UNIVERSIDADE
AbERTA
www.uab.pt

DESPACHO Nº 60/R/2023

Em conformidade com a habilitação legal que define a competência subjetiva e objetiva do Reitor da Universidade Aberta conferida, respetivamente, pelos artigos 76.º, n.º 2 e 112.º, n.º 7, da Constituição da República Portuguesa, pelo artigo 136.º do Código do Procedimento Administrativo (CPA), pelo artigo 110.º, n.º 2, alínea a), do Regime Jurídico das Instituições de Ensino Superior (RJIES), aprovado pela Lei n.º 62/2007, de 10 de setembro e pelos artigos 2.º, n.º 3, 98.º e 99.º do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD), tendo sido ouvida a comunidade académica com interesse direto na disciplina jurídica do presente âmbito regulamentar e tendo sido efetuada a correspondente consulta pública do projeto, nos termos e para efeitos do artigo 110.º, n.º 3, do RJIES e dos artigos 100.º e 101.º do CPA, aprovo, no uso da competência que me é conferida pela alínea o) do n.º 1, do artigo 92.º, do RJIES, o Regulamento de Proteção de Dados Pessoais da Universidade Aberta, anexo a este despacho e do qual faz parte integrante.

Lisboa, Universidade Aberta, 16 de junho de 2023

A Reitora

Carla Maria Bispo Padrel de Oliveira

UNIVERSIDADE
AbERTA
www.uab.pt

REGULAMENTO DE PROTEÇÃO DE DADOS PESSOAIS DA UNIVERSIDADE ABERTA

NOTA JUSTIFICATIVA

A Universidade Aberta, universidade pública de ensino a distância, doravante designada UAb, no âmbito do Modelo Pedagógico Virtual por si desenvolvido, utiliza os dados pessoais dos seus interlocutores e clientes, bem como o seu tratamento ao nível da proteção de dados, nomeadamente nas várias plataformas em que interage.

O Regulamento de Proteção de Dados Pessoais da UAb, doravante referido como Regulamento, é apenas uma das várias diligências que a UAb tem desenvolvido para responder às exigências em matéria de proteção de dados pessoais resultantes da entrada em vigor do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (doravante, "RGPD").

Pelo presente Regulamento, pretende a UAb fixar as regras que devem presidir ao tratamento de dados das pessoas singulares que se relacionam consigo.

Um dos objetivos fundamentais deste Regulamento consiste em a UAb cumprir elevados *standards* de qualidade e conduta, em conformidade com as regras previstas na lei vigente, que se traduzam não só no cumprimento da referida lei, mas também no respeito dos direitos, liberdades e garantias dos seus clientes e colaboradores.

Tendo em conta o potencial económico que a existência de bases de dados organizadas, com informação certificada, representa na atual sociedade, mas também o custo inerente à atualização, manutenção e controlo de segurança de dados pessoais, estabelecem-se ainda neste Regulamento de execução do RGPD regras relativas à utilização de serviços de divulgação autorizada de variados aspetos de determinados dados pessoais.

Quanto aos atos e formalidades relativos à formação, manifestação e execução de vontades tendentes à aprovação do presente Regulamento, dado o processo de digitalização da Universidade em curso, a Magnífica Reitora, como responsável pela direção do procedimento, decidiu não proceder à audiência dos interessados, de acordo com as disposições conjugadas do n.º 3 do artigo 110.º da Lei n.º 62/2007, de 10 de setembro (RJIES – Regime Jurídico das Instituições de Ensino Superior), e a alínea c), do n.º 3 do artigo 100.º do Código do Procedimento Administrativo (CPA), tendo, antes, o respetivo projeto sido objeto de consulta pública, nos termos do artigo 101.º do CPA, não tendo, contudo, sido prestados quaisquer contributos nesse período.

Assim, nos termos da habilitação legal conferida conjugadamente pelos artigos 76.º, n.º 2 e 112.º, n.º 7, da Constituição da República Portuguesa, pelo artigo 136.º do CPA, pelos artigos 92.º, n.º 1, alínea o) e 110.º, n.º 2, alínea a), da Lei n.º 62/2007, de 10 de setembro (RJIES – Regime Jurídico das Instituições de Ensino Superior), pelo artigo 7.º, dos Estatutos da Universidade Aberta, homologados pelo Despacho Normativo n.º 65-B/2008, publicados no

Diário da República, 2.ª série, n.º 246, de 22 de dezembro, pelo RGPD e pelas Leis n.º 58/2019 e n.º 59/2019, ambas de 8 de agosto, o presente regulamento, constituído pela presente nota justificativa e pelo seguinte articulado, é aprovado e torna-se definitivo.

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º
Objeto

1 – O presente Regulamento destina-se a definir e estabelecer as regras específicas a aplicar à proteção das pessoas singulares no que respeita ao tratamento de dados pessoais e à sua circulação e que deverão constituir o Sistema Integrado de Dados Pessoais da Universidade Aberta (SIDPUAb).

2 – Para efeitos do número anterior, os dados pessoais que a UAb recolhe e trata dependem sempre da natureza da atividade desenvolvida pela UAb, e podem incluir, nomeadamente:

a) Estudantes e Formandos;
b) Candidatos;
c) Docentes, Investigadores, Bolseiros, Tutores e Formadores;
d) Colaboradores não docentes;
e) Fornecedores e Prestadores de Serviços;
f) Auditores;
g) Visitantes e público em geral.

Artigo 2.º
Âmbito de aplicação

1 – O presente Regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados, no âmbito da UAb.

2 – O presente Regulamento aplica-se ainda ao tratamento de dados pessoais realizados e aos serviços e unidades orgânicas da UAb, nomeadamente no âmbito das suas atribuições.

Artigo 3.º
Definições relevantes

Para efeitos deste Regulamento entende-se por:

a) «RGPD», o Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, designado por Regulamento Geral da Proteção de Dados;

b) «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;

c) «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;

d) «Interconexão de dados», a forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiro mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade;

e) «Limitação do tratamento», a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro;

f) «Definição de perfis», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;

g) «Pseudonimização», o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;

h) «Perfilagem», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;

i) «Ficheiro», qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;

j) «Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; no caso do objeto do presente Regulamento interno, a UAb;

k) «Subcontratante», uma pessoa singular ou coletiva, a autoridade pública, ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;

l) «Destinatário», uma pessoa singular ou coletiva, a autoridade pública, ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades públicas que possam receber dados pessoais no âmbito de inquéritos específicos nos termos do direito da União ou dos Estados-Membros não são consideradas destinatários; o tratamento desses dados por essas autoridades públicas deve cumprir as regras de proteção de dados aplicáveis em função das finalidades do tratamento;

m) «Terceiro», a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais;

n) «Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual, o titular dos dados, aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;

o) «Violação de dados pessoais», uma 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;

p) «Dados relativos à saúde», dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde;

q) «Autoridade de controlo», a autoridade pública independente nacional, isto é, a Comissão Nacional de Proteção de Dados (CNPD);

r) «Objeção pertinente e fundamentada», uma objeção a um projeto de decisão que visa determinar se há violação do RGPD ou se a ação prevista relativamente à UAb ou ao subcontratante está em conformidade com o RGPD, demonstrando claramente a gravidade dos riscos que advêm do projeto de decisão para os direitos e liberdades fundamentais dos titulares dos dados e, eventualmente, para a livre circulação de dados pessoais;

s) «*Data Protection Officer (DPO)*», o Encarregado de Proteção de Dados (EPD), pessoa singular à qual é atribuída a tarefa e responsabilidade formal de informar e aconselhar a UAb para o cumprimento das disposições aplicáveis, mas também o

papel ativo de controlar, monitorizar e reportar à UAb a desconformidade da sua atuação, propondo-lhe soluções para alcançar a desejada conformidade com as regras do RGPD;

t) «*Data Privacy Impact Assessment (DPIA)», a* Avaliação de Impacto sobre a Proteção dos Dados (AIPD), isto é, a diligência e estudo prévio obrigatório no âmbito da proteção daqueles dados cujo tratamento seja suscetível de resultar num alto risco para os direitos e liberdades dos respetivos titulares, designadamente quando se esteja na presença de dados pessoais especiais;

u) «*Compliance*», a verificação da conformidade da atuação da UAb com o RGPD, designadamente quanto às suas regras, políticas, diretrizes e atividades, sem prejuízo da deteção de desvios e inconformidades e da sua resolução;

v) «*Accountability*», a responsabilização ética da UAb no sentido de serviço público e do cumprimento do RGPD, mediante a adoção de adequados procedimentos de controlo interno e de transparência na prestação de contas em relação a quantos interagem com a Universidade;

w) «*Privacy by Default*» (Privacidade por defeito), o que pretende assegurar que são colocados em prática, dentro de uma Organização, mecanismos para garantir que, por defeito, apenas os dados pessoais necessários são recolhidos, utilizados e conservados para cada tarefa, tanto em termos da quantidade de dados recolhidos, como do tempo pelo qual eles são mantidos. No que diz respeito ao período pelo qual os dados pessoais são retidos, devem ser respeitados os períodos de conservação definidos, findo os quais são descartados os dados que já não necessários - Princípio da Minimização dos Dados;

x) «*Privacy by Design*» (Privacidade desde a conceção), o que pretende levar o risco de privacidade em conta em todo o processo de conceção de um novo produto ou serviço, avaliando detalhadamente o risco e implementando medidas e procedimentos técnicos e organizacionais adequados desde o início, para garantir que o tratamento está em conformidade com o RGPD e protege os direitos dos titulares dos dados em causa. As soluções respeitam durante o seu ciclo de vida, a privacidade dos dados que tratam. É garantida através da incorporação dos conceitos de proteção de informação, minimização de acessos à informação e outras práticas e mecanismos que garantam a segurança da informação, em todas as fases da conceção (planeamento, desenvolvimento/ aquisição, *deployment*/disponibilização, *on-going*);

y) «Sistema Integrado de Dados Pessoais da UAb (SIDPUAb)», sistema de governação de informação para o tratamento de dados pessoais das pessoas singulares referidas no artigo 1.º, n.º 2 (adiante, «titular dos dados», ou «titular») organizado segundo critérios definidos em conformidade com o RGPD, linhas de orientação emitidas por autoridades europeias e nacionais, por cláusulas modelo aprovadas pela Comissão Europeia ou por autoridades de controlo, assim como por qualquer jurisprudência

relevante, regras legais e estatutárias aplicáveis à UAb e com este Regulamento interno.

Artigo 4.º
Finalidades

1 – É objetivo primacial do presente Regulamento a defesa dos direitos e das liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.

2 – O atual Regulamento tem ainda como finalidade estabelecer os contornos do tratamento de dados pessoais necessário ao exercício de funções de interesse público da UAb, prevendo disposições específicas nomeadamente sobre:

a) As condições gerais de licitude do tratamento dos dados;
b) Os tipos de dados objeto de tratamento;
c) Os titulares dos dados em questão;
d) As entidades a que os dados pessoais poderão ser comunicados e para que efeitos;
e) Os limites a que as finalidades do tratamento devem obedecer;
f) Os prazos de conservação;
g) As operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento;
h) As medidas relativas a outras situações específicas de tratamento em conformidade com objetivos de interesse público, proporcional ao objetivo legítimo prosseguido.

CAPÍTULO II

PRINCÍPIOS RELATIVOS AO TRATAMENTO DE DADOS PESSOAIS

Artigo 5.º
Princípios

1 — Através da adoção gradual de um conjunto de medidas técnicas e organizativas como, por exemplo, o controlo de acessos, a realização de avaliações de impacto, a elaboração de um registo das atividades de tratamento, a designação de um encarregado de proteção de dados, a aplicação de técnicas de anonimização e de pseudonimização, as recomendações da Resolução do Conselho de Ministros n.º 41/2018, de 28 de março de 2018, entre outras medidas, a UAb garante que os tratamentos de dados pessoais que realiza respeitam os princípios enunciados no artigo 5.º do RGPD, nomeadamente o princípio da licitude, lealdade e transparência, o princípio da limitação das finalidades, o princípio da minimização dos dados, o princípio da exatidão, o princípio da limitação da conservação, o princípio da integridade e confidencialidade e o princípio da responsabilidade.

Artigo 6.º

Princípio da licitude, lealdade e transparência

1 – Para que o tratamento seja lícito, leal e transparente em relação ao titular dos dados, tem de verificar-se pelo menos uma das seguintes situações:

a) Haja consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
b) O tratamento seja 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 seja necessário para o cumprimento de uma obrigação jurídico-legal a que a UAb esteja sujeita;
d) O tratamento seja necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
e) O tratamento seja necessário ao exercício de funções de interesse público;
f) O tratamento seja necessário para efeito dos interesses legítimos prosseguidos pela UAb 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;

2 – Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados, a UAb, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, deve ter em conta:

a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e a UAb;
c) A natureza dos dados pessoais, em especial as categorias especiais de dados pessoais, nomeadamente, os que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa;
d) Os dados pessoais relacionados com condenações penais e infrações e se estes são tratados sob o controlo de uma autoridade pública ou se o tratamento é autorizado por disposições do direito nacional, ou da União ou de um Estado-Membro, que prevejam garantias adequadas para os direitos e liberdades dos titulares dos dados; a verificação de que os registos completos das condenações penais só são conservados sob o controlo das autoridades públicas;
e) As eventuais consequências do tratamento posterior pretendido para os titulares dos dados;

f) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.

Artigo 7.º

Princípio da limitação das finalidades

1 – O princípio da limitação das finalidades consiste em que a recolha dos dados pessoais é feita para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades.

2 – 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 número seguinte.

3 – O tratamento para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, está sujeito a garantias adequadas, nos termos do RGPD, para os direitos e liberdades do titular dos dados. Essas garantias asseguram a adoção de técnicas e medidas organizativas a fim de assegurar, nomeadamente, o respeito do princípio da minimização dos dados. Essas medidas podem incluir a pseudonimização, desde que os fins visados possam ser atingidos desse modo. Sempre que esses fins possam ser atingidos por novos tratamentos que não permitam, ou já não permitam, a identificação dos titulares dos dados, os referidos fins são atingidos desse modo.

Artigo 8.º

Princípio da minimização dos dados

Os dados pessoais devem ser adequados, pertinentes e restritos ao que é necessário relativamente às finalidades para as quais são tratados.

Artigo 9.º

Princípio da exatidão

1 – Os dados pessoais devem ser exatos e atualizados sempre que necessário.

2 – 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.

Artigo 10.º

Princípio da limitação da conservação

1 – Os dados pessoais devem ser 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.

2 – Podem os dados pessoais 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 n.º 3 do

artigo 7.º, sujeitos à aplicação das técnicas e medidas organizativas adequadas exigidas pelo presente Regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados.

Artigo 11.º

Princípio da integridade e confidencialidade

O tratamento dos dados pessoais deve ser feito 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.

Artigo 12.º

Princípio da responsabilidade

A UAb é responsável pelo cumprimento de todos os princípios relativos ao tratamento de dados pessoais e deve ter em conta e observar o expresso no n.º 2 do artigo 6.º.

Artigo 13.º

Tratamento com base no consentimento

1 – Quando o tratamento for realizado com base no consentimento, a UAb deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.

2 – Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples; não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento.

3 – O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar.

4 – Ao avaliar se o consentimento é dado livremente, há que verificar se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato.

Artigo 14.º

Tratamento de dados pessoais especiais (dados sensíveis)

1 – É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma

inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

2 – O disposto no n.º 1 não se aplica se se verificar um dos seguintes casos:

a) Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas;
b) Se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos da UAb ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito nacional ou da União, ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados;
c) Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento;
d) Se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares;
e) Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;
f) Se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional;
g) Se o tratamento for necessário por motivos de interesse público importante, com base no direito nacional ou da União, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;
h) Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito nacional ou da União, ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.º 3;
i) Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e

dos medicamentos ou dispositivos médicos, com base no direito nacional ou da União, que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;

j) Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 7.º, n.º 3, com base no direito nacional ou da União, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados.

3 – Os dados pessoais referidos no n.º 1 podem ser tratados para os fins referidos no n.º 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito nacional ou da União, ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito nacional ou da União, ou de regulamentação estabelecida pelas autoridades nacionais competentes.

4 – O tratamento dos dados referidos no presente artigo deve ser previamente objeto de uma AIPD e implica o parecer obrigatório *do* EPD.

5 – Relativamente ao tratamento de dados pessoais relacionados com condenações penais e infrações, aplica-se a alínea d) do n.º 2 do artigo 6.º.

CAPITULO III

DIREITOS E DEVERES DOS TITULARES DOS DADOS

SECÇÃO 1 - Direitos

Artigo 15.º
Direito de informação e de acesso

1 – Os titulares dos dados, considerados nos termos deste Regulamento, têm o direito de obter da UAb informação sobre as condições de acesso, de apagamento, de retificação ou de bloqueio dos seus dados pessoais, devendo a UAb tomar as medidas adequadas para tal.

2 – Aquando da recolha, o titular dos dados deve ser informado sobre as finalidades do tratamento a que os mesmos se destinam, bem como sobre o fundamento jurídico-legal ou interesses legítimos para o tratamento e ainda sobre os destinatários deles, se for o caso.

3 – No momento da recolha, deve o titular dos dados na medida do que for possível, com vista a ser garantido um tratamento equitativo e transparente, ser ainda informado dos seguintes aspetos:

a) Comunicação de forma inteligível dos seus dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem desses dados, ou se os mesmos não são objeto de tratamento;

b) Conhecimento da lógica subjacente ao tratamento automatizado dos dados que lhe digam respeito;
c) Faculdade de solicitar á UAb, acesso aos dados pessoais que lhe digam respeito, bem como solicitar a sua retificação ou o seu apagamento, ou a limitação do tratamento no que disser respeito ao titular dos dados, ou o direito de se opor ao tratamento, bem como o direito à portabilidade dos dados, quando o tratamento não cumpra o disposto na lei ou neste regulamento, nomeadamente devido ao caráter incompleto ou inexato desses dados;
d) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;
e) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea a), ou no artigo 14.º, n.º 2, alínea a), a existência do direito de retirar o consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;
f) Direito de apresentar reclamação a uma autoridade de controlo;
g) 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;
h) Existência de decisões automatizadas, incluindo a definição de perfis e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados;
i) Quando os dados pessoais não forem recolhidos junto do seu titular, as categorias dos dados em questão e a sua origem e se provêm de fontes acessíveis ao público;
j) Quando haja a intenção de se proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos, deve ser informado desse fim antes do novo tratamento.

4 – Qualquer comunicação ao titular dos dados a respeito do tratamento, deve ser fornecida de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples.

5 – As informações são prestadas por escrito ou por outros meios, de preferência por meios eletrónicos.

6 – Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.

Artigo 16.º
Direito de retificação

1 – O titular tem o direito de obter junto da UAb a retificação dos dados pessoais inexatos que lhe digam respeito.

2 – 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.

Artigo 17.º

Direito ao apagamento

1 – O titular tem o direito de obter junto da UAb o apagamento (direito ao esquecimento) dos seus dados pessoais, quando:

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-legal para o referido tratamento, ou nos termos do n.º 3 do artigo 13.º (direito de retirar o consentimento);
c) O titular se opõe ao tratamento e não existem interesses legítimos prevalecentes que justifiquem o tratamento;
d) Os dados pessoais foram tratados ilicitamente;
e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação legal decorrente do direito nacional ou da União a que a UAb esteja sujeita.

2 – Quando a UAb tiver tornado públicos os dados pessoais e for obrigada a apagá-los nos termos do n.º 1, e sem prejuízo do expresso no número seguinte, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação.

3 – Os n.ºs 1 e 2 não se aplicam 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 dos dados pessoais, ao exercício de funções de interesse público;
c) Por motivos de interesse público no domínio da saúde pública;
d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, na medida em que o direito referido no n.º 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento;
e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Artigo 18.º

Direito à limitação do tratamento

1 – O titular dos dados tem o direito de obter junto da UAb a limitação do tratamento se os dados forem inexatos, se o tratamento for ilícito e o titular se opuser ao seu apagamento, ou se já não houver necessidade dos mesmos pela UAb.

2 – Quando o tratamento tiver sido limitado nos termos do n.º 1, os dados pessoais só podem, à exceção da conservação, ser objeto de tratamento com o consentimento do titular,

ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos ponderosos de interesse público.

3 – O titular que tiver obtido a limitação do tratamento nos termos do n.º 1 deve ser informado pela UAb antes de ser anulada a limitação ao referido tratamento.

Artigo 19.º

Direito de portabilidade dos dados

1 – O titular dos dados tem o direito de receber, da UAb, os seus dados pessoais, num formato seguro, de uso corrente e de leitura automática e transferi-los para outro responsável pelo tratamento.

2 – Sem prejuízo do regulado pelo restante segmento da norma do artigo 20.º do RGPD, o direito do titular, de portabilidade dos dados, não se aplica ao tratamento necessário para o exercício de funções de interesse público da UAb.

Artigo 20.º

Direito de oposição

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 que lhe digam respeito mas cujo tratamento foi necessário para prosseguir funções de interesse público ou interesse legítimo da UAb, incluindo a definição de perfis com base nesses interesses, devendo a UAb cessar 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 em 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.

4 – Até ao momento da primeira comunicação ao titular dos dados, o direito a que se referem os n.os 1 e 2 é explicitamente levado à atenção do titular dos dados e é apresentado de modo claro e distinto de quaisquer outras informações.

5 – No contexto da utilização dos serviços da sociedade da informação, e sem prejuízo da Diretiva 2002/58/CE, o titular dos dados pode exercer o seu direito de oposição por meios automatizados, utilizando especificações técnicas.

6 – Quando os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos, o titular dos dados tem o direito de se opor, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam

respeito, salvo se o tratamento for necessário para a prossecução de atribuições de interesse público.

Artigo 21.º

Decisões automatizadas, incluindo definição de perfis

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.º 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 a UAb;
b) For baseada no consentimento explícito do titular dos dados.

3 – Nos casos a que se referem o n.º 2, a UAb aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente podendo manifestar o seu ponto de vista e contestar a decisão.

4 – As decisões a que se refere o n.º 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9.º, n.º 1, a não ser que o n.º 2, alínea a) ou f), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

Artigo 22.º

Transparência e regras para o exercício dos direitos

1. – O titular dos dados apenas tem direito a uma cópia dos seus dados pessoais em fase de tratamento, sendo às demais cópias.

2 – As informações fornecidas nos termos dos artigos 15.º a 21.º e quaisquer comunicações e medidas tomadas nos termos dos mesmos artigos são fornecidas a título gratuito.

3 – Se os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, a UAb pode recusar-se a dar seguimento ao pedido.

4 – Se a UAb não der seguimento ao pedido apresentado pelo titular dos dados, informa-o sem demora e, o mais tardar, no prazo de um mês a contar da data de receção do pedido, das razões que o levaram a não tomar medidas e da possibilidade de apresentar reclamação a uma autoridade de controlo.

SECÇÃO 2 - Deveres

Artigo 23.º

Dever de colaboração

1 – Os titulares dos dados devem exercer os seus direitos com respeito pelos princípios da cooperação e da boa fé, prestando informações adequadas, claras, corretas e precisas à UAb, por forma a viabilizar um tratamento lícito, leal e transparente dos dados pessoais.

2 – É dever dos titulares dos dados comunicar, no prazo de 30 dias, qualquer mudança de residência ou de endereço eletrónico e prestar colaboração aos órgãos e serviços da UAb na atualização sistemática dos seus dados pessoais.
3 – A prestação de dados falsos à UAb, sem prejuízo da ponderação penal que possa ocorrer, é sancionável nos termos do presente Regulamento.

CAPÍTULO IV
RESPONSABILIDADE PELO TRATAMENTO DOS DADOS PESSOAIS

SECÇÃO 1 – Obrigações Gerais e Segurança no tratamento de Dados Pessoais

Artigo 24.º
Obrigações da UAb como responsável pelo tratamento

1 – A UAb, na qualidade de responsável pelo tratamento dos dados pessoais, representada, nos termos da lei e dos estatutos, pelo seu reitor, tendo em conta o objeto do presente Regulamento, está sujeita às seguintes obrigações ou responsabilidades gerais:

a) Responsabiliza-se por pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão, ou o acesso, não autorizados, nomeadamente sempre que o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito;
b) Sem prejuízo da ponderação dos conhecimentos técnicos disponíveis e dos custos resultante da sua aplicação, as medidas de segurança do tratamento a implementar devem assegurar um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger;
c) Deve assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente Regulamento e que as medidas adequadas são revistas e atualizadas consoante as necessidades e incluem a aplicação de políticas adequadas em matéria de proteção de dados;
d) Tem a obrigação de aplicar, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a utilizar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados;
e) Deve assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento, procedendo ao controlo da quantidade de dados pessoais recolhidos, da extensão do seu tratamento, do seu prazo de conservação e da sua acessibilidade; estas medidas asseguram que, por

defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares;

f) Tem o dever de comunicar a cada destinatário a quem os dados tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento a que se tenha procedido, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado;

g) Deve conservar um registo de todas as atividades de tratamento sob a sua responsabilidade, de acordo com as informações prescritas no artigo 30.º do RGPD.

2 – A UAb, ao nível das obrigações especiais de segurança, encetará as medidas adequadas no sentido de:

a) Impedir que suportes de dados possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada, devendo haver controlo desses suportes;

b) Impedir o acesso de pessoas não autorizadas às instalações utilizadas para o tratamento desses dados, devendo haver controlo das entradas;

c) Impedir que sistemas de tratamento automatizados de dados possam ser utilizados por pessoas não autorizadas através de instalações de transmissão de dados, devendo haver controlo da utilização;

d) Impedir a introdução não autorizada, bem como a tomada de conhecimento, a alteração ou a eliminação não autorizada de dados pessoais inseridos, devendo haver controlo da inserção;

e) Impedir que, na transmissão de dados pessoais, bem como no transporte do seu suporte, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada, devendo haver controlo do transporte;

f) Garantir que possa verificar-se à posteriori, em prazo adequado à natureza do tratamento, quais os dados pessoais introduzidos, quando e por quem, devendo haver controlo da introdução;

g) Garantir que as pessoas autorizadas só possam ter acesso aos dados abrangidos pela respetiva autorização, devendo haver controlo de acesso;

h) Aplicar a pseudonimização e a cifragem dos dados pessoais;

i) Assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;

j) Restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;

k) Garantir processos capazes para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas de modo a assegurar a segurança do tratamento.

Artigo 25.º

Partilha de dados pessoais com terceiros, destinatários e subcontratantes

1 – A UAb, no âmbito da sua atividade, poderá partilhar os dados pessoais com entidades terceiras, nomeadamente:

a) Consultores e prestadores de serviços relacionados com a gestão de contencioso;
b) Auditores e avaliadores relacionados com obrigações a que UAb está juridicamente sujeita;
c) Empresas prestadoras de serviços à UAb exclusivamente para os fins especificamente estabelecidos;
d) A pedido do respetivo titular e/ou com o seu consentimento;
e) Autoridades judiciárias, administrativas e a outras entidades, nomeadamente:
   i. Autoridade Tributária e Aduaneira;
   ii. Instituições de Segurança Social;
   iii. Caixa Geral de Aposentações;
   iv. Autoridade para as Condições de Trabalho;
   v. Órgãos de tutela, nomeadamente a Inspeção Geral da Educação e Ciência (IGEC).

2 – A UAb deverá escolher um subcontratante que ofereça garantias suficientes em relação às medidas de segurança técnica e de organização do tratamento a efetuar e deverá zelar pelo cumprimento dessas medidas.

3 – A realização de operações de tratamento de dados pessoais em subcontratação será regulada por um contrato ou outro instrumento jurídico que vincule o subcontratante à UAb e que estipule, nomeadamente, que o subcontratante apenas atua mediante instruções da Universidade e que estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais, as categorias dos titulares dos dados e as obrigações e direitos do responsável pelo tratamento, incumbindo-lhe igualmente o cumprimento das obrigações gerais e especiais do artigo 24.º deste Regulamento.

4 – Os artigos 26.º, 28.º e 30.º, do RGPD, funcionam como normas supletivas para as condições contratuais a estabelecer com o responsável conjunto ou com subcontratante, conforme aplicável.

5– O cumprimento de um código de conduta ou de um procedimento de certificação aprovados, por parte de uma entidade terceira, pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas no RGPD.

Artigo 26.º
Cooperação com a autoridade de controlo

A UAb e o subcontratante e, sendo caso disso, os seus representantes, cooperam com a autoridade de controlo, a pedido desta, na prossecução das suas atribuições.

Artigo 27.º
Sigilo profissional

1 – A UAb, bem como todas as pessoas que, no exercício das suas funções públicas, concessionadas ou contratadas, tenham conhecimento dos dados pessoais tratados, ficam obrigados a sigilo profissional, mesmo após o termo das suas funções ou contrato.

2 – O disposto no número anterior não exclui ou prejudica o dever de fornecimento das informações obrigatórias, nos termos legais, exceto quando constem de ficheiros organizados para fins estatísticos.

SECÇÃO 2 – Encarregado de Proteção de Dados (*EPD*)

Artigo 28.º
Perfil e designação do *EPD*

1 – A UAb designa um Encarregado de Proteção de Dados (EPD) a quem incumbe, o exercício das competências previstas na lei, em especial as descritas nos artigos 37.º a 39.º do RGPD.
2 – O EPD é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções contratadas.
3 – O EPD pode ser, ou não, um elemento do pessoal da UAb ou exercer as suas funções com base num contrato de prestação de serviços.
4 – Qualquer que seja o seu vínculo ou relação contratual com a UAb, o EPD deve ter um papel independente e estar obrigatoriamente sujeito a um contrato, ou instrumento jurídico equivalente, que espelhe todos os seus direitos e obrigações e recursos necessários, nomeadamente a sua posição e funções, nos termos do artigo 38.º do RGPD.
5 – A UAb publica os contactos do EPD e comunica-os à autoridade de controlo (CNPD).

Artigo 29.º
Competências do *EPD*

Incumbe ao EPD, designadamente:

a) Apoiar a UAb, mediar as relações com os titulares dos dados e cooperar com a autoridade de controlo (CNPD), emitindo pareceres e recomendações, enviando notificações e relatórios e procedendo a consultas prévias e consultas;
b) Informar, aconselhar e orientar a UAb, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações, de acordo com o presente regulamento;
c) Controlar a conformidade com o presente Regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas da UAb, relativas à proteção de dados pessoais, incluindo as auditorias correspondentes;
d) Prestar aconselhamento no que respeita à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e controlar a sua realização;
e) Prestar aconselhamento no desenvolvimento de novas políticas de proteção de dados e procedimentos internos de tratamento de dados; na elaboração de notas de privacidade; na elaboração de formulários para coleta de dados e nos incidentes de violação de dados;
f) Ponderar os riscos associados às operações de tratamento dos dados;
g) Promover a formação e a sensibilização dos colaboradores da UAb em matérias de proteção de dados pessoais;
h) Realizar auditorias periódicas para averiguar da conformidade com o RGPD.

SECÇÃO 3 – Avaliação de Impacto sobre a Proteção dos Dados (AIPD)

Artigo 30.º
Avaliação de impacto e consulta prévia à CNPD

1 – Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas, a UAb deverá, antes de iniciar o tratamento, encarregar-se da realização de uma avaliação de impacto das operações previstas sobre a proteção dos dados pessoais.

2 – Ao efetuar a avaliação referida no número anterior, a UAb solicita um parecer ao EPD.

3 – Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o RGPD.

4 – Sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco que a UAb não poderá atenuar através de medidas adequadas, atendendo à tecnologia disponível e aos custos de aplicação, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais.

5 – A realização de uma avaliação de impacto sobre a proteção de dados é obrigatória em casos de:

a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
b) Operações de tratamento em grande escala de categorias especiais de dados, ou de dados pessoais relacionados com condenações penais e infrações;
c) Controlo sistemático de zonas acessíveis ao público em grande escala.

6 – A UAb consulta a autoridade de controlo antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pela UAb para atenuar o risco.

SECÇÃO 4 – Política de Proteção de Dados, Códigos de Conduta e Certificação

Artigo 31.º
Notas de Privacidade e Política de Privacidade

1 – A UAb deve elaborar, publicitar e manter atualizada, nos seus sítios da Internet, notas e políticas de privacidade de dados.

2 – Os dados pessoais dos respetivos titulares que se relacionem com a UAb não são de acesso público, exceto quando seja necessária a publicidade para efeitos de prosseguimento

da sua missão e atribuições estatutárias, ou por superior interesse público, ou ainda por imposição legal.

Artigo 32.º

Conformidade (Compliance)

1 – A UAb deve proceder à recolha de toda a informação pertinente relativa aos dados pessoais suscetíveis de objeto de tratamento, determinando as medidas necessárias de validação, correção de procedimentos e implementação do presente Regulamento.

2 – A existência de um sistema de registo de todos os tratamentos que envolvam dados pessoais, que integre o SIDPUAb, deve documentar de forma detalhada e circunstanciada todas as atividades relacionadas com o tratamento de dados.

3 – A UAb deve conservar um registo de todas as atividades de tratamento sob sua responsabilidade.

4 – Funciona como prova de implementação e cumprimento do presente Regulamento, a garantia, e respetiva evidência, da prestação de informação ao titular dos dados, designadamente nos documentos de suporte à recolha de dados em suporte físico ou digital.

Artigo 33.º

Responsabilidade (Accountability)

A UAb, no domínio da responsabilidade ética e da missão de serviço público no contexto universitário português, deve:

a) Incrementar um sistema permanente e dinâmico de verificação da conformidade da sua atividade com o presente regulamento, através do SIDPUAb;
b) Promover auditorias no âmbito de um controlo contínuo e sistemático para aferir da eficácia das medidas implementadas, modificando-as sempre que necessário, em conformidade com este regulamento e mais legislação aplicável.

Artigo 34.º

Códigos de conduta e certificação

1 – A UAb pode promover a elaboração autónoma de códigos de conduta destinados a contribuir para a correta aplicação deste regulamento, tendo em conta as características da sua especificidade de ensino e formação a distância.

2 – Os intervenientes no tratamento de dados na UAb estão sujeitos a elevados padrões éticos, designadamente ao dever de sigilo, de acordo com o artigo 27.º deste Regulamento, e ao dever de confidencialidade, com vista à proteção de dados pessoais.

3 – A UAb prosseguirá todos os procedimentos que atestem a conformidade das operações de tratamento, como responsável pelo tratamento de dados pessoais, com vista à certificação em matéria de proteção de dados, podendo, se assim o entender, proceder à elaboração de manuais internos de procedimentos.

Capítulo V
GESTÃO E EXPLORAÇÃO DO SISTEMA INTEGRADO DE DADOS PESSOAIS DA UAb (SIDPUAb)

Artigo 35.º
Competências gerais

1– Os trabalhadores, colaboradores, pessoa jurídica ou pessoa física que desempenhe atividade do interesse da UAb, realize estágio ou preste serviço em caracter permanente ou eventual, podem ter acesso a dados pessoais, devendo esse acesso restringir -se, exclusivamente, às pessoas que tenham necessidade de os conhecer para cumprimento das suas funções ou tarefas.

2– O tratamento de dados pessoais realizado por pessoa que não tenha sido autorizada para tal é expressamente proibido, assim como o tratamento de dados pessoais para fins pessoais ou comerciais.

Artigo 36.º
Competências específicas

1– Por força do RGPD, a UAb deverá identificar e verificar a maturidade de partes terceiras à UAb — subcontratantes e responsáveis conjuntos — antes de recorrer à contratação dos respetivos serviços, se for esse o caso, ou antes de facilitar o acesso, realizar a transmissão ou outra operação de tratamento de dados pessoais a qualquer parte terceira à UAb.

2– Cabe ao EPD, se necessário em coordenação com responsáveis da unidade orgânica ou serviço, recolher junto dos fornecedores da respetiva unidade orgânica ou serviço, documentos e cláusulas contratuais relativas a operações de tratamento de dados pessoais e requerer parecer sobre os mesmos junto do EPD.

Artigo 37.º
Comissão de Acompanhamento

1 – O EPD é coadjuvado, em permanência, pelo Pró-reitor para Assuntos Jurídicos e Institucionais, pelo chefe de divisão dos Serviços de Informática, pelo Gestor de Segurança da Informação (CISO) e pelo chefe do Gabinete Jurídico que, juntamente, compõem o Comité de Segurança da Informação (CSI) da UAb.

Artigo 38.º
Supervisão dos mecanismos de proteção de dados

1– A determinação das medidas técnicas e organizativas para garantir a segurança dos dados pessoais é da competência do(a) Reitor(a).

2 – O Comité de Segurança da Informação (CSI) da UAb deve, continuamente, avaliar os ajustamentos necessários aos desenvolvimentos técnicos e mudanças organizativas.

3– A conformidade das operações de tratamento de dados pessoais com a legislação aplicável e com o presente regulamento interno deve ser verificada regularmente através de auditorias ou outros procedimentos de supervisão.
4– A realização das auditorias referenciadas no ponto 3, é determinada pelo(a) Reitor(a), segundo os requisitos que sejam definidos pelo Comité de Segurança da Informação (CSI).
5– Sempre que necessário, a UAb pode recorrer a empresas de auditoria ou a consultores técnicos para a realização das auditorias previstas no presente artigo, quando estas não possam ser desempenhadas pela própria UAb.
6– O EPD acompanhará o processo de auditoria e os trabalhos desenvolvidos para o efeito, mesmo quando haja recurso a empresas de auditoria ou a consultores técnicos.
7– Os resultados das auditorias ou outros procedimentos de supervisão devem ser transmitidos pelo Comité de Segurança da Informação (CSI) ao/à Reitor(a).

Artigo 39.º
Prazo de conservação dos dados pessoais

1– De modo a garantir a conservação dos dados pessoais apenas pelo período de tempo necessário, a UAb fixa prazos para o apagamento ou anonimização ou para a revisão periódica.
2– Os prazos de conservação dos dados pessoais são definidos de acordo com o artigo 21.º da Lei n.º 58/2019, de 8 de agosto.
3– A UAb poderá a conservar alguns dados pessoais por um período mais longo, de modo a respeitar, nomeadamente:

a. Obrigações legais, ao abrigo das leis em vigor, de conservação de dados por períodos predefinidos;
b. Prazos de prescrição, ao abrigo das leis em vigor;
c. A resolução definitiva de quaisquer eventuais litígios;
d. Orientações emitidas pelas autoridades de proteção de dados competentes.

4– No âmbito da proteção de dados pessoais serão observados os procedimentos constantes do documento relativo à Política de Conservação de Dados, documento integrante do SIDPUAb.

Artigo 40.º
Incidentes com dados pessoais

1– Assim que tomarem conhecimento, os trabalhadores e colaboradores da UAb devem informar imediatamente a chefia da respetiva unidade orgânica ou do respetivo serviço, conforme aplicável, que informará os Serviços de Informática sobre as situações de incidentes de segurança de informação, incidentes de violação de dados pessoais, violações do RGPD e demais disposições legais e regulamentares aplicáveis à segurança da informação, proteção de dados e privacidade.

2 – Os Serviços de Informática, após confirmação do incidente de segurança de informação, informará o Comité Segurança de Informação (CSI) da UAb.
3 – Os eventuais subcontratantes, com quem a UAb se relacione, estão obrigados a informar de ocorrências de incidentes de violação de dados logo após conhecimento do facto.
4 – Sempre que algum incidente de violação de dados pessoais cause um risco para os direitos, liberdades e interesses fundamentais dos seus titulares, o EPD informará a autoridade de controlo (CNPD), num prazo máximo de 72 horas.
5 – Os titulares dos dados deverão ser informados pelo EPD, quando o incidente de violação de dados represente um elevado risco para os seus direitos e liberdades, mediante comunicação escrita.

CAPÍTULO VI
DISPOSIÇÕES FINAIS

Artigo 41.º
Incumprimento

O trabalhador e colaborador da UAb que violar o presente Regulamento poderá ser sujeito a procedimento disciplinar ou jurídico, conforme aplicável.

Artigo 42.º
Casos omissos

Os casos omissos serão resolvidos por decisão do(a) Reitor(a), ouvido o Comité de Segurança da Informação da UAb.

Artigo 43.º
Vigência

O presente regulamento entra em vigor no dia seguinte ao da sua publicação no *Diário da República* de aviso informativo respeitante à respetiva publicitação, com vista à sua plena eficácia.

A Reitora

Carla Maria Bispo Padrel de Oliveira