade". No entanto, todos nós continuamos a receber publicidade e sabemos que as empresas utilizam os nossos dados pessoais e, até agora, houve apenas uma multa no âmbito do RGPD.

Em suma, para a implementação do RGPD ter sucesso é necessário criar *awareness* tanto ao nível dos clientes como a nível dos colaboradores e, depois, gerir a mudança nas organizações (ver capítulo 2.4 – Gestão da Mudança nas Organizações).

Capítulo 5 – Conclusões

5.1 Principais conclusões

Este projeto representa o meu primeiro contacto com o mundo empresarial e aplicação dos conhecimentos teóricos adquiridos ao longo do mestrado na prática. Devido à

inexistência de experiências de trabalho anteriores, muitos aspetos do projeto só se tornaram compreensíveis para mim na sua fase final. Durante a elaboração do relatório final, foi possível obter uma visão geral do trabalho realizado e compreender, assim, a metodologia seguida, a relevância do contacto inicial, com todas as áreas da empresa, realizado em forma de entrevistas, os pedidos de informação realizados, entre os quais, as políticas e procedimentos organizacionais e qual a importância da sua analise.

Considerei o projeto bastante útil, pois permite compreender o fluxo dos dados dentro da organização e consolidar conhecimentos de diferentes áreas, como gestão de dados; gestão de infraestrutura, redes e operações; privacidade e segurança de informação; planeamento organizacional, entre outros. Adicionalmente, este projeto possibilitou a aprendizagem de novos conceitos relacionados com exigências regulamentares.

Visto que se trata de um tema relativamente recente, não existe muita informação e sensibilização tanto a nível teórico como a nível prático por parte dos colaboradores da empresa. Durante as reuniões com os responsáveis pelas áreas de negócio, constatou-se a dificuldade de obter informação, pois a medida que se faziam perguntas relacionadas, por exemplo, com a partilha e armazenamento dos dados pessoais, houve a consciência de que não estavam a ser usados mecanismos de segurança adequados e, por isso, os colaboradores começavam a omitir informações durante os seus relatos. Este aspeto leva a concluir que não existe sensibilização suficiente dos colaboradores para assuntos relacionados com a segurança de informação e privacidade os dados, sendo que apenas os responsáveis das áreas relacionadas com sistemas de informação estão cientes dos riscos associados.

5.2 Lições aprendidas

O projeto permitiu-me, em primeiro lugar, desenvolver capacidades de trabalho em equipas multifacetadas; melhorar a comunicação escrita e oral, através da realização de entrevistas, envio de *e-mails* e comunicação direta com os colaboradores da empresa e elementos da equipa.

Aprendi que o sucesso do projeto está relacionado com dois fatores: a comunicação e o planeamento.

É importante partilhar o nosso ponto de vista, pois muitas vezes o facto de termos uma opinião diferente não significa que esteja errada. Mas mais importante ainda é ouvir e aceitar a opinião / crítica dos outros membros de equipa. A comunicação é crucial para o sucesso de qualquer projeto e deve ser feita entre os membros de equipa, com os responsáveis pelo projeto, com o cliente.

Outro aspeto fundamental é o planeamento, que deverá ser feito de forma detalhada no início e ajustado no decorrer do projeto. A realização de pontos de situação regulares ajuda a descobrir as dificuldades, a alinhar as expectativas de todos os *stakeholders* e a ajustar o tempo estimado para a conclusão de diferentes tarefas.

Por último, melhorei as minhas capacidades de gestão de tempo, pois tinha tarefas diárias e semanais que tinham de ser cumpridas.

5.3 Oportunidades de melhoria em projetos futuros

Dada a pouca experiência de trabalho que possuía durante a realização deste projeto, consegui identificar apenas duas oportunidades de melhoria.

Primeiramente, considero que o projeto poderia ser desfasado no tempo. Ou seja, seriam realizadas entrevistas para conhecer a organização e elaborar a lista de pedidos de informação. Posteriormente, a equipa saía de campo para dar tempo à empresa de recolher a informação solicitada e, posteriormente, a equipa regressava para fazer a análise. Este desfasamento otimizava a alocação dos recursos, aumentando o tempo de trabalho útil das equipas.

Em segundo lugar, a equipa de trabalho devia entrar em contacto direto com os responsáveis por cada área de negócio. A existência de um interlocutor por parte da organização é relevante numa fase inicial, em que não se tem um conhecimento da organização. No entanto, na fase de análise de informação surgem muitas dúvidas relacionadas com áreas específicas de negócio e a comunicação realizada via um ponto de contacto único dificulta e atrasa bastante a progressão do projeto.

Não obstante ao supramencionado, o projeto foi concluído com sucesso.

5.4 Questões de investigação futura

Visto tratar-se de um tema relativamente recente e com um grande impacto tanto a nível empresarial como ao nível dos consumidores, surgem várias questões que podem ser abordadas em investigações futuras. Estas poderão basear-se em:

- Avaliar qual o impacto do RGPD ao nível dos clientes / consumidores.
- Formas de implementação das recomendações apresentadas no presente trabalho.
- Avaliar o nível de maturidade global das empresas em Portugal face ao cumprimento do RGPD.
- Avaliar o tempo estimado de implementação do RGPD nas organizações de acordo com o sector de atividade em que operam / dimensão da empresa.
- Novas oportunidades e formas de crescimento do negócio com a implementação do RGPD.
- Definir uma metodologia / *framework* que permita ao Regulador avaliar o cumprimento das normas do RGPD numa organização.

Capítulo 6 – Referências Bibliográficas

Alter A. E. (1990), "The corporate make-over", CIO, 4, 3, 32-42.

Article 29 Data Protection Working Party (2017), "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", 17/EN, WP 248.

Bertino, E. (2015). Big Data – Security and Privacy. In Proceedings – 2015 IEEE International Congress on Big Data, Big Data Congress 2015.

Baškarada, S. & Koronios, A. (2014), "A Critical Success Factor Framework for Information Quality Management", Information Systems Management, 31 (4), 276 – 295.

Cummings T. (2004), "Organization development and change: foundations and Applications", Dynamics of Organizational Change and Learning, 23—42.

COBIT 5 (2012), "Business Framework for the Governance and Management of Enterprise IT", USA.

Davenport T.H. (1993), "Process Innovation: Reengineering Work Through Information Technology", Boston: Harvard Business School Press.

Fazendeiro A. (2017), Regulamento Geral Sobre a Proteção de Dados, 1 ed., Edições Almedina.

Givens, B. (2000). Identity theft: How it happens, its impact on victims, and legislative solutions. Written testimony for the U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information, 109th Congress.

Hoffer, Venkataraman, R. & Topi, H. (2016), Modern Database Management, 12 ed., Pearson.

Hammer M. & Champy J. (1993), "Reengineering the Corporation", New York: HarperCollins.

Jordan A. & Sowerby M. (2016), "Preparing for the General Data Protection Regulation – Digest", Information Security Forum Limited.

Kettinger W. J. & Grover V. (1995), "Special Section: Toward a Theory of Business Process Change Management", Journal of Management Information Systems, 12:1, 9-30.

Laudon, K. C. & Laudon J. P. (2014), Management Information Systems, 13 ed., Pearson.

Mathieson K. (1991), “Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior”, Information System Research, vol. 3 nº. 2, 173-91.

Romanosky S. & Telang R. & Acquisti A. (2011), “Do Data Breach Disclosure Laws Reduce Identity Theft?”, Public Policy Analysis and Management, 10. 1002 / pam.

Regulamento Geral sobre a Proteção de Dados (UE) 2016/679, do Parlamento Europeu e do Conselho.

Siponen T. M. (2000), "A conceptual foundation for organizational information security awareness", Information Management & Computer Security, Vol. 8 Iss

Senn J. (1991), “Reshaping business processes through reengineering”, SIM Network, 2, 4 – 7.

Thomson, M. E. & Von S. R. (1998), “Information security awareness: Educating your users effectively”, Information Management and Computer Security, vol. 6, 167 – 173.

1, 31 – 41.

Weber, R. H. (2010), “Internet of Things - New security and privacy challenges”, Computer Law and Security Review, 23 – 30.

Anexos

Anexo 1.1 – Matriz de Risco para sistemas de informação, recursos humanos e operações

						Sistemas de Informação	Recursos Humanos	Operações
I. Riscos associados ao ciclo de vida dos dados	40 %	I. Recolha de dados	25 %	I. Sem justificação para a recolha	3 %	4	3	1
				II. Volume de dados recolhidos	3 %	4	4	1
				III. Volume de pessoas com dados recolhidos	3 %	4	2	1
		II. Utilização de dados	25 %	I. Utilização dos dados com erros	1 %	1	1	1
				II. Utilização dos dados para além das expectativas do indivíduo	1 %	3	2	1
				III. Utilização que não é razoável de acordo com as normas sociais	1 %	1	1	1
				IV. Utilização dos dados sem justificação	1 %	3	2	1
				V. Processamento de dados sensíveis	1 %	1	2	1
				VI. Processamento de dados de pessoas vulneráveis	1 %	2	1	1
				VII. Processamento automatizado de dados/ *profiling*	1 %	1	1	1
				VIII. Processamento de dados que originem	1 %	1	1	1

				transferências internacionais				
				IX. Volume de terceiras partes que acedem aos dados	1 %	4	3	1
				X. Processamento de dados com novas tecnologias	1 %	3	2	1
				XI. Novo processamento de dados	1 %	2	1	1
		III. Gestão da divulgação de dados	25 %	I. Perda de dados	3 %	1	2	1
				II. Alteração de dados	3 %	1	1	3
				III. Roubo de dados	3 %	1	2	1
				IV. Comunicação ou acesso não autorizado de dados	3 %	1	2	1
		IV. Retenção e eliminação de dados	25 %	I. Armazenamento de informação inadequada, desnecessária ou desatualizada	3 %	1	2	1
				II. Armazenamento de informação sem mecanismos de segurança adequados	3 %	2	2	2
				III. Destruição acidental dos dados	3 %	1	1	1
Subtotal						21%	20%	12%
						52%	50%	30%
II. Impactos de um breach no manuseamento dos dados	60 %	I. Dano tangível	40 %	I. Dano físico	8 %	3	1	1
				II. Dano de propriedade intelectual	0 %	0	0	0

				III. Perda financeira/ económica	8 %	3	1	1
				IV. Perda de liberdade de circulação	8 %	3	1	1
		II. Dano intangível	60 %	I. Roubo de identidade/Fraude	9 %	3	2	1
				II. Perda de controlo sobre os próprios dados	9 %	3	2	1
				III. Intrusão inaceitável na vida pessoal (vigilância excessiva)	9 %	4	1	1
				IV. Dano que reprima ação/ cause discriminação	9 %	2	1	1
Subtotal						45%	20%	15%
Total						75%	33%	25%

Tabela 2 - Matriz de Risco para sistemas de informação, recursos humanos e operações

Anexo 1.2 – *Data Protection Impact Analysis* para sistemas de informação

1. Identificar necessidade do DPIA - Sistematização das razões pelo qual um determinado tratamento de dados é considerado de alto risco:

- Recolha de um elevado volume de dados envolvendo um grande número de indivíduos.
- Os dados são bastante exaustivos e podem ser utilizados para além das expectativas dos indivíduos, nomeadamente de pessoas vulneráveis (p.e. crianças).
- Elevada exposição/processamento de dados por terceiros, nomeadamente:
  - Realização de extrações de bases de dados por terceiros;
  - Inexistência de contrato específico para serviço de infraestrutura.
- Não existe modelo de governação de dados pessoais nem a política de classificação de informação.
- Armazenamento e partilha de informação sem mecanismos de segurança adequados, nomeadamente:
  - Existem muitos pedidos de extrações informais de dados que são solicitadas diretamente ao prestador externo de serviços relacionados com TI;
  - A informação da Entidade *Random* encontra-se armazenada fora de Portugal;
  - Os serviços de *data masking* são fornecidos por terceiros;
  - Os ecrãs do sistema *core* não limitam a visualização de dados de leitura de acordo com o nível de permissões;
  - As comunicações no Skype estão abertas a todas as federações e a contas individuais / pessoais;
- A ocorrência de um *breach* de segurança destes dados que são bastante exaustivos pode resultar em perdas financeiras / económicas ou tentativa de fraude.

3. Identificar riscos de privacidade - Identificação dos riscos pela sua origem, natureza e particularidade.

Circulação de dados	Não aplicável
Licitude e lealdade do tratamento de dados pessoais	Não aplicável
Finalidade	Não são claras as finalidades da recolha / utilização de dados pessoais. Não é solicitado o consentimento explícito de acordo com as finalidades.
Adequação e exatidão	Não existe transparência suficiente a nível dos conhecimentos dos direitos dos titulares dos dados. Não são claras as finalidades da recolha / utilização de dados pessoais.

Direitos e transparência	Não existe transparência suficiente a nível dos conhecimentos dos direitos dos titulares dos dados. Falta de simplicidade e objetividade nos procedimentos implementados para exercer os direitos dos titulares. Não são claras as finalidades da recolha / utilização de dados pessoais. Não estão implementados procedimentos para garantir que os titulares dos dados podem exercer o seu direito ao apagamento dos dados pessoais, à limitação do tratamento de dados pessoais, à portabilidade de dados pessoais e de oposição a decisões individuais automatizadas.
Segurança	Acesso não autorizado a informações confidenciais por lacuna na definição de classificação dos dados.
Conformidade	A política de privacidade não se encontra atualizada com as normas do novo regulamento, pelo que os dados podem estar a ser recolhidos de forma não justificável. A Entidade *Random* pode estar a utilizar dados para fins estatísticos e em promoções e ações de *marketing* direto, sem que tenha sido devidamente autorizado pelo titular dos dados. Por não estar em conformidade com o novo regulamento, a Entidade *Random* está sujeita às coimas previstas (até 20M ou 4% do volume de negócios anual).
Conservação	Não se encontra definida uma política de conservação de dados pessoais, bem como os períodos de retenção dos dados (*backups*) estão apenas definidos para a aplicação core.
Fornecedores	Não aplicável
Transferência de dados pessoais	Não aplicável
Categorias especiais de dados pessoais	Utilização dos dados que não estejam de acordo com a finalidade para a qual tenham sido recolhidos.
Definição de perfis	Não aplicável
Análise alargada de dados ("*Data analytics*")	Não aplicável
Gestão de incidentes	Não aplicável
4. Identificar soluções de privacidade - Medidas previstas para mitigação dos riscos já identificados	
Circulação de dados	Não aplicável
Licitude e lealdade do tratamento de dados pessoais	Não aplicável
Finalidade	Rever os diferentes formulários de clientes e garantir que é solicitado o consentimento positivo e explícito para as diferentes finalidades de tratamento, bem como garantir que são respeitados os princípios da minimização de dados.

Adequação e exatidão	Implementar procedimentos de minimização de dados (quando se remete informação para as respetivas áreas). Garantir que a recolha de informação é justificada. Garantir procedimentos de atualização de informação (alteração de morada, contactos, validação de e-mail, etc.).
Direitos e transparência	Rever os formulários para incluir informação clara acerca dos direitos dos titulares e das finalidades para a recolha / utilização de dados pessoais. Garantir que os procedimentos implementados asseguram a facilidade de exercício dos direitos pelos titulares de dados. Implementar procedimentos para garantir que os titulares dos dados podem exercer o seu direito ao apagamento dos dados pessoais, à limitação do tratamento de dados pessoais, à portabilidade de dados pessoais e de oposição a decisões individuais automatizadas.
Segurança	Classificar para todos os blocos de informação as suas finalidades de tratamento. Garantir que a classificação de dados (i.e. dados gerais, dados protegidos, dados restritos) é aplicada a todos os blocos de informação e diferenciado de acordo com as funções e responsabilidades. Encriptar todos os dispositivos utilizados pela Entidade *Random* (i.e.. computadores pessoais, telemóveis, pens). Restringir o acesso remoto às plataformas internas através de mecanismos seguros (por exemplo, utilização de VPN). Garantir que todos os colaboradores possuem contratos com cláusulas de confidencialidade.
Conformidade	Atualizar as políticas e procedimentos de acordo com as normas do novo regulamento. Rever o consentimento explícito pelo titular dos dados de acordo com as finalidades autorizadas.
Conservação	Definir uma política de retenção de dados, que estabeleça de forma clara e detalhada o início do período de conservação (i.e. retenção a partir da recolha, retenção após cessação de contrato, etc.), mecanismos de conservação (*tape*, *online*, *cloud*, etc.), entre outros. Alinhar o período de retenção dos dados, para todas as aplicações, com as exigências regulamentares.
Fornecedores	Não aplicável
Transferência de dados pessoais	Não aplicável
Categorias especiais de dados pessoais	Garantir que o titular dos dados tem conhecimento da finalidade de tratamento dos dados.
Definição de perfis	Não aplicável
Análise alargada de dados ("Data analytics")	Não aplicável
Gestão de incidentes	Não aplicável

Tabela 3 – *Data Protection Impact Analysis* para sistemas de informação

Anexo 1.3 – Exemplos de *Gaps* Identificados por Domínio de Maturidade

GAP 1 – Estratégia de privacidade

São poucas as áreas da Entidade Random que utilizam dados para fazer *profiling* e têm vindo a iniciar discussões relativamente a este tema de forma a criar *awareness.* No entanto, a organização não possui mecanismos que garantam que o uso de dados pessoais para *profiling* é adequado, nomeadamente a respetiva comunicação ao titular de dados.

A Entidade Random ainda não nomeou um Encarregado de Proteção de Dados (DPO) que será responsável por promover e monitorizar o cumprimento dos temas associados ao RGPD, de acordo com o artigo 37º e 39º.

Existem políticas na temática de privacidade (código de conduta, política de privacidade de dados, entre outros), no entanto, as mesmas não se encontram totalmente alinhadas com os requisitos do RGPD.

Não existe um conhecimento claro da circulação dos dados pessoais, desde a sua recolha, utilização, armazenamento, divulgação até à sua eliminação.

A Entidade Random carece de processos e procedimentos necessários para cumprir o RGPD nos domínios avaliados, tais como processos e procedimentos associados à função de DPO e aos reportes regulamentares, gestão da perceção pública, classificação de dados, gestão de dados externos e gestão da segurança dos dados. Adicionalmente, alguns dos processos e procedimentos existentes carecem de uma revisão de forma a assegurar o cumprimento com o regulamento, nomeadamente no que respeito ao requisito do *privacy by design and by default.*

GAP 2 - Política de privacidade

A Entidade Random possui várias políticas e procedimentos, nomeadamente código conduta, código de ética*, clean desk policy*, políticas e procedimentos de gestão reclamações, política de privacidade do *site*, política de *cookies*, procedimento de confidencialidade com fornecedores, entre outras. Porém, não possui um normativo

completo necessário para garantir o cumprimento das normas de privacidade exigidas pelo RGPD.Ainda não foi discutida a revisão destas políticas, embora a organização esteja consciente de que será necessário proceder a uma revisão da documentação.

Não se encontra implementado nenhum mecanismo de monitorização do cumprimento da política de privacidade, nem de avaliação da eficácia da implementação da mesma.

A organização não possui procedimentos concretos que permitam materializar as regras definidas ao nível das políticas de privacidade, nem reviu os procedimentos relativos aos dados pessoais que estão atualmente implementados na organização.

A Entidade Random não reviu os seus planos de formação para incluir a temática do RGPD na esfera de ações de formação obrigatórias para os colaboradores que lidem com dados de natureza pessoal.

A Entidade Random ainda não implementou procedimentos para a comunicação dos impactos do incumprimento de questões relacionadas com a privacidade dos dados aos colaboradores, fornecedores e outras partes interessadas, de modo a que estas compreendam os impactos decorrentes do mesmo.

***GAP* 3 - Formação e sensibilização**

A Entidade Random não oferece nenhuma formação obrigatória aos funcionários de modo a consciencializá-los da importância da privacidade e proteção de dados, bem como das respetivas responsabilidades associadas.

Na formação *on boarding* são comunicadas boas práticas de *clean desk policy*, medidas de autoproteção - *security and safety*, boas práticas de *passwords*, entre outras. No entanto, os recursos *outsourced* não estão abrangidos por esta formação.

Durante a sessão *on boarding*, em caso de incidentes de segurança e como boa prática, os colaboradores são instruídos para contactar a área de segurança, no entanto, estes temas são abordados de forma superficial apenas para *awareness* dos colaboradores.

***GAP* 4 - Reporte regulamentar**

A Entidade Random não possui um procedimento formal para recolher, tratar e gerar relatórios que respondam às solicitações de informação emitidas pela autoridade de controlo, no âmbito da nova regulamentação do RGPD, nomeadamente:

- Responsabilidades do controlador, controladores conjuntos e processadores envolvidos no processamento;
- Objetivos pretendidos para cada processamento de dados pessoais;
- Medidas e salvaguardas previstas para proteger os direitos e liberdades dos cidadãos em causa;
- Detalhes de contato do DPO;
- Resultados das Avaliações de Impacto de Privacidade (DPIA);
- Qualquer outra informação solicitada pela Autoridade de Supervisão.

A Entidade Random não tem ainda definidos canais de comunicação internos que permitam reportar ao Conselho de Administração os relatórios formais antes de estes serem entregues à autoridade de controlo, no âmbito do RGPD.

***GAP* 5 - Gestão da segurança dos dados**

A Entidade Random possui política e procedimentos formais de gestão de incidentes que descrevem como gerir incidentes de violação de privacidade, contudo não estão em plena conformidade com as exigências de RGPD, por exemplo, relativamente à necessidade de cumprimento dos prazos de notificação à autoridade de controlo estipulados de 72h após o responsável pelo tratamento ter tido conhecimento de uma violação de dados pessoais.

Nem sempre são feitas as diligências necessárias antes de contratar um terceiro que tenha acesso a dados pessoais e não se encontra definido um procedimento para imputar responsabilidades a terceiros se a violação da privacidade ocorrer durante o tratamento realizado por estes.

A Entidade Random carece de mecanismos que garantam que os seus *stakeholders* estão cientes das suas responsabilidades e das possíveis repercussões da violação ou não cumprimento das exigências relacionadas com a privacidade e a proteção dos dados pessoais.

Não são realizadas auditorias e acompanhamento a terceiros para monitorizar o seu cumprimento com as condições do regulamento, embora alguns contratos prevejam cláusulas de responsabilização pelo incorreto processamento dos dados pessoais.

***GAP* 6 - Classificação de dados**

A Entidade Random não possui políticas e procedimentos que:

- Definam claramente o que são dados pessoais de identificação e o que são categorias especiais de dados, conforme estabelecido no RGPD;
- Definam as regras de classificação dos dados estruturados e não estruturados.

Apesar de o modelo de governação definir o conceito de classificação de dados, não se encontra definida a aplicação desta classificação a todos os blocos de informação da organização, que permita diferenciar o acesso aos dados de acordo com as funções e responsabilidades.

***GAP* 7 - Recolha de dados adequados**

A Entidade Random notifica os titulares sobre a utilização dos seus dados pessoais, contudo esta comunicação não é aplicada transversalmente em toda a organização nem está totalmente alinhada com as normas de RGPD.

A Entidade Random não recolhe consentimentos através de ato positivo, claro, que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito.

Não existem procedimentos implementados que permitam aos titulares dos dados retirar o seu consentimento ou opor-se ao tratamento de dados pessoais que lhes digam respeito.

***GAP* 8 - Uso relevante dos dados**

A Entidade Random não possui um processo formalizado para identificar e registar as condições de processamento, nem implementou procedimentos para verificar se o processamento posterior dos dados está de acordo com as finalidades para as quais estes foram recolhidos.

***GAP* 9 - Retenção e eliminação apropriada**

A organização não possui uma política formalmente definida de retenção e eliminação de dados. Adicionalmente, não se encontra implementado um processo que garanta que:

- Os dados são mantidos apenas nos prazos necessários;
- A pessoa em causa foi informada dos respetivos períodos de retenção dos seus dados;
- Os terceiros que efetuam serviços de armazenamento de dados e documentação respeitam os períodos de retenção definidos.

A Entidade Random não realiza pseudonimização de dados, nem possui mecanismos de cifragem que possibilitem proteger todas as bases de dados, dispositivos móveis, bem como a partilha de dados com entidades terceiras.

***GAP* 10 - Exigências regulamentares**

A Entidade Random não nomeou nenhum DPO, nem definiu o modelo de governo associado a esta nova função na organização, nomeadamente responsabilidades, mecanismos de articulação com as restantes áreas da organização.

A Entidade Random deve desenvolver mecanismos que permitam evidenciar à autoridade de controlo de que o DPO age de forma independente, sem receber instruções sobre o exercício das suas tarefas.

A organização não definiu o canal nem os procedimentos para gerir a comunicação com a autoridade de controlo e outras entidades judiciais.

Anexo 1.4 – Exemplos de Recomendações

Definição de programa de formação e sensibilização

Realizar sessões de formação interna que transmitam aos seus colaboradores o conhecimento necessário acerca do RGPD e qual o impacto que este terá na sua atividade.

Revisão das políticas de privacidade

Orientar os quadros diretivos no alinhamento da estratégia corporativa com o RGPD, auxiliando os colaboradores que lidam com dados pessoais no desempenho das suas funções.

Desenho / revisão de processos

Garantir que a Entidade Random cumpre com os novos direito dos cidadãos exigidos pela regulamentação, minimizando os riscos de exposição e incumprimento face aos direitos dos titulares dos dados.

Revisão dos canais de comunicação

Garantir que todos os canais de comunicação da Entidade Random contêm avisos alinhados com RGPD, permitindo notificar os beneficiários do tratamento a dar aos dados pessoais, bem como obter o consentimento de forma explícita.

Gestão Documental

Desenvolver um modelo de gestão documental que permita à Entidade Random classificar os seus documentos, aplicar políticas de retenção de forma transversal e gerir o seu arquivo físico e digital de uma forma eficiente, segura e eficaz. Revisão das políticas relacionadas ao tema de segurança da informação de modo a alinhá-las com os requisitos do RGPD.

Gestão de incidentes

Definir mecanismos que permitam à Entidade Random uma reação rápida e eficaz caso ocorra um incidente relacionado com a perda de dados pessoais.

Gestão de terceiros

Garantir a segurança dos dados pessoais dos seus clientes e beneficiários no decorrer de processamento de dados pessoais por/de entidades terceiras.

Processo de elaboração e monitorização de DPIAs

Implementação de uma ferramenta para descrever o processamento, avaliar a necessidade e proporcionalidade do mesmo, determinar a conformidade com os requisitos do RGPD, ajudar a gerir os riscos para os direitos e liberdades de pessoas singulares, que resultam do processamento de dados pessoais e determinar as medidas apropriadas para abordar esses riscos.