escola superior de tecnologia e gestão
instituto politécnico de leiria

Impacto do RGPD nas Autarquias Locais
Caso de Estudo do Município de Pombal

Mestrado em Administração Pública

Virgínia dos Santos Moderno

Leiria, setembro de 2023

escola superior de tecnologia e gestão
instituto politécnico de leiria

Impacto do RGPD nas Autarquias Locais
Caso de Estudo do Município de Pombal

Mestrado em Administração Pública

Virgínia dos Santos Moderno

Projeto realizado sob a orientação do Professor Doutor Eugénio Lucas

Leiria, setembro de 2023

Originalidade e Direitos de Autor

O presente projeto de mestrado em Administração Pública é original, elaborado unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para o elaborar.

Reproduções parciais deste documento serão autorizadas na condição de que seja mencionada a Autora e feita referência ao ciclo de estudos no âmbito do qual a mesma foi realizado, a saber, mestrado em Administração Pública, no ano letivo 2022/2023 da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, Portugal, e, bem assim, à data das provas públicas que visaram a avaliação destes trabalhos.

Dedicatória

Dedico este trabalho a toda a minha família, que é a minha razão de ser, o meu ponto de partida e de chegada. O vosso apoio incondicional e amor constante foram a âncora que me sustentou ao longo de toda esta jornada.

Um agradecimento muito especial ao meu marido e à minha filha, o vosso amor é a luz que ilumina o meu caminho, obrigada por estarem sempre presentes na minha vida e por serem a minha bússola e a minha maior motivação.

Também à minha irmã e aos meus sobrinhos, por contribuírem para a minha estabilidade e enriquecerem esta minha jornada com o vosso amor e apoio inabaláveis.

Mas esta dedicatória não poderia estar completa sem uma referência àqueles que representam os alicerces que me permitiram ser a pessoa que sou hoje, os meus pais, o meu muito obrigado pelo vosso esforço, dedicação e privações a que se sujeitaram, sempre em prole do bem-estar das vossas filhas.

Agradecimentos

Começo por agradecer ao meu orientador Doutor Eugénio Lucas, por ter aceite esta missão, pela partilha de conhecimentos e por ter estado sempre presente e disponível, ao longo destes meses.

Agradeço, ainda, ao Município de Pombal, na pessoa do Senhor Presidente e amigo Pedro Alexandre Faustino Pimpão dos Santos, pela disponibilização e partilha de toda a informação que tornou possível este trabalho.

Resumo

Este projeto foi desenvolvido no âmbito do Mestrado em Administração Pública, na Escola Superior de Tecnologia e Gestão do Politécnico de Leiria. O trabalho tem como objetivo efetuar uma análise ao caminho percorrido e a percorrer pelo Município de Pombal, ao nível da implementação do Regulamento Geral de Proteção de dados naquela organização.

Inicialmente, aborda-se o essencial do diploma numa perspetiva mais teórica, seguido de uma abordagem mais prática, focada na implementação no Município de Pombal, tendo sempre em presença o contexto das autarquias, com a referência a algumas das problemáticas vividas por estas organizações.

Este trabalho aspira ser um guia, traçando o percurso realizado pelo Município de Pombal, detalhando as principais etapas e metodologias adotadas, bem como as dificuldades encontradas e os desafios superados, com o objetivo de garantir a melhor implementação deste Regulamento. Pretende-se que este trabalho seja um apoio para quem, dentro de uma autarquia local, tenha que lidar com o impacto que a realidade do RGPD trouxe a estas organizações.

A principal conclusão que ressalta do estudo realizado é que a implementação do RGPD no Município de Pombal tem sido um processo contínuo e progressivo, que requer uma constante atualização e monitorização. Enfrentou-se uma série de desafios e obstáculos, mas estes foram também oportunidades para o aperfeiçoamento e reestruturação de processos internos.

Palavras-chave: Regulamento Geral de Proteção de Dados, Autarquias Locais Implementação de RGPD, Privacidade de Dados, Direitos dos Titulares dos Dados, Proteção de Dados Pessoais, EPD (Encarregado de Proteção de Dados).

Abstract

This work aims to analyze the path taken and to be taken by the Municipality of Pombal regarding the implementation of the General Data Protection Regulation (GDPR) in that organization.

Initially, the essential aspects of the regulation are addressed from a theoretical perspective, followed by a more practical approach focused on the implementation in the Municipality of Pombal, always considering the context of local authorities and addressing some of the issues experienced by these organizations.

This work aims to be a guide, tracing the path taken by the Municipality of Pombal, detailing the main stages and methodologies adopted, as well as the difficulties encountered and challenges overcome, with the goal of ensuring the best implementation of this Regulation. It is intended to serve as support for those within a local municipality who have to deal with the impact that the reality of GDPR has brought to these organizations.

The main conclusion that emerges from the conducted study is that the implementation of the General Data Protection Regulation (GDPR) in the Municipality of Pombal has been an ongoing and progressive process, requiring constant updating and monitoring. A series of challenges and obstacles were faced, but they also presented opportunities for improvement and restructuring of internal processes.

Keywords: General Data Protection Regulation, Local Authorities, Implementation of GDPR, Data Privacy, Data Subject Rights, Personal Data Protection, DPO (Data Protection Officer).

Índice

Lista de Figuras

Lista de Tabelas

1. Introdução

*"A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito." (*Considerando (1) do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho). Esta afirmação justifica plenamente a importância da matéria a abordar neste trabalho.

A implementação do Regulamento Geral de Proteção de Dados, como hoje o conhecemos, trouxe algumas mudanças significativas, com um forte impacto nas organizações, que tiveram de se adaptar a esta nova realidade do tratamento dos dados.

Atendendo ao modelo de sociedade em que vivemos atualmente, uma sociedade de informação, que se caracteriza pela fácil partilha e disponibilização de conteúdos, a toda a hora e por todos, a questão da violação constante dos dados pessoais, tornou-se numa ameaça e a sua proteção, um constante desafio.

Por esse facto, esta matéria está longe de ser pacífica e gera, naturalmente, muita preocupação e controvérsia no seio de todas as organizações que têm de a implementar.

Assim e por ser um tema com o qual trabalho diariamente, o mesmo suscita-me particular interesse, tendo visto nele uma oportunidade de desenvolver um projeto, com o objetivo da obtenção do grau de mestre em Administração Pública, na Escola Superior de Tecnologia e Gestão do Politécnico de Leiria.

A escolha deste tema, prendeu-se essencialmente, pelo facto de, no âmbito profissional, contactar com estas matérias, nomeadamente com as várias problemáticas vividas pelas Autarquias Locais em geral e pelo Município de Pombal em particular, tanto ao nível da implementação do próprio RGPD na organização (pois a sua implementação numa autarquia implica um elevado investimento), como ao nível administrativo, quer ainda ao nível tecnológico, na análise e revisão de todos os processos que tratam dados pessoais.

No Município de Pombal tive a oportunidade de integrar a equipa que implementou o RGPD na organização. Este projeto realizado no âmbito deste mestrado, evidencia todo esse trabalho em que participei.

As questões a que este projeto pretende dar resposta são: como adaptar e implementar estes novos procedimentos do RGPD a uma organização pública?; Quais as etapas que se têm de verificar na sua implementação?; Quais as alterações a ser efetuadas na organização?

No Município de Pombal, tal implementação, ocorreu e continua a ocorrer, (por se tratar de uma matéria sempre em constante evolução), por etapas, e a metodologia adotada irá ser apresentada neste projeto, no Capítulo 4 ("Município de Pombal – Metodologia de Implementação").

Ao longo deste trabalho, que é composto por vários capítulos e subcapítulos, iremos começar por fazer uma abordagem ao regime jurídico europeu *(Regulamento Europeu, (UE) 2016/679, aprovado pelo Parlamento Europeu e pelo Conselho de 27 de abril de 2016 e publicado no Jornal Oficial da União Europeia (JOUE), em 04 Maio de 2016)* e ao regime jurídico que adapta a norma europeia ao nosso país *(Lei 58/2019, de 08 de agosto)*. A meu ver, esta abordagem teórica é de suma importância para uma mais fácil compreensão do tema.

Para além disso, tentarei ainda explorar alguns conceitos essenciais que lhe estão inerentes, tais como, o que são de dados pessoais, e quais os princípios gerais que devem nortear o seu tratamento.

Posteriormente seguir-se-á o capítulo sobre o impacto da implementação do RGPD nas Autarquias Locais, onde após uma introdução a esta temática, se fará referência a alguns casos mediáticos que ocorreram em algumas autarquias do nosso país, por falta de cumprimento deste Regulamento.

Seguir-se-á o capítulo, que no nosso entender é o mais importante deste projeto, que é sobre o Município de Pombal, onde se procederá a uma análise mais aprofundada e detalhada de todo o trabalho de implementação deste Regulamento naquela autarquia, (detalhando os cenários em 2018/2019, 2022/2023), abordando as principais alterações implementadas e ainda o impacto das mesmas, nos serviços e na organização em geral, naqueles momentos.

De seguida, far-se-á uma abordagem, mais crítica, de qual será o trabalho futuro a realizar pela organização, por forma a manter-se em *compliance* com o RGPD.

Em conclusão, tentar-se-á responder às questões colocadas inicialmente.

Sendo esta uma matéria relativamente recente, não existindo ainda muita literatura sobre o tema, faz com que os autores de referência, não tenham ainda efetuado análises mais aprofundadas sobre a temática.

Como nos refere, Tamburri (2020) o estado da arte em pesquisas sobre o Regime Geral de Proteção de Dados ainda é escasso e preliminar. Para este autor, a maioria dos estudos concentra-se, essencialmente, em compreender e formalizar trechos do Regulamento para fins de análise de políticas ou em pesquisar modos de formular políticas de privacidade e cibersegurança, em conformidade com o RGPD. Existem já alguns estudos académicos que também analisam o impacto do Regulamento nos negócios e na comercialização de dados na União Europeia e em todo o mundo, como por exemplo, sobre o impacto deste Regulamento nas relações empresariais entre os países da União Europeia e o Brasil, no entanto, não há ainda uma investigação sistemática do mesmo, que beneficie os profissionais e utilizadores abrangidos pelo RGPD.

Poderemos afirmar que o que existe em maior quantidade, são guias práticos, orientações de ajuda para a implementação e artigos científicos sobre as matérias mais controversas do Regulamento, o que torna este projeto ainda mais desafiante, pois o mesmo vai pautar-se, além do mais, pela perceção e análise mais crítica da autora.

Com este projeto pretende deixar-se um contributo relativamente a esta questão, dando alguns exemplos das dificuldades e dos desafios sentidos no Município de Pombal, ao longo do decurso do tempo e onde se percecionou o impacto que o RGPD trouxe às organizações com a sua implementação.

A metodologia de investigação adotada foi a revisão bibliográfica (uma metodologia do tipo qualitativo assente na recolha e análise bibliográfica e documental). Através da consulta de várias obras, artigos, discussões em fóruns, jurisprudência, acórdãos, pareceres e deliberações, respeitante às temáticas do Regulamento Geral sobre a Proteção de Dados, tendo sido efetuada, consequentemente, uma reflexão sobre os mesmos.

2. Regulamento Geral de Proteção de Dados

Segundo Campos, Foz & Gonçalves (2019): *"O RGPD não é um meteoro que tenha caído no mundo do Direito e dos direitos das pessoas. Não é um corpo estranho aos valores e às técnicas do Direito português ou de qualquer outro Direito europeu no âmbito do qual tenha de se aplicar. Não é um "ditado" que se aplique por si próprio sem discussão. Quer o consideremos bem elaborado ou parcialmente incorreto, temos de o acolher, entender e aplicar no âmbito do Direito português, iluminado pelos valores da pessoa. Sem reduzirmos o nosso papel de juristas a uma mera mecânica."* Com esta afirmação, estes autores reconhecem a importância e a relevância do RGPD no contexto legal europeu, realçando a necessidade de haver um entendimento sólido e uma aplicação cuidadosa da matéria, por parte dos juristas, nunca descurando os princípios que lhe estão subjacentes.

Entendem, também estes autores, ser importante integrar o RGPD no direito, situando-o, no "*âmbito, nos valores e nos interesses dos direitos de personalidade, basicamente, no direito à privacidade*."

2.1 Enquadramento jurídico (evolução)

Foi no Séc. XIX, nos Estados Unidos, que a ideia de *privacy* na perspetiva de direito fundamental começou a surgir, com a publicação a 15 de dezembro de 1890, na Harvard Law Review, do artigo de Samuel D. Warren e Louis D. Brandeis, intitulado "*The Right to Privacy.*" Nesse estudo, "*os autores colocam em evidência a ocorrência de transformações sociais, políticas e económicas, bem como o surgimento de novos inventos, como a fotografia, que contribuíram para a ocorrência de violações da vida privada das pessoas"* (Zanini, 2015).

Mais tarde com a Declaração Universal dos Direitos do Homem de 1948 que no disposto no artigo 12.º referia *"Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei",* conheceu-se o primeiro instrumento jurídico que consagrou o direito à privacidade.

No caso de Portugal, a Constituição da República Portuguesa, no n.º 1 do artigo 35.º sob a epígrafe, utilização da informática, refere que *"Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e a sua atualização*.", reconhecendo, assim, a proteção de dados pessoais como direito fundamental, desde a Constituição de 1976, tendo o nosso país sido pioneiro nesta matéria, a nível mundial.

Segundo Gomes Canotilho e Vital Moreira (2014), neste artigo da Constituição da República Portuguesa, encontram-se previstos os direitos de acesso e retificação dos registos informáticos, o direito ao sigilo desses mesmos dados e ainda o direito ao não tratamento de determinado tipo de dados pessoais.

Em 1991 foi publicada a Lei 10/91 de 29 de abril, denominada - Lei da Proteção de dados pessoais face à Informática – e nesta altura, a proteção de dados apenas abrangia os ficheiros informatizados e não os tratamentos de dados manuais, apesar de o quadro legal já se aplicar, quer ao setor público, quer ao setor privado.

Em 1998 é publicada a Lei 67/98 de 26 de outubro - Lei da Proteção Dados Pessoais, que transpôs para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho de 24/10/95, relativa à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Esta Lei veio criar a figura da autoridade nacional de controlo (Comissão Nacional de Proteção de Dados – CNPD) e esteve em vigor até dia 25 de maio de 2018, tendo sido posteriormente revogada pela Lei 58/2019, de 08 de agosto, atualmente em vigor.

O Regulamento Geral de Proteção de Dados da União Europeia (RGPD) ou, em Inglês, GDPR (*General Data Protection Regulation*), é um Regulamento (UE) 2016/679, aprovado pelo Parlamento Europeu e pelo Conselho de 27 de abril de 2016 e publicado no Jornal Oficial da União Europeia (JOUE), em 04 maio de 2016. Tal Regulamento, entrou em vigor a 24/05/2016, no entanto, nos termos do seu artigo 99.º, só se tornou de aplicação obrigatória, em todos os Estados-Membros, a partir de 25 de maio de 2018, volvidos dois anos após a sua publicação (período de transição até à sua implementação total em todos os Estados-Membros), e estabeleceu as regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas na UE, com vista a garantir uma aplicação uniforme, de algumas dessas regras, no espaço da União.

Mais tarde, a 8 de agosto de 2019, foi publicada a Lei 58/2019 que assegurou a execução, na ordem jurídica nacional, do Regulamento da EU 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

2.2 O que são dados pessoais

Uma das mais importantes definições para a compreensão do RGPD, e por isso fundamental para o trabalho desenvolvido neste projeto, é a de "dados pessoais."

Como entendem Tiago Freitas & Pedro Alves (2021), "*A Constituição emprega o conceito "dados pessoais" ao longo do seu artigo 35.º sem nunca o definir. (..) Contudo a Constituição não fornece nenhuma limitação exata do conceito de "dados pessoais", mas faculta algumas pistas."* A Constituição não densificou o conceito de dados pessoais, apenas referiu que dentro dos dados pessoais se teriam de incluir os dados sensíveis e teria de existir relação entre os dados e o seu titular. Assim, no n.º 1 do artigo 35.º da CRP, refere que os dados dizem respeito a cidadãos. No seu n.º 3, refere alguns exemplos de dados pessoais, como os referentes a convicções religiosas, filosóficas, filiação partidária, fé religiosa, etc.

Com efeito, a densificação deste conceito é efetuada no RGPD, definindo no seu artigo 4.º dados pessoais como: "*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."*

Para Menezes Cordeiro (2021), o conceito de dado pessoal é composto por quatro elementos autonomizáveis: (i) qualquer informação; (ii) relativa a; (iii) pessoa singular; e (iv) identificada ou identificável.

Para este autor, o RGPD prevê inúmeras concretizações setoriais do conceito de dado pessoal, como os dados relativos à saúde, os dados biométricos, os dados genéticos, as opiniões políticas, as convicções religiosas, os relativos à vida sexual ou orientação sexual, os dados relacionados com filiação sindical, condenações penais e infrações, etc.

Assim para este autor, *"apesar das diferenças regimentais que surgem associadas a estas diferentes modalidades, todas elas partilham uma base comum."* e essa base comum, passa pelos seguintes elementos*:*

(i) **qualquer informação**, à luz do RGPD, toda a informação é considerada relevante e o conceito de informação pessoal, neste caso, vai muito além do sentido que lhe é atribuído no âmbito dos direitos de personalidade. Neste caso abrange todos os aspetos relativos à nossa pessoa, quer sejam familiares ou sociais, privados ou públicos, físicos ou mentais. A título meramente exemplificativo, a informação pode dizer respeito a nome, data de nascimento, número de cartão de cidadão (elementos identificativos da pessoa), ou sexo, altura, peso, cor dos olhos (caraterísticas físicas), crenças, opiniões, desejos, (considerações íntimas), títulos académicos ou estatutos profissionais (dados profissionais), ou patrimoniais (direitos de propriedade);

(ii) **relativa a**, para ser considerado dado pessoal a informação tem de ser relativa a uma pessoa, ou seja, é a própria pessoa que é *objeto de análise*.;

(iii) **pessoa singular**, apenas pessoas singulares, independentemente da sua nacionalidade ou local de residência (Considerando (14) do RGPD);

(iv) **identificada ou identificável**, identificada, desde que lhe diga respeito diretamente, ou seja, a informação é suficiente para identificar diretamente e inequivocamente uma pessoa, ex: número de cartão de cidadão, impressões digitais. Identificável, sempre que haja uma probabilidade razoável de que se trata de uma pessoa, mas sejam necessárias informações adicionais para o concretizar (artigo 4.º n.1 do RGPD e considerando (26) do RGPD).

Na aceção de Francisco, D. & Francisco S. (2019) "*o teste decisivo para decidir se são dados pessoais para o RGPD ou não, consiste em avaliar se esses dados podem ser usados direta ou indiretamente para identificar uma pessoa. Enquanto o nome de uma pessoa identifica obviamente a mesma, a verdade é que algumas combinações de identificadores indiretos também permitem essa identificação."* Estes autores destacam a importância de avaliar se os dados podem identificar uma pessoa, seja diretamente ou indiretamente, referindo que, para além do nome, outras combinações de identificadores indiretos podem igualmente permitir essa identificação.

Para Miranda & Medeiros (2005), "*Cabem assim neste conceito de dados pessoais, dados ou elementos informativos da mais variada natureza (sinais ou elementos de natureza não convencional, ou convencional, como é o nome da pessoa, dados de natureza*

biométrica, de que fazem parte a identificação da retina, das impressões digitais, e da geometria da mão, dados genéticos, entre tantos outros).” Neste caso, estes autores definem dados pessoais de forma mais abrangente, incluindo outras informações convencionais.

Já para Catarina Sarmento e Castro, no comentário efetuado na Carta dos Direitos Fundamentais da União Europeia, na anotação ao art. 8º, pode ler-se: *“Deste modo, e a título meramente exemplificativo, são dados pessoais, para além do nome ou da morada, outros dados de identificação como o número de identificação civil, de passaporte, da segurança social, de contribuinte, ou de cliente de um estabelecimento comercial, assim como o número de telefone, o e-mail, o IP do nosso computador, uma chapa de matrícula, o valor de uma retribuição, o som da voz registada para permitir o acesso a uma conta bancária, as classificações escolares e curriculum, a história clínica, as dívidas e créditos, as compras que alguém efetua, o registo dos meios de pagamento que utiliza, desde que, por estarem associados a uma pessoa, permitam identificá-la. É também o caso de uma impressão digital, de uma imagem biométrica do rosto, de uma imagem recolhida através do uso de uma câmara, como nos casos da videovigilância, ou de um conjunto de fotografias divulgadas na internet.”* Aqui a autora apresenta diversos exemplos de tipos de dados, ainda mais abrangentes, demonstrando que qualquer informação associada a uma pessoa e que possa identificá-la, seja diretamente ou indiretamente, é considerada um dado pessoal à luz das leis da privacidade e proteção de dados.

No Manual da Legislação Europeia sobre Proteção de Dados da Agência dos Direitos Fundamentais da União Europeia e Conselho da Europa, (2014), refere sobre dados pessoais o seguinte: *“Nos termos do direito da União Europeia, bem como nos termos do direito do Conselho da Europa, considera-se que as informações contêm dados sobre uma pessoa se: essa pessoa estiver identificada nessas informações; ou, essa pessoa, embora não esteja identificada, estiver descrita nestas informações de forma que permita descobrir quem é a pessoa em causa efetuando pesquisas adicionais*.” Assim, segundo o direito europeu, as informações contêm dados pessoais se identificarem diretamente uma pessoa ou permitirem a identificação através de pesquisas adicionais. Essa definição ampla destaca a importância da proteção de dados pessoais nas leis europeias.

No Parecer 4/2007 adotado, sobre o conceito de dados pessoais, pelo Grupo de Trabalho de Proteção de Dados da União Europeia, pode ler-se: “*Relativamente às pessoas “<u>diretamente</u>” identificadas ou identificáveis, o nome da pessoa é, de facto, o identificador*

mais comum e, na prática, a noção de "pessoa identificada" implica na maioria das vezes a referência ao seu nome."

Todas as definições legais de dados pessoais não esclarecem exatamente em que casos se considera que uma pessoa poderá ser identificada. Obviamente, a identificação exige que estejam verificados elementos suficientes para a descrição de uma pessoa, por forma a distingui-la de todas as outras e de a tornar reconhecível enquanto indivíduo. Sendo certo que o nome de uma pessoa é o melhor exemplo desse tipo de elementos descritivos, no entanto em certos casos, outros elementos de identificação poderão produzir o mesmo efeito que o nome, veja-se como exemplo, o caso das figuras públicas, onde poderá ser suficiente mencionar o cargo (por ex. Presidente da República Portuguesa).

2.3 Os princípios subjacentes ao tratamento de dados pessoais

Para Rodrigues & Teves (2020) "*O RGPD acautela a proteção de dados pessoais dos titulares dos dados pessoais através de princípios orientadores que norteiam e enquadram os normativos relativos à proteção de dados pessoais, assim como as situações específicas de tratamento de dados pessoais."*

Assim, o tratamento dos dados pessoais, só poderá ser feito à luz dos princípios orientadores. No artigo 5.º do Regulamento Geral da Proteção de dados (RGPD), são elencados os princípios subjacentes ao tratamento dos dados pessoais. Da análise do leque de princípios que já existiam, antes da entrada em vigor do RGPD, verificamos que houve um reforço de alguns e o surgimento de novos.

É no n.1 alínea a) do referido artigo 5.º, que podemos ler: "*Os dados pessoais são: a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»).*"

Quanto à **licitude**, os dados só podem ser tratados em cumprimento com a lei, ou seja, qualquer dado só pode ser tratado, à luz da lei. Assim, o tratamento será lícito, se fundado numa das alíneas do artigo 6.º n.º 1, do artigo 7.º, e 8.º no que se refere ao consentimento, e no artigo 9.º ou 10.º, do RGPD, caso se tratem de dados pessoais sensíveis ou dados pessoais relacionados com condenações penais ou infrações.

No que toca à **lealdade**, este princípio consubstancia-se na garantia de que o responsável pelo tratamento dos dados, se guia por critérios de equidade. A lealdade impõe uma obrigação de que os dados serão tratados de acordo com o fim a que se destinam e não outro, baseando-se assim, na lealdade entre a organização, que trata os dados, e o seu titular.

No que respeita ao princípio da **transparência,** no considerando (39) do RGPD, pode ler-se: *(...) "A transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. (...) As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento."*

Quanto à **limitação das finalidades**, prevista na alínea b) do artigo 5.º, é fundamental que os dados sejam recolhidos para finalidades determinadas, explicitas, legítimas, e conhecidas aquando da sua recolha. O Considerando (61) do RGPD, concretiza este princípio acrescentando que: *(...) "Sempre que os dados pessoais forem suscetíveis de ser legitimamente comunicados a outro destinatário, o titular dos dados deverá ser informado aquando da primeira comunicação dos dados pessoais a esse destinatário. Sempre que o responsável pelo tratamento tiver a intenção de tratar os dados pessoais para outro fim que não aquele para o qual tenham sido recolhidos, antes desse tratamento o responsável pelo tratamento deverá fornecer ao titular dos dados informações sobre esse fim e outras informações necessárias. Quando não for possível informar o titular dos dados da origem dos dados pessoais por se ter recorrido a várias fontes, deverão ser-lhe fornecidas informações genéricas."* No entanto, o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89º, nº 1 do RGPD (conforme se verá adiante relativamente ao princípio da limitação da conservação).

O Princípio da minimização dos dados, recorda aos responsáveis pelo tratamento e recolha dos dados, que os dados pessoais recolhidos têm de ser adequados, pertinentes e limitados apenas ao necessário, ou seja, ao fim a que se destinam, não podendo ser utilizados para outro fim, ao qual o titular dos dados não tenha consentido, (alínea c) do artigo 5.º do RGPD), (Considerando (39) e (50) do RGPD).

O **Princípio da exatidão**, conforme disposto no artigo 5.º n.º 1, alínea d) do RGPD), implica que os dados recolhidos sejam: "*Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»)"*

As medidas adequadas referidas supra, exigem que o responsável pelo tratamento dos dados, sempre que exigido pelo titular desses dados, tenha as ferramentas necessárias para a prossecução do cumprimento da exatidão e atualização dos dados inexatos, assim como a sua eliminação ou retificação - (Considerando (39) do RGPD), não se podendo no entanto confundir esta obrigação de apagar ou retificar dados incorretos, com os direitos a exigir o apagamento dos dados, corretos ou incorretos, ou a sua retificação, previstos nos artigos 16.º e 17.º do RGPD, respetivamente.

Quanto ao **Princípio da limitação da conservação**, previsto na alínea e) do n.º 1 artigo 5.º do RGPD), que refere, que os dados pessoais devem ser:

"e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»)."

Os princípios da integridade e confidencialidade, remete-nos, nos termos da alínea f) o n.º 1 do artigo 5.º, para que todos os dados pessoais devam ser:

f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»);

No que toca ao **Princípio da Responsabilidade**, o mesmo prevê que o responsável pelo tratamento seja encarregue pelo cumprimento do disposto em todos os princípios previstos no artigo 5.º, n.º 1 do RGPD e referidos anteriormente, e tem de o poder comprovar, conforme previsto no n.º 2 do mesmo artigo. Este n.º 2, representa uma novidade no RGPD, uma vez que se traduz num reforço da conformidade do RGPD, por um lado, o responsável pelo tratamento deve atuar em cumprimento dos princípios elencados no artigo 5.º do RGPD

e por outro, tem o dever de comprovar o seu cumprimento, nomeadamente junto das autoridades de controlo e dos tribunais.

Como já referido, todo o tratamento de dados pessoais terá de ser feito sob a égide destes princípios, mas para que este tratamento seja possível, há que saber distinguir os dados "normais" e os dados "sensíveis".

No que se refere ao tratamento dos designados dados "normais", o artigo 6.º do RGPD estabelece, que tem que se verificar pelo menos uma das condições de licitude para o seu tratamento:

"Artigo 6.º

Licitude do tratamento

1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;

b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;

c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;

e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;

f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança. (...)"

Já nas situações em que ocorram o tratamento de categorias especiais de dados pessoais (dados considerados sensíveis), o artigo 9.º determina, em regra, que o seu tratamento seja proibido, exceto se houver, consentimento explícito do seu titular, se ocorrer para o cumprimento de obrigações laborais, de segurança social e proteção social, se for necessário ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem e exerçam a sua função jurisdicional, se estiver em causa o interesse público (que deve ser proporcional ao objetivo visado), se for para fins médicos, para proteção de

interesses vitais do titular dos dados ou de outro titular em caso de incapacidade, para fins de arquivo de interesse público, de investigação científica, de investigação histórica ou para fins estatísticos, e ainda para atividades legítimas, mediante garantias adequadas, por uma fundação, associação ou outro organismo para fins políticos, filosóficos, religiosos ou sindicais, ou se os dados pessoais tiverem sido manifestamente tornados públicos pelo seu titular.

Mas, quando se fala em interesse público e em interesses, nos termos da alínea e) do artigo 6.º do RGPD, transcrita acima, tem de existir cautela, por forma a que esta invocação não passe a ser tão abstrata e indeterminada, onde possa caber tudo e onde as organizações acabem por se refugiar, para poder aceder a todo o tipo de dado pessoal, sem qualquer escrutínio. Neste sentido (Oliveira, 2020) em "*O acesso à informação na Administração pública, no contexto do regime geral de proteção de dados"* diz-nos:

(…) "É necessário fazer uma interpretação estrita e a uma identificação clara, caso a caso, do interesse público em jogo e da autoridade pública que justifica o tratamento.

Nas palavras de JOÃO CAUPERS, o interesse público é entendido como o "(…) interesse de uma comunidade, ligado à satisfação das necessidades coletivas desta (…)". Paulo Otero, por seu lado, afirma que «O interesse público, tal como o bem comum, consubstancia as aspirações ou as necessidades de uma pluralidade de sujeitos que, consideradas como unidade que transcende a esfera de cada uma das suas componentes singulares, surge como "uma superior síntese" (…) tem sempre de articular, num processo avaliativo de hierarquia de valores, uma "correta compreensão da dignidade e dos direitos da pessoa."

Em jeito de conclusão poderemos afirmar que os princípios referidos supra, estabelecidos pelo RGPD, são os pilares estruturais fundamentais para uma implementação bem-sucedida do Regulamento pelas organizações, estabelecendo uma base sólida para o tratamento adequado dos dados pessoais dos cidadãos da União Europeia.

A implementação adequada desses princípios é crucial para as organizações, pois ajuda a garantir a conformidade com o RGPD, evitando assim sanções financeiras significativas, conforme poderemos verificar adiante no Subcapítulo 3.5 Exemplos Reais. Além disso, ao seguir esses princípios as organizações não estão apenas a cumprir uma obrigação legal, mas também a assumir uma obrigação ética e moral para com os dados pessoais dos cidadãos com quem lidam, ganhando assim a confiança dos seus clientes e demonstrando o seu compromisso em proteger a privacidade dos seus dados pessoais.

Em suma, as organizações devem assumir com responsabilidade e seriedade a implementação desses princípios e incorporá-los nas suas políticas e práticas de proteção de dados no dia a dia, com vista ao sucesso dessa implementação.

2.4 Direitos do titular dos dados

O RGPD estabelece vários direitos para os titulares dos dados, que são as pessoas cujos dados pessoais são recolhidos, armazenados e processados. As organizações, enquanto responsáveis pelo tratamento, têm de implementar e definir, políticas e critérios aplicáveis ao exercício dos direitos pelos titulares de dados, que sejam objeto de tratamento. O objetivo destas políticas é o de auxiliar a organização a garantir aos titulares dos dados o exercício dos seus direitos consagrados pelo RGPD, nomeadamente:

I. **Direito de informação:** (artigos 13º e 14º e considerando 63 e do RGPD) os titulares dos dados deverão ter o direito de aceder aos dados pessoais recolhidos e que lhes digam respeito e de exercer esse direito com facilidade, a fim de conhecer e verificar a tomar conhecimento do tratamento e ainda verificar a sua licitude.

II. **Direito de Acesso**, (artigo 15º do RGPD) os titulares dos dados têm o direito de obter confirmação de, se os seus dados estão sendo processados e, se for o caso, ter acesso a esses dados.

III. **Direito de Retificação**, (artigo 16º do RGPD) os titulares dos dados têm o direito de corrigir quaisquer dados pessoais inexatos que lhes digam respeito.

IV. **Direito ao Apagamento** ("direito a ser esquecido"), (artigo 17º do RGPD) os titulares dos dados têm o direito de solicitar o apagamento de seus dados pessoais, desde que não haja motivo válido para o processamento continuar.

V. **Direito à Limitação do Tratamento** (artigo 18º do RGPD), os titulares dos dados têm o direito de solicitar a limitação do processamento de seus dados pessoais em determinadas circunstâncias.

VI**. Direito de Portabilidade dos Dados** (artigo 20º do RGPD), os titulares dos dados têm o direito de receber os seus dados pessoais em formato estruturado, comumente utilizado e de leitura mecânica, e ter esses dados transmitidos para outro controlador de dados.

VII. **Direito de Oposição** (artigo 21º do RGPD), os titulares dos dados têm o direito de se opor ao processamento de seus dados pessoais, em determinadas circunstâncias.

VIII. **Direito a Retirar o seu Consentimento** (artigo 7º, n.º 3 do RGPD), os titulares dos dados devem ter a possibilidade de revogar o consentimento dado anteriormente para o processamento de seus dados pessoais, no entanto, esta retirada não pode afetar a legalidade do processamento baseado no consentimento concedido anteriormente.

IX. **Direito de não ser submetido a decisões automatizadas** (artigo 22º do RGPD) (aquelas que são tomadas sem intervenção humana, com base em algoritmos e processamento de dados), os titulares dos dados têm o direito de não ser submetidos a decisões baseadas unicamente em processamento automatizado, incluindo a criação de perfis, que produzam efeitos legais que os afetem de forma significativa.

Assim, no que se refere a esta matéria, o RGPD prevê direitos para os titulares dos dados, visando proteger a privacidade e os interesses dos indivíduos. Estes direitos já acima elencados, mesmo que de forma breve, permitem que os titulares dos dados tenham um maior controle sobre como os seus dados são tratados. É importante que os responsáveis pelo tratamento e os subcontratantes informem os titulares dos dados sobre os seus direitos e forneçam meios para que eles possam exercê-los, sendo fundamental que os mesmos sejam respeitados e protegidos para garantir a privacidade e a segurança dos titulares dos dados.

2.5 O responsável pelo tratamento e o subcontratante

No contexto do RGPD, o responsável pelo tratamento é a entidade ou indivíduo que decide, como e por que motivo os dados pessoais serão processados. É também legalmente responsável pelo processamento dos dados pessoais e deve garantir que as disposições do RGPD sejam cumpridas.

Nos termos do n.º 7 do artigo 4.º do RGPD, o responsável pelo tratamento é "(…) *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* (…)".

O responsável pelo tratamento é quem toma as decisões sobre as atividades de tratamento de dados, exercendo controlo total sobre os dados que estão a ser tratados.

No entanto, o responsável pelo tratamento numa organização, na grande esmagadora maioria das situações, não consegue sozinho tratar todos os dados, necessitando de recorrer

a subcontratantes. Esta figura do subcontratante, prevista no artigo 28.º do RGPD, é a empresa ou entidade contratada para processar dados em nome de outra organização, havendo assim lugar a uma subcontratação, e, naturalmente, à necessidade de firmar previamente as regras desta relação jurídica.

De acordo com o n.º 8 do artigo 4.º do RGPD o subcontratante "(…) *trata os dados pessoais por conta do responsável pelo tratamento destes*", agindo, por isso, sob sua autoridade, servindo os seus interesses.

O subcontratante, podendo ser pessoa coletiva, pessoa singular, autoridade pública, agência ou outro organismo, quando trata dados pessoais ultrapassando as instruções do Responsável, será responsável por esse mesmo tratamento de dados (artigo 28º, n.º 10 do RGPD). Um subcontratante pode querer subcontratar a totalidade ou parte do tratamento de dados a outro subcontratante, nesse caso, esta terceira figura será o sub-subcontratante.

Podemos dizer então que, neste contexto, existem dois papéis principais relacionados com o processamento de dados: o do responsável pelo tratamento (controlador de dados) e o do subcontratante (processador de dados). Ambos são responsáveis por estabelecer os objetivos e meios do processamento de dados e de garantir que essas decisões sejam coerentes com as disposições do RGPD.

No caso de uma autarquia, o responsável pelo tratamento é o Município ou a Freguesia e o subcontratante é a entidade que processa dados em nome do responsável pelo tratamento (subcontratante), ele é contratado pelo responsável pelo tratamento para realizar tarefas específicas relacionadas com o processamento de dados. O subcontratante tem obrigações legais específicas, nos termos do RGPD, incluindo a obrigação de proteger os dados pessoais e de cooperar com o responsável pelo tratamento, no cumprimento das suas obrigações legais. O Responsável pelo tratamento apenas pode contratar subcontratantes que (…) *apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos dados."* (vide artigo 28.º n.º 1).

O responsável pelo tratamento deve estabelecer acordos escritos, definindo políticas e procedimentos, com os subcontratantes, para garantir que estes cumpram as disposições do RGPD e protejam os dados pessoais que lhes são confiados, no âmbito das suas funções e que decorrem da relação contratual firmada. Além disso, o responsável pelo tratamento deve monitorizar regularmente o subcontratante, para garantir que ele cumpre as disposições do RGPD e consequentemente, as suas obrigações contratuais.

É no artigo 28.º do RGPD que podemos encontrar a previsão legislativa que estabelece, entre outras, as obrigações dos subcontratantes, e os termos que regulam a relação com o responsável pelo tratamento, no que diz respeito à proteção de dados pessoais.

Esta disposição legal prevê as exigências de, por exemplo:

"O subcontratante não contrata outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral. Em caso de autorização geral por escrito, o subcontratante informa o responsável pelo tratamento de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros subcontratantes, dando assim ao responsável pelo tratamento a oportunidade de se opor a tais alterações." (artigo 28.º n.º 2 do RGPD).

Também na alínea h) do n.º 3 do mesmo artigo 28.º, podemos ler, que o subcontratante:

"h) Disponibiliza ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no presente artigo e facilita e contribui para as auditorias, inclusive as inspeções, conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado. No que diz respeito ao primeiro parágrafo, alínea h), o subcontratante informa imediatamente o responsável pelo tratamento se, no seu entender, alguma instrução violar o presente regulamento ou outras disposições do direito da União ou dos Estados-Membros em matéria de proteção de dados."

Em conclusão, o responsável pelo tratamento e o subcontratante assumem papéis fundamentais na proteção de dados pessoais. Ambos são responsáveis pela proteção dos dados pessoais dos clientes e devem cumprir as regulamentações de proteção de dados aplicáveis. É importante que o responsável pelo tratamento estabeleça acordos claros, através da definição de procedimentos e políticas, com os subcontratantes para garantir a conformidade e a transparência no tratamento dos dados pessoais. É fundamental que o responsável pelo tratamento e o subcontratante trabalhem juntos para garantir a segurança dos dados pessoais e a privacidade dos seus clientes.

2.6 O Encarregado de Proteção de Dados

A existência de uma função chamada Encarregado de Proteção de Dados (EPD) ou *Data Protection Officer (DPO)*, apesar de não ser obrigatória em todas as organizações, é recomendada, em todas as que tratem dados pessoais ou sensíveis.

Esta figura tem o seu regime jurídico previsto nos Artigos 37º, 38º e 39º do RGPD, ficando sujeita ao dever de sigilo e confidencialidade, bem como ao dever de incompatibilidade, não podendo exercer quaisquer funções e atribuições que resultem de um conflito de interesses para o exercício das funções. A ausência de conflitos de interesses está intimamente ligada ao requisito de independência dos EPD. O considerando 97 refere, além disso, que os EPD, *"sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência."*

Mas o conceito de EPD não é novo, a Diretiva 95/46/CE3 não obrigava nenhuma organização a nomear um EPD, mas, ainda assim, a prática da nomeação de EPD tem vindo a desenvolver-se em vários Estados-Membros ao longo dos anos. (Diretiva 95/46/CE do Parlamento Europeu e do Conselho Conselho, 1995).

Assim, a nomeação do EPD, nos termos do artigo 37º, n.º 1, do RGPD, é apenas obrigatória em três situações:

a) sempre que o tratamento seja efetuado por uma autoridade ou um organismo público, com exceção dos tribunais no exercício da sua função jurisdicional;

b) sempre que as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que exijam um controlo regular e sistemático dos titulares dos dados em grande escala;

c) sempre que as atividades principais do responsável pelo tratamento ou do subcontratante compreendam operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações.

Decorre, pois, que as autarquias se enquadram na previsão da alínea a), acima citada, isto é, tem obrigatoriedade de designar um EPD. O artigo 12.º da Lei 58/2019 regula mais concretamente a designação de EPD em entidades públicas.

A designação do EPD deve ser efetuada, em função das competências profissionais da pessoa a designar, a mesma deve deter conhecimentos avançados em matéria de proteção de dados e deve ser capaz de cumprir as tarefas atribuídas no artigo 39º, relacionadas com a segurança e proteção de dados, nomeadamente:

– Sensibilizar e informar todos os que tratem dados pessoais;

– Assegurar o cumprimento das políticas de privacidade e proteção de dados;

– Controlar e regular a conformidade do RGPD;

– Recolher informação para identificar atividades de tratamento, mantendo-as atualizadas;

– Controlar e acompanhar a produção das Avaliações de Impacto sobre Proteção de Dados;

– Realizar a avaliação na exposição aos riscos de violações de privacidade e mitigá-los com ações de melhoramento;

– Controlar o cumprimento de contratos escritos subcontratante;

– Promover formações de boas práticas para a proteção de dados;

– Ser o ponto de contacto com os titulares de dados de forma a esclarecer questões relacionadas com o tratamento dos dados;

– Ser o ponto de contacto com as autoridades de controlo (Portal do DPO[1])

Uma vez que o EPD é quem assume todas as operações de tratamento realizadas pelo responsável pelo tratamento ou pelo subcontratante, idealmente deveria ser alguém com um perfil capaz de conciliar conhecimentos de, pelo menos, três áreas, consideradas fundamentais, a tecnológica, a da gestão e a do direito (legal).

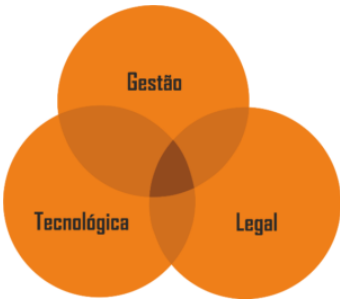


Figura 1: Perfil do EPD - Imagem retirada do site https://www.portaldodpo.pt/funcoes-do-dpo/

A detenção de perfil com experiência nestas três áreas seria, sem sombra de dúvida, uma mais-valia para qualquer profissional desempenhar as suas funções nesta área, com maior qualidade, rigor e competência.

O EPD deve também exercer as suas funções com a máxima independência e ser sempre envolvido de forma adequada e em tempo útil em todas as decisões em matéria de RGPD, apoiado, sempre que possível, por uma equipa multidisciplinar, que reúna competências nas mais diversas áreas (tais como, financeira, direito, recursos humanos, tecnológica, marketing, arquivo, entre outras) fornecendo assim, os recursos necessários para o desempenho das suas funções com a maior competência possível.

O EPD assume, assim, a responsabilidade na aplicação da estratégia para proteção dos dados e conformidade do RGPD. Todas as eventuais não conformidades e incidentes ou

[1] https://www.portaldodpo.pt/funcoes-do-dpo/

violações que ocorrerem serão imputadas ao responsável pelo tratamento, em última instância à administração. Trata-se, por tudo isto, de uma função bastante exigente, mas também bastante aliciante e certamente um perfil muito procurado nos próximos tempos, e assim uma das profissões do futuro.

Para Costa (2017) "*Com a reforma do quadro jurídico europeu em matéria de proteção de dados, os DPOs desempenham um papel importante, uma vez que devem assegurar que as entidades públicas e privadas cumpram as novas decisões em matéria de proteção de dados. É uma posição altamente responsável, especialmente dado o uso generalizado da coleta de dados na sociedade atual."*

Mais adiante, no Capítulo 3 – "Impacto nas Autarquias Locais", abordaremos a problemática da opção de escolha entre um profissional interno ou externo à organização.

2.7 Autoridade de Controlo

As autoridades de controlo são outra das figuras que desempenham um papel importante no cumprimento e na aplicação do RGPD em toda a União Europeia.

Estas entidades são responsáveis por supervisionar o cumprimento das disposições do RGPD pelas organizações e pelos indivíduos no seu país de jurisdição, supervisão essa que inclui a realização de auditorias, mas também está no âmbito das suas competências, dar seguimento às queixas efetuadas e tomar as medidas corretivas quando necessário, com vista ao cumprimento da norma. Às autoridades de controlo cabe também o poder coercivo para aplicar coimas e outras sanções administrativas, nos casos em que as organizações não cumpram as disposições do RGPD.

Mas estas autoridades de controlo também desempenham um papel importante na orientação e na "educação" das organizações e indivíduos sobre as disposições do RGPD, compete-lhes emitir orientações, publicar boas práticas e realizar eventos de sensibilização, para ajudar as organizações a compreender e cumprir as suas obrigações no âmbito do RGPD, o mesmo será dizer que também desempenham uma missão pedagógica. Além disso, as autoridades de controlo atuam também como uma espécie de elo de ligação entre as diversas Autoridades Nacionais e a Comissão Europeia, colaborando e cooperando com outras autoridades de controlo em toda a União Europeia, para garantir uma aplicação consistente do RGPD.

A autoridade de controlo para o cumprimento do RGPD em Portugal, é a denominada, Comissão Nacional de Proteção de Dados (CNPD), que é uma autoridade administrativa independente, responsável por supervisionar o cumprimento das disposições do RGPD no nosso país.

A CNPD é uma entidade administrativa independente, com personalidade jurídica de direito público e com poderes de autoridade, dotada de autonomia administrativa e financeira, que funciona junto da Assembleia da República.

A CNPD controla e fiscaliza o cumprimento do RGPD da Lei 58/2019 e da Lei 59/2019 de 8 de agosto e ainda da Lei 41/2004 de 18 de agosto, bem como das demais disposições legais e regulamentares em matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos dos seus dados pessoais. A CNPD tem poderes regulatórios, fiscalizadores e sancionatórios para assegurar a conformidade com as leis de proteção de dados.

A CNPD age com independência na prossecução das suas atribuições e competências (previstas designadamente nos artigos 57.º do RGPD, 6.º da Lei 58/2019 de 8 de agosto, e 44.º da Lei 59/2019 de 8 de agosto) e no exercício dos seus poderes (cf. Artigos 58.º do RGPD, 8.º da Lei 58/2019 de 8 de agosto, e 45.º da Lei 59/2019 de 8 de agosto).

2.8 Transferências Internacionais

As transferências internacionais de dados pessoais também estão, obviamente, sujeitas à regulamentação do RGPD. Esta é uma matéria de extrema importância e que se reveste de grande sensibilidade dado que exige a convergência de vários ordenamentos jurídicos.

O RGPD é aplicável a qualquer tratamento de dados pessoais realizado por uma organização estabelecida na União Europeia, independentemente de onde o tratamento ocorra. Isso significa que as organizações estabelecidas na União Europeia têm de assegurar o cumprimento das disposições do RGPD, quando transferem dados pessoais para fora do espaço europeu.

Mas a verdade é que, ainda não existe uma uniformização das regras da proteção de dados a nível mundial. Como defende Doneda, (2006) *"Alguns estudiosos do tema apontam, há mais de uma década, para a existência de uma tendência à convergência das regras internacionais sobre proteção de dados. Tomando como força motriz deste fenómeno a forte*

penetração da tecnologia da informação na sociedade moderna, esta convergência é o resultado de atitudes similares a seu respeito, em diferentes países, bem como do reduzido espaço que é destinado às peculiaridades locais."

Efetivamente, não podemos ainda afirmar que existem normas ou tratados de âmbito global que tratem diretamente e de forma eficaz o problema da proteção dos dados, o que temos são normativos de caráter nacional, além de instrumentos internacionais mais restritos a blocos de países, como é o caso da União Europeia.

Doneda, (2006), continua defendendo que: *"A convergência dos modelos de proteção de dados pessoais em direção a um patamar global comum é tido por alguns autores como um passo natural no desenvolvimento da matéria. Os termos nos quais isto poderá ocorrer, porém, são objeto de pura especulação."* Por este motivo é que se constata, que a intenção deste Regulamento de ser um instrumento para a formulação de uma visão unificadora da legislação sobre a proteção de dados, em toda a União Europeia, não terá sido ainda conseguida na sua plenitude, quer ao nível de cada uma das legislações nacionais, quer ainda ao nível da transferência de dados para fora do espaço europeu.

Uma transferência internacional de dados ocorre, quando os dados pessoais são transferidos para um país fora da União Europeia, esta situação pode acontecer, por exemplo, quando os dados são transferidos para um servidor localizado noutro país, quando os dados são compartilhados com uma empresa estabelecida fora da União Europeia, ou quando os dados são transmitidos para um país fora da União Europeia, situações que, com o avanço da tecnologia, são cada vez mais frequentes.

A questão que se impõe é a seguinte: os direitos dos titulares dos dados estão protegidos fora do espaço europeu?

O RGPD estabelece requisitos para garantir que as transferências internacionais de dados sejam realizadas, de forma segura e protejam os direitos dos titulares dos dados, isso inclui a necessidade de uma base legal para a transferência, como o consentimento do titular, um acordo de cláusulas contratuais padrão ou decisões de adequação emitidas pela Comissão Europeia, conforme melhor se verá adiante. Além disso, é ao EPD, de cada organização que cabe supervisionar as transferências internacionais e garantir a conformidade com o RGPD. As organizações devem garantir que os direitos dos titulares dos dados são protegidos e que eles os possam exercer de forma eficaz.

Assim, uma das principais preocupações quando se trata de transferências internacionais de dados é a falta de garantia da proteção de dados no país de destino,

equivalente à existente no país de origem. A transferência de dados pessoais para fora da União Europeia é permitida, desde que sejam tomadas medidas adequadas de proteção de dados, que garantam que os países de destino salvaguardem os direitos dos titulares dos dados, à semelhança do que acontece na União Europeia.

Atualmente, as medidas consideradas adequadas têm passado pela utilização de cláusulas contratuais padronizadas, aprovadas pela Comissão Europeia, (quadro que protege os direitos fundamentais de todas as pessoas na EU, cujos dados pessoais são transferidos para os Estados Unidos e proporciona segurança jurídica para as empresas que recorram às transferências transatlânticas de dados) e pelo estabelecimento de mecanismos de transferência de dados com base em adequação, como foi o caso dos instrumentos denominados "Porto Seguro" e "Escudo de Privacidade UE-EUA" (este último, tratou-se de um acordo político celebrado em 2 de fevereiro de 2016 entre a Comissão Europeia e o Governo Norte-Americano, sobre um novo quadro para o intercâmbio transatlântico de dados pessoais para fins comerciais). Nestes casos, no entanto, acórdãos proferidos pelo Tribunal de Justiça da União Europeia, invalidaram destas decisões de adequação[2], pois o Tribunal de Justiça da União Europeia concluiu, que os EUA violaram os padrões de privacidade estabelecidos pela UE.

Neste sentido, podemos concluir que a transferência de dados para fora da União Europeia, ainda é uma questão controversa, pois muitos países fora da UE não possuem nos seus ordenamentos jurídicos, leis de proteção de dados tão rigorosas quanto as do espaço europeu. Isso pode colocar os dados pessoais dos cidadãos da UE em risco de serem usados de forma indevida ou não autorizada. Além disso, a transferência de dados para países com leis de vigilância mais frágeis, também pode levar a preocupações redobradas, não só em relação à privacidade, mas também em relação a questões de liberdade de expressão.

Um exemplo recente e mediático da problemática existente com a transferência de dados para fora da UE, foi o caso do Facebook e da Google. A estas empresas foram aplicadas coimas pela Comissão Europeia, por não cumprirem as regras de proteção de dados, ao transferir dados de utilizadores da UE para os Estados Unidos. Este incidente ficou conhecido pelo caso Schrems II (Acórdão do Tribunal de Justiça, 2020).

Ainda assim, este tema continua, na ordem do dia, sendo um dos temas da atualidade em matéria de proteção de dados, que está em constante transformação, sempre com o

[2] https://ec.europa.eu/commission/presscorner/detail/pt/IP_16_2461.

objetivo de garantir aos cidadãos que os seus dados pessoais sejam protegidos, mesmo quando são transferidos para países que não têm as mesmas leis de proteção de dados que a União Europeia.

Senão vejamos: ainda no passado dia 27.12.2022 as cláusulas-tipo utilizadas para realização de transferências internacionais, publicadas através da Decisão 2010/87/EU[3], foram atualizadas através da Decisão de Execução 2021/914 da Comissão de 4 de junho de 2021. Esta decisão veio fornecer mais um conjunto de cláusulas contratuais-tipo que podem ser usadas por empresas para transferir dados pessoais para países terceiros que não oferecem um nível adequado de proteção de dados.

Neste mesmo sentido, e no intuito de aumentar a segurança dos dados que circulam, o Comité Europeu para a Proteção de Dados, em 18 de junho de 2021, através da Recomendação 01/2020 adotou medidas complementares aos instrumentos de transferência, para assegurar o cumprimento do nível de proteção dos dados pessoais da UE[3]. Nessa recomendação, os responsáveis pelo tratamento, ou subcontratantes, agindo como exportadores, são responsáveis por verificar, caso a caso, a segurança da transferência internacional de dados, bem como identificar e aplicar as medidas adicionais que entendam adequadas, com vista a garantir tal segurança. Assim, e em atenção ao princípio da responsabilidade, devem estar aptos a comprovar a adoção de tais medidas complementares, sendo recomendável a realização de avaliações de impacto prévias a uma transferência internacional de dados.

Atualmente, as transferências internacionais de dados pessoais para países terceiros ou para organizações internacionais, são realizadas de acordo com as condições estabelecidas no Capítulo V do RGPD, que impõe que tais transferências, somente sejam realizadas, quando seja possível assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo Regulamento. Acresce que, nos casos em que seja inexistente uma decisão de adequação da Comissão Europeia, as transferências internacionais de dados deverão observar as condições enunciadas pelo Comité Europeu para a Proteção de Dados, nas suas Recomendações 01 2020, relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento ao nível de proteção de dados pessoais da UE versão 2.0 (adotado em 18 de junho de 2021, citada supra).

[3] EDPB_Recommendations_202001(Vo.2.0)_PT.docx (europa.eu)

2.9 RATs – Registo de Atividades de Tratamento

Os Registos de Atividades de Tratamento, estão previstos no artigo 30.º do RGPD e são uma ferramenta utilizada para documentar e registar as atividades relacionadas com o tratamento de dados pessoais. São uma exigência que tem como objetivo, garantir que a organização cumpre com as suas obrigações de conformidade, bem como, permite que a CNPD ou outra autoridade de controlo, possam verificar se a organização está a cumprir com as regras do Regulamento.

De acordo com o artigo 30.º do RGPD *"cada responsável pelo tratamento (...) conserva um registo de todas as atividades de tratamento sob a sua responsabilidade..."*, sendo que, *"o subcontratante (...) conserva um registo de todas as categorias de atividades de tratamento realizadas em nome de um responsável pelo tratamento (...)"*.

Estes registos devem conter informações como:

- Identificação da entidade responsável pelo tratamento, e sendo caso disso, do EPD;
- As finalidades do tratamento;
- A descrição das categorias de dados pessoais tratadas;
- A descrição das categorias de indivíduos a quem os dados se referem;
- As categorias de destinatários a quem os dados foram ou serão divulgados;
- As transferências de dados pessoais para países terceiros ou organizações internacionais;
- Os prazos de conservação dos dados;
- As medidas técnicas e organizacionais implementadas para garantir a segurança do tratamento;
- O fundamento de licitude para o tratamento

A obrigação de manter um registo de todas as atividades de tratamento aplica-se aos Responsáveis pelo Tratamento ou Subcontratantes que tenham pelo menos 250 trabalhadores. No entanto, determinadas organizações que tenham menos de 250 trabalhadores têm de manter, igualmente, um registo sempre que o tratamento de dados efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, o tratamento não seja ocasional e abranja as categorias especiais de dados a que se

refere o n.º 1 do artigo 9.º do RGPD, como sejam os dados de saúde, dados biométricos, dados de origem racial ou étnica, opiniões políticas ou filosóficas, dados genéticos ou dados pessoais relativos a condenações penais e ou outras infrações, conforme referido no artigo 10.º RGPD.

Esta obrigação, tem como objetivo poder demonstrar de forma fácil e ágil a existência do levantamento das várias atividades de tratamento. Manter estes registos atualizados, a par com a existência de EPD, acaba por ser a forma de demonstrar a conformidade com a lei perante nas Autoridades de Controlo.

Como nos diz Fazendeiro (2018) "*Isto é, as entidades que procedem ao tratamento dos dados pessoais devem manter um registo atualizado desses tratamentos, por forma a poderem demonstrar em qualquer momento, e de forma transparente, o cumprimento da lei."* Esta atualização constante das atividades de tratamento é obrigatória, uma vez que as consequências do não cumprimento do artigo 30.º do RGPD, determina que a organização que esteja obrigada a manter o registo de atividades de tratamento, fique sujeita à aplicação de coimas até € 10M ou até 2% do seu orçamento anual, nos termos do n.º 4 do artigo 83.º do RGPD.

A Autoridade de Controlo (CNPD) disponibiliza modelos *standard*[4], para facilitar o cumprimento destas obrigações pelos responsáveis pelo tratamento.

2.10 Avaliações de Impacto

Segundo Kloza (2017), as avaliações de impacto surgiram da necessidade de lidar com a incerteza e o risco associados aos novos perigos para as questões sociais. Estas avaliações proliferaram em áreas, que vão desde avaliações de impacto ambiental, até à proteção de dados pessoais e privacidade. As avaliações de impacto de privacidade e de proteção de dados surgiram nos anos 90 e foram adotadas de formas diferentes e em vários níveis de obrigatoriedade em diferentes países.

O artigo 35.º do RGPD introduz o conceito de Avaliação de Impacto sobre a Proteção de Dados (AIPD). Segundo as Orientações relativas à AIPD e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento (UE) 2016/679, adotadas em 4 de abril de 2017, revistas e adotadas pela última vez em 4 de outubro de 2017, do Grupo de Trabalho 29:

[4] https://www.cnpd.pt/organizacoes/obrigacoes/registo-de-atividades-de-tratamento/

"Uma AIPD é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos. As AIPD são instrumentos importantes em matéria de responsabilização, uma vez que ajudam os responsáveis pelo tratamento não apenas a cumprir os requisitos do RGPD, mas também a demonstrar que foram tomadas medidas adequadas para assegurar a conformidade com o regulamento." (Grupo de Trabalho do Artigo 29.º 2017). Em resumo, comprova-se que as AIPD são uma parte essencial da governança de dados, pois não auxiliam apenas na garantia da conformidade com o RGPD, mas também promovem a transparência e a responsabilidade, ao avaliar e gerir os riscos associados ao tratamento de dados pessoais.

Como nos refere também Fazendeiro (2018) "*Uma avaliação de impacto consiste, em traços gerais, numa avaliação levada a cabo pelo responsável pelo tratamento de dados para identificar e minimizar os riscos por incumprimento das regras de proteção de dados."*

Por outras palavras, uma AIPD é um processo que visa estabelecer e demonstrar a conformidade e guiar a realização do procedimento da AIPD e a mesma justifica-se, sempre que o tratamento seja suscetível de resultar num elevado risco para os direitos e as liberdades das pessoas.

As organizações devem adotar procedimentos e políticas que definam as medidas necessárias para fazer face ao risco, incluindo medidas de segurança e procedimentos de proteção dos dados pessoais, descrevendo as operações de tratamento previstas e as finalidades das mesmas, avaliando a necessidade e a proporcionalidade desse tratamento em relação aos objetivos, avaliando e gerindo os riscos associados aos direitos e às liberdades dos titulares dos dados.

Ao implementar estas políticas e procedimentos, o objetivo é auxiliar as organizações a perceber o que é uma AIPD, os casos em que é obrigatória a sua realização, em que momento a devem fazer, que metodologias devem ser seguidas e que partes devem intervir neste procedimento, com o intuito de abordar e mitigar os riscos identificados e demonstrar a conformidade com o RGPD.

Nos termos e para os efeitos do previsto no artigo 36.º do RGPD, quando a avaliação de impacto indicar que o tratamento de dados que se pretende efetuar, apesar das medidas mitigadoras a adotar, resulta ainda num elevado risco para os direitos e liberdades dos

indivíduos, o responsável pelo tratamento submete o tratamento de dados em causa a consulta prévia da Autoridade de Controlo, no caso de Portugal, à CNPD.

3. Impacto nas Autarquias Locais

O RGPD é uma regulamentação da União Europeia que entrou em vigor em maio de 2018 e tem como objetivo proteger os direitos e liberdades dos indivíduos em relação ao tratamento de dados pessoais. As autarquias locais são entidades públicas que também têm de seguir as regras do RGPD, mas podem enfrentar algumas dificuldades na sua implementação.

Uma das principais dificuldades com que as autarquias se deparam, é a falta de recursos financeiros e humanos para se adequar às exigências do RGPD. Muitas autarquias locais não têm orçamentos suficientes para contratar especialistas em proteção de dados e para implementar as medidas necessárias com vista ao cumprimento das regras.

Outra dificuldade é a complexidade da regulamentação, o RGPD é uma regulamentação detalhada e complexa, e as autarquias locais podem ter dificuldades em compreender e aplicar as suas exigências, isso pode levar a erros na implementação do RGPD, o que pode resultar em sanções económicas.

Além disso, as autarquias locais enfrentam desafios na gestão dos dados pessoais que processam. Muitas autarquias locais lidam com uma grande quantidade de dados pessoais, incluindo informações sobre cidadãos, funcionários e fornecedores a ainda o tratamento de dados sensíveis, tais como, dados de saúde, dados financeiros, dados de menores, dados assistência social, etc. Isso pode tornar ainda mais difícil garantir a segurança e a privacidade dos dados, pois esse tipo de dados requer um nível ainda mais elevado de proteção e, portanto, as autarquias locais têm de estar preparadas para tomar medidas específicas para garantir que esses dados sejam tratados de acordo com as normas do RGPD.

Este cumprimento abrange todos os processos da organização que recolhe ou processa dados pessoais, sendo obrigatoriedade da autarquia, neste caso, identificar onde são feitos os processamentos dos dados, onde são guardados, e demonstrar de forma rápida que os mesmos podem ser eliminados e atualizados, a qualquer momento, independentemente da sua localização.

Todos estes procedimentos irão aumentar os níveis transparência e confiança, entre a administração e os cidadãos, titulares dos dados.

Por fim, as autarquias locais também podem enfrentar desafios na comunicação com os cidadãos sobre o tratamento dos seus dados pessoais. As autarquias locais devem garantir que os cidadãos estejam informados sobre as suas políticas de privacidade e os seus direitos.

Um dos aspetos críticos na implementação do RGPD nas autarquias locais é a falta de recursos, pois muitas delas não possuem os recursos financeiros ou humanos necessários para implementar as normas do RGPD e isso poderá levar a atrasos na implementação e a possíveis violações da norma.

Em resumo, as autarquias locais enfrentam desafios significativos na implementação do RGPD, nomeadamente a falta de recursos financeiros e humanos, a complexidade da regulamentação, a gestão dos dados pessoais e a comunicação com os cidadãos. É importante que as autarquias locais sejam conscientes destes desafios e tomem medidas para garantir que cumprem as suas obrigações em matéria de proteção de dados.

A implementação do RGPD nas autarquias locais reflete uma mudança de paradigma para estas entidades públicas, associada à obrigatoriedade de cumprimento das regras do RGPD, pois caso contrário, as consequências poderão ser muito gravosas, atendendo ao montante das coimas associadas ao seu incumprimento. As autarquias passaram por uma a fase inicial de adaptação e implementação de práticas, que acautelassem o cumprimento dos requisitos do RGPD e controlos para mitigar os riscos decorrentes deste quadro regulamentar, no entanto, atualmente coloca-se um novo desafio, o de avaliar se as medidas implementadas permitem, efetivamente, corresponder aos objetivos e se as mesmas são as mais adequadas à realidade atual e à dinâmica própria de cada autarquia.

3.1 Impacto nos processos/procedimentos

A implementação do RGPD numa autarquia local provoca, naturalmente, alterações significativas na estrutura e no modo de funcionamento da organização, pois praticamente toda a atividade Municipal faz tratamento de dados pessoais, logo é um Regulamento que abrange toda a estrutura, sendo por isso, inevitável a existência de uma adaptação em cada processo e procedimento e em cada Unidade Orgânica.

O processo transversal a ter em consideração, com vista a esta implementação, será o da gestão dos dados, para tal, será necessário colocar em marcha em toda a organização, o levantamento de todos os processos onde existam registos de atividades de tratamento. Para

isso, a CNPD disponibiliza modelos que a organização poderá adotar, quer para si, quer para as entidades subcontratantes[5].

Este procedimento do registo de atividades de tratamento de dados, pode ser ainda útil para a organização, pois pode permitir também a identificação de eventuais problemas de conformidade, fornecendo evidências da forma como a organização regista e gere as suas atividades de tratamento de dados pessoais, com vista à implementação das respetivas melhorias.

Além disso, a realização desta atividade permitirá também uma sensibilização por parte dos colaboradores que participam nela, na medida em que permitirá ficarem, desde logo, despertos para as suas atividades diárias no que concerne ao tratamento de dados e com isso, melhorarem os aspetos relacionados com os procedimentos a adotar. Posteriormente, a existência das políticas e procedimentos provocará também uma alteração nos comportamentos e nos modos de atuação na própria organização, nomeadamente através da obrigatoriedade da verificação de determinados requisitos (direitos dos titulares dos dados, consentimento, finalidades, etc…), toda esta metodologia terá impacto na forma como a organização tratará os dados.

Assim, como exemplo de alguns tipos de políticas e procedimentos, poderemos ter:

- **Procedimento de gestão de consentimento**: procedimento escrito que explica em que situações e como a organização obtém o consentimento explícito dos indivíduos, antes do tratamento dos seus dados pessoais, garantindo que os mesmos sejam tratados apenas com o seu consentimento explícito (para tal será necessário a elaboração de modelos de formulários de consentimento e de procedimentos para registar e armazenar o consentimento dos indivíduos);
- **Política de segurança de dados**: política que detalhe as medidas de segurança que a organização deve implementar, para proteger os dados pessoais contra qualquer forma de violação;
- **Procedimento de notificação de violações de dados**: procedimento escrito que explica como a organização notificará a CNPD e os indivíduos afetados em caso de violação de dados;

[5] https://www.cnpd.pt/organizacoes/obrigacoes/registo-de-atividades-de-tratamento/

- **Política de retenção e conservação de dados**: política que especifica por quanto tempo a organização retém os dados pessoais e como eles são excluídos quando deixam de ser necessários.
- **Procedimentos de gestão de dados sensíveis**: procedimento específico para lidar com dados sensíveis, tais como informações sobre saúde ou orientação sexual, garantindo que esses dados sejam tratados de forma adequada e segura;
- **Procedimentos de auditoria e avaliação de conformidade**: procedimento regular de auditoria e avaliação de conformidade para garantir que as operações de proteção de dados estão em conformidade com as normas do RGPD;
- **Medidas técnicas e organizativas**: medidas de segurança adequadas para garantir que os dados pessoais dos indivíduos sejam protegidos contra qualquer forma de violação, podendo incluir a criptografia de dados, a implementação de *firewalls* e a realização de *backups* regulares.

A par de todas estas metodologias, será muito importante planear formação dos colaboradores sobre as políticas e procedimentos emanados, para que estes possam aplicá-las às suas atividades diárias.

3.2 Impacto na tecnologia

Um dos principais impactos que as Autarquias terão de ter em consideração, é ao nível da tecnologia, no entanto esse impacto pode ser analisado em duas vertentes:

1. Na vertente das alterações à tecnologia já em uso e existente na organização;
2. Na vertente da utilização da tecnologia necessária para ajudar na implementação do RGPD;

Relativamente ao primeiro ponto, será necessário efetuar uma análise/avaliação aos sistemas existentes para verificar se os mesmos estão em conformidade com o RGPD, muito provavelmente nos sistemas mais antigos, tal não acontecerá. Assim, após essa análise e dependendo do resultado, a Autarquia terá de solicitar aos fornecedores de software alterações, que poderão redundar em:

- Atualização de medidas de segurança, pois poderá ser necessário atualizar as medidas de segurança existentes, para garantir que os dados pessoais sejam

protegidos contra qualquer forma de violação, como a criptografia, a autenticação de utilizadores e a proteção contra ciberataques;

- Adição de funcionalidades de gestão de consentimento, pois poderá ser necessário adicionar funcionalidades de gestão de consentimento, como formulários de consentimento digital, para garantir que a organização possa obter o consentimento explícito dos cidadãos antes de tratar seus dados pessoais;
- Atualização de políticas e procedimentos, podendo ser necessário atualizar as políticas e procedimentos existentes, para garantir a conformidade com o RGPD, incluindo políticas de privacidade, procedimentos de gestão de consentimento e procedimentos de notificação de violações de dados;
- Monitorização e auditoria, poderá ser necessário adicionar ou atualizar funcionalidades de monitorização e auditoria, para garantir que as organizações possam auditar as atividades relacionadas ao tratamento de dados.

Relativamente à segunda vertente, a tecnologia é uma parte crucial da implementação do RGPD, pois é através dela, que os dados pessoais são armazenados e processados. Esta importância pode ser verificada por várias razões, quer através do armazenamento seguro (a tecnologia permite que as organizações armazenem os dados pessoais de forma segura, com medidas de segurança adequadas para evitar qualquer forma de violação de dados), através do controlo de acesso, (a tecnologia permite que as organizações controlem quem tem acesso aos dados pessoais, garantindo que somente as pessoas autorizadas possam aceder e processar os dados), através da gestão de consentimento, (a tecnologia permite que as organizações implementem processos de gestão de consentimento, onde os indivíduos podem controlar e dar consentimento explícito para o tratamento de seus dados pessoais), quer ainda através da monitorização e auditoria, (a tecnologia permite que as organizações monitorizem e auditem as atividades relacionadas ao tratamento de dados, garantindo que as regras do RGPD estejam a ser cumpridas).

3.3 Encarregado de Proteção de Dados

A designação da figura do EPD que é uma das obrigações do Regulamento, definida no Artigo 37.º do RGPD, como já acima se referiu no subcapítulo 2.6, também é aplicável

às Autarquias Locais. O objetivo desta designação é garantir que a organização detém alguém, especializado e independente, responsável por garantir a conformidade com as regras do RGPD, além de também ter a função de aconselhar a organização, monitorizando as atividades de tratamento de dados e fornecendo orientação e suporte aos indivíduos sobre os seus direitos de proteção de dados.

Também o considerando 97.º do RGPD estabelece que "*os encarregados de proteção de dados, sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência*."

Mas será que, dada a independência exigida para este cargo, como já acima se explanou, ele é compatível com a função, por exemplo, de Técnico Superior, uma vez que esta categoria profissional da função pública, está naturalmente, sujeita a diretivas e orientações superiores (nos termos da Lei do Trabalho em Funções Públicas – Lei 35/2014 de 20/06)?

Neste sentido, na perspetiva de Inês Oliveira (2018), com a qual concordamos, atualmente estas funções não são compatíveis com as que elencam o conteúdo funcional desta categoria profissional. Assim, para esta autora, poderemos aqui estar perante a necessidade de criar, no futuro, uma nova categoria na carreira profissional de Técnico Superior, com especificidades próprias, para assim poder acolher de forma mais segura estas funções dentro das próprias organizações.

Assim, também Ana Fazendeiro (2018) refere que as funções do EPD exigem que o seu exercício se faça com autonomia, trabalhando em estreita ligação com o órgão superior de gestão da entidade, "*Se o encarregado de proteção de dados for trabalhador da entidade, não pode ser destituído ou penalizado por esta pelo facto de exercer as suas funções."*

Nesta perspetiva também, José Noronha Rodrigues e Daniela Medeiros Teves (2020) defendem que :*"A opção da nomeação de um trabalhador em funções públicas poderá gerar problemas laborais, uma vez que na maioria das situações, "as funções de EPD acumulam às funções originárias, sendo que o EPD "não recebe instruções relativamente ao exercício das suas funções (...) não podendo ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções", sendo que quanto às suas funções originárias encontra-se subordinado juridicamente, pelo que será necessário definir os limites e contornos dessa nomeação."*

Em resumo, poderemos afirmar que o EPD é uma figura-chave no esforço para colocar a organização em conformidade com o RGPD, pois é o responsável por garantir que

as organizações cumpram as regras de proteção de dados e por assegurar que os cidadãos tenham acesso a informações precisas e transparentes sobre como os seus dados são tratados. Também desempenham um papel importante na comunicação com as autoridades de controlo e na resolução de quaisquer questões relacionadas com a temática da proteção de dados.

Neste âmbito é obrigatório que uma Autarquia Local tenha de nomear um EPD. Como tal, a existência desta figura nas Autarquias Locais também irá trazer um impacto para estas organizações, na medida em que será uma autoridade consultiva e ao mesmo tempo fiscalizadora, nos termos das suas funções (elencadas no capítulo 3.7 supra).

Nesse sentido, o EPD introduzirá grande impacto nas Autarquias Locais, dadas as incumbências que lhe são atribuídas, pois será mais um "órgão" do corpo da organização. Uma das questões suscitadas com o surgimento deste novo cargo/função é o de saber, se deve existir um EPD nomeado internamente, isto é, se deve ser um funcionário da organização ou se deve contratar-se o serviço de EPD a uma empresa externa, como acima se referiu. Na nossa opinião, o mesmo, se for designado internamente, colidirá com as funções que exerce na organização, sendo difícil garantir a isenção, imparcialidade e independência, dadas as características das funções a desempenhar.

A decisão de contratar o serviço de EPD a uma empresa externa ou designá-lo internamente dependerá da sensibilidade da autarquia local para a matéria, no entanto, parece-nos que a primeira opção garante de forma mais eficaz e isenta o cumprimento da função, nomeadamente para poder manter a imparcialidade e total transparência nesta matéria. Essa solução garantirá que as normas do RGPD sejam cumpridas de forma eficiente e eficaz, sem que a autarquia local tenha que investir recursos humanos adicionais. Ademais, essas empresas externas geralmente possuem conhecimentos e experiência especializada na proteção de dados, o que pode ser uma mais-valia para a autarquia local.

No entanto e na verdade, o Regulamento refere claramente que o EPD a designar, pode ser funcionário da organização, por esse motivo e em qualquer dos casos, o importante é garantir que o EPD tenha os conhecimentos e competências necessários para cumprir as suas funções e que tenha acesso às informações e recursos suficientes para garantir a conformidade com as normas do RGPD.

No quadro seguinte, elencar-se-ão algumas das vantagens e desvantagens de cada uma das opções:

Tipo de nomeação	Vantagens	Desvantagens
Externalização do serviço	• Experiência especializada: As empresas externas geralmente possuem conhecimento e experiência especializada na proteção de dados, o que pode ser valioso para a autarquia local. • Independência: O EPD contratado externamente é independente da autarquia local, garantindo uma maior imparcialidade e objetividade.	• Custos elevados: A contratação de um EPD externo pode ser mais onerosa do que a nomeação interna. • Falta de conhecimento da organização: O EPD contratado externamente pode não ter conhecimento detalhado da organização, o que pode dificultar a implementação de medidas de proteção de dados. • Falta de flexibilidade: A contratação externa pode implicar menos flexibilidade, já que a autarquia local não tem tanto controle sobre as operações de proteção de dados.
Nomeação Interna	• Conhecimento detalhado da organização: O EPD nomeado internamente tem conhecimento detalhado da organização, o que facilita a implementação de medidas de proteção de dados. • Maior flexibilidade: A nomeação interna garante maior flexibilidade, já que a autarquia	• Falta de recursos financeiros e humanos: A autarquia local pode não ter recursos humanos suficientes para nomear um EPD internamente. • Falta de experiência especializada: O EPD nomeado internamente

	local tem mais controle sobre as operações de proteção de dados. • Maior facilidade de comunicação: A nomeação interna garante uma maior facilidade de comunicação entre o EPD e os outros funcionários da autarquia local.	pode não ter experiência especializada na proteção de dados, o que pode dificultar a implementação de medidas de proteção de dados.

Tabela 1: Encarregado de Proteção de dados (tabela elaborada pela autora).

Esta decisão também terá um peso significativo nos impactos na organização, independentemente da escolha que se faça, conforme supra se tentou enunciar, no entanto e na nossa opinião a contratação externa do EPD é aquela que maior garantia de imparcialidade e independência dá aos cidadãos que contatam com a organização, em matéria de proteção de dados.

3.4 Impacto na cultura organizacional

A implementação do RGPD provoca naturalmente uma alteração na cultura organizacional, com uma maior consciência e responsabilidade sobre a proteção de dados pessoais dos indivíduos e vem fazê-lo de várias formas, uma vez que impõe a obrigação de proteger os dados pessoais dos indivíduos e a privacidade dos mesmos, colocando-os num patamar de prioridade mais elevada. Nas autarquias locais, a responsabilidade em relação à proteção de dados, passa a ser partilhada entre os vários agentes da organização, o que também pode levar a mudanças, para garantir que todos entendam e cumpram as suas responsabilidades.

Neste sentido Van der Sloot, Hoofnagle & Zuiderveen Borgesius (2019) referem que *"o RGPD também traz mudanças significativas. O RGPD insere os dados pessoais num regime regulamentar complexo, detalhado e protetor, o que terá implicações profundas. Por exemplo, o RGPD incentiva as organizações a pensar cuidadosamente sobre suas práticas de dados pessoais, tenta fazer com que as organizações levem a privacidade a sério. O RGPD incentiva as organizações a verificar se os fornecedores de serviços estão em conformidade com as regras. Outra inovação é que o RGPD reforça a importância dos responsáveis pela privacidade, dentro das organizações*."

Desta forma, também se impõe uma maior transparência no tratamento dos dados pessoais, o que leva necessariamente as autarquias locais a mudar a sua cultura organizacional, para garantir que os indivíduos saibam como os seus dados estão a ser tratados e que tenham acesso a informações sobre esse tratamento. Consequentemente a mudança na gestão de dados e na cultura de segurança, impõe por um lado, uma gestão mais rigorosa dos dados pessoais, para garantir que haja um processo de gestão de dados eficiente e eficaz, mas também, uma maior consciencialização na organização, da necessidade de não ter comportamentos de risco que coloquem em causa a segurança desses mesmos dados.

Para Rodrigues e Teves (2020) *"A implementação do RGPD no seio da administração pública demonstra-se ardilosa, obrigando o envolvimento de toda organização e a implementação de mudanças, sendo que implica um conhecimento vasto da própria organização, devendo as entidades públicas identificar que dados pessoais tratam, em que processos sucede o tratamento e se estes tratamentos se encontram conforme o estabelecido no RGPD, sendo certo que, embora o regime da proteção de dados não seja novidade, não consubstanciava um preocupação de muitas entidades."* Esta mudança na cultura irá "contaminar" todos dentro da organização, desde o funcionário do atendimento municipal, à equipa de desenvolvimento de software e à gestão de topo, pois ninguém quererá ficar associado a um problema de incumprimento das regras do RGPD, e por isso a preocupação será de todos e constante, logo a mudança organizacional será inevitável e acontecerá naturalmente.

Mas, mesmo partindo do princípio de que não haverá fórmula milagrosa, há fatores que podem determinar o sucesso ou insucesso da implementação do RGPD nas Autarquias locais, sendo que talvez o mais importante deles, seja a criação de uma estrutura interna para gerir o processo. E isso deve acontecer mesmo que a opção recaia sobre a contratação de uma empresa de consultoria externa à organização, para apoiar o programa de implementação.

O conhecimento de um programa tão impactante como é o RGPD, deve permanecer de forma estável e interna na organização, porque a implementação do programa não termina, o RGPD não é um projeto, é um processo que tem de ser gerido continuamente e que está em constante mutação e evolução.

No entanto, existem medidas que as autarquias locais poderão tomar, por forma a aliviar o impacto do RGPD dentro do seu funcionamento, nomeadamente, apostando na formação dos seus técnicos, sendo esta a chave das autarquias para o cumprimento do

RGPD, crucial para garantir o sucesso da implementação, conseguindo assim um melhor desempenho das suas funções em matéria de proteção de dados.

Também ao nível da liderança, o impacto será sentido, na medida em que os executivos Municipais devem ter agora uma preocupação que não tinham no passado, a implementação do RGDP pode ter um impacto significativo a nível do executivo municipal (gestão de topo). Algumas das preocupações que um Presidente de Câmara ou Vereador com a responsabilidade com este pelouro, deverão ter nesta matéria, passam pela consciencialização das responsabilidades legais existentes, imputáveis aos responsáveis pelo tratamento de dados pessoais, tomando medidas para garantir que a organização esteja em conformidade, evitando assim o risco de coimas para as organizações que não cumprem as suas obrigações.

Existe também o risco de impacto na reputação da própria organização, pois uma violação de dados pode causar danos significativos à reputação da autarquia local e a liderança deve estar ciente desse risco e tomar medidas para garantir que a organização esteja preparada para lidar com uma violação de dados, quer ao nível financeiro, quer ao nível reputacional, como poderemos verificar nalguns dos exemplos abordados no subcapítulo seguinte.

3.5 Exemplos reais de violações do RGPD na Administração Pública

Neste capítulo iremos fazer uma breve abordagem a três dos casos, talvez dos mais mediáticos que atingiram o nosso país, nomeadamente, o Município de Lisboa, o Município de Setúbal e o Instituto Nacional de Estatística, no que se refere à violação do RGPD, no âmbito das suas atividades.

3.5.1 O Município de Lisboa

A Câmara Municipal de Lisboa foi condenada numa coima no valor de um milhão duzentos e cinquenta mil euros pela CNPD, devido a violações do RGPD, nomeadamente, por violação do princípio da licitude, lealdade e transparência, violação do principio da minimização dos dados, na vertente de *need to know*, violação do dever de prestar as informações previstas no artigo 13.º do RGPD, violação do princípio da limitação da

conservação e da violação da obrigação da realização de AIPD, no âmbito do caso que ficou conhecido como *Russiagate*.

De acordo com a CNPD, a Câmara de Lisboa violou vários artigos do RGPD ao "*comunicar os dados pessoais dos promotores de manifestações a entidades terceiras*", neste caso a embaixadas de diferentes países, conforme consta do Projeto de Deliberação[6].

A Autoridade de Controlo, acusou a Câmara Municipal de Lisboa de ter enviado dados pessoais de cidadãos portugueses para as embaixadas de vários países, sem o consentimento dos seus titulares, violando assim os artigos 5.º e 6.º do RGPD, que impõem a obrigação de garantir a segurança dos dados pessoais e a obrigação de garantir que estes dados só sejam tratados, com o consentimento explícito dos seus titulares. Além disso, a CNPD também acusou a Câmara Municipal de Lisboa de ter enviado dados pessoais para as autoridades russas, sem o consentimento dos seus titulares. A Câmara Municipal de Lisboa foi notificada da coima em julho de 2021 e a decisão da condenação veio a ocorrer a 21 de dezembro de 2021, tendo sido uma das maiores coimas aplicadas pela CNPD, até àquela data, destacando a importância de as organizações cumprirem com as suas obrigações legais, em matéria de proteção de dados.

Além do envio de dados para a embaixada da Rússia, que deu início ao processo, o Município de Lisboa terá partilhado também informação com as embaixadas de Israel, China e Venezuela. Uma auditoria revelou que, no total, terão sido partilhados dados referentes a 52 manifestações, depois da entrada em vigor do RGPD, que aconteceu em 2018.

A queixa à CNPD partiu dos próprios ativistas lesados, a 19 de março de 2021, que se queixaram que os seus dados tinham sido enviados à embaixada da Rússia, tal como noticiou o Observador (Ferreira & Simões, 2021).

Até mesmo no interior da organização os dados foram comunicados a serviços que não deveriam ter sido, desde o Gabinete do Vereador, à Direção Municipal de Higiene Urbana, por exemplo.

O Município de Lisboa interpôs recurso da decisão de contraordenação junto dos tribunais judiciais. Até o momento, não há uma decisão definitiva sobre o processo. No decorrer do mesmo, foram levantadas questões quanto à competência dos tribunais para julgar o recurso, (Tribunal da Comarca de Lisboa ou Tribunal Administrativo e Fiscal de Lisboa), estando, por isso, ainda longe uma decisão final.

[6] https://www.cnpd.pt/media/ttuoknbh/proj_deliberacao_2021_16_redacted.pdf

3.5.2 O Município de Setúbal

A CNPD sancionou o Município de Setúbal quanto ao tratamento de dados de refugiados ucranianos, com a aplicação de coima e de duas repreensões.

Na coima única de cento e setenta mil euros, incluiu-se a violação do princípio da integridade e confidencialidade dos dados e a violação da obrigação de designar um EPD, já as repreensões dizem respeito à violação do dever de facultar informações ao titular, aquando da recolha de dados e à violação do princípio da limitação da conservação dos dados.

Foi a primeira vez, em Portugal, que a CNPD aplicou uma coima pelo facto de a organização não ter designado um EPD, em conformidade com o n.º 1 do artigo 37.º do RGPD.

A CNPD afirmou que a Câmara Municipal de Setúbal não obteve o consentimento explícito dos refugiados antes de compartilhar os seus dados pessoais com terceiros, e também não implementou medidas adequadas para garantir a segurança desses mesmos dados. (CNPD, 2022).

Não ficou assim garantida a integridade e confidencialidade, por falta de acordo para o tratamento de dados, com a associação em questão. Para além do exposto não se encontravam definidos os prazos de conservação dos dados, nem os critérios para a sua determinação. O formulário utilizado para recolha de dados não cumpria com o preconizado no RGPD. Ademais, o formulário remetia para legislação de proteção de dados que se encontrava já revogada, que não identificava todos os terceiros com quem a informação era transmitida e não fazia qualquer referência aos direitos dos titulares dos dados. Por fim, verificou-se que o município também não tinha nomeado um EPD, como obriga o Regulamento. (CNPD, Deliberação/2022/1040, 2022).

A Câmara Municipal de Setúbal decidiu impugnar as sanções aplicadas pela CNPD, junto do Tribunal Administrativo e Fiscal de Almada, por entender que ao Município, deveria ter sido dada a oportunidade, (uma vez que se tratou de uma conduta meramente negligente), de regularizar a situação, sendo que só deveria ter sido aberto processo sancionatório e, eventualmente, aplicadas as coimas, caso essa regularização não se verificasse.

3.5.3 O Instituto Nacional e Estatística (INE)

A maior coima aplicada em Portugal, em matéria de proteção de dados, pela autoridade de controlo (CNPD), foi ao Instituto Nacional e Estatística, em 2 de novembro de 2022 no valor de quatro milhões e trezentos mil euros.

Na comunicação pública efetuada pela CNPD, relativa à Deliberação/2022 /1072 , (CNPD, CNPD sanciona INE por cinco contraordenações, 2022) pode ler-se que: " *a CNPD decidiu que o Instituto Nacional de Estatística (INE) tratou dados pessoais relativos à saúde e religião de forma ilícita, não cumpriu os seus deveres de informação aos respondentes do questionário do Censos 2021, violou os deveres de diligência na escolha do subcontratante, infringiu as disposições legais relativas à transferência internacional de dados e incumpriu a obrigação de realizar uma avaliação de impacto sobre a proteção de dados relativa à operação censitária."*

A CNPD entendeu ainda que, "*não foi cumprido o dever de diligência na escolha do subcontratante, considerando que a verificação dos requisitos do n.º 3 do artigo 28.º do RGPD, deve ser substantiva e não formal, não se limitando à escolha de um qualquer clausulado -padrão. No caso, apesar da existência de um escritório da empresa em Lisboa, o contrato foi feito com a empresa sediada nos EUA, tendo sido contratualizado que o foro para dirimir conflitos entre o INE e a Cloudflare, Inc. seria o Tribunal da Califórnia (incumprindo assim com a garantia do tratamento dos dados em espaço europeu).*"

O INE, discordando da decisão, interpôs recurso de impugnação judicial, no sentido de impugnar a coima aplicada pela CNPD, estando o mesmo ainda a decorrer.

Assim, podemos concluir que, o RGPD representa um grande desafio para as autarquias locais, com grande impacto no seu modo de atuação, definindo uma mudança na forma como os dados dos seus "clientes" são tratados, com consequências, essencialmente, ao nível da responsabilidade, conforme os exemplos referidos supra. As Autarquias que não se adaptarem a esta nova realidade, terão muitas dificuldades em garantir a conformidade legal face a este Regulamento, quer em termos reputacionais, quer em termos financeiros.

Nada mais será como antes e é muito importante que os executivos Municipais tenham a consciência, que será necessário investir neste tema, quer em recursos financeiros, quer em recursos humanos. Os colaboradores também terão de alterar e adaptar procedimentos para garantir a privacidade por defeito (*privacy by default e by design*), para

permitir que os cidadãos possam exercer os seus direitos, agora determinados e regulados pelo RGPD.

No capítulo seguinte abordaremos o caso prático da implementação do RGPD no Município de Pombal e a forma como esta organização enquadrou e abordou o tema, chegando ao ponto em que se encontra atualmente, no que se refere ao nível de conformidade com o RGPD.

4. Município de Pombal – Metodologia de Implementação

4.1 Caracterização do Município de Pombal

4.1.1 Localização Geográfica

O Concelho de Pombal está localizado no centro litoral português e possui uma área geográfica de 626.23 Km2. Situa-se entre os concelhos de Ansião, Alvaiázere, Ourém, Leiria, Soure e Figueira da Foz estendendo-se a Oeste até ao Oceano Atlântico.

Pombal, encontra-se a cerca de 150 Km das cidades de Lisboa e Porto, a 33 Km de Coimbra, a 26 Km de Leiria e a 30 Km da Figueira da Foz. Na Figura 2, pode-se observar a localização geográfica da cidade de Pombal:

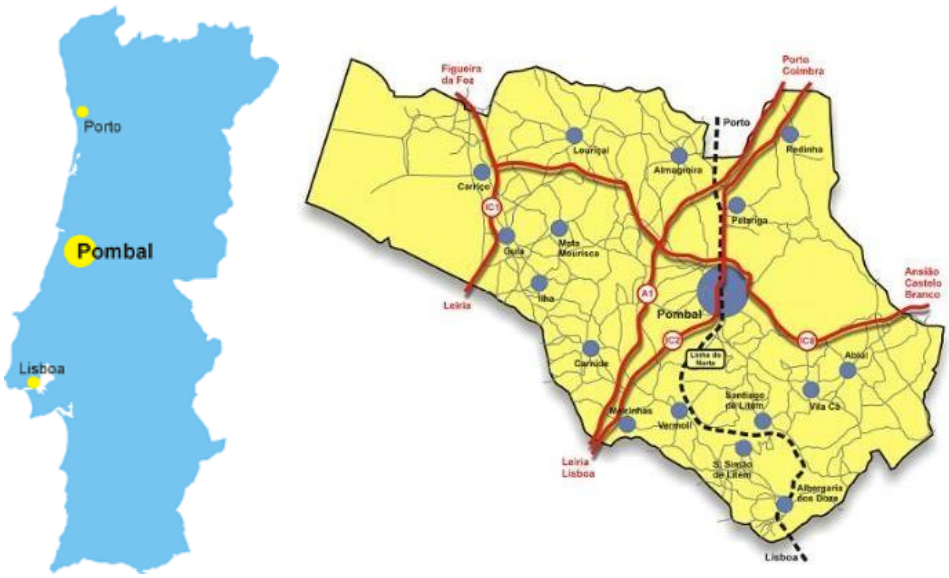


Figura 2: Localização geográfica da cidade de Pombal (imagem retirada do site do Município de Pombal)

4.1.2 Órgãos representativos do Município

Os órgãos representativos do Município são a Assembleia Municipal e a Câmara Municipal, conforme previsto no Artigo 250.º da Constituição da República Portuguesa (CRP), atenta a Lei Constitucional n.º 1/2005, de 12 de agosto, bem assim o n.º 2, do Artigo 5.º, do Regime Jurídico das Autarquias Locais (RJAL).

Nos termos dos Artigos 251.º e 252.º da CRP e n.ºs 1 e 2, do Artigo 6.º, do RJAL, a Assembleia Municipal é o órgão deliberativo do Município e a Câmara Municipal é o órgão executivo colegial do mesmo, encontrando-se a sua constituição, composição e organização reguladas na Lei n.º 169/99, de 18 de setembro, na atual redação (cfr. n.º 3, do referido Artigo 6.º, do RJAL).

Sem prejuízo doutras competências legais, e de acordo com o disposto no acima referido Artigo 3.º do RJAL:

A Assembleia Municipal "*(...) tem as competências de apreciação e fiscalização e as competências de funcionamento (...)*" previstas, nomeadamente, nos Artigos 25.º e 26.º do RJAL, conforme o Artigo 24.º, do mesmo Regime, encontrando-se atribuídas ao «Presidente da Assembleia Municipal» as competências inscritas nos n.ºs 1 e 2, do Artigo 30.º, daquele Regime; e

A Câmara Municipal "(…) tem as competências materiais e as competências de funcionamento (…)" prescritas, designadamente, nos Artigos 33.º e 39.º do mesmo RJAL, conforme o Artigo 32.º deste Regime, cabendo ao Presidente da Câmara, entre outras, o conjunto de competências previstas no Artigo 35.º daquele RJAL, competindo-lhe, igualmente, nos termos do Artigo 37.º deste Regime, a coordenação dos Serviços Municipais

Nos termos constantes no Despacho n.º 7428/2023, publicado em Diário da República, 2.ª série, n.º 136, de 14 de julho de 2023, a organização interna dos serviços municipais, desta Autarquia, obedece a modelo de estrutura misto, a que corresponde uma componente hierarquizada, constituída por unidades orgânicas nucleares e flexíveis, e uma componente matricial, constituída por equipa multidisciplinar, conforme estipulado no n.º 2, do Artigo 9.º, do Decreto-Lei n.º 305/2009, de 23 de outubro (que estabelece o Regime Jurídico da Organização dos Serviços das Autarquias Locais), e dispõe de Regulamento de Organização dos Serviços Municipais (ROSM) e de respetivo Organograma, conforme inerente aprovação em reunião de Câmara Municipal, realizada em 22 de junho de 2023, e em sessão da Assembleia Municipal, celebrada em 29 de junho de 2023. A referida

estrutura orgânica tem associada representação gráfica nos termos constantes no Anexo I ao ROSM, sob a epígrafe organograma, e é composta, conforme inscrito no Artigo 13.º, do mesmo Regulamento, por gabinetes operacionais, unidades orgânicas (nucleares e flexíveis, subunidades orgânicas e gabinetes de projetos, pelos quais são responsáveis, Membros do Órgão Câmara Municipal (Presidente da Câmara e Vereadores a tempo inteiro) e titulares de cargos dirigentes.

Assim,

Diário da República, 2.ª série — PARTE H
N.º 136 — 14 de julho de 2023 — Pág. 249

Alteração da Estrutura Orgânica Interna dos Serviços Municipais

ANEXO 1

Organograma

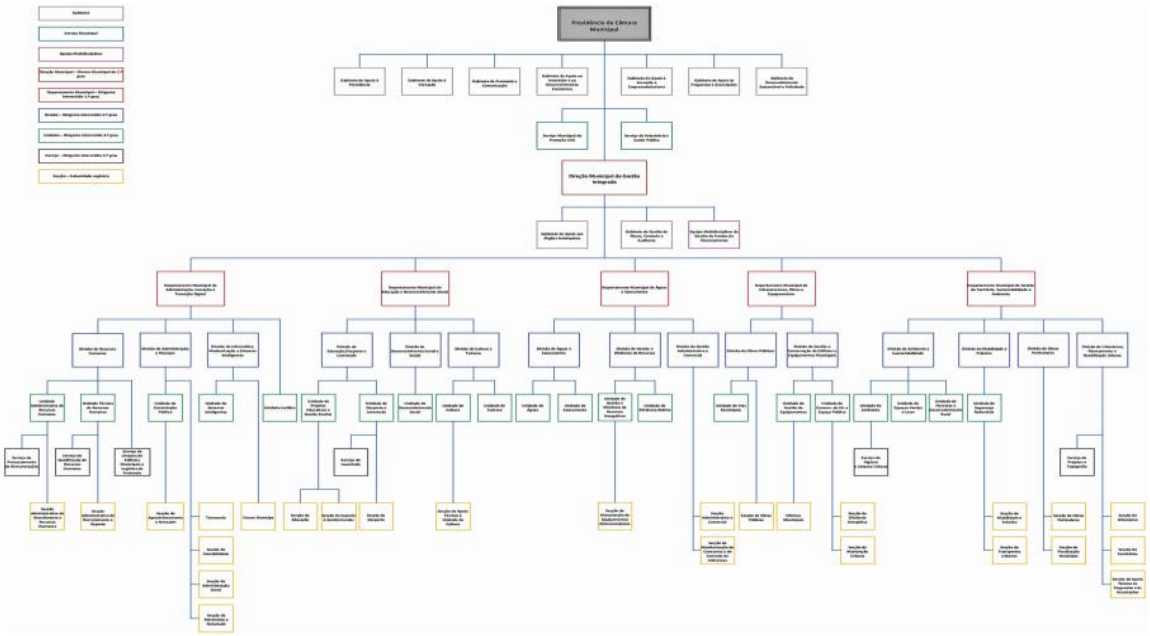


Figura 3: Anexo 1 – Organograma dos Serviços Municipais do Município de Pombal, Despacho n.º 7428/2023, Diário da República, 2.ª Série, de 14 de julho de 2023

Feita a caraterização do Município de Pombal, e voltando ao tema deste projeto, esta autarquia, abordou a conformação do RGPD em duas fases distintas. Após a entrada em

vigor do RGPD, em 2018, avançou apenas para a primeira fase, com uma implementação mais concetual, realizando um *assement* à privacidade e proteção de dados, posteriormente em 2021 alargou o âmbito da atuação, abordando também as questões da cibersegurança e da ISO27001 (Sistemas de Gestão de Segurança de Informação).

Nos capítulos seguintes, descrevem-se as metodologias de implementação adotadas, no que se refere ao RGPD. Neste projeto iremos acompanhar a trajetória percorrida pela equipa responsável pela implementação do RGPD (da qual faço parte), no Município de Pombal, em matéria de proteção de dados, descrevendo as metodologias utilizadas e os caminhos seguidos, sem esquecer as opções, quer técnicas, quer políticas efetuadas, com vista à melhor implementação do Regulamento.

O bem maior, sempre presente, foi a proteção dos dados pessoais de todos os clientes que interagem com o Município de Pombal (*stakeholders*), assim como, o cumprimento do Regulamento e da legislação aplicável à matéria.

4.2 Ponto de situação em 2018/2019

De modo a iniciar este capítulo optámos por analisar como se encontrava o Município de Pombal, em matéria de proteção de dados, no momento da entrada em vigor do RGPD.

Em 25 de maio de 2018, com a entrada em vigor, com caráter obrigatório, do Regulamento, as entidades públicas e privadas dos Estados-Membros da União Europeia, tiveram obrigatoriamente de se adaptar, reformulando e revendo todos os seus procedimentos, com vista à implementação e aplicação do RGPD e o Município de Pombal não foi exceção. O Município de Pombal, àquela data não tinha, ainda desencadeado nenhuma ação para a implementação do RGPD na organização e em novembro de 2018, decide com recurso a consultoria externa, proceder ao levantamento de requisitos e informação para aferir conformidades e ações de melhoria, à luz do RGPD.

Nos termos da nova legislação, na altura, o Município de Pombal deveria rever a forma como tratava os dados pessoais a que tinha acesso e que detinha na sua esfera de ação, conhecê-los e enquadrá-los à luz das novas regras, analisando as obrigações deste Regulamento e percebendo como identificar as medidas necessárias para estar em *compliance* com esta nova realidade. Essa avaliação foi efetuada pela empresa de consultoria, à data, da qual resultou o respetivo Relatório, cuja metodologia adotada para a mesma, se junta no Anexo I.

Em resultado do referido relatório, foi no mesmo indicado que a preparação do cumprimento dependeria da elaboração de um plano de ação, com vista à implementação do RGPD, de forma a envolver todas as Unidades Orgânicas da autarquia.

Dada a complexidade associada à implementação de um projeto deste género, numa organização com alguma dimensão, como é o caso do Município de Pombal, entendeu-se no seio da organização que este procedimento deveria ser focado na operacionalização e dividido em quatro fases distintas (1.Avaliar, 2.Planear, 3.Implementar, 4.Gerir) por forma a atender às necessidades e a atingir a conformidade desejada do RGPD.

Em 2018/2019, o Município focou-se na fase 1 **(Avaliar)** em que se procedeu a um levantamento das necessidades e dos procedimentos existentes, com vista à implementação do Regulamento conforme metodologia demonstrada no Anexo I.

Assim, conforme se pode observar na Figura 4, teremos as 4 fases em sequência, onde se destacam as ações da fase 1 - Avaliar:

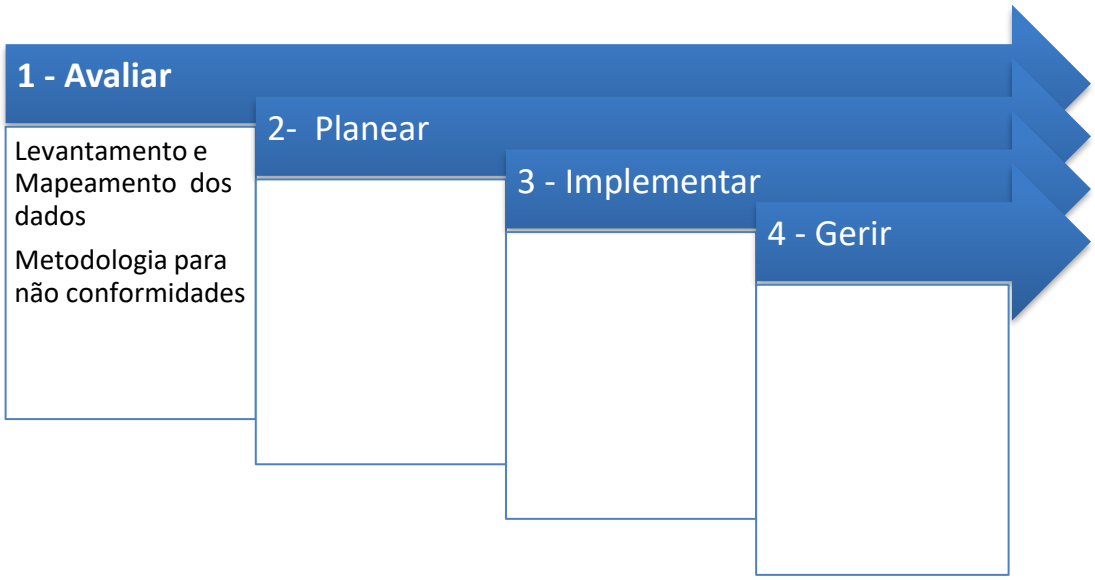


Figura 4: Evolução das fases de implementação do RGPD no Município de Pombal – Fase 1 (quadro elaborado pela autora).

4.2.1 Metodologia para Não Conformidades - Recomendações ou/e Ações de melhoria

As não conformidades ou melhorias por Unidade Orgânica (UO) detetadas, tiveram por base as entrevistas e a aplicação da *framework*, com requisitos de *compliance* e *assessment*, propostos. pela consultora.

O RGPD exige ao Município de Pombal, que lida com dados pessoais, a implementação de novas práticas de segurança da informação e das redes e sistema de informação, adotando medidas técnicas e organizativas que garantissem que os riscos identificados para a confidencialidade, integridade e disponibilidade da informação fossem mitigados.

Da análise da informação contida nos processos, a mesma foi classificada e salvaguardada, definindo níveis de acesso restrito e controlado, com definição de mecanismos que permitissem o acesso às áreas seguras, unicamente a pessoas autorizadas.

Foi também efetuada a classificação dos dados, tendo em conta a segregação da informação pelo número mais restrito possível de pessoas, de acordo com a criticidade da mesma. Foram assim, identificadas as matrizes de análise, associadas a cada processo identificado por cada UO e feito um levantamento exaustivo, tendo sido identificados todos os processos que tratam com dados pessoais na organização.

Na sequência do levantamento suprarreferido e do levantamento de todos os processos, foram pela empresa consultora, apontadas algumas recomendações, das quais destacamos apenas parte, das que consideramos mais importantes, para que possamos ter uma perceção da situação existente em 2018/2019 e posteriormente em 2021/2022, em matéria de RGPD.

4.2.2 Recomendações

Conforme mencionado no subcapítulo anterior, enunciam-se de seguida as recomendações emanadas do relatório:

Política de Gestão de Risco

Foi proposto rever a análise de risco já realizada, com identificação do risco de tratamento de dados pessoais, e implementar através da *Política de Gestão de Risco*, a definição do sistema de gestão de riscos relevantes para o regular exercício da sua atividade, identificando os grandes riscos, limitando-os e assegurando estratégias e meios de evitar ocorrências, de que é exemplo máximo, a implementação do sistema de controlo interno.

Fruto da implementação do RGPD foi emitida a recomendação para que fosse considerado um novo risco na atividade do Município de Pombal que, podendo não ser elevado, não era de desvalorizar: o risco associado ao tratamento indevido de dados pessoais,

fossem eles de munícipes, trabalhadores, fornecedores ou outros, sendo certo que este risco tanto poderia decorrer de uma falha humana, de uma falha informática, ambas inocentes, ou de atuações maliciosas.

A concretização do grau de detalhe deste risco caberia ao Município de Pombal, concorrendo para esta decisão uma ponderação entre as probabilidades da ocorrência, a confiança que tinham nos seus sistemas de conservação documental física, digital e de sistemas, bem como, nas pessoas que manuseavam a informação, entre outros. Através da definição de um conjunto de procedimentos, permitir-se-ia implementar uma Política de Gestão de Risco onde se identificariam, avaliariam e mitigariam os riscos concretos associados à atividade do Município de Pombal.

Elaboração de Políticas, Procedimentos e Manuais de Boas Práticas

Foi recomendado que, pese embora o Município de Pombal apresentasse um acervo documental e procedimental bastante completo e abrangente, deveria procurar completá-lo, elaborando documentação que suportasse evidências, que definisse procedimentos, com vista ao cumprimento dos requisitos de tratamento de dados pela conceção e por defeito, nomeadamente, politicas de segurança, politicas de privacidade, instruções de procedimento, recomendações, diretrizes, códigos de conduta, modelos e formulários, etc.

Verificou-se que não existia nenhuma política de Segurança de Informação documentada e instituída, dado que ainda não existiam políticas e regras de encriptação dos Dados Pessoais.

A ausência de todo este conjunto de procedimentos determinava a existência de um conjunto importante de fatores de risco associados ao tratamento destes dados, que foram sendo identificados, de entre outros, os riscos associados ao envio de email, aos ficheiros não encriptados, ao acesso a todos os dados pessoais dos sistemas, à possibilidade de ser retirada e utilizada informação sem permissão dos munícipes, trabalhadores e outros, à possibilidade de guardar no próprio computador informação de dados pessoais e de ter informação na rede, em ficheiros pdf e excel, acessível a qualquer pessoa do Município de Pombal.

Encarregado para Proteção dos Dados (EPD)

No que concerne ao encarregado da proteção de dados, o Município de Pombal de acordo com o n.º 1 do Artigo 37.º teria que designar um EPD, por ser um organismo público.

A sua designação deveria ser comunicada à Autoridade de Proteção de Dados no link seguinte https://www.cnpd.pt/bin/notifica_rgpd/epd_dpo.html, e este teria a função de aconselhar e auxiliar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores, em todas as questões relacionadas com a proteção de dados pessoais.

Foi ainda recomendado ser de extrema importância, nomear, à data, e de imediato um encarregado da proteção de dados (EPD) e de acordo com o Artigo 38.º do RGPD, o encarregado da proteção de dados deveria ser envolvido, de forma adequada e em tempo útil, em todas as questões relacionadas com a proteção de dados pessoais e acompanhar a implementação das obrigações nos termos do Regulamento e outras disposições de proteção de dados da União ou nacionais.

Era obrigação do Município de Pombal, fornecer ao EPD os recursos necessários ao desempenho dessas funções e à manutenção dos seus conhecimentos, bem como, dando-lhe acesso aos dados pessoais e às operações de tratamento, com vista a controlar a conformidade dos dados pessoais e do seu tratamento e as respetivas auditorias, com o RGPD.

De acordo com n.º 6 Artigo 37.º o EPD poderia ser um elemento do quadro de pessoal do Município de Pombal, ou alguém a exercer as suas funções com base num contrato de prestação de serviços.

Aconselhavam ainda que a função do EPD fosse externalizada, sob reserva de haver conflitos de interesses no exercício da sua função, se optassem pela nomeação interna para desempenhar a mesma. Além da salvaguarda do conflito de interesses, o Município de Pombal, poderia não dispor de ninguém, entre os seus Recursos Humanos, disponível e com as qualificações necessárias ao exercício da função.

4.2.3 Nível *compliance* - Resumo

Em conclusão, à data, janeiro de 2019, e tendo por base a informação recolhida nas várias reuniões com as UO, durante as quais foi aplicada a metodologia suprarreferida, foi identificado pela consultora, um nível de conformidade **RGPD BAIXO,** no Município de Pombal**.**

Neste sentido, foi aconselhado o desenvolvimento de um plano de implementação que assegurasse e comprovasse, com evidências, que as medidas técnicas e organizativas

seriam implementadas e mantidas, tendo sido definidas várias medidas Estruturais de *Governance*, para *Compliance* do RGPD.

As estratégias a seguir, passariam por definir elevados níveis de responsabilização (*accountability*), por parte do Município de Pombal pelo tratamento de dados pessoais, que deveriam ser comprovados, através de evidências, de que os procedimentos com vista ao tratamento dos dados decorriam de acordo com o planeado, tendo em consideração uma visão holística da organização, garantindo assim a proteção de dados, a deteção de riscos potenciais, com vista à implementação das medidas corretivas conforme necessário, que se resumem na Figura 5.

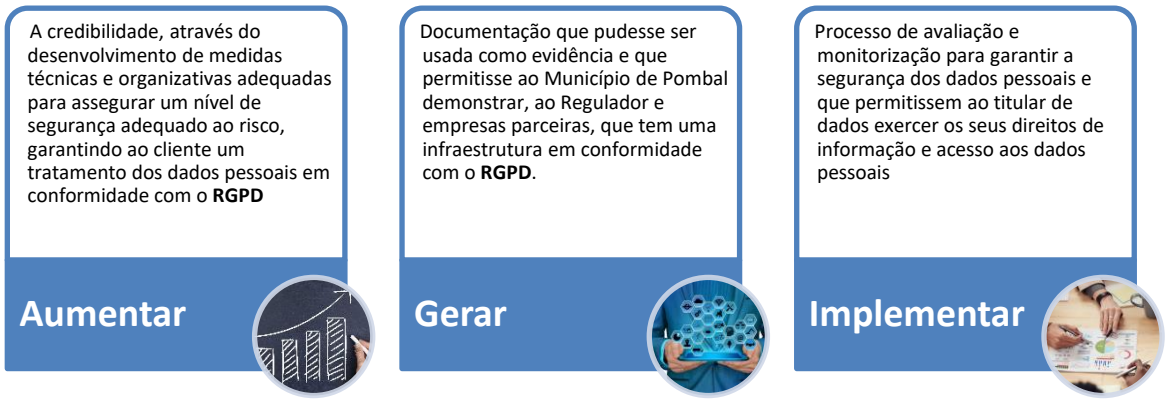


Figura 5: Fases do planeamento (quadro elaborado pela autora)

Decorreu também do relatório, a identificação dos riscos que o Município de Pombal estaria sujeito, caso não fosse cumprido o Regulamento, estes riscos, além do financeiro, (pois estaria sujeitos à aplicação de coimas), também o risco de credibilidade e reputacional seria elevado, porque o Município de Pombal, trata grande volume de dados confidenciais dos seus clientes.

Foi ainda recomendado, por esse motivo, criar rever as políticas e procedimentos internos existentes relacionados com a proteção de dados, à luz das novas regras, e criar ainda mecanismos de controlo eficazes, no sentido de garantir o respetivo cumprimento do Regulamento.

Em 2021/2022, e terminada a 1ª fase de avaliação, o Município entrou na fase 2 **(planear)**, sobre a qual nos debruçaremos nos capítulos seguintes:

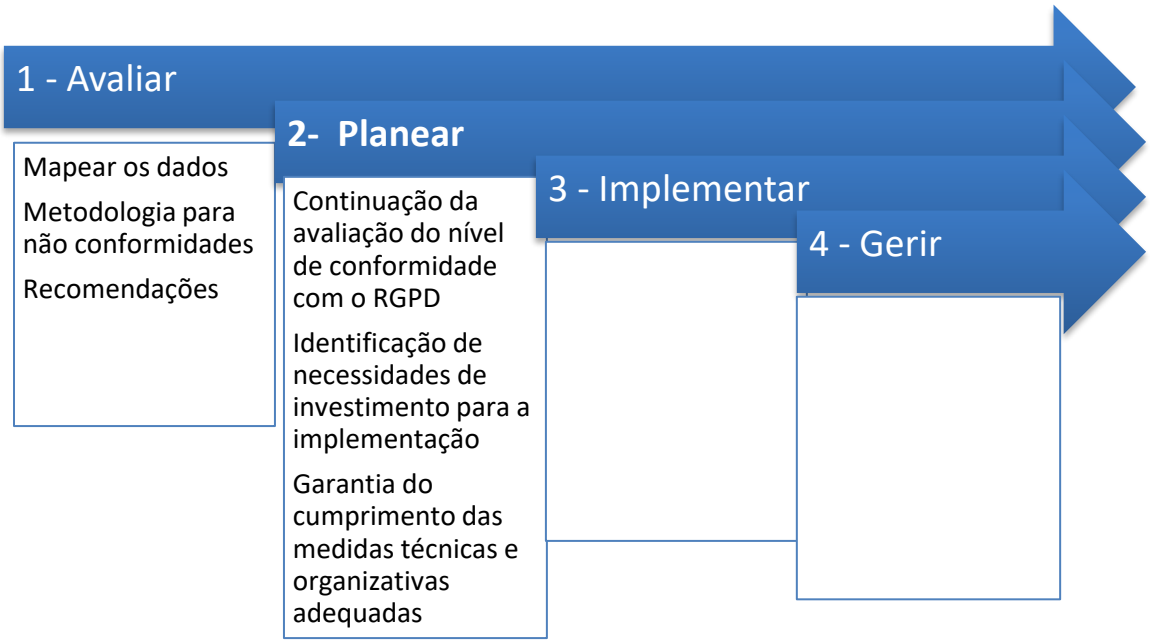


Figura 6: Evolução das fases de implementação do RGPD no Município de Pombal – Fase 2 (quadro elaborado pela autora).

4.3 Ponto de situação em 2022/2023

4.3.1 Implementação do Regulamento Geral de Proteção de Dados

Atendendo às recomendações apresentadas anteriormente e ao ponto de situação em que se encontrava a implementação em 2019, conforme referido no capítulo anterior, foram assumidas pelo Município de Pombal, as fragilidades existentes e as necessidades urgentes, no que concerne à matéria do RGPD, o que levou a que se definissem os requisitos, com vista à aquisição de novos serviços de consultoria para a continuação da implementação do Regulamento na organização, atendendo, quer às recomendações apresentadas em 2019, quer às dificuldades sentidas na operacionalização da metodologia seguida até àquele momento, com vista à obtenção dos resultados esperados.

Enquadramento

Em 2021, o Município de Pombal, pretendeu reforçar, além do RGPD, a área da cibersegurança, onde a implementação de regras e procedimentos também já estava a ser desenvolvida pela UO com a função Informática, garantindo a conformidade do seu modelo de gestão e da sua infraestrutura tecnológica, de acordo com as melhores práticas e normas existentes (ISO/lEC 27001, ISO/lEC 27002).

Estas auditorias aos sistemas de informação do Município de Pombal, teriam como principais objetivos medir/avaliar e incrementar um nível de segurança da organização e, simultaneamente, avançar para um processo contínuo de evolução do nível de segurança interno, face às exigências com que o Município de Pombal se deparada diariamente.

Pretendeu-se ainda um apoio ao Município de Pombal, na continuidade de incremento de cumprimento de regras de privacidade e proteção de dados e ainda um auxilio na definição de um modelo que fosse conforme e se adequasse às exigências impostas pelo RGPD, incluindo-se, neste contexto, a conformação de minutas/*standard's* e da documentação de suporte à generalidade dos procedimentos administrativos processados pelos diversos serviços municipais, com o RGPD e legislação conexa, e a compaginação com a matéria de acesso a documentos administrativos e informação administrativa, de acordo com o quadro legal aplicável, designadamente, Lei de Acesso aos Documentos Administrativos (LADA), de que deveria resultar um plano de ações e procedimentos a rever e a implementar.

Assim, na área da Privacidade e Proteção de Dados, a prestação de serviços deveria contemplar os seguintes objetivos:

a) Continuação da avaliação do nível de conformidade face aos requisitos legais, em particular face aos que se encontram definidos no Regulamento Geral sobre Proteção de dados Pessoais (RGPD);
b) Identificar necessidades de investimento para a implementação do Regulamento Geral sobre Proteção de dados Pessoais (RGPD) a curto, médio e longo prazo (plano de evolução versus investimento);
c) Garantir o cumprimento das medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação utilizados pelo Município de Pombal;

O prestador de serviços deveria assegurar a disponibilização de um EPD externo, tendo como principais funções, as referidas acima no Capítulo 3 – "Encarregado de Proteção de Dados", destacando-se naturalmente a de aconselhar o Município de Pombal no respeito pelas normas de privacidade e proteção de dados e coordenar, sempre que solicitado, as ações de controlo da conformidade dos processos de tratamento de dados pessoais levados a cabo pelo Município, nomeadamente, através de ações de sensibilização internas, formação e auditorias.

Para cumprimento das funções descritas no número anterior, deveria ser criada uma equipa multidisciplinar a afetar à sua execução, de preferência com competências no domínio das normas e práticas de proteção de dados nacionais e europeus, incluindo um conhecimento profundo do RGPD, deveria ainda ter conhecimento das operações de tratamento efetuadas na área da Administração Pública, e das tecnologias da informação e da segurança dos dados, do setor público e inovação tecnológica e ainda capacidade para promover uma cultura de proteção de dados no seio da organização. Deveria ainda salvaguardar a prestação de serviços de formação, ajustando um plano de formação às necessidades encontradas,

Neste sentido, o que se pretendeu foi a garantia de resultados, que originassem, nomeadamente, a potencialização do conhecimento do estado de segurança da informação nos sistemas de informação e plataformas tecnológicas de suporte bem como a entrega de documentos e relatório confidencial relativo a auditoria e diagnóstico. Ao longo do projeto deveriam ainda existir momentos como a reunião de *kick off* para definição estratégica do âmbito e das prioridades, bem como, reuniões presenciais, com periodicidade mínima trimestral de *steering* para pontos de situação e acompanhamento de projeto. Do trabalho realizado (auditoria interna) deveriam ser apresentados um relatório de *top findings* de vulnerabilidades e um relatório de análise de resultados, com vista à correção das falhas identificadas.

4.3.2 A criação da Comissão de Segurança de Informação e Privacidade (CSIP)

Em 2021, em resposta aos desafios enfrentados nesta área, o Município de Pombal decidiu criar internamente uma comissão, designada Comissão de Segurança da Informação

e Privacidade (CSIP). Esta comissão, composta por quadros técnicos superiores da autarquia, com formação em diversas áreas (direito, auditoria, sistemas de informação e informática), tinha como objetivo contribuir de forma significativa para o sucesso da implementação do Regulamento na organização.

A criação desta Comissão, surgiu após a perceção, por parte da gestão de topo/órgãos representativos do Município de Pombal, da necessidade de promoção contínua e ativa da segurança da informação, a qual deveria ser assegurada, nomeadamente, pela definição de princípios orientadores e pela formação de uma equipa dedicada à gestão de questões relacionadas com a segurança da informação, tendo-lhe sido formalmente atribuídas funções e responsabilidades nesse sentido.

4.3.2.1 Âmbito e Referências

O âmbito de atuação da CSIP inscreve-se no quadro da implementação do Sistema de Gestão de Segurança da Informação (SGSI) do Município de Pombal, que abrange o universo dos Serviços Municipais, orientando-se, designadamente, pelos referenciais da Norma ISO/IEC 27001 e do Regulamento Geral sobre Proteção de Dados (RGPD) (Regulamento UE 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, transposto para a ordem jurídica nacional pela Lei n.º 58/2019, de 8 de agosto, bem assim, pela Lei n.º 26/2016, de 22 de agosto, na atual redação (vulgo Lei de Acesso aos Documentos Administrativos (LADA)).

4.3.2.2 Composição da CSIP (Comissão de Segurança de Informação e Privacidade)

Nos termos deliberados pelo órgão Câmara Municipal, integram a CSIP:

- O Vereador do Pelouro respetivo;
- O Diretor Municipal;
- O Chefe da DIMSI;
- O Chefe da Unidade Jurídica;
- Um Especialista de Informática;
- Um Técnico Superior de Auditoria e Controlo; e
- Um Técnico Superior de Direito do Apoio aos Órgãos Autárquicos.

Para além dos membros designados internamente, conforme acima deliberado, a CISP é ainda, composta por membros da empresa de consultoria, associados às vertentes da

cibersegurança, privacidade e segurança de informação. De seguida elencam-se as responsabilidades da Comissão de Segurança da Informação e Privacidade (CSIP) do Município de Pombal, no âmbito da criação, coordenação, manutenção e renovação do SGSI.

4.3.2.3 Responsabilidades da CSIP

A CSIP é responsável pela conformação documental relacionada com o SGSI (políticas, procedimentos e instruções de trabalho) e respetiva remessa para aprovação por parte do executivo municipal, em ordem a definir e implementar uma estratégia de Segurança da Informação (SI), tendo em conta a evolução da maturidade dos respetivos suportes tecnológicos, sistemas de informação e do nível de segurança da informação adequados e pretendidos. À CSIP caberá, ainda, concorrer para o controlo do mesmo SGSI, através, nomeadamente, do estabelecimento de métricas de avaliação interna contínua, de forma a garantir a priorização e gestão de esforços e investimentos, em cumprimento das obrigações que, nesta matéria, se impõem ao Município de Pombal (conforme referido supra).

4.3.2.4 Funções dos membros da CSIP

Em linha com as responsabilidades da CSIP, acima enunciadas, e sem prejuízo da função agregadora do Vereador, com o pelouro nos domínios da inovação tecnológica e energia, compete a todos os membros desta Comissão, designadamente, o seguinte:

- *"Garantir a conformação documental relacionada com o SGSI (políticas, procedimentos e instruções de trabalho) e respetiva remessa para aprovação por parte do Executivo Municipal;*
- *Definir e organizar ações a desencadear para sensibilização de todos quantos integram o universo dos Órgãos e Serviços Municipais, em matéria de segurança da informação e referenciais normativos aplicáveis, nos termos das políticas, procedimentos e instruções de trabalho, oportunamente divulgadas;*
- *Verificar, no universo dos serviços municipais, o cumprimento dos pressupostos e operacionalização do controlo do SGSI, através, nomeadamente, do estabelecimento de métricas de avaliação interna*

contínua, de forma a garantir a priorização e gestão de esforços e investimentos, em cumprimento das obrigações que, nesta matéria, se impõem ao Município de Pombal.

- *Aos membros da CSIP com responsabilidades funcionais na área da tecnologia, no caso, o Vereador, o Chefe da Divisão de Informática, Modernização Administrativa e Sistemas Inteligentes (DIMSI) e o Especialista de Informática, competirá em especial a prossecução das matérias associadas às TI e ao robustecimento dos SI, nos termos previstos, entre outros, no Artigo 55.º do Regulamento de Organização dos Serviços Municipais (ROSM) deste Município, sem prejuízo do cumprimento de demais aspetos conexos."* – Funções da CSIP, constantes da deliberação da Câmara Municipal de Pombal, na ata da reunião de 16 de julho de 2021, disponível portal em www.cm-pombal.pt.

4.3.2.5 Funções do *Security Officer* - SO

O *Security Officer* é a entidade externa de consultoria / auditoria de segurança da informação *(SO)*, que fornece serviços especializados, no âmbito da disciplina de segurança da informação, orientados para a estratégia do Município de Pombal.

O *SO* certifica-se que todas as aplicações desenvolvidas *in-house* ou, incorporadas por *outsiders*, incluem medidas de controlo adequadas no âmbito e criticidade da sua atuação. O *SO* deve ter assento em outras comissões ou *task-forces* criadas pelo Município de Pombal, sendo reconhecido como o especialista *in-house* da disciplina de segurança da informação, promovendo, constantemente, a evolução do nível de segurança do Município de Pombal face à sua estratégia:

O objetivo é que estas duas figuras, CSIP e SO, trabalhem em total parceria e colaboração, com o intuito de definir as medidas técnicas e organizativas, bem como os procedimentos adequados, com vista à implementação do RGPD na organização.

É nesta altura, que me é lançado o desafio por parte do executivo municipal, para integrar, enquanto jurista do Município, esta Comissão, dando assim, o meu contributo, essencialmente na componente jurídica e administrativa, a este grupo de trabalho.

4.3.3 Políticas, Procedimentos e Manuais de Boas Práticas

Por conseguinte, em resultado do trabalho efetuado pela CSIP, em parceria com todos os serviços da organização e sob a égide da consultora, foi elaborado um vasto conjunto de documentação, que foi aprovada pelo órgão com competência, no caso, a Câmara Municipal, que se consubstanciou em várias políticas e procedimentos. Toda essa documentação aprovada encontra-se disponível na intranet do Município de Pombal, no entanto procedeu-se à seleção dos documentos que se entendeu serem mais relevante no âmbito do presente trabalho e efetuado uma tabela, contendo o nome do documento e a respetiva descrição sumária, que se junta como Anexo II.

Todos os serviços do Município de Pombal, nos termos constantes no organigrama alojado no portal institucional, em https://www.cm-pombal.pt/, são responsáveis por concorrer para a manutenção das políticas, normas e controlos de segurança da informação definidos, bem assim, para a implementação e monitorização de controlos fixados, de forma a garantir a integridade, disponibilidade e confidencialidade da informação.

São ainda responsáveis por colaborarem ativamente com a CSIP, no tratamento de assuntos no âmbito de segurança da informação, sempre que tal lhes seja exigível e solicitado.

Todos os colaboradores associados ao universo dos serviços municipais e todas entidades externas com acesso à informação, são responsáveis pela proteção daquela a que têm acesso, em função da política e procedimentos de SI, que se encontram definidos e aprovados, os quais devem conhecer, respeitar e fazer respeitar.

A inobservância desta responsabilidade, pelos colaboradores e entidades externas poderá ser passível de instauração de processo disciplinar, quando aplicável, sem prejuízo de eventual responsabilidade civil e criminal a que haja lugar.

4.3.4 Designação do Encarregado de Proteção de Dados - EPD

Em conformidade e por despacho, do Presidente da Câmara Municipal de Pombal, de 18/11/2019, foi designado EPD deste Município, para efeitos do RGPD, o *CIO*, da empresa de consultoria, a quem compete, no desempenho das suas funções, ter em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do mesmo, bem assim, as seguintes responsabilidades:

- Informar e aconselhar o responsável pelo tratamento ou subcontratantes, bem como todos os colaboradores associados ao universo dos serviços municipais que tratem dados, a respeito das suas obrigações, nos termos do RGPD, de outras disposições de proteção de dados da União ou dos Estados-Membros e do ordenamento jurídico nacional;
- Controlar a conformidade com o RGPD, bem como com outras disposições de proteção de dados da União ou dos Estados-Membros e do ordenamento jurídico nacional, com as políticas do responsável pelo tratamento ou dos subcontratantes relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, promover a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes (internas, externas, programadas ou não programadas);
- Prestar aconselhamento, quando tal lhe for solicitado, no que respeita à AIPD e controlar a sua realização nos termos do RGPD;
- Cooperar e articular com a autoridade de controlo as questões relacionadas com o tratamento, incluindo a consulta prévia e consulta (se aplicável), a esta autoridade, sobre qualquer outro assunto.

Em setembro de 2022, foi efetuada uma nova auditoria que teve como objetivo, aferir e classificar o estado de conformidade do Município de Pombal, em relação à legislação aplicável em matéria de proteção de dados, fornecendo, assim, um relatório detalhado acerca de todos os requisitos, com relevância operacional e legal no tratamento de dados pessoais.

A Auditoria de conformidade realizada às operações de tratamento de dados pessoais executadas pelo Município de Pombal na qualidade de Responsável pelo Tratamento, visou apoiar esta organização na análise e cumprimento dos requisitos jurídicos estabelecidos pelo RGPD e demais legislações complementares, permitindo identificar as suas lacunas e apresentando, simultaneamente, propostas para a sua efetiva correção.

Concluiu o relatório, do que de mais relevante se possa considerar, dada a confidencialidade do mesmo, que o que se revelou como mais crítico, foi a matéria associada às transferências internacionais de dados pessoais, para a qual o Município de Pombal não apresentava qualquer nível de conformidade, àquela data.

4.3.5 Plano de Ações

Na sequência da auditoria/do levantamento efetuado e das fragilidades ainda detetadas, foi apresentado um plano de ações, ínsito num relatório, abarcando as várias matérias, a tratar/melhorar pelo Município.

Optou-se por retirar do referido plano de ações constante do relatório, aquelas matérias que se entendeu serem as mais pertinentes fazendo uma abordagem à luz dos princípios do RGPD, de forma resumida, como seguidamente se elenca. Entramos agora na fase 3 **(Implementar)**

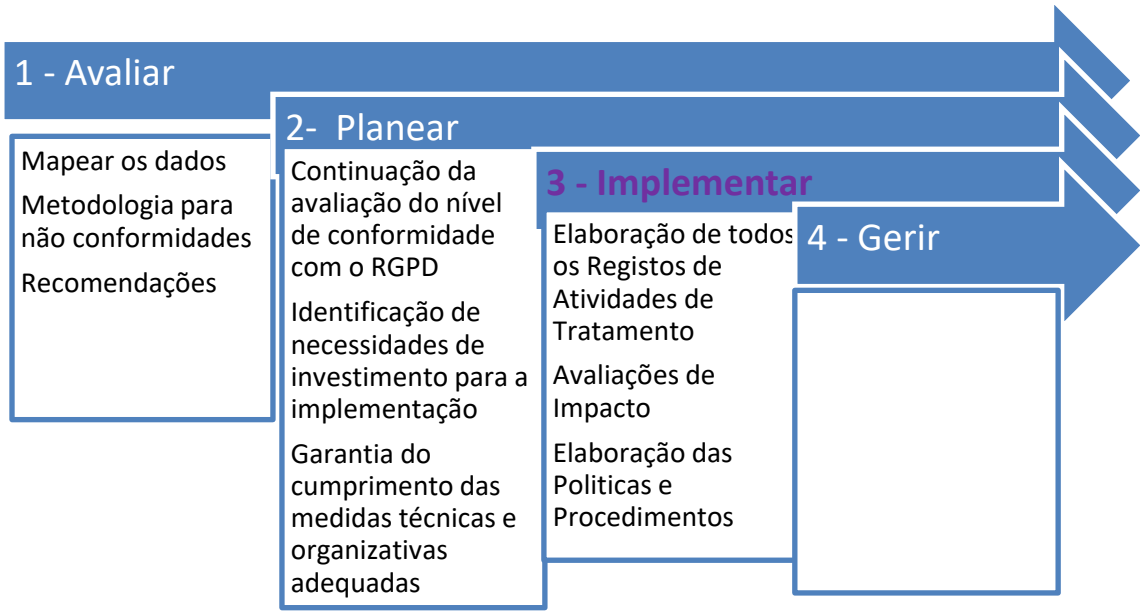


Figura 7: Evolução das fases de implementação do RGPD no Município de Pombal – Fase 3 (quadro elaborado pela autora).

No que se refere aos princípios aplicáveis ao tratamento, ficou evidente, que no que se refere ao princípio da licitude, houve necessidade de rever e atualizar os registos de atividades de tratamento, identificando com maior precisão e detalhe as suas operações de tratamento de dados. Quando, neste âmbito, se aplicar a necessidade de prosseguir uma função de interesse público, deveria o responsável pelo tratamento identificar a norma jurídica ou o conjunto de normas jurídicas que correspondem ao interesse público, tendo em consideração o Direito da União Europeia ou o Direito Interno.

No plano do cumprimento dos princípios da lealdade e transparência, foi proposto incluir em todos os pontos de recolha de dados pessoais (formulários, requerimentos, etc.) informação relativa à operação de tratamento de dados, informando o titular de dados, de modo claro, objetivo e simples, acerca do âmbito das operações de tratamento de dados em

causa e rever o aviso de proteção de dados disposto no website (vulgarmente, "Política de Privacidade")[7], por forma a providenciar informação objetiva e completa, expurgando as formulações genéricas e abstratas que nele constam, uma vez que a politica e privacidade existente e utilizada àquela data, não se encontrava ainda conforme.

Foi ainda recomendado, providenciar ao titular de dados um conjunto mínimo de informações, tais como, a identidade e os contactos do responsável pelo tratamento, os contactos do Encarregado da Proteção de Dados, bem como as finalidades do tratamento a que os dados pessoais se destinam. Nas situações em que o fundamento de licitude fosse o consentimento, deveria informar-se, ainda, o titular dos dados da existência dos vários direitos de que o mesmo goza nos termos do RGPD, incluindo o direito de retirar o consentimento em qualquer altura, sem comprometer a licitude do tratamento, efetuado com base no consentimento previamente dado.

Deveria também, desenvolver-se uma política aplicável ao tratamento de dados realizados através das redes sociais. Finalmente no âmbito desta matéria da lealdade e da transparência, dispor, junto dos locais de recolha de imagens, de um aviso informativo contendo a seguinte menção: «Para sua proteção, este local é objeto de videovigilância», informando igualmente, se aplicável, qual a entidade de segurança privada autorizada a operar o sistema, pela menção do nome e alvará/licença, indicando ainda qual o responsável pelo tratamento dos dados recolhidos perante quem os direitos de acesso e retificação poderiam ser exercidos.

No que se refere à Limitação das Finalidades as recomendações apresentadas, passaram por identificar claramente as finalidades e os dados pessoais a recolher, realizando uma avaliação de compatibilidade entre as diferentes finalidades, antes de usar os dados pessoais para uma finalidade diferente da recolhida originalmente, tendo em conta os requisitos previstos no n.º 4 do artigo 6.º do RGPD.

Também na matéria da Minimização dos Dados, para garantir a proteção de dados pessoais, foi recomendado identificar e justificar os dados pessoais necessários ao tratamento, cessar a recolha de dados desnecessários, estabelecer prazos de conservação de dados e registá-los no registo de atividades de tratamento (RAT´s), o que não acontecia.

[7] https://www.cm-pombal.pt/politica-de-privacidade-e-termos-de-utilizacao/

Também era indispensável adotar um procedimento de destruição de dados após o período de conservação (identificando os vários prazos de conservação, nos termos da Portaria 1253/2009, de 14 de outubro), com registo e prova da sua destruição.

Em matéria de *accountability* foi recomendado criar um mecanismo, num formato estruturado de registo de atividades de tratamento, em que cada serviço identificaria as diversas atividades desempenhadas que tratassem dados pessoais, com vista ao levantamento exaustivo de todos os processos, identificando o responsável pelo tratamento em cada uma dessas atividades e quais as ações que deveriam tomar em casa uma delas, servindo de guia de implementação das regras de atuação, caso a caso.

Em matérias de direitos dos titulares dos dados e direito de acesso, foi ainda recomendado que se definissem processos objetivos e concretos para permitir o acesso aos dados pessoais e sua transmissão ao titular de dados, além de divulgar uma política de exercício dos direitos dos titulares e definir um procedimento que permita a agregação dos dados pessoais em toda a extensão das atividades de tratamento. Quanto ao direito de retificação, teriam de se definir campanhas regulares para a atualização de dados pessoais, com um procedimento interno e responsabilidades claras, criando um procedimento para comunicar pedidos de retificação aos titulares de dados, campanhas essas que deveriam ocorrer pelo menos uma vez por ano. No caso do direito ao apagamento o Município deveria criar um procedimento que permitisse comunicar a existência de um pedido de apagamento apresentado pelo respetivo titular de dados.

Na questão do direito à limitação do tratamento seria recomendável definir procedimentos objetivos para limitar o tratamento de dados quando o titular exerce o direito de limitação, bem como definir as condições para a recolha e obtenção de consentimento, a fim de garantir a continuidade do tratamento de dados que tenha sido limitado.

Na matéria de direito de portabilidade dos dados teria de se desenvolver procedimentos que permitissem assegurar que, no âmbito do direito à portabilidade dos dados, seriam fornecidos ao respetivo titular os seus dados pessoais num formato estruturado, de uso corrente e de leitura automática. Já em matéria do exercício do direito de oposição, recomendou-se o desenvolvimento de procedimentos para garantir que, quando o titular dos dados exercesse o direito de oposição, o tratamento dos seus dados pessoais cessaria, exceto se se mantivessem outras obrigações legais. Seria importante criar um procedimento interno para avaliar a existência de razões imperiosas e legítimas para o tratamento, que prevalecessem sobre os interesses, direitos e liberdades do titular dos dados.

No quadro das obrigações do responsável pelo tratamento e subcontratante, recomendou-se também a inclusão, nos procedimentos de contratação pública, dos requisitos que permitissem aos concorrentes demonstrar a sua conformidade com o RGPD. Devendo definir-se um procedimento de avaliação das garantias apresentadas ou fixar critérios específicos de ponderação para a aferição dessa mesma conformidade. Devendo identificar todos os subcontratantes e estabelecer um acordo sobre o tratamento de dados pessoais com eles.

Seria ainda essencial ao bom sucesso da implementação, o levantamento do registo das atividades de tratamento (RAT), que se consubstanciariam no mapeamento e documentação de todas as operações de tratamento de dados, identificando as operações que exigiriam a identificação do titular de dados, incluindo a menção aos subcontratantes e identificando os acordos com estes no RAT. Também se recomendou estabelecer fundamentos de licitude e um ponto de contacto interno para comunicações com a Autoridade de Controlo.

Finalmente em matéria de segurança dos dados pessoais e do seu tratamento, recomendou-se a realização de avaliação de risco, identificando o risco inerente a todas as atividades de tratamento de dados, bem como a definição de medidas técnicas e organizativas adicionais. Foi ainda recomendado estabelecer um processo de revisão periódica das medidas técnicas e organizativas e identificar os locais físicos onde os dados pessoais eram armazenados, catalogando-os e definindo medidas de segurança para mitigar o acesso indevido. Recomendou-se ainda, a definição de uma política de secretária-limpa e uma metodologia de gestão de risco para as operações mais críticas. Foi necessário estabelecer um plano de auditorias periódicas, uma política de password forte e uma política quanto ao sistema de circuito de TV interno. Quanto às transferências internacionais de dados, foi suscitada a necessidade de identificar, implementar e documentar as medidas técnicas e organizativas adequadas para a transmissão desses dados pessoais.

Quanto à violação de dados pessoais, sugeriu-se que fosse definido um plano de recuperação de desastres para incidentes físicos ou técnicos, tais como, os desastres naturais, cortes de energia, ciberataques ou outros imprevistos, realizando testes periódicos ao website para identificação de vulnerabilidades e difundindo uma política e procedimento de violação de dados pessoais, no sentido de sensibilizar os colaboradores na identificação e comunicação de eventuais violações.

Também foram analisadas as questões das matérias relacionadas com eventuais avaliações de impacto sobre a proteção de dados e foi recomendado definir e/ou atualizar-se a política de AIPD, definindo uma metodologia que permitisse determinar quais os casos em a mesma seria exigida, identificando o nível de risco dessas operações.

Finalmente e no que concerne à transferência de dados pessoais com base numa decisão de adequação, deveria o Município incluir no registo de atividades de tratamento a referência (caso existisse) à decisão de adequação, identificando os países terceiros ou organizações internacionais relativas às quais a Comissão Europeia, haja adotado uma decisão de adequação.

No caso de transferências sujeitas a garantias adequadas, deveria identificar-se e documentar o conjunto de operações que implicariam a realização de transferência de dados para países terceiros ou organizações internacionais, quais os destinatários dessas transferências, invocando o fundamento de licitude das transferências internacionais de dados pessoais.

Deveriam ser incluídas nas políticas e procedimentos adotados, as respetivas referências à realização de transferências internacionais de dados pessoais para países terceiros ou organizações internacionais, designadamente, através da utilização de *cookies* do *Google Analytics;*

Deveria ainda identificar-se os fundamentos de licitude utilizados para a recolha de dados pessoais através da ferramenta *WebChat* disponível no *website*, informando os titulares de dados que a utilização da ferramenta *WebChat* implicaria a realização de transferências internacionais dos seus dados para outros países.

Fechado o ciclo da fase 3 - Implementação, seguir-se-á a fase 4 – Gerir, conforme se pode observar na Figura 8.

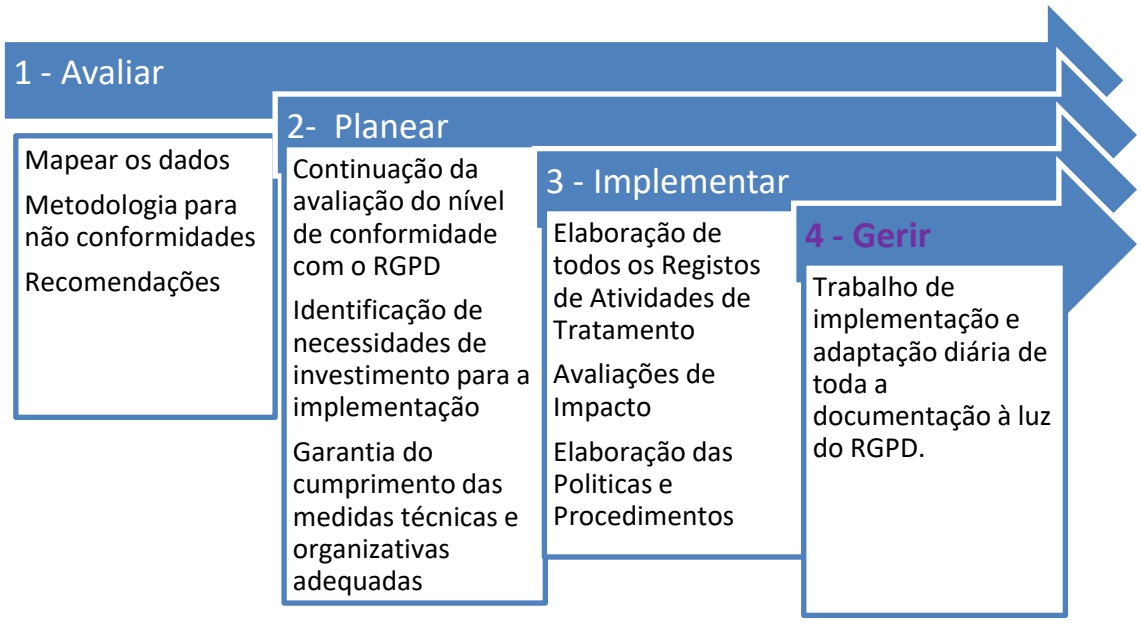


Figura 8: Evolução das fases de implementação do RGPD no Município de Pombal – Fase 4 (quadro elaborado pela autora)

Tornou-se assim crucial para o Município manter as suas políticas e processos internos em consonância com as diretrizes estipuladas pelo RGPD, mantendo uma revisão e atualização periódica destes documentos e procedimentos, estando assim a garantir a conformidade com o Regulamento, sendo por isso, a fase de gestão, uma fase de acompanhamento contínuo.

4.3.6 Município de Pombal – Casos Práticos

Elencam-se de seguida, algumas situações concretas que ocorreram no Município de Pombal, que refletem as dúvidas e as dificuldades dos próprios serviços no tratamento das matérias ligadas à Proteção de Dados.

Em conjunto com a Divisão de Informática Modernização e Sistemas Inteligentes do Município de Pombal, foi desenhado pela CSIP um procedimento para fazer chegar à Comissão, as solicitações dos colaboradores relativas a pedidos de esclarecimentos relacionados com os assuntos de Privacidade Proteção de Dados.

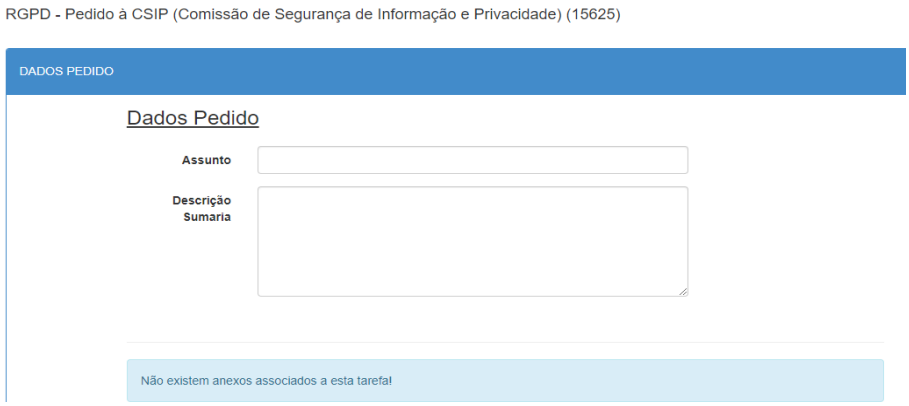


Figura 9: Aplicação desenvolvida pelo Município para a tramitação de pedidos à CSIP.

No desempenho das minhas funções enquanto membro da CSIP, esta comissão procedeu à análise e tratamento de alguns casos, que agora se relatam, referindo, desde já, que as informações que se seguem foram extraídas de quatro processos que deram entrada no Município de Pombal, em matéria de RGPD, e nesse sentido far-se-á uma breve explanação desses casos, omitindo, naturalmente quaisquer identificações, ou dados dos seus intervenientes.

a) Solicitação de direito a ser esquecido

Pedido: solicita-nos um munícipe, ao abrigo do nº 1 alínea a) do Artigo 17º do RGPD, o exercício do direito ao apagamento dos dados («direito a ser esquecido») dos seus pais, já falecidos, assim como os seus, da Divisão de Obras Particulares, uma vez que os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento.

Resposta: na sequência do pedido e da prévia auscultação do EPD do Município de Pombal, foi pela Comissão de Segurança de Informação e Privacidade do Município de Pombal, informado ao munícipe que, nos termos do Considerando 27, do RGPD, este "não se aplica aos dados pessoais de pessoas falecidas. Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas."

Efetivamente, o exercício dos direitos em relação a dados pessoais de titulares falecidos, quando estejam em causa dados sensíveis (cf n.º 1 do artigo 9.º do RGPD) ou dados que se reportem à intimidade da vida privada, à imagem ou a dados relativos a comunicações, são exercidos por quem tenha sido designado para o efeito pelo titular ou, na sua falta, pelos respetivos herdeiros.

Todavia, no caso em apreço, não estando em causa dados sensíveis (n.º 1 do artigo 9.º do RGPD) ou dados que se reportem à intimidade da vida privada, à imagem ou a dados relativos a comunicações, não subsistem dúvidas de que o RGPD não é aplicável.

No que se reporta aos dados pessoais do munícipe, oportunamente, recolhidos e tratados junto da Divisão de Obras Particulares, foi informado que o pedido seria encaminhado para os serviços municipais competentes, para a adoção das medidas técnicas e organizativas adequadas, ante o quadro legalmente aplicável, na medida em que não existe fundamento de licitude para o tratamento dos dados estes deverão ser apagados de todas as bases de dados e quaisquer operações de tratamento devem ser imediatamente cessadas, excetuando-se os casos em que exista uma obrigação legal para os manter. No caso de os dados do titular em questão terem sido partilhados com entidades terceiras, o Município de Pombal deveria solicitar junto dessas entidades a cessação das operações de tratamento e o apagamento dos dados.

No caso de existir uma obrigação legal para manter os dados do titular, o Município de Pombal deverá ainda informar o titular dos dados das razões que justificam esse posicionamento.

b) Solicitação de direito ao apagamento

Pedido: solicita-nos um munícipe no uso do exercício de direitos relativos aos seus dados pessoais, o exercício do direito de Apagamento, nos termos do artigo 17º do Regulamento Geral de Proteção de Dados.

Resposta: foi informado o requerente que não se poderia atender ao seu pedido, pois os dados, eram necessários para o cumprimento de obrigações legais, em atendimento ao exigido pelo artigo 17º, 3, b, do RGPD. De acordo com a Portaria 1253/2009, de 14 de outubro. Assim, dando cumprimento à legislação em vigor, não se poderia proceder à eliminação dos dados pessoais constantes no contrato de abastecimento de água e respetivas faturas.

c) Canil Municipal

Pedido: solicita o Serviço do Canil Municipal informação sobre se pode proceder à partilha de imagens nas redes sociais, nomeadamente à recolha de fotografias, no momento da adoção, de visitas e outras semelhantes. Tendo em conta que, o que se pretende, é que a divulgação dos animais adotados não cesse.

Resposta: é prudente a adoção de medidas/procedimentos que mais se compaginem com o cumprimento do RGPD, assim o assunto terá de ser robustecido em consonância como DPO, no entanto consensualizou-se, em sede de CSIP que até lá, seria prudente os serviços absterem-se, designadamente, de partilharem nas redes sociais em nome do Município de Pombal, ou serviços respetivos, conteúdos, sejam imagens ou outras, que contenham dados pessoais (regista-se que as fotografias dos animais, não consubstanciam dados pessoais e poderão ser úteis para divulgar atividades), isto, diga-se independentemente de qualquer consentimento dado.

Referiu-se ainda que o suprarreferido, não prejudica a publicação de conteúdos para divulgação de atividades Municipais, antes, apela a todos, cuidados redobrados relativamente ao que se divulga, na medida em que, o que está em causa, é a transferência de dados pessoais para fora do espaço Europeu e, por isso em colisão com as regras do RGPD (ex: transferência de dados pessoais para os EUA) que em todo o caso, em nome do Município, estamos obrigados a cumprir.

d) Transmissões online das Reuniões de Câmara e Assembleias Municipais

O Município de Pombal, procedia às transmissões online das Reuniões de Câmara e das Assembleias Municipais, no âmbito do princípio da transparência e por ser uma forma de levar o poder local até mais próximo da população, quer a nível local, quer a todos os Pombalenses espalhados pelo mundo. No entanto, com a entrada em vigor do RGPD, esta passou a ser uma matéria sensível, de acordo com o preconizado no Parecer 2022/62 da CNPD, após a cessação da vigência do regime excecional e transitório (Lei n.º 1-A/2020, de 19 de março - medidas excecionais e temporárias de resposta à situação epidemiológica provocada pelo coronavírus SARS-CoV-2 e da doença COVID-19) deixou de existir previsão legal que reconhecesse às autarquias locais, uma específica função de divulgação mediática da sua atividade plenária.

Nestes termos, no exercício das minhas funções, atempadamente emiti uma proposta junto da CSIP, no sentido de alertar os órgãos políticos, para o facto de podermos estar perante um incumprimento das regras do RGPD, por um lado, por falta de consentimento dos intervenientes, membros e público em geral que participa nas sessões, e por outro, no que se refere à transferência de dados para fora do espaço europeu.

Posto isto, não existindo norma legal que preveja especificamente a transmissão online e em direto das reuniões públicas dos órgãos das autarquias locais, nem que

reconheça às autarquias locais uma específica função de divulgação mediática da sua atividade plenária habitual, nem se afigurando necessária para a realização do princípio da publicidade das reuniões das assembleias municipais, concluiu-se que o consentimento prévio e expresso de todas as pessoas abrangidas pela filmagem e transmissão, aparecia como única condição suscetível de legitimar o referido tratamento de dados.

Assim, foi decidido pelos órgãos políticos, quer em sede de Câmara, quer em sede de Assembleia, proceder à recolha dos respetivos consentimentos de todos os intervenientes nas sessões e passar a fazer as transmissões das reuniões no portal do Município e não nas redes sociais, garantindo assim, que não existia transferência de dados para fora do espaço europeu.

Assim, e nesta sequência, foi elaborado e remetido o formulário de consentimento a todos os membros dos órgãos do Município, relativo à transmissão online e em direto das reuniões públicas dos órgãos das autarquias locais, com vista à recolha do respetivo consentimento de todos os intervenientes nas reuniões.

Estas foram algumas das situações que ocorreram e vão ocorrendo no Município de Pombal relativamente à matéria de RGPD e que aqui deixámos apenas a título meramente exemplificativo. A noção que vamos tendo, é que os cidadãos, cada vez mais informados, vão exercendo estes seus direitos mais amiúde, quer em sede de atendimento municipal, alegando, por exemplo, que não permitem a digitalização do seu cartão de cidadão, mas apenas a recolha dos dados suficientes para o fim a que se destinam, quer em sede de pedidos específicos para o exercício dos seus direitos, como verificámos acima.

Como nos diz Rodrigues e Teves (2020) *"As evoluções introduzidas pelo RGPD demonstram-se essenciais ao desenvolvimento do Mercado Único Digital, assim como à proteção de dados das pessoas singulares, que até então viam os seus dados pessoais a ser constantemente violados, e com poucos mecanismos de defesa dos seus direitos, sendo que o RGPD representa uma oportunidade dos responsáveis de tratamento de refazerem os seus modelos de tratamento de dados, não devendo por este modo ser encarado como um sistema penalizador e obrigacional aos responsáveis pelo tratamento, mas sim um regime protecionista dos dados pessoais."*

Vivendo num mundo cada vez mais digital, e havendo um conhecimento mais abrangente da existência destas regras por parte, quer dos cidadãos, quer da administração, faz com que tentemos todos os dias prestar um melhor serviço ao cidadão, sempre em

cumprimento das normas legais em vigor e sem nunca perder de vista a proteção dos dados dos seus titulares.

5. Trabalho futuro

No contexto atual da era em que vivemos, essencialmente digital, a proteção dos dados pessoais tornou-se uma preocupação fundamental para as autarquias, nomeadamente para os municípios. O RGPD é uma legislação abrangente que visa garantir a privacidade e a segurança dos dados pessoais dos cidadãos.

Para cumprir as exigências do RGPD, os municípios devem estabelecer medidas adequadas de proteção e implementar práticas eficazes de governança de dados. No Município de Pombal, entidade sobre a qual nos debruçámos no âmbito deste projeto, apesar de já se ter feito uma parte do caminho, a verdade é que muito há a desenvolver, no sentido de continuar a assegurar a conformidade contínua com o RGPD e proteger os direitos e liberdades dos seus cidadãos.

Uma das etapas cruciais para atingir melhores resultados é a da realização de Avaliações de Impacto de Proteção de Dados (AIPD), com vista a identificação e mitigação dos riscos associados ao tratamento de dados pessoais. O Município deve continuar a promover a realização regular dessas avaliações, especialmente com a implementação de projetos que envolvam o processamento de dados sensíveis. A AIPD permite uma análise criteriosa dos riscos à privacidade e proporciona uma base sólida para a implementação de medidas de segurança apropriadas.

A continuidade de um processo de conscientização e de formação contínuas, são essenciais para garantir que todos os agentes municipais compreendem plenamente as suas responsabilidades e o seu papel, em relação à proteção de dados. O Município deve continuar a investir em programas de formação atualizados sobre o RGPD, destacando as melhores práticas para a recolha, armazenamento e utilização segura dos dados pessoais.

As políticas e procedimentos internos do Município devem continuar a estar alinhados com as disposições do RGPD. É essencial rever e atualizar regularmente esses documentos para refletir as mudanças nas práticas de tratamento de dados e nas regulamentações aplicáveis. A aposta na continuidade de um programa de gestão de políticas permite monitorizar a conformidade e garantir que todos os colaboradores sigam as diretrizes estabelecidas.

A segurança dos dados continua a ser um dos aspetos fundamentais do RGPD, neste sentido o Município deve continuar a adotar medidas técnicas e organizacionais adequadas para proteger os dados pessoais contra o acesso não autorizado, a sua perda ou destruição.

Além disso, é importante continuar a manter-se atualizado sobre as ameaças de segurança emergentes e adotar medidas proativas para mitigar esses riscos.

Em suma, o cumprimento do RGPD é um processo contínuo e evolutivo para os municípios. Garantir a proteção adequada dos dados pessoais requer esforços contínuos, desde a implementação de políticas e procedimentos adequados até a formação dos funcionários e de todos os agentes municipais. Além disso, a atualização constante das práticas de segurança e a gestão eficaz das parcerias e subcontratantes são essenciais para garantir uma abordagem holística da proteção de dados. Ao adotar essas medidas e priorizar a privacidade dos cidadãos, o Município estará melhor posicionado para enfrentar os desafios futuros relacionados com o RGPD e assim continuar a proteger os direitos dos seus munícipes.

6. Conclusão

A implementação do RGPD nas autarquias tem sido um processo desafiante, uma vez que essas instituições lidam com um grande volume de dados pessoais sensíveis, desde informações de identificação pessoal, até informações financeiras e de saúde.

Uma das principais dificuldades com que as autarquias se deparam, tem sido a falta de recursos, tanto financeiros como humanos, para implementar as mudanças necessárias para estar em conformidade com o RGPD. Além disso, muitas autarquias têm processos e sistemas de informação antigos, que tornam mais difícil a implementação das medidas de segurança adequadas e das atualizações necessárias.

Outro desafio enfrentado pelas autarquias é a sensibilização e capacitação de seus funcionários. Muitos trabalhadores dessas instituições ainda têm pouco conhecimento sobre o RGPD e as suas implicações, o que pode levar a práticas inseguras de manuseio de dados.

No entanto, é importante ressaltar que a implementação do RGPD nas autarquias é fundamental para garantir a proteção dos direitos fundamentais dos indivíduos e evitar violações da privacidade. As autarquias precisam ser capazes de proteger os dados pessoais que detêm, a fim de evitar riscos como a violação da privacidade dos cidadãos e a divulgação de informações sensíveis.

Portanto, é necessário que as autarquias priorizem a implementação do RGPD, alocando e capacitando os recursos necessários ao seu cumprimento, garantindo assim a proteção dos dados pessoais dos cidadãos e, ao mesmo tempo, evitando as consequências a nível contraordenacional, nomeadamente, a aplicação das coimas previstas pelo RGPD, em caso de violações.

As questões a que nos propusemos responder no início deste projeto, (de saber como adaptar e implementar estes novos procedimentos do RGPD numa organização pública? Quais as etapas que se têm de verificar? Quais as alterações que devem acontecer?), encontra respostas ao longo de todo o nosso trabalho. Acreditamos ter conseguido ter dado algumas respostas e apontado alguns caminhos, com vista a facilitar a tarefa de quem tenta implementar o RGPD numa organização, nomeadamente, numa autarquia local.

Em resposta às perguntas colocadas sobre como adaptar e implementar os novos procedimentos do RGPD numa organização pública, o processo pode ser detalhado de acordo com os seguintes passos.

Primeiramente, é crucial a organização ter consciência da necessidade de implementar o RGPD. Isto implica a compreensão do impacto e relevância do RGPD na gestão dos dados pessoais dentro da organização.

Em seguida, é necessário identificar a capacidade interna para implementar e gerir o processo. Este passo pode resultar na contratação de ajuda externa, especialmente se a complexidade da tarefa for além das competências internas da organização. No caso do Município de Pombal, a opção foi exatamente por recorrer a um apoio externo.

Após a avaliação da capacidade interna, o próximo passo é iniciar um levantamento de todos os procedimentos onde ocorre o tratamento de dados pessoais. Este levantamento é fundamental para se ter uma visão clara do estado atual da organização em relação à conformidade com o RGPD.

O passo seguinte é o planeamento da implementação do RGPD. Isto envolve a continuação da avaliação do nível de conformidade com o RGPD e a identificação das necessidades de investimento para a sua implementação. Com o planeamento feito, inicia-se a fase de implementação do RGPD. No Município de Pombal, isto envolveu a criação de um grupo de trabalho multidisciplinar, a CSIP. Esta comissão foi responsável por atividades como a elaboração do RAT, a realização de AIPD e a elaboração de políticas e procedimentos adequados, quer ao nível da proteção e privacidade dos dados, quer a nível das boas práticas para a segurança de informação, contemplando obviamente os aspetos relacionados com a cibersegurança.

Por fim, a gestão contínua de todo o processo é fundamental. Isto implica um acompanhamento ativo e contínuo das atividades relacionadas com a privacidade e o tratamento de dados pessoais na organização. É importante notar que este esforço vai além da fase inicial de implementação do RGPD, sendo uma atividade permanente que deve ser incorporada na rotina da organização. No caso do Município de Pombal esta incumbência está atribuída à CSIP.

Pretende-se também que este projeto possa constituir um apoio, um auxílio para quem, dentro de uma autarquia local, tenha que lidar com o impacto que esta realidade do RGPD trouxe a estas organizações, fazendo um levantamento das necessidades e das dificuldades encontradas.

Mas a verdade é que, após me ter debruçado mais atentamente sobre as várias matérias que constituíram este trabalho, também concluí que a intenção deste Regulamento de ser um instrumento fundamental para a formulação de uma visão unificadora da legislação

sobre proteção de dados em toda a União Europeia, não terá sido conseguido na sua plenitude, uma vez que ainda há muito caminho a ser percorrido, quer no âmbito de cada uma das legislações nacionais, quer em matéria de transferência de dados para fora do espaço europeu.

O facto de, concretamente no caso português, a Autoridade de Controlo (CNPD) ter de emanar, por diversas vezes, deliberações e pareceres, com vista à clarificação das várias desconformidades existentes entre o Regulamento (EU) 2016/679 e a Lei Nacional (Lei 58/2019 de 8/08), são a prova de que este caminho está longe de estar terminado.

Nesta era cada vez mais digital em que vivemos, este Regulamento constitui um verdadeiro ponto de viragem, na medida em que todos os Estados-Membros buscam um alinhamento para a construção de uma União Europeia mais forte e resistente perante os desafios emergentes. Efetivamente, os desafios ainda são muitos e, embora as autarquias locais tenham de estar preparadas para os acompanhar, a verdade é que a prioridade dessas entidades tem sido claramente a salvaguarda dos direitos dos cidadãos europeus. As autarquias, apesar de todas as complexidades e dificuldades na implementação do RGPD, estão empenhadas em garantir a proteção de dados e a privacidade dos seus munícipes, elevando os seus direitos acima de quaisquer obstáculos.

7. Bibliografia

Agência dos Direitos Fundamentais da União Europeia (FRA), Conselho da Europa e Secretaria do Tribunal Europeu dos Direitos do Homem (2014). Manual da Legislação Europeia sobre Proteção de Dados. doi:10.2811/73790.

Campos, Diogo Leite, Foz, Teresa & Gonçalves, Nuno (2019). Estrutura Jurídica do Regulamento Geral de Proteção de Dados (Rgpd) em Direito Português. Revista Jurídica Luso Brasileira. https://www.cidp.pt/publicacao/revista-juridica-lusobrasileira-ano-5-2019-n-1/186

Canotilho, Gomes & Moreira, Vital (2014). Constituição da República Portuguesa, Anotada. Coimbra: Coimbra Editora.

Comissão Nacional de Proteção de Dados (11 de novembro de 2022). Obtido de https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/historico-da-cnpd/.

Comissão Nacional de Proteção de Dados (16 de novembro de 2022). Obtido de https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-aplica-primeira-sancao-por-falta-de-epd/

Comissão Nacional de Proteção de Dados (12 de dezembro de 2022). CNPD sanciona INE por cinco contraordenações. Obtido de https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-sanciona-ine-por-cinco-contraordenacoes/

Comissão Nacional de Proteção de Dados (16 de novembro de 2022). Deliberação/2022/1040. Obtido de CNPD aplica a primeira sanção por falta de EPD: https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-aplica-primeira-sancao-por-falta-de-epd/

Comissão Nacional de Proteção de Dados (16 de novembro de 2022). Obtido de https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-aplica-primeira-sancao-por-falta-de-epd/

Comissão Nacional de Proteção de Dados (12 de dezembro de 2022). CNPD sanciona INE por cinco contraordenações. Obtido de https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-sanciona-ine-por-cinco-contraordenacoes/

Cordeiro, A. Barreto Menezes Cordeiro (2021). Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019. Faculdade de Direito da Universidade de Lisboa: Almedina Editora.

Costa, André Mendes (13 de junho de 2017). "Data Protection Officer according to GDPR" Obtido em 5 de março de 2023, de https://officialblogofunio.com/2017/06/13/2014/

Fazendeiro, Ana (2018) "Regulamento Geral Sobre a Proteção de Dados." Editora Almedina.

Ferreira, B., & Simões, S. (1 de julho de 2021). Comissão de Dados acusa Câmara de Lisboa de 225 infrações por ter divulgados dados pessoais de manifestantes. Obtido de O Observador: https://observador.pt/2021/07/01/envio-de-dados-a-embaixadas-comissao-nacional-acusou-camara-de-lisboa-de-ter-violado-regulamento-de-protecao-de-dados/

Francisco, Daniel & Francisco Sandra (2019), Regulamento Geral de Proteção de Dados – 7 passos para uma metodologia de implementação do RGPD na Administração Pública, Edições Sílabo.

Freitas, Tiago Fidalgo & Alves, Pedro Delgado (2021), "O Acesso à informação Administrativa." Coleção: CJP/CIDP. Editora Almedina.

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (2017). Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679

WP248rev.01. Disponível no portal: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (2017). Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 WP250rev.01. Disponível no portal: https://www.cnpd.pt/bin/rgpd/docs/wp250rev01_pt.pdf

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (2018). Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679 WP251rev.01. Disponível no portal: https://www.cnpd.pt/bin/rgpd/docs/wp251rev01_pt.pdf

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (2010). Parecer 8/2010 sobre a Proteção de Dados relativo à legislação aplicável 0836-02/10/PT WP 179. Disponível no portal: https://www.gpdp.gov.mo/uploadfile/others/wp179_pt.pdf

Grupo de Trabalho do art. 29º da Diretiva da Diretiva 95/46/CE para Proteção de Dados – Diretrizes de aplicação e fixação de coimas para efeitos do Regulamento 2016/679, 17/PT, WP 253, adotadas em 3 de outubro de 2017. [Consulta em 04/10/2020]. Disponível para consulta em: http://bit.ly/2VRYiCx

Grupo de Trabalho do Artigo 29.º sobre o encarregado da proteção de dados https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf

GT29-WP248. (2017). Grupo de Trabalho do Artigo 29.º. Obtido de Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679 WP248rev.01: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Kloza, D., Van Dijk, N., Gellert, R., Borocz, I., Tanas, A., Mantovani, E., & Quinn, P. (2017).https://www.researchgate.net/publication/346155402_Data_protection_impact_assessments_in_the_European_Union_complementing_the_new_legal_framework_towards_a_more_robust_protection_of_individuals

Miranda, Jorge e Medeiros, Rui (2005), Constituição Portuguesa Anotada, Tomo I, Coimbra Editora.

Oliveira, Inês (2018), "O Encarregado de Proteção de Dados no setor público: uma nova categoria da carreira de Técnico Superior." Revista Vida Judiciária. maio/junho 2018.

Oliveira, João Pedro Costa Perdigão Maia (2020). O acesso à informação na Administração pública, no contexto do regime geral de proteção de dados pessoais e das tecnologias de informação. Obtido de Faculdade de Direito, Universidade de Lisboa: https://repositorio.ul.pt/bitstream/10451/49612/1/ulfd0148984_tese.pdf

Portal do DPO - Encarregado de Proteção de Dados (s.d.). Obtido em: https://www.portaldodpo.pt/funcoes-do-dpo/

Ribeiro, Carolina R. Ramos (2020). "O impacto do novo regulamento geral de proteção de dados nas relações empresariais entre Brasil e União Europeia." https://repositorioaberto.uab.pt/handle/10400.2/10429.

Rodrigues, José Noronha & Teves, Daniela Medeiros (2020), A Proteção de Dados Pessoais e a Administração Pública, o Novo Paradigma Jurídico, AAFDL Editora. Livraria Almedina.
Doneda, Danilo (2006), "Da privacidade à Proteção de Dados Pessoais" Editora Renovar.

Silveira, Alessandra e Canotilho, Mariana (2013), Carta dos Direitos Fundamentais da União Europeia, Comentada, Editora Almedina.

Tamburri, Damian. A. (2020). "Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation" Information Systems 91.
Samuel D. Warren e Louis D. Brandeis, The Right to Privacy", Harvard Law Review. Vol. 4, N.º 5 (Dec.15, 1890) https://doi.org/10.2307/1321160

Van der Sloot, B., Hoofnagle, C. J., & Zuiderveen Borgesius, F. (2019). The European Union general data protection regulation. "what it is and what it means, Information & Communications Technology Law" doi:10.1080/13600834.2019.1573501

Zanini, L. E. de A. (2015). O surgimento e o desenvolvimento do right of privacy nos Estados Unidos. Revista de Doutrina da 4a Região, Porto Alegre, nº 64, 2.

8. Anexos

ANEXO I - Levantamento de Requisitos e Informação para aferir Conformidades e Ações de melhoria à luz do Regulamento Geral de Proteção de Dados. No Município de Pombal.

ANEXO II – Políticas e procedimentos do RGPD no Município de Pombal.

1 ENQUADRAMENTO GERAL

1.1 ENQUADRAMENTO DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS E SEUS REQUISITOS, PRINCÍPIOS DE PROCESSAMENTO DE DADOS PESSOAIS E DIREITOS DOS TITULARES DOS DADOS PESSOAIS

O Regulamento Geral de Proteção de Dados (de ora em diante, **RGPD**) EU n.º 2016/679, de 27 de abril de 2016, que se aplica ao tratamento de dados pessoais automatizados ou não, contidos em ficheiros ou a eles destinados (Artigo 2º) é uma mudança regulamentar com vista ao fortalecimento do direito dos indivíduos, à proteção dos seus dados pessoais, um suporte ao livre fluxo de dados, à redução de dados e a um maior controlo dos dados pessoais.

O RGPD estabelece regras relativa à proteção dos dados pessoais[1] de pessoas singulares, ao seu tratamento[2] e aos direitos que aos seus titulares assiste no que à livre circulação dos mesmos diz respeito.

Logo aqui, deparamo-nos com a primeira grande exceção: o RGPD não abrange os dados de pessoas coletivas, logo toda essa parte da atividade do **Município de Pombal** está excluída, o que não a exime, contudo, do dever de observar as regras do Regulamento para efeitos de tratamento dos dados pessoais dos Eleitos, Dirigentes, Munícipes, Trabalhadores, Fornecedores, Clientes e Protocolos existentes.

[1] 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;

[2] Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

O **Município de Pombal** é o órgão autárquico que tem por missão definir e executar políticas tendo em vista a defesa dos interesses e satisfação das necessidades da população local.

Cabe-lhe desta forma, promover o desenvolvimento do município em todas as áreas da vida, como a saúde, a educação, a ação social e habitação, o ambiente e saneamento básico, o ordenamento do território e urbanismo, os transportes e comunicações, o abastecimento público, o desporto e cultura, a defesa do consumidor e a proteção civil.

O **Município de Pombal** enquanto órgão autárquico é responsável pelo tratamento de Dados Pessoais e, neste sentido, terá que implementar os requisitos do Regulamento Geral sobre a Proteção de Dados, com objetivo de estar em conformidade com o mesmo.

De acordo com o Regulamento, os dados pessoais são quaisquer informações relacionadas com a pessoa identificada ou identificável (Nome, foto, endereço de e-mail, detalhes bancários, atualizações em sites de redes sociais, detalhes de localização, perfil da pessoa, informações médicas ou um endereço IP do computador, etc).

Nos termos da nova legislação o **Município de Pombal** deverá rever **a forma como trata os Dados Pessoais** a que tem acesso, **conhecer as novas regras, analisar as obrigações** deste regulamento e perceber como identificar que medidas são necessárias para estar em compliance:

- Políticas internas transparentes de proteção de dados, aprovadas pelo mais alto nível de gestão da organização;

- implementar políticas de sensibilização e consciencialização sobre o tratamento dos Dados Pessoais junto de todos os colaboradores;

- sensibilizar a organização para o cumprimento do Regulamento através da monitorização, avaliação, correção e demonstração de evidências do seu cumprimento;

- a implementação do **RGPD** tem que garantir o princípio de Responsabilidade, conforme definido no artigo 5º (2), que procura reafirmar e fortalecer a responsabilidade do **Município de Pombal** como Controlador e Processador de Dados, exigindo que demonstre a conformidade dos seis princípios **RGPD** (1):

O Regulamento determina que o **Município de Pombal** no processo de tratamento de dados pessoais obedeça a um conjunto de princípios que enunciamos de seguida:

1. Os dados pessoais deverão ser objeto de um tratamento **lícito, leal e transparente** em relação ao titular dos dados («licitude, lealdade e transparência»)[3]

   Para que se verifique a licitude do tratamento deverá dar-se por cumprida uma das condições previstas no artigo 6.º do Regulamento sendo que para o caso em concreto do **Município de Pombal** apenas atentaremos nas que se seguem:

- ou porque o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
- ou porque o tratamento é necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
- ou porque o tratamento é necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento está sujeito;

Seja qual for o motivo que legitime e torne lícito a recolha e o tratamento dos dados pessoais por parte do **Município de Pombal** o paradigma máximo a respeitar deverá ser sempre o da transparência.

Mas, mais uma vez, e no respeito pela transparência, e apesar da justificação para a recolha e tratamento dos dados pessoais recolhidos estar encontrada e justificada, o **Município de Pombal** não está desonerado de dar conhecimento aos Titulares dos Dados da razão da recolha da informação e qual o destino que lhes dará.

Finalmente, e nos casos em que o tratamento de dados pessoais tenha por base o consentimento prévio do titular dos dados – situações, por exemplo, em que o **Município de Pombal** preveja a

[3] Alínea a) do n.º 1 do artigo 5.º do Regulamento

necessidade de realizar ações de marketing, divulgação de produtos e serviços, contactos com clientes para outros fins que não apenas e tão só aqueles relacionados com os contratos assinados e para os quais não foi necessário obter consentimento, deverá verificar-se se esse consentimento foi dado de forma livre e esclarecida e no cumprimento das regras determinadas pelo artigo 7.º do Regulamento.

2. Recolhidos para **finalidades determinadas, explícitas e legítimas** e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades;

Quando o **Município de Pombal** procede ao tratamento dos dados pessoais, através das diferentes áreas de negócio com quem eles interagem, deverão ter sempre em consciência que aqueles dados são dados pessoais de pessoas singulares, que devem ser tratados para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; caso se entenda haver necessidade de tratar esses dados para outra finalidade deverá ser o cliente informado desse facto, recolhido consentimento para tal ou celebrado novo contrato nesse sentido.

3. **Adequados, pertinentes e limitados** ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);

Este princípio, o da conservação dos dados pessoais pelo mínimo período de tempo possível e apenas pelo período de tempo necessário para as finalidades para as quais foram recolhidos é um calcanhar de Aquiles em quase todas as Instituições, mas no caso das Autarquias Locais, existe um Regulamento Arquivístico fruto da legislação especifica aplicável às regras de conservação de documentos.

Determina o Regulamento Arquivístico para as Autarquias Locais que;

A) – O processo de avaliação dos documentos do arquivo das autarquias locais obedeça à determinação do seu valor para efeitos de conservação permanente ou eliminação, findos os respetivos prazos de conservação administrativa (os referidos prazos de conservação são contados a partir da data final dos procedimentos administrativos);

B) – É da responsabilidade dos serviços de arquivo de cada autarquia local a aplicação dos prazos de conservação dos documentos respeitando o constante da tabela anexada no Regulamento Arquivístico (anexonº1)

Contudo, o **Município de Pombal** não está exonerado, antes pelo contrário, de adotar **medidas seguras para efeitos de cumprimento dos pontos que se seguem e para efeitos de segurança dos dados conservados**.

4. **Exatos e atualizados** sempre que necessário, devendo ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»), procurando implementar mecanismos de retificação céleres, particularmente quando a falta de exatidão for apontada pelos próprios titulares dos dados por força de reclamações deduzidas;

5. **Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados**;

6. Tratados de uma forma que garanta a sua **segurança**, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («**integridade e confidencialidade**»);

O **Município de Pombal** deve definir os processos, procedimentos e atividades necessários para assegurar o respeito pelos Direito dos Titulares dos Dados:

Note-se que, independentemente da forma que legitime o tratamento dos dados por parte do **Município de Pombal**, e uma vez que os dados pessoais são recolhidos junto do cliente deverão ser prestadas, um conjunto de informações[4] que enunciamos:

- a identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
- os contactos do encarregado da proteção de dados;

[4] Vide artigos 13.º e 15.º do Regulamento

- as finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
- prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;
- a existência do direito de solicitar ao responsável pelo tratamento, o acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;
- se o tratamento dos dados se basear no consentimento a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;
- o direito de apresentar reclamação à designada para o efeito a Comissão Nacional de Proteção de Dados (CNPD);
- se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;
- a menção ao direito de obter, pelo titular dos dados, sem demora injustificada, do responsável pelo tratamento, a retificação dos dados pessoais inexatos que lhe digam respeito.
- a menção ao direito de obter, do responsável pelo tratamento, o apagamento dos seus dados pessoais, sem demora injustificada, desde que os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento ou o titular retire o consentimento que permitiu, *ab initio,* o tratamento inicial.[5]

[5] Note-se, contudo, que o exercício do direito ao esquecimento não é livre e não acontecerá se na medida em que o tratamento se revele necessário:

a) Ao exercício da liberdade de expressão e de informação; b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado- Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento dos Dados.

DIREITOS DOS TITULARES DADOS	DESIGNAÇÃO
Direito à Transparência (Art. 12.º)	Fornecer ao titular dos dados, a título gratuito, as informações a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples. Fornecer informações sobre as medidas tomadas sem demora injustificada e no prazo de um mês a contar da data de receção do pedido. Esse prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos. Se o titular dos dados apresentar o pedido por meios eletrónicos, a informação é, sempre que possível, fornecida por meios eletrónicos, salvo pedido em contrário do titular.
Direito de Acesso (Art. 15.º)	1.O titular dos dados tem o direito de aceder aos seus dados pessoais e às seguintes informações: A) As finalidades do tratamento dos dados; B) As categorias dos dados pessoais em questão; C) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais; D) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo; E) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento; F) O direito de apresentar reclamação a uma autoridade de controlo; G) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados; H) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º e informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados. 2.Quando os dados pessoais forem transferidos para um país terceiro ou uma organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas, nos termos do artigo 46. relativo à transferência de dados. 3.O responsável pelo tratamento fornece uma cópia dos dados pessoais em fase de tratamento. Se o titular dos dados apresentar o pedido por meios eletrónicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrónico de uso corrente.

Direito de Retificação (Art.16.º)	O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.
Direito de Apagamento ou Esquecimento (Art. 17.º)	1. O titular tem o direito de obter do responsável pelo tratamento, o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: A) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; B) O titular retira o consentimento em que se baseia o tratamento dos dados e se não existir outro fundamento jurídico para o referido tratamento; C) O titular opõe-se ao tratamento nos termos do artigo 21.1 Direito de oposição, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.2 Definição de perfis na medida em que esteja relacionada com a comercialização direta; D) Os dados pessoais foram tratados ilicitamente; E) Os dados pessoais deverão ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; F) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8. .
Direito à Limitação do Tratamento (Art. 18º)	O titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, se contestar a exatidão dos dados pessoais, se o tratamento for ilícito, se o responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento deve o responsável implementar procedimentos eficazes para comunicação a terceiros a quem tenha transmitido os dados e limitação do tratamento.
Direito à Notificação (Art. 19.º)	O responsável pelo tratamento comunica a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento
Direito à Portabilidade (Art. 20.º)	O titular dos dados terá o direito de receber os dados pessoais que lhe digam respeito num formato estruturado, de uso corrente e de leitura automática e que tenha facultado a um responsável pelo tratamento bem como o direito de transmitir esses dados a outro responsável pelo tratamento sem qualquer impedimento;
	1.O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais

Direito de Oposição (Art. 21.º)	que lhe digam respeito com base no artigo 6. Licitude 1, e) Interesse público ou f) Interesses legítimos, ou 6.4 Segurança do Estado, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial. 2.Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta. 3.Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim.
Decisões Individuais Automatizadas, incluindo definição de Perfis (Art. 22º)	1.O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. 2.O n. 1 não se aplica se a decisão: A) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; B) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou C) For baseada no consentimento explícito do titular dos dados.

2 LEVANTAMENTO E MAPEAMENTO DOS DADOS E RECOLHA DE INFORMAÇÃO

O **Município de Pombal**, enquanto instituição responsável pelo tratamento de Dados Pessoais e por força da sua atividade, deverá implementar as Medidas Técnicas e Organizativas que forem adequadas para assegurar e comprovar que o tratamento dos Dados Pessoais é realizado nos exatos termos determinados pelo Regulamento.

Neste sentido, a [redacted] efetuou o levantamento e avaliação de todos os processos de modo a aferir o grau de conformidade com o RGPD e identificar áreas de intervenção necessária e graus de conformidade.

Recorreu-se, como modelo de governo, ao mapeamento dos dados utilizados pelo **Município de Pombal** de acordo com os requisitos e obrigações do Regulamento. Analisou-se, globalmente, a dinâmica da organização, identificando-se todas as áreas onde o Regulamento terá impacto; analisaram-se as práticas atuais relativas ao tratamento e proteção de dados pessoais e o posicionamento da organização relativamente aos requisitos e princípios do Regulamento.

Esta abordagem permitiu-nos ficar com uma visão clara e abrangente dos dados que estão a ser tratados no **Município de Pombal** e quem os está a tratar, permitindo um maior e melhor controlo de segurança, portabilidade e respetiva monitorização.

Durante esta fase, e em conjunto com a [redacted] foi realizada uma análise global da instituição. Foram identificadas as Unidades Orgânicas que interagem com Dados Pessoais e os respetivos interlocutores a convocar para cada sessão de esclarecimento:

- DAF - Direção Administrativa Financeira
- DCultura - Divisão Cultura
- DDSocialSaúde - Divisão Desenvolvimento Social e Saúde
- DEducação - Divisão de Educação
- DGCEEM - Divisão de Transportes Urbanos e Gestão de Equipamentos
- DIMSI - Divisão de Informática Modernização e Sistemas Inteligentes
- DMAS – Departamento Municipal de Águas e Saneamento
- DMGTSA – Departamento Municipal de Gestão do Território, Sustentabilidade e Ambiente
- DMIOE – Departamento Municipal de Infraestruturas, Obras e Equipamentos
- DMRH - Departamento Municipal de Recursos Humanos
- EMPEACI – Equipa Multidisciplinar de Planeamento Estratégico, Auditoria, Controlo e Investimento
- Executivo
- GAOA - Gabinete Apoio Órgãos Autárquicos
- GPCF - Gabinete Proteção Civil e Florestas
- SVeterinarioSP - Serviço de Veterinária e Saúde Pública
- UDesporto - Unidade Desporto
- Unidade Jurídica

2.1 METODOLOGIA PARA O MAPEAMENTO DOS PROCESSOS / UNIDADES / SUBUNIDADES

Foram identificados os processos que interagem com dados pessoais como forma de analisar o estado da informação em todo o ciclo de vida e garantir a sua segurança.

Assim sendo, identificou-se ao longo da nossa análise:

- A segregação da informação
- A Identificação dos os riscos e forma de mitigar vulnerabilidades
- Minimizar os dados ao tratamento absolutamente necessário para atingir a finalidade pretendida
- Análise dos Consentimentos de acordo com o tratamento dos dados
- Adotar medidas de Pseudonimização quando necessária
- Identificar e controlar os seus subcontratantes responsabilizando-os da proteção e segurança dos dados pessoais assinando contrato.

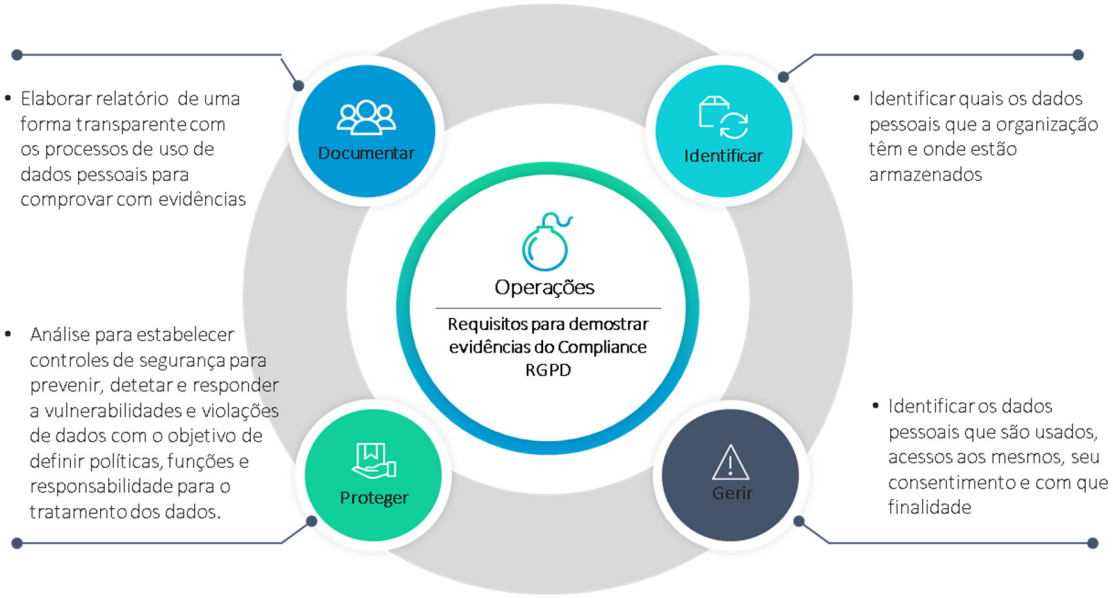
Nestas sessões de trabalho foram identificadas algumas operações efetuadas em sede de tratamento de dados pessoais - *"Data Flow"*. Concluiu-se que as operações em questão tanto podem ser feitas por meios automatizados ou não automatizados, o que determina a sua sujeição ao cumprimento de um conjunto de obrigações no tratamento dos dados, tal como:

- Recolha e registo;
- Organização e Estruturação;
- Conservação e Adaptação;
- Alteração e Recuperação;
- Consulta e Utilização;
- Divulgação e Disponibilização;
- Comparação/interconexão;

- Limitação;
- Apagamento e Destruição.

O objetivo das sessões foi obter uma perceção da realidade atual, no que diz respeito aos requisitos de *"Compliance"* do Regulamento, e os principais constrangimentos sentidos na prossecução do seu trabalho e a identificação das principais necessidades de melhoria.

Foi solicitado aos interlocutores de cada Unidade Orgânica, a descrição detalhada dos processos e atividades de tratamento de dados, conforme a ilustração seguinte:



O **Município de Pombal**, como responsável pelo tratamento de Dados Pessoais, tem que assegurar que:

- Os Dados Pessoais são recolhidos para finalidades determinadas, explícitas e legítimas e que os dados recolhidos não sejam posteriormente tratados de forma incompatível com as finalidades da recolha;
- Apenas são recolhidos os dados pessoais adequados, pertinentes, e não excessivos relativamente às finalidades da recolha – Princípio de Minimização;

- Os Dados Pessoais recolhidos são exatos e atualizados;
- Os Dados Pessoais apenas são conservados durante o período necessário para as finalidades da recolha/tratamento;
- São disponibilizadas ao Titular dos Dados todas as informações relacionadas com o tratamento efetuado, concedendo-lhe o direito de Acesso e Retificação dos seus dados;
- É obtido o Consentimento do Titular para o tratamento dos seus dados, exceto nos casos em que tal consentimento é dispensado nos termos da lei, como é o caso do tratamento de dados para a finalidade de proteção de interesses vitais do seu titular;
- São postas em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais, designadamente contra a sua destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizado e qualquer outra forma de tratamento ilícito;
- O tratamento dos dados encontra-se devidamente notificado à Comissão Nacional de Proteção de Dados (CNPD) e, quando legalmente exigido, é obtida a respetiva autorização prévia.

O **Município de Pombal** tem que **Planear, Implementar e Manter** medidas técnicas e medidas organizativas, que permitam assegurar e comprovar (demonstrar) que o tratamento dos dados pessoais é feito em conformidade com o **RGPD**.

Nesta fase foram informadas as pessoas chave, em cada Unidade Orgânica, seguindo o mapeamento dos tratamentos de dados pessoais com a seguinte matriz/*Framework*:

***Assessment* geral**	**Descrição**
Quais os Dados Pessoais tratados na organização?	⇨ Dados dos colaboradores (Atuais, Candidatos e Ex-Candidatos) ⇨ Dados de clientes (Atuais, Potencias e Ex-Clientes) ⇨ Organizações Profissionais ⇨ Dados de Prestadores de Serviço
Descrição dos Processos	⇨ Descrição sumária dos Processos e Fluxos dos processos e identificação de eventuais subcontratados
Quem trata os Dados na organização? **Quem é responsável pelos Dados Pessoais?**	⇨ Recursos Internos ⇨ Recursos Externos
Qual é origem dos Dados?	⇨ Como os Dados Pessoais são obtidos (Ex: Email, Telefone, Via Site, Online, Aquisição de Base Dados, Linkedin) ⇨ Origem dos dados e destinatários dos dados

Onde estão localizados na organização, onde armazenam os dados?	⇨ Em servidores e em Base Dados estruturadas ⇨ Em PC e em redes partilhadas e disperso por ficheiros (Word, EXCEL, PDF, TXT, XLM, JPG, PNG) ⇨ Em Tablets e Telemóveis ⇨ Na Clould ⇨ Em Papel
Quem tem acesso aos dados?	⇨ Identificar quem tem acesso à informação
Que tipo de Dados são tratados e como é feito o seu tratamento?	⇨ Que informações têm que ser reportadas com o Tratamento dos dados ⇨ Que dados são necessários ⇨ Que dados apagar ⇨ Que período de tempo para apagar ⇨ Como apagar
Qual a Finalidade do Tratamento de Dados?	⇨ Por necessidade do negócio ⇨ Por interesse no negócio ⇨ Por solicitação de Entidades Externas ⇨ Por interesse publico ⇨ Estatísticas
Licitude do tratamento dos Dados	⇨ Qual o enquadramento legal
Identificar os Sistemas existentes e quais são?	⇨ Aferir os sistemas existentes, e quais as implicações que o **RGPD** vai ter sobre os mesmo para perceber eventuais alterações a fazer ⇨ A localização dos sistemas e sistemas de backup que contém os dados

Tempo de retenção dos Dados? Transmissões? Qual o período de Conservação de cada tratamento?	⇨ Quanto tempo é necessário para tratamento dos Dados e a Periodicidade da sua utilização
Que Medidas de Segurança estão implementadas? Quem as implementou?	⇨ Que medidas de segurança dos dados estão implementadas na organização e as métricas de analise e auditoria
Que Informação é partilhada?	⇨ A quem é que a informação é divulgada ⇨ Com quem é compartilhada (Ex: Fornecedores, Empresas Terceiras)
Interconexões entre sistemas	⇨ O sistema envia ou transfere informações para outros sistemas e/ou intervenientes

Políticas e procedimentos do RGPD no Município de Pombal.

Nome do documento	Descrição Sumária
Política de Princípios Aplicáveis ao Tratamento	Tem como objetivo auxiliar o Município a garantir que observa os princípios consagrados no RGPD quando trata dados pessoais, designadamente os seguintes: . Licitude; . Lealdade e transparência; . Limitação das finalidades; . Minimização dos dados; . Exatidão; . Limitação da conservação; . Integridade e confidencialidade; *Accountability* (Responsabilização
Política de Âmbito de Aplicação Material e Territorial do RGPD	Política que visa auxiliar o Município na ponderação quanto à aplicabilidade do RGPD aos tratamentos de dados levadas a cabo no quadro das suas atividades.
Política Exercício Direitos	Tem como objetivo auxiliar a organização na garantia aos titulares dos dados, do exercício dos seus direitos consagrados pelo RGPD, no caso, direito de informação, direito de acesso, direito de retificação, direito de apagamento dos dados, direito à limitação do tratamento, direito de oposição, direito de portabilidade, direito de não ficar sujeito a decisões individuais automatizadas e direito a retirar o consentimento.
Política de Privacidade para Colaboradores	Descreve os termos em que o Município de Pombal, enquanto responsável pelo tratamento de dados, recolhe e trata dados pessoais, no âmbito das relações

	laborais, prestações de serviços, prestações contratuais, nomeações, estabelecidas com os seus colaboradores, de acordo com o RGPD.
Política de Avaliação de Impacto sobre a Proteção de Dados (AIPD)	Destina-se a guiar a realização do procedimento da avaliação de impacto sobre a proteção de dados (AIPD). O objetivo desta política é auxiliar o Município a perceber o que é uma AIPD, os casos em que é obrigatória a sua realização, em que momento a deve fazer, que metodologia deve ser seguida e que partes devem intervir neste procedimento.
Política do Encarregado de Proteção de Dados (EPD/DPO)	O objetivo desta política é auxiliar o Município de Pombal a identificar as funções do DPO e qual a relação que aquele deve manter com o Município.
Política de Conservação de Dados Pessoais	Auxiliar os eleitos, membros dos gabinetes de apoio, dirigentes, trabalhadores, prestadores de serviços e demais colaboradores do Município de Pombal, a perceber quais as suas obrigações, em matéria de conservação dos dados pessoais, constantes em suporte papel ou em suporte digital, garantindo uma aplicação consistente e uniforme em toda a organização.
Política de Segurança dos Dados	O objetivo desta política é ajudar o Município tratar os dados pessoais de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, através da implementação de medidas técnicas e organizativas para o efeito.
Política de Obrigações do Responsável pelo	O objetivo desta política é auxiliar o Município a identificar o seu papel face a um determinado

Tratamento e Subcontratante e do Sub-Subcontratante	tratamento de dados (se intervém na qualidade de responsável pelo tratamento, subcontratante ou corresponsável), a definir quais as suas obrigações, em termos de RGPD e o modo como estas obrigações, devem ser operacionalizadas.
Procedimento para Exercício de Direito dos Titulares dos Dados	Define a atuação do Município de Pombal, no âmbito da análise dos pedidos de exercícios de direitos dos titulares de dados em matéria de RGPD e de acesso aos documentos administrativos.
Procedimento para Registo de Consentimentos	Visa auxiliar o Município de Pombal a conhecer o procedimento a adotar com vista a registar os consentimentos para tratamento de dados pessoais, bem como, a sua retirada, sempre que solicitada.
Aviso de Privacidade para Clientes e Fornecedores	Descreve a forma como são recolhidos e utilizados os dados pessoais dos titulares dos dados (clientes e fornecedores) de acordo com o RGPD.
Política de Gestão de Incidentes	Política que permite definir e identificar se determinada ocorrência consubstancia incidente, aplicando-se às atividades a desenvolver no âmbito do processo de gestão de incidentes, estabelecendo as obrigações relativas ao reporte de eventos acidentais e vulnerabilidades de Segurança da Informação, violação de dados pessoais sensíveis e não sensíveis, responsabilidades, etc.
Comissão de Segurança da Informação e Privacidade (CSIP)	Este documento tem por finalidade concretizar as responsabilidades da Comissão de Segurança da Informação e Privacidade (CSIP) do Município de Pombal (equipa responsável pela gestão das matérias relacionadas com a segurança da informação e

	atribuição formal das respetivas funções e responsabilidades).
Modelo para Formalização da Relação Responsável pelo Tratamento - Subcontratante	Regista modelo para formalização da relação Responsável pelo tratamento – Subcontratante
Modelo de Resposta Automática a Candidatura	Regista o empenho do Município de Pombal em garantir a segurança e a privacidade dos dados pessoais dos titulares que apresentam candidatura, nomeadamente, no âmbito dos processos de recrutamento.
Modelo de Comunicação de Violação de Dados Pessoais aos respetivos Titulares	Contém modelo de comunicação de violação de dados pessoais aos respetivos titulares.
Formulário de Exercício de Direitos pelo Titular de Dados Pessoais	Formulário modelo para o exercício dos direitos pelos titulares de dados.
Formulário de Comunicação de Incidente de Segurança de Dados Pessoais	Modelo de formulário de comunicação de incidentes de segurança de dados pessoais, tendo como finalidades registar o incidente, instruir o correspondente processo e proceder à necessária apreciação, identificando o serviço e o responsável pelo tratamento, a descrição da natureza do incidente de dados pessoais, (as categorias e tipos, número aproximado de titulares envolvidos) e a descrição das medidas adotadas ou propostas para a respetiva reparação.

Aviso de Privacidade do Website	Procedimento que indica que o tratamento de dados pessoais, no website, é lícito, leal, transparente e limitado às finalidades.
Aviso sobre Cookies - Website	Procedimento que alerta para o uso de cookies para aceder e navegar no website do Município, pressupondo concordância com o Aviso.
Aviso de Privacidade em Processos de Recrutamento	Regista o empenho do Município de Pombal em garantir a segurança e a privacidade dos dados pessoais dos titulares que se propõem a processos de recrutamento.