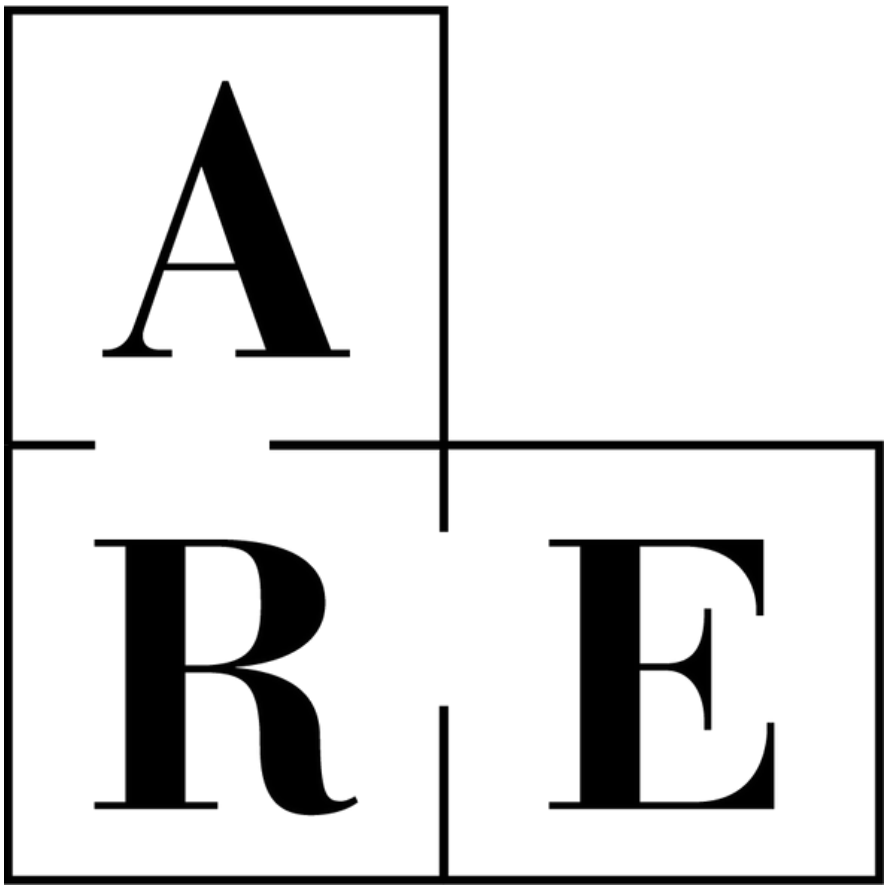
ASSEMBLEIA DE REVISÃO DE ESTATUTOS

ASSOCIAÇÃO ACADÉMICA DE COIMBRA



RELATÓRIO FINAL

Comissão Especializada de Regulamento Geral de Proteção de Dados

Março de 2023

Índice

Parte I - Considerandos

A Comissão Especializada de RGPD (Regulamento Geral sobre a Proteção de Dados) da Assembleia de Revisão de Estatutos da Associação Académica de Coimbra, doravante designada por CERGPD, foi constituída com o intuito de analisar e discutir a lei em vigor para as normas que estabelecem as regras relativas ao tratamento, por parte da AAC, de dados pessoais relativos a pessoas e dirigentes.

Esta Comissão foi inicialmente constituída por Beatriz Ribeiro, Paulo Nogueira Ramos e André Ribeiro. Destes, na primeira reunião da Comissão foi eleito por unanimidade como relatora a membro Beatriz Ribeiro e como vice relator o membro André Ribeiro. No decorrer dos trabalhos, foram adicionados os elementos Félix Rodrigues, Gonçalo Simões, César Sousa, Luísa Lobo e Carlos Rodrigues. À data da realização deste relatório a comissão continha apenas 5 elementos ativos: André Ribeiro, Beatriz Ribeiro, César Sousa, Gonçalo Simões e Paulo Nogueira Ramos.

Parte II – Análise e Investigação

Metodologia

O objetivo principal desta Comissão prendeu-se com a obtenção de informação, por forma a saber a obrigação que lei traduz quanto a esta temática e como a Associação Académica de Coimbra nos seus vários órgãos consegue adotar as várias normas face à sua realidade. Além de se identificar problemas, procurou-se encontrar possíveis soluções para melhorar a transparência e a informatização dos dados, como também e essencialmente, a verificação do cumprimento do RGPD à qual a AAC, como organização, é obrigada a seguir.

Para a obtenção de informação, numa primeira fase, iniciou-se a pesquisa documental através do Regulamento Geral de Proteção de Dados (RGPD) - Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril; Lei da Proteção de Dados Pessoais - Lei n.º 59/2019, de 8 de agosto, lei que aprova regras de prevenção, deteção, investigação ou repressão de infrações penais e Lei n.º 58/2019, de 8 de agosto, lei que assegura a execução do RGPD em Portugal. Para além deste estudo nas normas vigoradas na atualidade foi importante visualizar vários pareceres sobre temáticas importantes para o funcionamento da AAC, como o Parecer do Encarregado de Proteção de Dados da Universidade de Coimbra (EPD-UC) relativamente ao acesso dos dados dos Cadernos Eleitorais para eleições de um órgão da AAC; Parecer Jurídico do Dr. Luís Silva (advogado da AAC) sobre a Necessidade de Assinatura em Papel para Inscrição como Associado Seccionista; Diretrizes da Comissão Nacional de Proteção de Dados (CNPD) sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais (diretriz 2023/1) e disponibilização de dados pessoais dos estudantes, dos docentes e demais trabalhadores no sítio da internet das instituições (diretriz n.º 1/2018). Deste modo, procedeu-se para a segunda etapa que se frisa na realização da entrevista com a entidade individual, o Encarregado de Proteção de Dados da UC. A entrevista ao Encarregado de Proteção de Dados (EPD) foi semiestruturada, permitindo espaço para se explorar respostas que advieram das perguntas pré-estipuladas. É de referir que a entrevista foi realizada simultaneamente por duas comissões (RGPD e de Digitalização e Informatização), sendo que, apesar do cruzamento de interesses em diversas afirmações do EPD, apenas decidimos considerar as que diziam respeito a esta Comissão, descartando as que não abordavam de forma direta o RGPD. Foi também considerada uma intervenção de uma

entrevista realizada pela Comissão Especializada de Informatização e Digitalização quanto ao uso de câmaras por parte da AAC no edifício da AAC. A terceira etapa caracterizou-se pela identificação das considerações e propostas provenientes de fóruns de discussão, tais como os descritos no Documento de Disposições Transitórias da anterior Assembleia de Revisão de Estatutos da AAC, as propostas provenientes do período de Auscultação Pública, bem como das conclusões tidas nas sessões de RGPD das duas edições do Fórum ARE.

Análise às normas em vigor quanto à temática de Proteção de Dados

De forma a saber como as Estruturas da AAC adotam a Proteção de Dados à sua realidade, esta Comissão optou por fazer uma análise exaustiva ao RGPD , na qual se identifica nos seguintes tópicos os principais assunto a ter em conta:

a. Definições, como se entende:

- "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;
- "Consentimento" - 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 ;
- "Tratamento" - 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;

- “Responsável pelo Tratamento” - a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro ;
- “Dados Biométricos” - dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;
- “Violação de dados pessoais” - violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

b. Informação e acesso aos dados pessoais;

   O RGPD estabelece que as organizações devem fornecer informações claras e precisas sobre o tratamento de dados pessoais, incluindo o propósito do tratamento, as categorias de dados pessoais envolvidas, a base legal para o tratamento, entre outras informações. Além disso, as organizações devem permitir que os titulares dos dados acessem seus dados pessoais e solicitem correções ou exclusões.

c. Princípios relativos ao tratamento de dados pessoais;

   O RGPD estabelece vários princípios fundamentais para o tratamento de dados pessoais, incluindo a necessidade de tratar dados pessoais de forma justa, transparente e lícita, de limitar a finalidade do tratamento, de minimizar a quantidade de dados pessoais coletados, de garantir a exatidão dos dados pessoais, de armazenar dados pessoais apenas pelo tempo necessário e de garantir a segurança dos dados pessoais.

d. Tratamento de dados pessoais e sua licitude;

   O RGPD estabelece várias bases legais para o tratamento de dados pessoais, incluindo o consentimento do titular dos dados, a necessidade de tratamento para a execução de um contrato ou para o cumprimento de uma obrigação legal, e o interesse legítimo do

responsável pelo tratamento ou de terceiros. O RGPD também estabelece que algumas categorias de dados pessoais são consideradas sensíveis e requerem um nível mais elevado de proteção.

e. Direito de acesso do titular dos dados (Transparência e regras para o exercício dos direitos dos titulares dos dados);
   O RGPD estabelece que os titulares dos dados têm o direito de aceder aos seus dados pessoais e de solicitar correções ou exclusões. As organizações devem responder a essas solicitações sem demora indevida e devem fornecer informações claras e precisas sobre o tratamento de dados pessoais.

f. Condições aplicáveis ao consentimento;
   O RGPD define o consentimento como uma das bases legais para o tratamento de dados pessoais. Para que o consentimento seja válido, ele deve ser livre, específico, informado e inequívoco. Além disso, as organizações devem ser capazes de comprovar que o consentimento foi obtido de forma adequada.

g. Retificação e apagamento dos dados;
   O RGPD concede aos titulares dos dados o direito de solicitar a retificação ou exclusão de seus dados pessoais. As organizações devem tomar medidas razoáveis para garantir que os dados sejam precisos e atualizados. Além disso, quando solicitado pelo titular dos dados, as organizações devem apagar os dados pessoais sem demora injustificada.

h. Responsabilização pelo tratamento e subcontratante dos dados;
   O RGPD estabelece que as organizações são responsáveis pelo tratamento dos dados pessoais e devem implementar medidas técnicas e organizacionais adequadas para garantir a proteção dos dados. Além disso, as organizações que subcontratem o tratamento de dados pessoais devem garantir que seus subcontratantes estejam em conformidade com o RGPD e estabelecer contratos que garantam a proteção dos dados pessoais.

i. Encarregado/a de Proteção de Dados (EPD).
   O RGPD exige que algumas organizações nomeiem um Encarregado/a de Proteção de Dados para supervisionar a conformidade com o RGPD e garantir a proteção dos dados

pessoais. O DPO (termo usado em inglês, que é equitativo ao utilizado em Portugal com o termo EPD) deve ser independente, ter conhecimento especializado em proteção de dados e ter recursos adequados para desempenhar suas funções.

Face ao exposto anteriormente dá-se a ressalva do que consta na Lei de Proteção de Dados (LPDP). Quanto à Lei 58/2019, de 8 de agosto - Lei que assegura a execução do RGPD em Portugal, esta estabelece as regras para o tratamento de dados pessoais, visando proteger os direitos fundamentais de privacidade e proteção de dados dos titulares dos dados. Desta forma, cabe salientar a importância que a LPDP dá quanto à definição de dados pessoais, como qualquer informação relacionada com uma pessoa singular identificada ou identificável, direta ou indiretamente, em particular por referência a um identificador, como um nome, número de identificação, dados de localização, entre outros; estabelecimento de requisitos específicos para a obtenção de consentimento para o tratamento de dados pessoais, incluindo a necessidade de que o consentimento seja dado de forma livre, específica, informada e inequívoca; o direito de acesso, retificação, apagamento, limitação do tratamento, portabilidade dos dados e oposição ao tratamento são direitos dos titulares dos dados. Cabe ainda dar ênfase à explicitação da Comissão Nacional de Proteção de Dados como autoridade de supervisão independente responsável pela aplicação da lei, a CNPD controla e fiscaliza o cumprimento do RGPD e da presente lei, 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 de dados pessoais. Assim para além do que está definido em RGPD, importa aqui salientar que lhe compete também pronunciar -se, a título não vinculativo, sobre as medidas legislativas e regulamentares relativas à proteção de dados pessoais, bem como sobre instrumentos jurídicos em preparação, em instituições europeias ou internacionais, relativos à mesma matéria; fiscalizar o cumprimento das disposições do RGPD e das demais disposições legais e regulamentares relativas à proteção de dados pessoais e dos direitos, liberdades e garantias dos titulares dos dados, e corrigir e sancionar o seu incumprimento. É importante salientar também as situações específicas de tratamento de dados pessoais que esta lei enumera, tais como: a liberdade de expressão e informação (desde que respeite o princípio da dignidade da pessoa humana consagrado na Constituição da República Portuguesa), a qual estabelece, que a proteção de dados pessoais, nos termos do RGPD e da presente lei, não prejudica o exercício da liberdade de expressão, informação (porém, não legitima a divulgação de dados pessoais como moradas e contactos) e imprensa, incluindo o tratamento de dados para

fins jornalísticos e para fins de expressão académica, artística ou literária; acesso a documentos administrativos que contenham dados pessoais (Lei n.º 26/2016, de 22 de agosto , art.º 6 - restrições ao direito de acesso) onde se realça que o acesso aos documentos administrativos preparatórios de uma decisão ou constantes de processos não concluídos pode ser diferido até à tomada de decisão, ao arquivamento do processo ou ao decurso de um ano após a sua elaboração, consoante o evento que ocorra em primeiro lugar e caso se trate de um terceiro só tem direito de acesso a documentos nominativos se estiver munido de autorização escrita do titular dos dados que seja explícita e específica quanto à sua finalidade e quanto ao tipo de dados a que quer aceder e um terceiro só tem direito de acesso a documentos administrativos que contenham segredos comerciais, industriais ou sobre a vida interna de uma empresa se estiver munido de autorização escrita desta ou demonstrar fundamentadamente ser titular de um interesse direto, pessoal, legítimo e constitucionalmente protegido que justifique o acesso à informação. Por último, esta lei define as várias contraordenações e crimes para os vários tipos de sanções administrativas e penais que se possam verificar no caso de violações da lei, incluindo multas e a possibilidade de responsabilidade civil.

Quanto à Lei n.º 59/2019, de 8 de agosto - Lei que aprova regras de prevenção, deteção, investigação ou repressão de infrações penais, para além do que esta estipula um conjunto abrangente de direitos e obrigações em relação ao tratamento de dados pessoais, alinhado com as disposições do Regulamento Geral de Proteção de Dados da UE, como os princípios gerais de proteção de dados, direitos de titulares de dados e responsabilidade pelo tratamento e subcontratante cabe realçar as normas estipuladas no capítulo VI da presente lei que estabelece a CNPD como autoridade de controlo e explicita as funções, poderes e a responsabilidade de elaborar um relatório anual de atividades sobre a fiscalização da aplicação e do cumprimento da presente lei, o qual pode incluir uma lista dos tipos de violações notificadas e dos tipos de sanções aplicadas. Consequentemente, esta lei tem como objetivo garantir a proteção dos direitos fundamentais das pessoas, especialmente o direito à privacidade, quando esses dados pessoais são tratados em contextos criminais, estabelecendo as regras para a investigação criminal e para a cooperação internacional em matéria de proteção de dados pessoais. Caso seja aplicável, esta estabelece um quadro sancionatório para as violações às normas de proteção de dados pessoais cometidas no contexto de infrações penais, podendo ir desde multas a outras medidas administrativas e disciplinares, que variam de acordo com a gravidade da violação.

Importa, aqui, salientar a Diretriz 1/2018 da CNPD sobre a disponibilização de dados pessoais dos estudantes, dos docentes e demais trabalhadores no sítio da internet das instituições de ensino superior - estabelece que a disponibilização dos dados pessoais deve ser feita com o consentimento prévio e expresso dos titulares dos dados, de forma clara e inequívoca; o acesso aos dados pessoais disponibilizados nos websites deve ser restrito apenas aos utilizadores autorizados, através de mecanismos de autenticação e autorização; as instituições devem garantir a segurança da informação e proteger os dados pessoais contra acessos, perdas, alterações, destruição ou qualquer forma de tratamento ilícito ou não autorizado; os titulares dos dados têm direito a solicitar a correção, eliminação ou limitação do tratamento dos seus dados pessoais, bem como a apresentar queixas à CNPD. É, também, relevante considerar a Diretriz 1/2023 da CNPD quanto às medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais que enfatiza os responsáveis pelos tratamentos e os subcontratantes para as suas obrigações no domínio da segurança dos tratamentos de dados pessoais. Assim, como explicita nas medidas técnicas e organizativas a adotar pelo responsável pelo tratamento e pelo subcontratante, estes são incentivados a definir antecipadamente e a colocar em prática planos de prevenção, para que possam proteger os seus sistemas e infraestrutura e ter mecanismos prontos a detetar uma violação de dados pessoais e mitigar rapidamente os efeitos negativos sobre os direitos dos respetivos titulares (aqui deve-se incluir uma avaliação do risco para estas pessoas singulares, que permita ao responsável pelo tratamento concluir se deve notificar a violação de dados, quer à autoridade de controlo, quer aos titulares dos dados afetados).

Realça-se, também, nesta observação, o parecer do EPD sobre uso dos cadernos eleitorais e o parecer do Dr. Luís Silva quanto à necessidade de assinatura em papel para inscrição de associado seccionista. Quanto ao primeiro parecer destaca-se a licitude para este tipo de tratamento de dados na qual é invocada a norma constitucional de liberdade de associação que permite que estes dados possam ser tratados, não podendo ser disponibilizados no site da Académica qualquer informação relativa ao Caderno Eleitoral em caso de reclamação para consulta dos cadernos eleitorais é necessário apresentar requerimento à Comissão Eleitoral. É de se destacar alguns pontos que o EPD acentuou, quanto à possibilidade da AAC detetar irregularidades em atos eleitorais e com o cruzamento dos dados, verificar e construir cadernos eleitorais credíveis, como também, a possibilidade deste tipo de tratamento de dados ser autorizado pelos titulares dos dados e constar só nome completo do eleitor e seu número de estudante (excluindo o número de matrícula).

Quanto ao parecer sobre a necessidade de assinatura em papel para a inscrição de novos associados seccionistas e de quais procedimentos possíveis para verificar a identidade do requerente no processo de inscrição sublinha-se a ausência de informação quanto ao ato de inscrição propriamente dito, nem sobre a necessidade (ou possível dispensa) de uma assinatura em papel do requerente que se pretenda inscrever como associado seccionista. É realçado o RGPD quanto ao consentimento próprio para tratamento e armazenamento de dados que tem de ser fornecido de forma expressa.

Entrevistas a elementos de relevância para o tema

Na identificação de pessoas a entrevistar, por não haver muito conhecimento e ou prática na área decidiu-se entrevistar o Encarregado de Proteção de Dados da Universidade de Coimbra, pela experiência que tem e pela entreajuda que tem com a AAC, até ao presente.

Bases jurídicas

O EPD apontou duas importantes fontes jurídicas para o que diz respeito a uma boa gestão da proteção de dados.

1. RGPD – estas normas, que, segundo o mesmo, podem ser mais consideradas princípios que normas procedimentais, constituem o documento basilar daquilo que é a proteção de dados. Foi mencionado, no entanto, que existem versões explicativas das ideias gerais e que as mesmas podem ser consideradas para aprofundar as ideias gerais necessárias para a prossecução deste documento legal.

2. Lei 58 e 59 de 28 de agosto de 2019 – esta regulamentação subsidiária assenta em especificidades (58) e numa lógica de aplicação numa segunda fase (59) relativamente ao RGPD.

Neste sentido, podem ser aplicadas várias políticas de privacidade diferentes, consoante a interpretação, havendo, obviamente, o bom senso a cumprir.

Higienização dos Dados

A higienização dos dados – limpeza de dados que não sejam úteis para a finalidade da AAC - é um fator importante e pode ser feito ou por mecanismos de *opt-in* (ter de tomar uma ação afirmativa para ficar na base de dados) ou *opt-out* (ter de informar do seu interesse de ser removida/removido da base de dados). Dependendo do tipo de dados e da sua finalidade, podemos escolher um ou outro. Os associados efetivos poderiam ser questionados pelo mecanismo de *opt-out* para evitar possíveis perdas massificadas pelo atrito natural de algo que exige ação para participar ao invés de ação para sair.

Licitude dos Dados

O EPD mencionou, igualmente, artigo 6º do RGPD - "Licitude de Tratamento" – é importante no que diz respeito ao consentimento informado e à finalidade dos dados (https://www.privacy-regulation.eu/pt/6.htm). Referiu que o foco deveria estar em responder de forma correta a estas duas questões, garantindo que as finalidades apresentadas correspondem àquilo para o que vão servir os dados e que o consentimento informado é garantido (dentro dos limites do que é o aceitável para a lei não ser apenas asfixiante ao bom funcionamento da organização).

Conteúdo versus Forma

À pergunta "Que normas considera interessantes aplicar na regulação da Plataforma de Eleições e noutras plataformas com criticidade elevada?" o EPD respondeu referindo que o problema não está na lei em si (conteúdo) e sim no facto da lei não ser posta em prática, talvez por ela ser um pouco confusa (forma).

Avaliação de Impacto e de Robustez

No entanto, este também mencionou que a plataforma tem um risco elevado de não passar na Comissão Nacional de Proteção de Dados (CNPD). Esta deverá ser feita com base no artigo 35º e, consequente deliberação da CNPD sobre a avaliação de impacto. Neste sentido, tem de ser provado que ninguém se consegue fazer passar, de alguma forma, por outro cidadão e que se consegue meter o risco a um nível aceitável. Se isto chegar à CNPD, eles vão além do risco e vão tentar ver a robustez da plataforma – por robustez entenda-se a capacidade da plataforma de garantir parâmetros de segurança aos seus utilizadores e aos dados que os mesmos cedem direta ou indiretamente.

Confidencialidade dos Envolvidos no Acesso aos Dados

O EPD mencionou que os dirigentes e não dirigentes que lidassem com informação de associados deveriam assinar um contrato de confidencialidade de forma a garantir que seriam responsabilizados por uma utilização indevida dos dados.

Inscrição de Associados

Relativamente à pergunta "Como considera que deverá ser o procedimento para efetuar inscrição de associados através de plataformas online, de forma a respeitar o RGPD?" o EPD disse que a interpretação do advogado da AAC – presente no parecer sobre esta mesma questão aquando da apresentação desta problemática pela Comissão de Digitalização e Informatização da Assembleia de Secções Culturais - está correta, mas que é demasiado rígida e que a interpretação da Comissão é igualmente válida. Ele aconselhou que fosse dada uma escolha de dar a oportunidade das pessoas que não quisessem ir presencialmente à secretaria entregar a ficha de associado poderem enviar o seu documento identificativo que teria como finalidade comprovar que era realmente a pessoa e depois seria apagado. Também foi referido que uma sms ou um email de verificação seria suficientemente válido para a inscrição de associados. Neste sentido, a informação seria guardada durante um tempo a definir até a verificação ser feita. Caso depois desse tempo a pessoa não responda, os seus dados devem ser apagados.

Mais uma vez foi referido que é importante demonstrar que os dados a serem pedidos são necessários para a finalidade pretendida e, com isto, justificar os identificadores que estamos a pedir. Se esses dados não forem necessários para registros funcionais ou históricos, não devem ser pedidos. O EPD referiu que a ficha de inscrição dos associados seccionistas pede alguns dados que podem não ser necessários para a finalidade da mesma.

Privacy e Proteção de Dados

O EPD diferenciou o termo "*privacy"* do termo "proteção de dados", sendo que referiu a forma liberal que os Estados Unidos da América, por exemplo, interpretam estas questões, vendo a privacidade como escolha do indivíduo e a forma como a União Europeia interpreta como direitos que têm de ser protegidos independentemente se o indivíduo afetado concorda ou não com eles.

Plenários

No que diz respeito à pergunta "Que cuidados há a ter na realização de reuniões plenárias online e/ou em regime misto?", o EPD referiu que a câmara deveria estar ligada em momentos de votação e de intervenções por parte dos associados. Referiu igualmente que a gravação deveria ser consentida pelos indivíduos, mas que poderia existir forma de considerar que foi uma escolha deles não participar caso não consentissem. Este consentimento deve ter, mais uma vez, capacidade de responder à finalidade, que neste caso deveria ser para questões de elaboração das atas. Seria guardada essa gravação até ao momento em que a ata fosse aprovada em plenário seguinte.

Gestão Automática e Quotas

À questão "Concorda com a implementação do pagamento de quotas e da gestão automática de associados por plataformas? (Que obstáculos podem surgir desse mecanismo?)" o EPD afirmou que concorda e deve ser feito e referiu que os cuidados que devem ser tidos são principalmente externos a Associação, visto que o que se passa dentro da Associação só se torna problema em termos de proteção de dados se 1) não responder à finalidade proposta e se 2) se externalizar para fora dela (enquanto a informação estiver nos circuitos internos da AAC o problema não se demonstra considerável).

Repositório Digital

Relativamente à questão "Concorda com a implementação de um repositório de documentação oficial da Associação Académica de Coimbra equivalente à progressiva digitalização do arquivo de secretaria? (Que precauções nos aconselha a ter relativamente à sua implementação?)" o EPD afirmou, mais uma vez, que concorda. Relativamente a este tópico o mesmo aconselha a decidirmos o que são os tipos de dados que temos guardados e definir prazos associados às suas finalidades para ficarem guardados pela AAC. Assim seria mais fácil gerir os fluxos de digitalização de informação dos arquivos e de ver formas de proteger os dados das partes envolvidas.

Videovigilância na AAC

Este ponto provém de uma entrevista realizada pela Comissão Especializada de Digitalização e Informatização que gentilmente cedeu a esta comissão para análise deste tópico. O entrevistado, funcionário de uma empresa prestadora de serviços à AAC, informa que lhe foi

transmitido que a Direção Geral da AAC iria colocar câmeras de vigilância no edifício, mais especificamente nas entradas do edifício, na zona de acesso ao bar, como também na sala de estudo (não especificando mais locais em concreto). Para este, o cerne da questão não é o seu uso, mas quem seria o titular das imagens e/ou som das gravações. Revela que mesmo em zonas alocadas ao bar, para o entrevistado e de acordo com o conhecimento que obteve, deveria ser a AAC a titular destas gravações e não poderia ceder essa titularidade a outrem.

Propostas provenientes do Documento de Disposições Transitórias

Do Documento de Disposições Transitórias elaborado, aprovado e divulgado pela anterior Assembleia de Revisão de Estatutos da AAC, não constava qualquer informação quanto ao tema de proteção de dados.

Propostas provenientes da Audição Pública

Durante o período de audição pública, que decorreu de 1 de setembro a 31 de outubro de 2022, não se obteve nenhuma proposta quanto a esta temática.

Propostas provenientes das duas edições do Fórum ARE

Relativamente à primeira edição deste evento, realizado a 21 de outubro de 2022, foram relatados os seguintes problemas quanto a esta temática:

a. Falta de adaptação ao enquadramento legal exigido e a figura do Encarregado de Proteção de Dados;

Em relação à adequação das normas e procedimentos atualmente em vigor na AAC ao quadro legal nacional e europeu em matéria de proteção de dados, foi evidenciado que existe um significativo atraso na adaptação das normas e processos àquilo que são os princípios e condicionantes que as novas regras vêm impor. Sendo assim, para os participantes é necessário proceder às adaptações que a lei indica, começando esse

encaminhamento pelo EAAC. Quanto à figura do Encarregado de Proteção de Dados, imposta pelo quadro legal atualmente em vigor, considerou-se que é algo que deve estar devidamente enquadrado nos Estatutos e ainda que esta figura deva ser escolhida preferencialmente de entre os funcionários da casa, de forma a que não esteja sujeito a constantes alterações da pessoa que desempenha este papel, como é o caso dos cargos de natureza eletiva, caracterizados por alterações constantes, habitualmente numa base anual.

b. Falta de formação dos funcionários da AAC;

Para que as normas em vigor tenham verdadeiramente eficácia ficou explanado como essencial que haja uma forte aposta na formação tanto de funcionários, que seguindo a proposta transata são quem irá desempenhar o papel de Encarregado de Proteção de Dados, como também são os principais agentes de recolha e tratamento de dados pessoais (neste caso com especial foco nos Serviços de Secretaria e Tesouraria). É realçado que os dados que dirigentes que pela natureza das suas funções se vejam obrigados a lidar com os dados pessoais de qualquer Associado devem ter a indicação de como proceder, podendo para os inquiridos, esta necessidade fica também desde logo prevista nos nossos Estatutos.

c. Recolha de dados para candidatura e empossamento de qualquer associado enquanto dirigente (ex. morada);

Relativamente aos dados recolhidos para candidatura e empossamento de qualquer associado enquanto dirigente considerou-se excessiva a obrigatoriedade de entrega e recolha da morada, por não existir no entender dos visados um fim para a utilização destes dados, bem como a solicitação de fotocópia do Cartão de Cidadão ou outro documento identificativo.

d. Disponibilização dos cadernos eleitorais por parte da Universidade de Coimbra, para uso nas eleições da Associação Académica de Coimbra;

De acordo com os participantes, parece-lhes que a utilização de Cadernos Eleitorais de forma desmaterializada, conforme tem sido realizado nas últimas eleições, é um procedimento que oferece mais garantias ao nível da segurança e controlo de acesso aos dados recolhidos.

Nota: considerando o quadro sancionatório aplicável às infrações ao disposto no Regulamento em apreço e a importância que tem hoje a segurança dos dados pessoais para a opinião pública, os participantes consideraram que os custos acrescidos relatados em algumas propostas são um investimento necessário e razoável, tendo em conta os possíveis danos tanto financeiros como reputacionais que as infrações ao presente Regulamento possam trazer para a AAC.

Quanto à segunda edição do Fórum ARE, realizada a 18 de fevereiro de 2023, foram relatados os seguintes pontos quanto a esta temática:

a. Recolha de Dados e sua finalidade;

Para os participantes é importante perceber as necessidades de recolha de dados da AAC, sendo uma dessas barreiras a recolha de dados para a realização de atos eleitorais, devendo ser recolhido o nome completo, nº de estudante (p.e. 20212(xxxx)6) e email de todos os associados para este fim. É assim necessário, averiguar as limitações com a Lei de Proteção de Dados, recolher informação no âmbito dos associados seccionistas, como também, recolher todos os dados possíveis no limite da lei. Desta forma, é também salientado a necessidade de haver uma responsabilidade na gestão e controlo de informação.

b. Formas de obtenção de consentimento informado;

Face a este tema, a opinião é que deve haver uma autorização através de assinatura seja em eventos presenciais ou online, sendo que para este último caso deve ser feita uma autenticação da pessoa.

Quanto ao ato da matrícula dá-se a nota que deveria constar uma informação que notifica o estudante em como seria automaticamente associado da AAC facilitando o tratamento dos dados que são fornecidos pela UC à AAC tornando este tratamento mais seguro e mais coerente com a lei (como também haveria um procedimento para caso alguém não concorde em ser associado).

Relacionado a este tópico, é também bom realçar que para os intervenientes é importante contratualizar esta cedência de dados entre a Universidade de Coimbra e AAC.

c. Regulamento Geral de Proteção de Dados próprio da AAC;

Durante a discussão, os participantes falaram sobre a criação de um Regulamento de Gestão do Espaço Digital. No entanto, para estes pode acabar por ser redundante uma vez que irá resultar sempre em última instância na Lei de Proteção de Dados. Assim, para estes deveria ser colocado nos EAAC algo mais Geral e as questões mais técnicas deveriam encontra-se em um Regulamento de RGPD ou na Contratualização com a UC.

d. Responsabilidade de Encarregado/da de Proteção de Dados (EPD);

Para estes quem deveria ficar responsável e ter esta tarefa de RGPD seria a Secretaria da AAC, uma vez que executa a maioria do tratamento dos dados e teria assim competência para tratar das tarefas como EPD.

e. Formação sobre RGPD.

Sobre este tópico, é relatado que deve haver formação com uma entidade externa. É especificado que esta iniciativa seria um complemento à formação dos funcionários, como também, seria importante uma formação para dirigentes que tenham de tratar dados/informação na plataforma (ou plataformas a existir).

Parte III e IV – Conclusões e Propostas de Recomendação ao Plenário

Concluída a fase de obtenção de informação, cabe a esta Comissão concluir acerca dos vários tópicos a discutir em Plenário por parte da atual ARE em funções, relativa ao tema de Proteção de Dados.

Criação do Cargo de EPD da AAC

A AAC não tem alguém alocado exclusivamente à função de EPD. Isto faz com que esta função seja fragmentada e que possam ocorrer lacunas naquilo que é a recolha e armazenamento de dados. A figura do EPD possibilitava começar a posicionar esta área como prioritária para a nossa organização e, com isto, garantir uma metodologia centralizada que permite o apoio às estruturas para que haja cumprimento adequado do RGPD sem prejudicar as dinâmicas ótimas da casa em termos sociais e organizacionais.

Inscrição de Associados à Distância

A AAC deve permitir a inscrição de associados seccionistas e extraordinários através da verificação final por sms ou email. Assim possibilita-se o respeito pelo consentimento informado do fornecedor de dados e não se prejudica ou se cria atrito ao funcionamento da Casa. Este método deve ser apresentado no artigo 9º - ou equivalente dos futuros EAAC –, de forma a deixar clara esta possibilidade.

Robustez da AAC na Proteção de Dados

A AAC deve garantir robustez na proteção de dados, tanto nas suas plataformas digitais, como nos seus repositórios e processos físicos. Esta garantia deve ser normalizada de modo a garantir que as estruturas e órgãos da Casa ficam vinculados a boas práticas neste âmbito.

Responsabilização de Dirigentes e Não Dirigentes

O uso individual de dados e a sua cedência não autorizada devem ser alvos de processos disciplinares e sancionados em caso de prova do delito. Deve-se, no entanto, considerar a figura de "fuga inocente de dados" em casos que possa haver a) incapacidade de evitar a passagem de informação, b) caso essa informação seja passada sem intenção de o fazer e/ou c) caso essa fuga se revele inofensiva para as vítimas da cedência. No entanto, ressalva-se o terreno

movediço que esta área tem: a intencionalidade por parte de quem partilha é algo difícil de analisar e o impacto da fuga também não se revela, em certos casos, de medição fácil. Destarte, a proposta mantém-se, visto que não proteger os associados e outras personalidades jurídicas de fugas de dados é não garantir que há procedimentos que permitam a efetivação do RGPD.

Higienização e Licitude da Informação

A AAC deve exigir que, procedimentalmente, a aquisição de dados responda a três critérios: 1) que as finalidades sejam compreensíveis e pouco vagas, 2) que se peça apenas informação necessária para essas finalidades e 3) que essa partilha tenha consentimento das partes envolvidas, salvo em casos especificamente considerados pela Comissão Disciplinar ou Conselho Fiscal em caso de estar em risco a própria AAC na sua totalidade ou nas suas diferentes partes. Nestes casos, esta partilha deve ser antecedida por um parecer jurídico caso não seja por coação judiciária.

Criação de um Guia Interno para implementação das normas de proteção de dados na AAC

De forma que haja uma adaptabilidade e agilidade para a execução dos trabalhos dentro e fora do edifício AAC, no concerne aos vários órgãos da AAC, recomenda-se que haja um documento síntese e exemplificativo de como atuar para o cumprimento das normas de proteção de dados para cada caso, por ex.: informação necessária para uma candidatura, inscrições em atividades e/ou eventos, entre outros.

Formação dos funcionários e dirigentes

Em complementaridade ao exposto anteriormente, a AAC deve garantir que os elementos que interagem com este tipo de matérias tenham a oportunidade de aprender como aplicar e executar o seu trabalho em favor do cumprimento do RGPD, de forma a evitar que a AAC seja sancionada pelo previsto na lei com o não cumprimento da proteção de dados.

Regulamentação nos EAAC quanto ao fornecimento de dados por parte da UC para a AAC

Os dados pessoais adquiridos pela Universidade de Coimbra, no ato da matrícula, que posteriormente é usado pela AAC para uso de Cadernos Eleitorais, elemento identificador de quem é ou não associado e está assim disponível para votar, deve ser orientado por um consentimento por escrito por ambas as partes de forma a regulamentar em definitivo os

direitos e deveres de ambas as partes, ocorrer sempre pelo predisposto e regularizar os processos, por forma a se saber qual a procedimento a aplicar.

Criação de uma Plataforma para uso de todos os órgãos da AAC

Por forma a manter um único registro das atividades de processamento de dados pessoais, a AAC deve manter um registro de todas as atividades de processamento de dados pessoais que realiza. Neste sentido, formulários para inscrição de eventos, único local para pesquisa de associados, entre outras medidas, deve constar tudo numa única plataforma de forma a armazenar-se a informação de dados pessoais num único local e a AAC ser o único responsável e titular pelo tratamento de dados (ao contrário que acontece ao usar os formulários da Microsoft ou Google, os quais a estes é reservado a titularidade e a acesso aos dados), para cumprimento da proteção de dados e assim, não ocorrer a possibilidade de penalizações judiciárias.

Implementação de videovigilância no edifício da AAC e o uso de Biometria no edifício da AAC

Quanto às temáticas supracitadas realça-se com o novo regulamento europeu de proteção de dados, já não é necessário pedir autorização ou fazer alguma notificação à CNPD para ter um sistema de videovigilância. De acordo com a com a Lei n.º 34/2013, de 16 de maio, um bar que tenha uma área superior a 200m² é considerado um estabelecimento de restauração e bebidas e é obrigado a ter câmeras de vigilância. Assim, é importante salientar que a colocação das câmaras deve ter em conta a estrita necessidade de manter um perímetro de segurança e de controlar os acessos a partir do exterior, de modo adequado às circunstâncias do local e de modo proporcionado para não restringir excessivamente os direitos dos cidadãos. Deste modo, as câmaras não podem incidir sobre as vias públicas, propriedades limítrofes ou outros locais que não sejam do domínio exclusivo do responsável; não podem incidir sobre o interior de áreas reservadas a clientes ou utentes como, instalações sanitárias, zonas de espera, áreas técnicas de cabeleireiros, zonas de descanso ou lazer, o interior dos elevadores, salas de refeições, esplanadas, vestiários, interior de piscina ou ginásio; não podem incidir sobre a zona de digitação de códigos de caixas multibanco ou outros terminais de pagamento ATM. Realça-se que é proibida a captação de som, exceto no período em que as instalações estejam encerradas, isto é, sem pessoas a trabalhar nas zonas vigiadas.

Para o cumprimento das normas estipuladas para a videovigilância atenta-se os seguintes cuidados: a obrigatoriedade de afixar um aviso informativo, os titulares dos dados têm o direito a ser informados sobre a utilização de sistemas de videovigilância (o aviso informativo deve respeitar o previsto no artigo 31.º, n.ºs 5 e 6, da Lei 34/2013 e no artigo 115.º e no Anexo VIII da respetiva portaria regulamentar) e a conservação das imagens deve ocorrer pelo período de 30 dias, sendo obrigatório eliminar as imagens até 48 horas após os 30 dias (sem prejuízo de ser necessário manter as imagens por mais tempo, no âmbito de processo criminal em curso).

No que se refere ao uso de biometria convém salientar que dados biométricos são considerados dados pessoais. Sendo assim, é necessário estabelecer garantias para a defesa dos direitos dos titulares e caso haja o consentimento do titular dos dados, nos termos legalmente exigíveis para o consentimento, é preciso assegurar que o consentimento é explícito, informado, específico e dado livremente.

No caso da Associação, estes dados são usados pelos funcionários da entidade como forma de controlo de assiduidade e de acessos às instalações do empregador. Neste sentido cabe certificar os seguintes pontos para o cumprimento da proteção de dados: deve assegurar-se que só são utilizadas representações do dado biométrico (template) e que o processo não permita a reversibilidade dos dados (artigo 28.º, n.º 6, da Lei 58/2019); deve garantir que tem na sua posse uma declaração do fabricante do sistema atestando a existência destas características; caso haja a necessidade de ocorrer alterações ao tratamento de dados biométricos previamente autorizado pela CNPD e às condições aí fixadas, a autorização perde a sua validade (caduca), em consequência, terá de cumprir todas as exigências legais como se estivesse a projetar um tratamento de dados pela primeira vez.

Parte V - Anexos

1. Exemplos de elementos de identidade ou identificadores que em separado, ou em conjunto, podem identificar uma pessoa.

Descrição do identificador	Singulares	Físicos	Identificação	Contacto	Biométricos	Saúde	Vida	Patrimoniais	Profissionais	Académicos	Criminais	Outros
Altura / Peso		🔒										
Cor da Pele / Cabelo / Olhos		✎										
Idade / Faixa etária		🔒	🔒									
Piercings / Tatuagens	●	🔒										
Deficiências físicas ou mentais	●	✎				✎						
Sexo biológico / Género		✎	🔒									
Impressões Digitais / Íris / Imagem / Voz	●	🔒			✎							
Idiomas / Dialetos falados		🔒					🔒			🔒		
Nacionalidade / Étnia / Raça		✎	🔒									
Tamanho do vestuário		🔒										
Endereço eletrónico	●			🔒								
Endereço postal				🔒								
Nº de telefone / telemóvel / fax	●			🔒								
Nome	●		🔒									
Data / Local de Nascimento			🔒									
Fotos	●		✎									
Estado Civil			🔒				🔒					
Assinatura	●		🔒									
N.º Segurança Social / IF / CC / Carta Condução	●		🔒									
N.º Passaporte / Utente	●		🔒									
N.º Membro / Dador de Sangue	●		✎				✎					
Grupo sanguíneo						✎						
Código ADN	●					✎						
Histórial médico pessoal / familiar	●					✎						
Registos e Prescrições médicas	●					✎						
Resultados de exames/análises clínicas	●					✎						
Baixas e Declarações Médicas	●					✎						
Dados Seguro de Saúde / Vida	●					✎						
Estilo de Vida	●					✎	✎					
Ficha de aptidão para o trabalho	●					✎						
Afiliações Políticas / Sindicais							✎					
Características Pessoais	●						🔒					
Crenças Filosóficas / Religiosas							✎					
Estrutura familiar (filiação, irmãos, conjuge,	●						✎					
Comportamento / Gostos / Não Gostos							🔒					
História pessoal	●						🔒					
Hobbies							🔒					
IP-address (estático) / MAC adress	●						🔒		🔒			
Localização (GPS, país, número do quarto)	●						🔒		🔒			
Matrícula do carro próprio/de serviço	●						🔒		🔒			
Mensagens de email ou voz	●				✎		🔒					
Músicas preferidas							🔒					
Nº PIN / IBAN	●						🔒	🔒				
Objectivos / intenções	●						🔒		🔒			
Opiniões e Comentários	●						✎					
Características de Personalidade	●						✎					
Regime matrimonial							🔒					
Reputação Geral	●						🔒					
Viagens e Deslocações em serviço	●						🔒		🔒			
Vida sexual (orientação, tendências, histórias)	●						✎					
N.º Conta Bancária / Cartão Débito/Crédito	●							🔒				
Registos conta bancária / Extratos / Hábitos de consumo	●						🔒	🔒	🔒			
Salário / Prémios / Subsídios e outras remunerações	●							🔒	🔒			
Escalões de rendimento								🔒				
Empréstimos / Hipotecas / Impostos	●							🔒				
Receitas / Despesas	●							🔒				
Propriedades (adquiridas, arrendadas, emprestadas)	●							🔒				
Transações de compra ou de venda	●							🔒				
Situação Fiscal	●							🔒	🔒			
Empregador									🔒			
Profissão									🔒			
Títulos / Cargos / Nível									🔒			
Dados de Contrato de trabalho	●								🔒			
ID de empregado	●								🔒			
Contactos Profissionais	●								🔒			
Ações disciplinares	●								✎	✎	✎	
Avaliações de Desempenho	●								🔒			
Controlo de Assiduidade e Pontualidade	●								🔒			
Histórico Profissional / Entrevistas / Formações	●								🔒			
Informação de Seguros Vida / Acidentes	●								✎			
Notas / Percurso / Grau académico	●									🔒		
Curriculum Vitae	●									🔒		
Certificações / Competências técnicas										🔒		
Caligrafia	●											🔒
ID / Perfil rede social	●											🔒
ID de cookies												🔒
Password												🔒
Acusações	●										✎	
Condenações	●										✎	
Multas	●										✎	
Perdões ou indultos	●										✎	
Categoria especial ✎												

2. Parecer nº4/2022 do EPD/UC - Disponibilização de elementos para a constituição dos cadernos eleitorais para a eleição do Conselho Fiscal da AAC;

3. Parecer Jurídico - Necessidade de assinatura em papel para inscrição como associado seccionista.