Disponível em www.bad.pt/publicacoes
Paper

O RGPD: a articulação entre a gestão da informação e a gestão da segurança da informação

[a]Alexandra Fonseca, [a]Alexandra Lourenço, [a]Hélio Balinha,

[a]José Martins, [a]José Dinis, [a]Liliana Marques

[a] Associação Portuguesa de Bibliotecários, Arquivistas e Documentalistas, Portugal, bad@bad.pt

Resumo

O Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679) avizinha-se como um normativo que vai mudar a realidade das organizações no contexto europeu.
A adaptação das entidades constitui um desafio a ser levado a cabo por uma equipa interdisciplinar. Nesta fase inicial, em que as metodologias se encontram em desenvolvimento, esse processo tende a aplicar normativos e ferramentas existentes, conciliando-as, numa perspetiva complementar, com vista ao alinhamento com os requisitos do RGPD.
A presente proposta de comunicação apresenta as reflexões decorrentes da aplicação em curso do RGPD a uma associação profissional, integrando uma visão interdisciplinar, resultante da reunião de competências provenientes da área da gestão da informação com a gestão da segurança da informação.
Pretende-se demonstrar a necessidade de complementaridade de conhecimentos, valorizando a componente da gestão da informação no RGPD e dando a conhecer uma metodologia passível de replicação.

Palavras-chave: Regulamento Geral de Proteção de Dados, Dados pessoais, Gestão da Informação, Gestão da Segurança da Informação.

Introdução

O Regulamento Geral de Proteção de Dados (RGPD) é o novo diploma legal que regula o tratamento de dados pessoais de pessoa singulares residentes no território da União Europeia (UE). Este documento traz novidades assinaláveis ao nível dos deveres das organizações e dos direitos dos cidadãos relativamente ao tratamento dos dados pessoais. O RGPD foi aprovado em 27 de abril de 2016 e entrou em vigor a 25 de maio de 2018, dando às organizações cerca de dois anos de preparação para a implementação do Regulamento.

O RGPD cumpre os pressupostos do n.º1 do artigo 8º da Carta dos Direitos Fundamentais da União Europeia, bem como do n.1 do artigo 16º do Tratado sobre o Funcionamento da União Europeia, segundo os quais «todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito» (Parlamento Europeu e Conselho da União Europeia, 2016a, 2016b). O primeiro documento também prevê, no ponto 2 do artigo 16º, que os dados devem ser objeto de um tratamento leal e para fins específicos, estando previsto o consentimento do interessado, e também se assegura o direito de acesso aos dados e à retificação dos mesmos (Parlamento Europeu e Conselho da União

Europeia, 2016a). Também a Constituição da República Portuguesa estabelece, no artigo 35º, o direito de acesso aos dados informatizados que digam respeito ao cidadão, à retificação, à atualização e a conhecer a finalidade a que se destinam (Constituição da República Portuguesa, 2005).

Conforme previsto no RGPD, o Governo português apresentou a Proposta de Lei 120/XIII para especificar a aplicação das regras do Regulamento. Os pontos de destaque da Proposta residem na exclusão da Administração Pública da aplicação do RGPD por três anos e na nomeação da Comissão Nacional para a Proteção de Dados como autoridade nacional de controlo, à qual serão reportadas as falhas de segurança no tratamento dos dados pessoais. A CNPD apresentou o parecer 20/2018, que propunha a supressão ou revisão de mais de metade dos artigos propostos. A Proposta de Lei foi chumbada no Parlamento, estando, à data de produção desta comunicação, em preparação um novo diploma legal.

O RGPD revogou a Diretiva 95/46/CE, que visava a proteção das pessoas no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados entre os Estados-Membros (Parlamento Europeu e Conselho da União Europeia, 1995), que foi transposta para a ordem jurídica portuguesa pela Lei n.º 67/98. O RGPD tem como objetivo uma uniformização da execução e aplicação da legislação no que se refere ao tratamento dos dados pessoais, garantindo segurança jurídica e a atividade económica, sem entraves e uma livre concorrência.

O RGPD define os direitos dos titulares dos dados pessoais e os deveres dos responsáveis pelo tratamento desses dados. Estes titulares, conforme definidos pelo Regulamento, são todas as pessoas singulares e no âmbito de atividades exercidas na União Europeia ou de dados referentes a atividades de oferta de bens e serviços e de controlo de comportamento pertencentes a pessoas residentes no espaço, ainda que o tratamento seja realizado fora das fronteiras da União.

No artigo 5º, o RGPD estabelece os princípios relativos ao tratamento dos dados pessoais: a lealdade, licitude e transparência do tratamento dos dados pessoais; a limitação das finalidades; a minimização dos dados; a exatidão dos dados; a limitação da conservação; a integridade; e a responsabilidade. Também são estabelecidos os seguintes direitos dos titulares dos dados pessoais: de acesso, ao apagamento, à limitação do tratamento, de portabilidade dos dados, de oposição e de decisões individuais automatizadas (*profiling*).

Segundo Boardman, os princípios e direitos deste Regulamento valorizam ações e papéis no tratamento da proteção e tratamento dos dados pessoais, muitos já previstos na Diretiva, mas agora com definições e âmbitos mais alargados. Este alargamento reflete-se, por exemplo, nos seguintes aspetos:

- Obtenção do consentimento dos titulares dos dados (incidindo também sobre o papel dos menores de idade nos serviços da sociedade de informação);
- Clarificação do que é o tratamento legítimo dos dados e em que situações o tratamento para uma

nova finalidade é incompatível com o objetivo da recolha inicial;

- Sujeição acrescida dos legítimos interesses dos responsáveis pelo tratamento dos dados aos direitos e liberdades dos titulares dos dados;
- Inclusão de novos tipos de dados no tratamento de dados sensíveis, dados genéticos e biométricos e de saúde.

O Regulamento estabelece responsabilidades acrescidas às organizações na garantia de conservação dos dados pelo tempo indispensável necessário, a utilizá-los somente para a finalidade para que foram recolhidos e para que protejam os dados na sua posse, nomeadamente através da implementação de medidas de segurança da informação que mitiguem os riscos de quebra de segurança dos dados, uma vez que as organizações passam a ser responsáveis pela comunicação das quebras de segurança à autoridade de controlo.

Garantir a segurança dos dados pessoais implica que as organizações analisem o nível de risco de segurança no tratamento, que avaliem o impacto sobre a proteção de dados (PIA – Privacy Assessment Impact) e que adotem medidas de conformidade para reduzir os riscos, podendo algumas delas passar pela pseudonimização dos dados, isto é, a cifragem dos dados (Boardman *et al.*, 2016, p. 4). Todas as ações para garantia da segurança dos dados devem ser documentadas, pois o RGPD impõe às organizações uma responsabilidade proactiva a nível do desenvolvimento de medidas técnicas e organizacionais para garantir que o tratamento dos dados se realiza em conformidade com o Regulamento e é adequado a cada risco identificado, de modo a que tal possa ser demonstrado aos interessados, bem como às autoridades de controlo (Fernández Cuesta, 2018, p. 30).

A comunicação de quebras de segurança dos dados à autoridade nacional de controlo é realizada pelo Encarregado da Proteção de Dados (EPD). Esta figura já existia na Diretiva anterior, mas sem carácter obrigatório. Contudo, à luz do RGPD, a nomeação deste responsável torna-se uma obrigatoriedade para todas as autoridades e organismos públicos e outras organizações que tenham como atividade principal o controlo de pessoas de forma sistemática e em grande escala, ou que tratem categorias especiais de dados em larga escala. Define-se o papel do EPD do seguinte modo:

> «Além de facilitar a conformidade ao RGPD através da implementação de instrumentos de responsabilização (p. ex. viabilização de avaliações de impacto sobre a proteção de dados ou viabilizando auditorias), os EPD servem de intermediários entre as partes interessadas (p. ex. as autoridades de controlo, os titulares de dados e as unidades empresariais dentro de uma organização)» (Grupo do Artigo 29.º para a Proteção de Dados, 2017, p. 5).

A necessidade de adaptação das organizações à legislação europeia relativamente à proteção de dados pessoais motivou a criação de grupos de trabalho e a produção de documentos técnicos de apoio. Em 1996, foi criado o Grupo do Artigo 29.º para a Proteção de Dados, um grupo composto por elementos das autoridades nacionais de proteção de dados dos Estados-Membros, da Comissão Europeia e pelo Supervisor Europeu de Proteção de Dados. Este grupo trabalhou, desde 1996, ao abrigo da Diretiva 95/46/CE para providenciar aconselhamento independente relativamente à proteção de dados e para

auxiliar no desenvolvimento de políticas harmonizadas para a proteção de dados nos Estados-Membro da União Europeia. Após a entrada em vigor do RGPD, este grupo foi extinto e passou a designar-se European Data Protection Board (https://edpb.europa.eu/). O Grupo de Trabalho produziu orientações ou diretrizes para a implementação do RGPD, nomeadamente sobre o consentimento, a transparência, sobre decisões individuais automatizadas e *profiling*, sobre notificações de falhas de segurança na proteção dos dados pessoais, sobre aplicação e afixação de coimas, sobre autoridades nacionais de controlo, sobre encarregados de proteção de dados, sobre avaliação de impacto sobre a proteção de dados (os textos podem ser consultados na página da Internet de *guidelines* do grupo, encontrando-se disponíveis os textos traduzidos nas línguas dos Estados-Membro).

As organizações ligadas à gestão da informação têm um papel fundamental a desempenhar na implementação do RGPD, uma vez que

> «[…]o modelo de responsabilidade proactiva e de proteção de dados desde a arquitetura [dos sistemas de gestão de dados] e por defeito promovido pelo RGPD leva a que a gestão de documentos – e, dentro desta, a identificação e avaliação, no sentido que aparece, por exemplo, na norma ISO 15489:2016 – se converta numa ferramenta imprescindível para a sua implementação, na medida em que permite determinar que documentos é necessário criar, capturar, como desenhar e que requisitos terá a sua gestão e por quanto tempo é necessário conservá-los» (Fernández Cuesta, 2018, p. 31)

Os pressupostos anteriormente enunciados, concedem um papel central aos gestores de informação, pela inerência das suas funções, nomeadamente na arquitetura dos sistemas de gestão da informação, na determinação de quais os documentos a capturar e por quanto tempo devem ser preservados. A generalidade das organizações tem seguido a lógica incutida pelo n.º 5 do artigo 37º do RGPD, segundo o qual o EPC deve ser designado com base nas suas qualidades profissionais, com especial incidência nos conhecimentos no domínio do direito e das práticas de proteção de dados, designando como EPD profissionais da área do Direito. O RGPD implica uma abordagem multidisciplinar, que passa pelo Direito, pela Gestão da Informação e pela Segurança da Informação. Somente uma abordagem integrada permite implementar e cumprir o Regulamento de forma eficiente.

Na União Europeia, vários foram os países que constituíram grupos especiais de trabalho ao longo dos últimos anos, fosse ao abrigo da Diretiva, fosse por pressão do Regulamento.

Em França, tendo em vista a adaptação ao RGPD, foi constituída a Commission Nationale d'Informatique et des Libertés (CNIL), que, além de orientações, fornece ferramentas e metodologias para a análise do estado das organizações relativamente à conformidade com o Regulamento. Uma das ferramentas que fornecem é a ferramenta *PIA* (*Outil PIA*), um *software* em acesso aberto que sistematiza a realização e formalização de análises de impacto de proteção de dados pessoais. Na mesma página onde se pode descarregar a ferramenta, encontra-se disponibilizado um estudo de caso que utiliza a mesma.

A Agencia Española para la Protección de Datos (AEPD) fornece diversos serviços relacionados com o RGPD, nomeadamente portais para *report* de falhas de proteção de dados pessoais, para a

comunicação de quem é nomeado EPC ou para responder a dúvidas do EPC. A AEPD também disponibiliza informação sobre as entidades que certificam o EPC, guias sobre o RGPD, e a ferramenta *Facilita RGPD*, destinada às pequenas e médias empresas, em que mediante o preenchimento de um questionário recebem orientação quanto ao tratamento de dados pessoais e qual o nível de risco que afeta esses dados.

Em Portugal, a Comissão Nacional para a Proteção de Dados (CNPD) apresenta na sua página de Internet o Espaço RGPD, no qual disponibiliza as orientações em português do Grupo de Trabalho do Artigo 29.º A CNPD, à data deste artigo, lançou o Projeto de Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a avaliação de impacto sobre proteção de dados, que está em consulta pública, recebendo contributos para integrar mais exemplos de tratamentos de dados pessoais que devem ser sujeitos à avaliação de impacto sobre proteção de dados.

O RGPD também trouxe necessidades acrescidas de adaptação aos serviços de gestão da informação, estando ainda muito trabalho por fazer no que diz respeito ao equilíbrio entre a garantia dos direitos dos titulares dos dados pessoais e as derrogações a realizar no tratamento de dados pessoais para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos. Essa definição afeta particularmente os serviços de gestão da informação, onde existe uma necessidade premente de clarificação relativamente à utilização e difusão dos dados pessoais constantes naqueles serviços.

No âmbito do artigo 40.º do RGPD, foi desenvolvido um Código de Conduta para os Serviços de Arquivo pelo European Archives Group da Comissão Europeia e pelo European Board of National Archivists, que esteve em consulta pública e foi alvo de uma sessão nacional de auscultação dos profissionais, promovida pela Direção Geral do Livro, dos Arquivos e das Bibliotecas (DGLAB) e pela Associação Nacional de Bibliotecários, Arquivistas e Documentalistas (BAD). Este código estabelece a responsabilidade e o compromisso que os serviços se propõem cumprir as orientações a seguir no tratamento da informação e no acesso da mesma, bem como as regras a cumprir pelos seus utilizadores. O documento define também quem tem a obrigatoriedade de implementar este código e a quem reportar quebras de conduta.

Método

A BAD, enquanto associação de utilidade pública, está sujeita tal como outras entidades públicas e privadas a observar os princípios preconizados no RGPD. Neste sentido, cientes da necessidade de adequar a Associação às novas exigências, e movidos pela vontade de demonstrar que os profissionais da informação jogam um papel fundamental na adequação das entidades às imposições do RGPD, foi constituído um grupo de projeto, e escolhida a BAD para o desenvolvimento de um estudo de caso.

O grupo de projeto que desenvolveu esta abordagem nasceu do Grupo de Trabalho de Gestão de

Documentos de Arquivo (GT-GDA), um grupo de trabalho da BAD, ativado em 2012, que tem prosseguido como objetivo o estudo, reflexão, debate e atuação com vista à implementação no país dos princípios e boas práticas de gestão documental. Assim, enquanto o grupo de projeto recolhia e analisava dados, as reuniões do GT-GDA serviam para discussão de conceitos e técnicas, bem como para a realização de pontos de situação.

Em termos metodológicos, foram considerados os contributos de metodologias da área da gestão da informação, muito particularmente, o DIRKS (ISO 15489), e da área das normas de segurança da informação e gestão do risco, alargadas para contemplar a proteção dos dados pessoais, e conciliadas com os normativos e instrumentos aplicáveis à gestão da informação.

DIRKS é um acrônimo para *Designing and Implementing Recordkeeping Systems*, uma metodologia desenvolvida pelo National Archives of Australia em colaboração com a State Records Authority of New South Wales, que esteve na génese da ISO 15489. Esta metodologia está dividida em oito etapas, nas quais todas as dimensões do negócio, ou quase todas, são analisadas tendo em vista a gestão da informação e a produção de instrumentos de gestão dessa informação[1].

No domínio das normas de segurança da informação e gestão do risco, recorremos a três fontes para desenhar a nossa aproximação à realidade informacional:

- Framework de Zackman: embora nãos seja uma verdadeira metodologia, antes uma ontologia, permite de forma bidimensional analisar a arquitetura de sistemas corporativa de uma entidade.
- ISO 27001:2013: a norma tem como princípio geral a adoção pela organização de um conjunto de requisitos, processos e controlos, com o objetivo de mitigarem e gerirem adequadamente o risco da organização, garantindo assim, a segurança da informação.
- *European Union Agency for Network and Information Security* (ENISA) (https://www.enisa.europa.eu/): esta entidade desenvolve, desde 2004, trabalho no domínio da cybersegurança, através da realização de estudos e ferramentas, bem como da consciencialização dos cidadãos no domínio da segurança da informação.

Para o desenvolvimento deste projeto foram identificadas as seguintes etapas:

1. Realização de sessões de discussão do RGPD, de normativos complementares e de bibliografia de apoio, no âmbito das reuniões do GT-GDA;
2. Realização de sessões de discussão dos referenciais, normativos e metodologias base da área da gestão de informação e gestão de segurança da informação, bem como de normas nacionais

[1] Disponível em http://www.records.nsw.gov.au/recordkeeping/advice/designing-implementing-and-managing-systems/dirks-manual/dirks-manual

e internacionais consideradas relevantes;

3. Planeamento do projeto, integrando a dimensão da gestão de informação e da gestão de segurança da informação, complementadas com a vertente jurídica, por forma a aferir a conformidade legal, técnica e organizativa com o RGPD;
4. Preparação do processo de implementação - Fase "AS IS":
    a. Sensibilização dos colaboradores da entidade;
    b. Recolha dos instrumentos de gestão da informação existentes;
    c. Identificação dos processos de negócio e do seu relacionamento informacional, com foco nos dados pessoais;
    d. Construção de uma matriz para recolha dos elementos previstos no art.º 5.º do RGPD, integrados na abordagem processual;
    e. Auditoria de segurança da informação aos sistemas existentes.
5. Identificação e avaliação dos riscos, através de matriz de identificação e avaliação dos riscos por processos e categorias de dados pessoais, e avaliação de Impacto sobre a Proteção de Dados (PIA).
6. Modelação do processo de implementação – Fase "TO BE":
    a. Criação de uma política de gestão de dados pessoais;
    b. Modelação dos processos de negócio e de suporte;
    c. Identificação das oportunidades de melhoria nos Sistemas de Informação;
    d. Revisão dos formulários para a conformidade do RGPD (suporte físico e digital);
    e. Matriz de identificação, avaliação e tratamento dos riscos;
    f. Ação de sensibilização dos colaboradores com enfoque na implementação;
    g. Registo das atividades de tratamento (art. 30.º RGPD).
7. *Design* de um plano de gestão de incidentes (notificações) e de *Disaster Recovery.*
8. Validação final do processo de implementação do RGPD:
    a. Monitorização e auditorias ao sistema implementado para garantir a conformidade com o RGPD;
    b. Plano de implementação de controlos de segurança da informação (e.g., controlos organizacionais, jurídicos, físicos, tecnológicos);
    c. Processo de melhoria contínua, especialmente através da revisão pela gestão do

sistema implementado.

Resultados

Na fase inicial, a recolha dos instrumentos de gestão de informação existentes (plano de classificação e tabela de seleção) foi a base para a identificação dos processos de negócio e do seu relacionamento informacional, com foco nos dados pessoais. Permitiu, ainda, a definição, à partida, dos prazos de conservação desses dados e do seu destino final.

Para uma melhor caracterização dos processos, articulando-os com os requisitos do RGPD, procedeu-se à construção de uma matriz estruturada em alinhamento com o art. 5.º do RGPD, bem como outros campos que foram considerados relevantes, sendo constituída pelas seguintes zonas de informação: i) identificação os processos de negócio, ii) recolha, iii) tratamento, iv) conservação, v) segurança, vi) acessibilidade e viii) documentação e impressos, conforme consta no quadro abaixo:

1. IDENTIFICAÇÃO DOS PROCESSO DE NEGÓCIO	1.1. Título e descrição
	1.2. Atividades
	1.3. Ações
2. RECOLHA	2.1. Que informação recolho?
	2.2. Minimização dos dados
	2.3. De que forma recolho a informação?
	2.4. Qual a finalidade da informação recolhida?
	2.5. Tenho autorização para utilizar a informação?
3. TRATAMENTO	3.1. O que fazemos aos dados recolhidos?
	3.2. Qualidade dos dados (exatidão)
	3.3. Legitimação legislativa/normativa

4. CONSERVAÇÃO	4.1. Onde encontramos os dados (papel/digital/híbrido)?
	4.2. Durante quanto tempo conservamos?
5. SEGURANÇA	5.1. Avaliação global de impacto
	5.1.1. Impacto de perda de confidencialidade
	5.1.2. Impacto da perda de integridade
	5.1.3. Impacto da perda de disponibilidade
	5.2. Probabilidade global de ataque
	5.2.1. Probabilidade de ataque à rede e aos recursos técnicos
	5.2.2. Probabilidade de ataque aos processos e procedimentos
	5.2.3. Probabilidade de ataque às pessoas e entidades envolvidas
	5.2.4. Probabilidade de ataque ao sector de atividade
6. ACESSIBILIDADE	6.1. Níveis de segurança (público, não classificado, reservado)?
7. DOCUMENTAÇÃO E IMPRESSOS	7.1. Os procedimentos estão documentados? Quais os documentos?
	7.2. Quais os impressos utilizados?
	7.3. Quais os outputs deste processo?

A aplicação desta matriz permitiu a separação do uso primário dos dados pessoais, inerente ao processamento da ocorrência, do seu uso secundário, i. e., a reutilização em contexto de interação de processos. De igual modo, foi ainda possível a identificação da fonte de legitimidade para o tratamento e utilização dos dados, nomeadamente se a mesma decorria de uma relação legal ou contratual, ou se para o uso desses dados era necessário obter consentimento do titular. Possibilitou ainda a modelação

da interação das principais áreas de intervenção da BAD, distinguindo o tipo de uso dos dados pessoais (primário e secundário), bem como os princípios que legitimam o seu tratamento e utilização, conforme explícito no esquema abaixo:

Figura 1 – Modelação da interação entre áreas funcionais no processamento de dados pessoais

A fase seguinte centrou-se na avaliação do risco e na identificação do impacto potencial de uma quebra de segurança dos dados. E, neste ponto, seguimos de perto as recomendações da ENISA.

O primeiro passo, segundo a ENISA, é a avaliação de impacto de uma possível quebra da segurança dos dados, a qual obedece a uma escala qualitativa e tem em conta aspetos como o tipo de dados pessoais, o volume de dados ou as características da entidade controladora. Segue-se a identificação das potenciais ameaças e da sua probabilidade de ocorrer. Estas ameaças dependem dos ambientes interno e externo nos quais ocorre o processamento dos dados pessoais. Esta análise encerra-se com o cruzamento de leituras entre níveis de impacto e probabilidades de ocorrência das ameaças, donde resulta uma matriz face à qual as entidades têm de decidir quais as áreas de intervenção prioritária e aquelas onde estão disponíveis para assumir os riscos associados a uma ausência de medidas. Este trabalho constitui a base para a produção da avaliação de Impacto sobre a Proteção de Dados (PIA) da BAD, em que se recorrerá complementarmente à ISO 29134:2017 Information technology. Security techniques. Guidelines for privacy impact assessment.

Conhecida a realidade, partiu-se para a modelação do processo de implementação, o qual teve início com a revisão e publicitação da política de gestão de dados pessoais, integrando os requisitos do novo regulamento de proteção de dados.

Destaca-se nesta politica[2], o compromisso da BAD com a segurança da informação pessoal.

Este compromisso implicou uma nova modelação dos processos de negócio e de suporte, tendo sido,

[2] Disponível em https://www.bad.pt/web/politica-de-privacidade-da-bad/

quando necessário, redefinida a forma de recolha, tratamento e reutilização dos dados pessoais na interação entre processos.

A área de intervenção relativa à "Divulgação das atividades BAD" constituiu uma das que requereu maiores alterações. Habitualmente, a BAD comunicava as suas atividades e eventos para os endereços de email recolhidos ao longo dos anos no âmbito de diversos processos de negócio, como os relativos aos associados, formação ou organização de eventos.

O RGPD vem requerer que os dados pessoais apenas possam ser utilizados no âmbito da finalidade para que foram recolhidos, não podendo ser efetuados outros processamentos ou reutilizações que não estejam previstas legalmente ou contratualmente. Noutras situações de uso, passa a ser necessário solicitar expresso consentimento ao titular.

No caso do processo da "Divulgação de atividades BAD" foi redefinido o processo de negócio, criando-se uma nova componente no sistema de informação para a produção de *newsletters*, de subscrição voluntária[3],

Procedeu-se ainda à revisão dos formulários em que constam dados pessoais, minimizando a sua recolha e solicitando consentimento para outros usos, quando aplicável, também devidamente identificados.

Paralelamente, e decorrente da auditoria de segurança, foram elencados um conjunto de requisitos que se traduziram na identificação de oportunidades de melhoria nos sistemas de informação da BAD. Refiram-se, a título exemplificativo, os processos híbridos relativos à formação, processados com recurso a ferramentas do Office, parcelarmente em papel, com autenticação através de assinatura manual e ainda a integração com a plataforma da DGERT.

Constitui ainda peça fundamental na modelação do processo de implementação, a definição da Matriz de identificação, avaliação e tratamento dos riscos. Este instrumento em contínuo desenvolvimento forneceu as bases para a aplicação das principais medidas de controlo, quer ao nível tecnológico, nos sistemas de informação, quer ao nível físico.

A futura mudança de instalações da sede da BAD contribuiu também para a redefinição dos circuitos físicos de processamento da informação e de armazenamento e para a aquisição de mecanismos e instrumentos de mitigação do risco, reforçando a segurança no acesso e preservação dos dados.

As ações de sensibilização dos colaboradores revelaram-se essenciais para a implementação das alterações, nomeadamente ao nível do registo das atividades de tratamento, quando não é processado automaticamente.

Encontra-se em curso a documentação de procedimentos dos vários processos de negócio que permitirá a sedimentação de boas práticas no tratamento dos dados pessoais, associadas à qualificação

[3] Disponível em https://www.bad.pt/web/

da gestão informacional da BAD.

Discussão

O projeto encontra-se em curso, sendo expectável um processo incremental de implementação, dada a sua complexidade e os recursos envolvidos. Encontra-se ainda por desenvolver o Plano de gestão de incidentes (notificações) e de *Disaster Recovery* e a *v*alidação do processo de implementação do RGPD.

Da fase inicial resulta um maior conhecimento da organização, dos seus processos de negócio e fluxos informacionais, com especial incidência nos que contêm dados pessoais, bem como, uma auditoria de segurança e informação.

As normas de gestão de informação, por exemplo, as ISO 15489-1:2016, ISO 16175-2:2011, ISO 23081:2011, e ISO 26122:2008, apoiaram o processo de identificação dos processos de negócio, essenciais para a contextualização da recolha, tratamento, acesso e conservação dos dados pessoais.

Os instrumentos base da gestão de informação, como o Plano de Classificação, a Tabela de Seleção e os registos de documentos, constituíram elementos chave para o preenchimento da matriz para recolha dos elementos previstos no art.º 5.º do RGPD. Demonstraram a sua importância para apoiar o processo de fundamentação da recolha e da determinação da finalidade, inerentes à definição dos prazos de conservação pelo tempo estritamente necessário e para as finalidades para os quais são tratados. Evidenciou-se a importância da contextualização dos dados pessoais no âmbito do processo de negócio em que são produzidos para a definição integrada do seu ciclo de vida. Esta contextualização permitiu, ainda, a justificação da conservação durante períodos mais longos, quando tratados para fins de arquivo e de investigação, em conformidade com o artigo 89.º do RGPD.

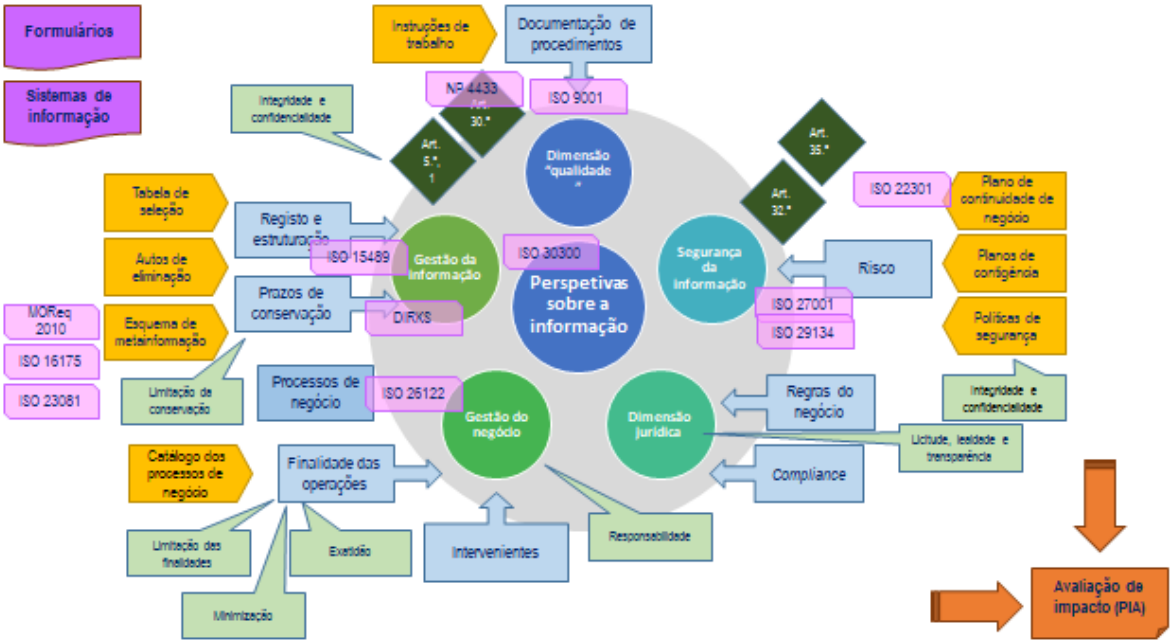
As normas internacionais de segurança da informação (ISO/IEC 27001: 2013, ISO / IEC 27002: 2013) foram essenciais para referenciar os controlos de segurança implementados, bem como o seu nível de maturidade e ainda para identificar e avaliar os riscos (NP ISO 31000: 2012) dos Sistemas de Informação da Organização, de modo a serem posteriormente mitigados.

Os elementos produzidos nestes momentos iniciais são ainda essenciais para a elaboração da avaliação de riscos e para a avaliação de Impacto sobre a Proteção de Dados, instrumentos de apoio cruciais para a tomada de decisão e implementação da fase "TO BE".

Os resultados apresentados ainda não são conclusivos e carecem da discussão entre pares. Os testes para a aplicação do modelo permitirão aferir a sua aplicabilidade e a eventual necessidade de ajustes.

Este trabalho reflete a necessidade de interação entre as várias perspetivas sobre a informação, como

se explicita no esquema abaixo:



Conclusões

Este projeto tem-nos permitido perspetivar o tratamento da informação de diferentes ângulos, numa ótica de complementaridade entre as áreas do conhecimento, demonstrando a necessidade da interdisciplinaridade para a implementação do RGPD.

A metodologia desenvolvida tem por finalidade poder ser replicada, constituindo-se como um dos modelos integradores de abordagem ao alinhamento com os requisitos para a proteção dos dados pessoais.

Pretende-se afirmar o profissional de informação como interveniente essencial neste contexto de mudança, face às suas competências diferenciadas no que concerne ao tratamento da informação.

Os profissionais da informação constituem-se como agentes privilegiados para dirimir os potenciais dilemas que possam surgir na aplicação do RGPD em serviços de gestão de informação e arquivo, nomeadamente os relativos ao estabelecimento do equilíbrio entre a proteção dos interesses das pessoas e a proteção da liberdade de informação.

São eles a peça fundamental para assegurar a integridade e autenticidade dos documentos, mantendo-os inalterados no longo prazo, sem eliminações parciais, garantindo a proteção dos direitos dos cidadãos e dos seus antepassados, bem como o valor probatório dos documentos.

Referências bibliográficas

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS – Guías y Herramientas. *Guías*. [Em linha]. Madrid. [Consult. 18 Jul. 20189]. Disponível em WWW:<URL: https://www.aepd.es/guias/index.html>.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS – Guías y Herramientas. *Herramientas*. [Em linha]. Madrid. [Consult. 18 Jul. 20189]. Disponível em WWW:<URL: https://www.aepd.es/herramientas/index.html>.

BOARDMAN, Ruth; MULLOCK, James; MOLE, Ariane – Bird & Bird & guide to the General Data Protection Regulation [Em linha]. Bird & Bird, 2017. [Consut. 11 Jul. 2018]. Disponível em WWW: <URL: https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf>.

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS (2018) – *Parecer n.º 20/2018*. [Em linha]. Lisboa. [Consult. 12 Jul. 20189]. Disponível em WWW:<URL: https://www.cnpd.pt/bin/decisoes/Par/40_20_2018.pdf>.

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS (2018) - *Projeto de Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a avaliação de impacto sobre proteção de dados*. [Em linha]. Lisboa. [Consult. 18 Jul. 20189]. Disponível em WWW:<URL: https://www.cnpd.pt/bin/consultapublica/Projeto_regulamento_1-2018.pdf>.

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS – RGPD. *Espaço RGPD*. [Em linha]. Lisboa. [Consult. 18 Jul. 20189]. Disponível em WWW:<URL: https://www.cnpd.pt/bin/rgpd/rgpd.htm>.

COMMISSION NATIONALE D'INFORMATIQUE ET DES LIBERTÉS – Les outils de la conformité. L'analyse d'impact relative à la protección des données (AIPD). *Outil PIA: téléchargez et instalez le logiciel de la CNIL*. [Em linha]. Paris. [Consult. 23 Jul. 2018]. Disponível em WWW: <URL: https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>.

CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA. Diário da República Eletrónico [Em linha]. (2005), p. 4642 – 4686 [Consult. 12 jul. 2018]. Disponível em WWW: <URL: https://dre.pt/constituicao-da-republica-portuguesa>.

EUROPEAN ARCHIVES GROUP DATA PROTECTION WORKING GROUP – *Code of conduct for archive services*. [Em linha]. [Consult. 18 Jul. 20189]. Disponível em WWW:<URL: http://dglab.gov.pt/wp-content/uploads/2017/06/201705_code_conduite_v1_EN_version_diffusee.pdf>.

EUROPEAN COMMISSION. Justice and Consumers. Newsroom. Data Protection. *Guidelines* [Em linha]. Brussels. [Consult. 23 Jul. 20189]. Disponível em WWW:<URL: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360&tpa_id=6936>.

FERNÁNDEZ CUESTA, Pablo (2018) – La excepción a la norma: los archivos en el nuevo reglamento General de Protección de Datos. Archivamos [Em linha]. N.º 107. [Consult. 23 Jul. 2018]. Disponível em WWW: <URL:http://publicaciones.acal.es/index.php/archivamos/article/view/684/584>. ISSN 1576-320X.

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS (2017) – *Orientações sobre os encarregados de proteção de dados (EPD)*. [Em linha]. [Consult. 23 Jul. 2018]. Disponível em WWW: <URL: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>.

LEI 67/98. Diário da República Eletrónico [Em linha]. (1998), p. 5536-5546 [Consult. 12 jul. 2018]. Disponível em WWW: <URL: https://dre.pt/application/file/a/239889>.

PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA (1995) – Directiva 94/96/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial da União Europeia [Em linha]. P. L 281/31 – L 281/50 [Consult. 12 jul. 2018]. Disponível em WWW: <URL: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>.

PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA (2016a) – Regulamento (EU) n.º 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Jornal Oficial da União Europeia [Em linha]. P. L 119/1 – L 119/88 [Consult. 12 Abr. 2018]. Disponível em WWW: <URL: https://publications.europa.eu/pt/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-pt>.

PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA (2016b) - Carta dos Direitos Fundamentais da União Europeia (2016/C 202/02). Jornal Oficial da União Europeia [Em linha]. P. C 202/389 – C 202/405 [Consult. 09 jul. 2018]. Disponível em WWW: <URL:https://publications.europa.eu/pt/publication-detail/-/publication/c483a582-2c70-11e6-b497-01aa75ed71a1/language-pt/format-PDF/source-73617436>.

PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA (2016c) - Tratado sobre o Funcionamento da União Europeia. Jornal Oficial da União Europeia [Em linha]. P. C 202/1 – C 202/388 [Consult. 09 jul. 2018]. Disponível em WWW: <URL:https://publications.europa.eu/pt/publication-detail/-/publication/f1bcba61-0d85-4e7f-b41e-a72c42eb5c49/language-pt/format-PDF/source-73617497>.

PRESIDÊNCIA DO CONSELHO DE MINISTROS (2018) – *Proposta de Lei n.º 120/XIII*. [Em linha]. Lisboa. [Consult. 12 Jul. 20189]. Disponível em WWW:<URL: http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679595842774f6a63334e7a637664326c756157357059326c6864476c3259584d7657456c4a535339305a58683062334d76634842734d5449774c56684a53556b755a47396a&fich=ppl120-XIII.doc&Inline=true>.