DIÁRIO DA REPÚBLICA

2.ª série
N.º 181
17-09-2026

UNIVERSIDADE POLITÉCNICA DE COIMBRA

Despacho n.º 11473/2026

Sumário: Regulamento que estabelece o Código de Conduta e Boas Práticas na Proteção de Dados Pessoais na Universidade Politécnica de Coimbra.

Nos termos do disposto nos artigos 24.º e 40.º do Regulamento Geral sobre a Proteção de Dados — Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, do n.º 2 do artigo 15.º da Lei n.º 58/2019, de 8 de agosto, e da alínea n) do n.º 1 do artigo 35.º dos Estatutos da Universidade Politécnica de Coimbra, homologados pelo Despacho Normativo n.º 59-A/2008, de 14 de novembro, publicado no *Diário da República*, 2.ª série, n.º 225, de 19 de novembro, alterados e republicados pelo Despacho Normativo n.º 21/2021, publicado no *Diário da República*, 2.ª série, n.º 139, de 20 de julho;

Promovida a consulta pública do projeto de regulamento;

Ouvido o Conselho de Gestão;

Aprovo o Regulamento que estabelece o Código de Conduta e Boas Práticas na Proteção de Dados Pessoais na Universidade Politécnica de Coimbra, em anexo ao presente despacho.

11 de setembro de 2026. — A Reitora da UPCoimbra, Prof.ª Doutora Cândida Maria dos Santos Pereira Malça.

Regulamento que estabelece o Código de Conduta e Boas Práticas na Proteção de Dados Pessoais na Universidade Politécnica de Coimbra

Preâmbulo

A Universidade Politécnica de Coimbra, enquanto instituição pública de ensino superior, assume como prioridade estratégica e dever institucional a garantia da privacidade, confidencialidade e segurança dos dados pessoais de todos os membros da sua comunidade, incluindo estudantes, docentes, investigadores, pessoal técnico e de gestão, bem como de utilizadores e de parceiros externos. No exercício das suas atribuições académicas, científicas, culturais e administrativas, a instituição lida diariamente com um volume significativo de informação, o que exige uma cultura de responsabilidade e de estrito cumprimento legal.

A entrada em vigor do Regulamento Geral sobre a Proteção de Dados — Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 — e a sua execução na ordem jurídica nacional através da Lei n.º 58/2019, de 8 de agosto, vieram impor um quadro normativo rigoroso e exigente, focado no princípio da responsabilidade acrescida (*accountability*). Este regime exige que as organizações não só cumpram a lei, mas sejam capazes de demonstrar, de forma proativa, que o tratamento de dados pessoais é realizado com licitude, lealdade, transparência e segurança.

Atenta a estrutura descentralizada e multidimensional que caracteriza a Universidade Politécnica de Coimbra, torna-se imperativo harmonizar práticas, consolidar procedimentos de segurança e definir com clareza as competências e responsabilidades de cada uma das suas Escolas, Serviços Centrais e demais unidades orgânicas.

Assim, ao abrigo e nos termos do disposto nos artigos 24.º e 40.º do RGPD, no n.º 2 do artigo 15.º da Lei n.º 58/2019, de 8 de agosto, na alínea a) do n.º 2 do artigo 110.º do Regime Jurídico das Instituições de Ensino Superior, aprovado pela Lei n.º 62/007, de 10 de setembro, na sua atual redação, alínea *o*) do n.º 1 do artigo 92.º do Regime Jurídico das Instituições de Ensino Superior, e no artigo 35.º, n.º 1, n), dos Estatutos da Universidade Politécnica de Coimbra, dota-se a instituição de Código de Conduta e Boas Práticas na Proteção de Dados Pessoais.

CAPÍTULO I

Disposições Gerais

Artigo 1.º

Objeto

O presente Código de Conduta estabelece a política da Universidade Politécnica de Coimbra (UPCoimbra), os princípios e as regras aplicáveis em matéria de proteção de dados, à luz da disciplina plasmada no Regulamento Geral sobre a Proteção de Dados (RGPD) — Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD) e na Lei n.º 58/2019, de 8 de agosto (LPDP).

Artigo 2.º

Âmbito de aplicação

O presente Código de Conduta aplica-se a todo o tratamento de dados pessoais realizado na UPCoimbra, nomeadamente através das suas unidades orgânicas e dos Serviços de Ação Social (SAS-UPCoimbra).

Artigo 3.º

Definições

Para efeitos de aplicação do presente Código de Conduta, adotam-se os seguintes conceitos do artigo 4.º do RGPD:

a) "Anonimização": operação de tratamento de dados pessoais que torna impossível identificar, direta ou indiretamente, a pessoa singular a quem os dados respeitam, por forma a que os mesmos deixem de poder ser considerados dados pessoais para efeitos de aplicação do RGPD.

b) "Consentimento", 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;

c) "Dados biométricos": os 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;

d) "Dados pessoais": a informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados"), considerando-se como tal a 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;

e) "Dados sensíveis": 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 de forma inequívoca uma pessoa singular, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa singular;

f) "Dados relativos à saúde": os 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;

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

Despacho n.º 11473/2026

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) "Subcontratante": uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta da UPCoimbra;

i) "Terceiro": a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, não sendo o titular dos dados, a UPCoimbra, o subcontratante ou outra pessoa sob autoridade direta da UPCoimbra ou do subcontratante, esteja autorizado a tratar os dados pessoais;

j) "Tratamento": a operação ou conjunto de operações efetuadas sobre 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;

k) "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.

CAPÍTULO II

Tratamento de Dados Pessoais

Artigo 4.º

Atividades de tratamento dos dados pessoais

No pleno exercício da sua missão, a UPCoimbra desenvolve atividades específicas que envolvem o tratamento de dados pessoais, designadamente:

a) Divulgação e gestão de eventos;

b) Ensino;

c) Elaboração de projetos, planos de atividades, estratégicos e de investigação;

d) Gestão académica;

e) Gestão administrativa e financeira;

f) Gestão de controlo de acessos;

g) Gestão de recursos humanos;

h) Gestão de sistemas de informação e comunicações eletrónicas;

i) Gestão e atribuição de apoios sociais;

j) Gestão e promoção de investigação;

k) Prestação de serviços à comunidade;

l) Promoção do desenvolvimento, bem-estar e saúde.

Despacho n.º 11473/2026

Artigo 5.º

Princípios e regras gerais

1 — O tratamento de dados pessoais na UPCoimbra obedece aos princípios estabelecidos no artigo 5.º do RGPD, a saber:

a) Princípio da exatidão, por força do qual os dados pessoais tratados devem ser exatos e atualizados sempre que necessário, adotando a UPCoimbra todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades de tratamento, sejam, sem demora, apagados ou retificados;

b) Princípios da licitude, lealdade e transparência, segundo os quais os dados pessoais são objeto de um tratamento lícito, leal e transparente em relação ao respetivo titular;

c) Princípio da limitação da conservação, que determina que, em regra, a conservação dos dados pessoais de modo a permitir a identificação dos respetivos titulares é limitada ao período necessário à finalidade do tratamento, apenas se admitindo a conservação por prazos mais longos exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos;

d) Princípio da limitação das finalidades, em observância do qual os dados pessoais são recolhidos para finalidades determinadas, explícitas e legítimas e não podem ser tratados posteriormente de forma incompatível com tais finalidades;

e) Princípios da integridade e confidencialidade, por força dos quais os dados pessoais devem ser tratados de forma que garanta a sua segurança, devendo adotar-se as medidas técnicas ou organizativas adequadas à proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental;

f) Princípio da minimização dos dados, do qual decorre que apenas são tratados os dados adequados, pertinentes e necessários face à finalidade de tratamento, assumindo especial relevo quando se decida sobre a utilização de novas tecnologias;

g) Princípio da responsabilidade, que impõe à UPCoimbra o dever de comprovar o cumprimento dos princípios elencados nas alíneas anteriores.

2 — A UPCoimbra garante a proteção dos dados desde a conceção e por defeito, definindo em cooperação com o seu Encarregado da Proteção de Dados (EPD), medidas técnicas e organizativas que assegurem que só são tratados os dados pessoais estritamente necessários, adequados e pertinentes para cada finalidade específica do tratamento no âmbito das atividades enumeradas no artigo anterior.

3 — A definição e implementação das medidas a que alude o número anterior são precedidas da análise da proporcionalidade do tratamento, de modo a garantir o equilíbrio entre os direitos de privacidade dos titulares dos dados e o interesse legítimo no tratamento, em particular nos casos em que se revele necessário o tratamento de categorias especiais de dados pessoais.

4 — O tratamento de dados pessoais da responsabilidade da UPCoimbra, fora do contexto das suas atividades, é expressamente proibido e, a existir, é da responsabilidade de quem definir as finalidades desse tratamento e poderá, em função da gravidade da situação, ser objeto de sanções legalmente previstas.

5 — A criação, aquisição, contratação, desenvolvimento, integração, alteração substancial ou desativação de sistemas, plataformas, serviços digitais ou processos que envolvam tratamento de dados pessoais é precedida de uma avaliação de conformidade, proporcional ao risco, que assegure a consideração atempada dos requisitos de proteção de dados, segurança da informação e, quando aplicável, de utilização de sistemas de inteligência artificial.

6 — A avaliação prevista no número anterior é realizada nos termos de procedimento interno aprovado pela UPCoimbra, com intervenção do Encarregado de Proteção de Dados e dos serviços competentes em matéria de tecnologias da informação e comunicação, sem prejuízo das competências próprias de outras estruturas institucionalmente relevantes.

Despacho n.º 11473/2026

Artigo 6.º

Regras especiais no âmbito dos ambientes digitais e do ensino a distância

1 — Para além do disposto no artigo anterior, o tratamento dos dados pessoais para as finalidades inerentes ao ensino em ambientes digitais e a distância obedece, ainda, às seguintes regras:

a) Os dados não podem ser utilizados fora do contexto escolar;

b) É proibida a gravação de imagens ou som das aulas não presenciais;

c) A recolha e a gravação de imagens e som nas aulas presenciais pode ser permitida nos seguintes casos:

i) Quando tal seja comprovadamente imprescindível ao desenvolvimento das atividades educativas planeadas; ou

ii) Quando tal seja previamente definido e autorizado pelos titulares dos dados (docentes e/ou discentes);

d) É proibida a duplicação das imagens ou som captados ao abrigo do preceituado na alínea anterior, devendo estes ser eliminados imediatamente após atingido o objetivo pedagógicos;

e) É obrigatório o registo de todas as atividades de tratamento;

f) Devem ser utilizadas plataformas e serviços digitais institucionais ou expressamente autorizados pela UPCoimbra, que assegurem níveis adequados de proteção de dados, segurança da informação, controlo de acessos, registo de atividade e gestão de conservação, nos termos das normas técnicas e orientações aplicáveis.

2 — As condições de autorização, configuração, gravação, conservação, eliminação, partilha e controlo de acessos às plataformas utilizadas em contexto de ensino digital ou a distância são definidas em norma técnica ou procedimento complementar, atendendo à natureza da atividade, às categorias de dados tratadas e ao nível de risco.

Artigo 7.º

Licitude do tratamento

O tratamento de dados pessoais é lícito nos seguintes casos:

a) Execução de contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;

b) Cumprimento de uma obrigação jurídica a que a UPCoimbra esteja sujeita;

c) Defesa dos interesses do titular dos dados ou de outra pessoa singular;

d) Exercício de funções de interesse público ou no exercício da autoridade pública de que está investida a UPCoimbra;

e) Tratamento necessário para prossecução dos interesses legítimos da UPCoimbra ou de terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se este for uma criança;

f) Consentimento do titular dos dados para uma ou mais finalidades específicas.

Despacho n.º 11473/2026

Artigo 8.º

Consentimento do titular dos dados pessoais

1 — O consentimento deve ser obtido em momento anterior a qualquer tratamento de dados pessoais.

2 — O consentimento pode ser recolhido em suporte escrito, por via eletrónica ou por outro meio adequado que permita comprovar, de forma verificável e auditável, a manifestação de vontade do titular, a informação que lhe foi prestada, a finalidade do tratamento, a data da recolha e, quando aplicável, a retirada do consentimento.

3 — O consentimento deve ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente o tratamento dos dados que lhe digam respeito.

4 — O pedido de consentimento deve ser separado de outros termos e condições e apresentado numa linguagem clara e simples.

5 — É assegurado que o consentimento é facilmente prestado e, em termos análogos, pode ser facilmente retirado.

6 — Incidindo o tratamento sobre dados pessoais de menores de idade, o consentimento deve obedecer ao seguinte:

a) Caso o objeto do tratamento seja relativo à oferta direta de serviços da sociedade de informação, o consentimento é lícito quando prestado pelo menor que tenha completado 13 anos de idade;

b) Caso o objeto do tratamento seja o referido na alínea anterior e o menor tenha idade inferior a 13 anos de idade, o tratamento só é lícito se o consentimento for dado pelo seu representante legal, de preferência com recurso a meios de autenticação segura e com o assentimento do menor;

c) Nos restantes casos, o tratamento só é lícito se o consentimento for dado pelo seu representante legal, de preferência com recurso a meios de autenticação segura, e for obtido o assentimento do menor.

7 — O responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.

8 — Os mecanismos de recolha e gestão do consentimento devem assegurar, designadamente, a conservação de registo suficiente para demonstrar a sua validade, a associação à versão aplicável da informação prestada ao titular e a possibilidade de retirada com facilidade equivalente à da prestação

Artigo 9.º

Conservação dos dados

1 — Os dados pessoais são armazenados e conservados, em cada tratamento de dados, apenas durante o período necessário para as finalidades para as quais são tratados, incluindo os prazos fixados por norma legal ou regulamentar.

2 — Na ausência de tal norma, os dados são armazenados e conservados apenas pelo período mínimo necessário para as finalidades que motivaram a sua recolha ou o seu posterior tratamento, findas as quais são anonimizados ou destruídos.

3 — Sem prejuízo do disposto nos números anteriores, a UPCoimbra, na prossecução de uma finalidade de tratamento, pode ser obrigada a conservar alguns dados por um período mais longo, de modo a respeitar, designadamente:

a) Obrigações legais, em que virtude das quais os dados devam ser conservados até à verificação do prazo de prescrição dos direitos correspetivos;

Despacho n.º 11473/2026

b) Obrigações perante entidades financiadoras;

c) A resolução de litígios;

d) Orientações emitidas pelas autoridades de proteção de dados competentes.

4 — Alguns dados podem, ainda, ser conservados exclusivamente para fins de arquivo de interesse público, fins de investigação científica ou histórica, ou para fins estatísticos, desde que sejam adotadas medidas técnicas e organizativas adequadas a garantir os direitos dos respetivos titulares.

5 — A UPCoimbra aprova e mantém atualizados instrumentos de definição de prazos de conservação, critérios de anonimização, eliminação, bloqueio ou arquivamento, adequados às diferentes atividades de tratamento e articulados com as obrigações legais, regulamentares, arquivísticas, contratuais e de segurança aplicáveis.

6 — Sempre que tecnicamente viável e adequado ao risco, os sistemas de informação devem dispor de mecanismos que apoiem a aplicação dos prazos de conservação e das decisões de anonimização, eliminação, limitação ou arquivamento.

Artigo 10.º

Tratamento de Dados sensíveis

1 — Por força do disposto no n.º 1 do artigo 9.º do RGPD, é proibido o tratamento dos dados considerados sensíveis na UPCoimbra.

2 — O tratamento de dados pessoais sensíveis na UPCoimbra, devidamente enquadrado na ressalva prevista no n.º 2 do artigo 9.º do RGPD, tem como finalidades específicas, nomeadamente a prevenção de acidentes de trabalho e doenças profissionais, a prestação de serviços de saúde à comunidade, a gestão de contratos de trabalho ou a atribuição de apoios sociais, arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos.

3 — Ao tratamento de dados de saúde e dados genéticos aplica-se o disposto no artigo 29.º da Lei n.º 58/2019, de 8 de agosto.

Artigo 11.º

Comunicação de dados pessoais

1 — Na prossecução das suas atribuições e em cumprimento de obrigações legais e/ou contratuais, e mediante a devida fundamentação, a UPCoimbra procede à comunicação de dados pessoais a outros destinatários, nomeadamente:

a) Serviços e organismos da Administração direta e indireta do Estado, designadamente:

i) Autoridade Tributária e Aduaneira;

ii) Autoridade para as Condições de Trabalho;

iii) Caixa Geral de Aposentações, I. P.;

iv) Órgãos e serviços com poderes e competências de fiscalização e inspeção, nomeadamente a Inspeção-Geral da Educação e Ciência;

v) Instituto da Segurança Social, I. P.;

vi) Direção-Geral do Ensino Superior.

b) Entidades administrativas independentes;

Despacho n.º 11473/2026

c) Entidades financiadoras de projetos e Entidades gestoras de programas de financiamento nacionais, comunitários ou internacionais, designadamente:

i) Agências da União Europeia;

ii) Fundação para a Ciência e a Tecnologia;

iii) Organizações nacionais ou internacionais que financiem investigação e desenvolvimento de tecnologia;

d) Organismos de certificação, de inspeção e de auditoria, nacionais ou europeus;

e) Advogados e outros mandatários, no âmbito da gestão de contencioso;

f) Empresas prestadoras de serviços à UPCoimbra;

g) Instituições financeiras;

h) Órgãos de polícia criminal;

i) Tribunais;

j) Seguradoras;

k) Quaisquer interessados que se encontrem munidos de autorização escrita do titular dos dados, explícita e específica quanto à finalidade e tipo de dados, ou demonstrem possuir um interesse legítimo, pessoal e direto, constitucionalmente protegido e suficientemente relevante que justifique o acesso pretendido, nos termos da legislação em vigor.

2 — A pedido do respetivo titular, ou com o seu consentimento, os dados poderão ser partilhados com outras entidades identificadas pelo próprio.

3 — A divulgação de dados pessoais em ambiente de intranet, internet ou noutros circuitos de comunicação, quando não resulte diretamente de obrigação legal, deve ser objeto de avaliação prévia de conformidade nos termos de procedimento interno aprovado pela UPCoimbra, com intervenção do EPD, nos casos definidos em função da natureza, escala, sensibilidade, destinatários, meios de divulgação ou impacto potencial do tratamento.

4 — O EPD é informado de todas as comunicações de dados pessoais que sejam, ou que se prevê que venham a ser, realizadas periodicamente, no âmbito do cumprimento de uma obrigação jurídica a que a UPCoimbra esteja sujeita.

CAPÍTULO III

Titular dos Dados Pessoais

Artigo 12.º

Categorias de titulares de dados pessoais

No âmbito e em função da natureza das atividades que desenvolve, a UPCoimbra trata os dados pessoais de um conjunto alargado de titulares, incluindo, nomeadamente:

a) Estudantes;

b) Trabalhadores;

c) Bolseiros;

d) Investigadores;

e) Candidatos;

Despacho n.º 11473/2026

f) Fornecedores e clientes, no âmbito dos contratos com eles celebrados;

g) Utentes ou beneficiários de apoios concedidos pela UPCoimbra;

h) Colaboradores que atuem no âmbito de projetos, centros ou unidades de investigação da UPCoimbra;

i) Titulares dos órgãos da UPCoimbra ou das suas unidades orgânicas que não integrem alguma das categorias das alíneas anteriores;

j) Titulares de contactos para partilha e divulgação de eventos na UPCoimbra.

Artigo 13.º

Direitos

1 — Ao titular dos dados pessoais tratados pela UPCoimbra assistem os seguintes direitos:

a) Informação e acesso;

b) Retificação e apagamento;

c) Limitação do tratamento;

d) Portabilidade dos dados;

e) Oposição ao tratamento;

f) Não sujeição a decisões individuais automatizadas.

2 — A UPCoimbra assegura a existência de procedimento interno para receção, registo, validação de identidade, análise, decisão, resposta e arquivo dos pedidos apresentados pelos titulares dos dados.

3 — O procedimento referido no número anterior estabelece os pontos de contacto dos serviços e unidades orgânicas, os mecanismos de articulação com o EPD, os prazos internos de resposta, os critérios de apreciação e as medidas de segurança aplicáveis.

4 — Os sistemas e serviços que tratem dados pessoais devem dispor de informação atualizada que permita identificar, de forma proporcionada, as categorias de dados tratadas, os responsáveis funcionais, os destinatários relevantes, os prazos de conservação e os mecanismos disponíveis para satisfazer os direitos dos titulares.

Artigo 14.º

Informação e acesso

1 — O titular dos dados tem o direito de obter informações claras, transparentes e inteligíveis, prestadas numa linguagem simples, e de fácil acesso, sobre o modo como a UPCoimbra utiliza os seus dados e de ser cabalmente esclarecido quanto aos seus direitos.

2 — O titular dos dados tem igualmente o direito de obter a confirmação de que os seus dados pessoais são, ou não, objeto de tratamento e, se for esse o caso, o direito de aceder, tanto aos seus dados pessoais como às seguintes informações:

a) Os contactos do EPD;

b) As finalidades do tratamento dos dados e respetivo fundamento legal;

c) As categorias dos dados pessoais em questão;

Despacho n.º 11473/2026

d) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou possam ser divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;

e) O prazo previsto de conservação dos dados pessoais, ou, se ainda não estiver estabelecido, os critérios usados para fixar esse prazo;

f) A existência dos demais direitos elencados no artigo anterior;

g) A existência do direito de retirar o consentimento, sem prejuízo da licitude do tratamento já realizado;

h) A possibilidade de apresentar reclamação ou queixa junto da Comissão Nacional de Proteção de Dados (CNPD), cujos contactos se encontram disponíveis em www.cnpd.pt;

i) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;

j) A existência de decisões automatizadas.

3 — O titular dos dados tem ainda o direito a ser informado sobre qualquer violação de dados pessoais.

4 — As informações a que aludem os números anteriores são prestadas por escrito, nomeadamente através de meios eletrónicos, salvo se o titular dos dados, cuja identidade deve ser devidamente comprovada, solicitar que as informações sejam prestadas oralmente.

5 — A UPCoimbra pode recusar a prestação da informação solicitada sempre que, para satisfazer o pedido do titular dos dados, tenha de revelar dados pessoais de outra pessoa, que não tenha previamente consentida a tal divulgação, ou quando conclua, após análise casuística, que aquela pode prejudicar os direitos de outra pessoa.

Artigo 15.º

Retificação e apagamento

O titular dos dados pode, a qualquer altura, solicitar:

a) A retificação dos seus dados pessoais que estejam incorretos ou incompletos;

b) O apagamento dos seus dados, salvo nos casos previstos no n.º 3 do artigo 17.º do RGPD.

Artigo 16.º

Limitação do tratamento

O titular dos dados tem o direito de obter a limitação do tratamento quando:

a) Pretenda contestar a exatidão dos dados pessoais, durante um período que permita à UPCoimbra verificar a sua exatidão;

b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização;

c) A UPCoimbra já não precisar de tratar os dados pessoais, mas estes sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;

d) Se tiver oposto ao tratamento, até se verificar que os motivos legítimos da UPCoimbra prevalecem sobre os seus.

Despacho n.º 11473/2026

Artigo 17.º

Comunicação da retificação ou apagamento dos dados pessoais ou da limitação do tratamento

Na sequência do exercício dos direitos previstos nos artigos anteriores, a UPCoimbra comunica, a cada destinatário a quem os dados pessoais tenham sido transmitidos, as operações de retificação, apagamento ou limitação do tratamento realizadas.

Artigo 18.º

Portabilidade dos dados

O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido à UPCoimbra, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que a UPCoimbra o possa impedir, se:

a) O tratamento for necessário para o cumprimento de um contrato ou se basear no consentimento; e

b) O tratamento for realizado por meios automatizados.

Artigo 19.º

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, quando a base legal para a respetiva operação de tratamento seja:

a) O interesse público [alínea e) do n.º 1 do artigo do RGPD);

b) Os interesses legítimos do responsável pelo tratamento, ou de terceiros [alínea f) do n.º 1 do artigo 6.º do RGPD];

c) O n.º 4 do artigo 6.º do RGPD, ou seja, quando há uma reutilização dos dados para uma finalidade distinta, mas compatível, daquela que motivou a sua recolha inicial, incluindo a definição de perfis.

2 — Nos casos previstos no número anterior, o responsável cessa o tratamento, a menos que apresente razões imperiosas e legítimas que prevaleçam sobre os interesses, direitos e liberdades do titular, ou para efeitos de exercício de um direito num processo judicial.

Artigo 20.º

Não sujeição a decisões individuais automatizadas

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, exceto:

a) Se o consentir;

b) Se a decisão for necessária para a celebração ou a execução de um contrato com a UPCoimbra;

c) Se for autorizada pelo direito da União Europeia ou pela ordem jurídica nacional; ou

d) Se a licitude de tratamento se basear no interesse ou autoridade pública, e envolver categorias especiais de dados pessoais.

Despacho n.º 11473/2026

Artigo 21.º

Procedimento

1 — Salvo se existirem mecanismos automáticos para o efeito, os direitos a que aludem os artigos anteriores são exercidos pelo titular dos dados mediante contacto com a UPCoimbra, através do endereço de correio eletrónico epd@ipc.pt.

2 — A UPCoimbra responde ao pedido do titular dos dados sem demora injustificada e no prazo máximo de 30 dias a contar da receção do pedido, salvo em casos de especial complexidade, em que o prazo de resposta pode ser prorrogado até dois meses.

3 — A decisão de prorrogação a que alude o número anterior e respetivos fundamentos são comunicados ao titular dos dados.

4 — A intenção de recusa do pedido, devidamente fundamentada, é notificada ao titular dos dados, dispondo de prazo não inferior a 10 dias úteis para, querendo, se pronunciar.

5 — Se o pedido for manifestamente infundado ou excessivo, nomeadamente devido ao seu carácter repetitivo, a UPCoimbra reserva-se o direito de recusar dar seguimento ao mesmo ou de cobrar custos administrativos.

CAPÍTULO IV

Responsável pelo Tratamento, Contratos com Terceiros e Subcontratantes

Artigo 22.º

Responsabilidade

1 — A UPCoimbra, enquanto pessoa coletiva de direito público, é a responsável pelo tratamento dos dados pessoais abrangidos pelo presente Código, sendo representada, para esse efeito, pelo Reitor.

2 — O Reitor pode, mediante despacho, designar outro titular de órgão, dirigente ou trabalhador da UPCoimbra para assegurar, no âmbito das respetivas atribuições, a prática de atos, a coordenação de procedimentos ou o acompanhamento de operações de tratamento de dados pessoais, sem prejuízo da responsabilidade da UPCoimbra enquanto responsável pelo tratamento e das competências legalmente atribuídas ao Reitor.

3 — A designação prevista no número anterior deve identificar, de forma expressa, o seu âmbito material, as atividades de tratamento abrangidas, os poderes conferidos, os deveres de articulação com o Encarregado da Proteção de Dados e os mecanismos de prestação de informação, acompanhamento e controlo aplicáveis.

4 — Cada Unidade Orgânica e os Serviços de Ação Social da UPCoimbra designam um interlocutor para a proteção de dados pessoais, assegurando a respetiva identificação e contactos atualizados junto do Encarregado de Proteção de Dados e do Reitor ou da pessoa por este designada, tendo em vista a articulação necessária ao cumprimento tempestivo, adequado e demonstrável das obrigações decorrentes do Regulamento Geral sobre a Proteção de Dados, da Lei n.º 58/2019, de 8 de agosto, e do presente Código.

5 — Os interlocutores previstos no número anterior colaboram, no respetivo âmbito de atuação, na prestação das informações e na adoção das medidas necessárias ao cumprimento das obrigações em matéria de proteção de dados, designadamente quanto à atualização do registo das atividades de tratamento, à apreciação de novos tratamentos, à resposta a pedidos dos titulares dos dados, à implementação de orientações e procedimentos internos e à comunicação de incidentes e violações de dados pessoais.

Despacho n.º 11473/2026

6 — A designação dos interlocutores não lhes confere a qualidade de responsável pelo tratamento, não prejudica as competências próprias dos órgãos, dirigentes e serviços envolvidos, nem afeta a autonomia e a independência funcional do Encarregado de Proteção de Dados.

7 — Os trabalhadores, dirigentes e demais colaboradores que intervenham em operações de tratamento atuam sob a autoridade da UPCoimbra e apenas podem tratar os dados pessoais de acordo com as instruções, regras, procedimentos e autorizações aplicáveis, sem prejuízo da responsabilidade disciplinar, civil, contraordenacional ou criminal que possa resultar de atuação ilícita ou culposa.

Artigo 23.º

Contratos com terceiros

1 — A contratação, renovação ou alteração de serviços prestados por terceiros que impliquem acesso, alojamento, conservação, transmissão ou outra forma de tratamento de dados pessoais é precedida de avaliação proporcional ao risco, incidindo, designadamente, sobre a natureza e criticidade do serviço, as categorias de dados, o nível de acesso concedido, as medidas de segurança, a localização do tratamento, os subcontratantes, os mecanismos de continuidade e as condições de cessação do serviço.

2 — Os contratos a celebrar devem incluir cláusulas específicas de proteção de dados que limitem o tratamento dos dados à execução do contrato e às instruções da UPCoimbra, que proíbam expressamente o tratamento, direta ou indiretamente, para qualquer outra finalidade, bem como para proveito próprio ou de terceiros e, ainda, prever medidas de proteção dos dados por parte da entidade contratada.

3 — Após a cessação do contrato, o terceiro apaga ou devolve os dados pessoais à UPCoimbra e destrói todas as cópias dos mesmos, salvo se, comprovadamente, existir uma obrigação legal ou contratual que exija a sua conservação.

4 — A UPCoimbra promove o inventário progressivo dos terceiros que disponham de acesso direto ou indireto a dados pessoais sob a sua responsabilidade e procede à revisão contratual em função do risco, criticidade, natureza dos dados tratados, prazo contratual remanescente e necessidade de adequação às disposições legais aplicáveis.

5 — A avaliação e o acompanhamento dos terceiros são realizados através de procedimento institucional que articula os serviços responsáveis pela contratação, o EPD, os serviços jurídicos e os serviços competentes em matéria de tecnologias da informação e comunicação.

Artigo 24.º

Subcontratantes

1 — Quando a UPCoimbra recorrer a subcontratantes para, em seu nome e de acordo com as suas instruções, procederem ao tratamento de dados pessoais, deve o respetivo contrato estabelecer, em termos claros e precisos, a duração do serviço, a natureza e as finalidades do tratamento, o tipo de dados pessoais, as categorias de titulares de dados, a obrigação de notificar qualquer violação de dados pessoais, bem como os termos da obrigação de confidencialidade da entidade subcontratante e as medidas técnicas e organizativas que esta deve implementar para assegurar a segurança dos dados.

2 — As entidades subcontratantes devem fornecer à UPCoimbra a documentação necessária para demonstrar o adequado cumprimento de todas as obrigações referentes à proteção de dados pessoais, em especial no que diz respeito ao RGPD, bem como facilitar e contribuir para as auditorias, inclusive as inspeções, conduzidas pela UPCoimbra ou por auditor por esta mandatado.

3 — É proibido ao subcontratante transmitir os dados pessoais a terceiros, incluindo outro subcontratante, sem a prévia autorização escrita da UPCoimbra.

4 — Após a cessação do contrato, o subcontratante apaga ou devolve os dados pessoais à UPCoimbra e destrói todas as cópias dos mesmos, salvo se, comprovadamente, existir uma obrigação legal ou contratual que exija a sua conservação.

Despacho n.º 11473/2026

5 — A avaliação e o acompanhamento dos terceiros são realizados através de procedimento institucional que articula os serviços responsáveis pela contratação, o EPD, os serviços jurídicos e os serviços competentes em matéria de tecnologias da informação e comunicação.

6 — Os contratos e instrumentos de contratação devem prever, em função do risco, mecanismos de prestação de informação, verificação de conformidade, gestão de incidentes, continuidade do serviço, devolução ou eliminação dos dados e transição segura no termo da relação contratual.

Artigo 25.º

Registo das atividades de tratamento

1 — A UPCoimbra mantém um registo atualizado das atividades de tratamento sob a sua responsabilidade, contendo os elementos legalmente exigidos e a informação necessária à gestão, monitorização e demonstração da conformidade, designadamente as finalidades, fundamentos de licitude, categorias de titulares e dados, destinatários, transferências, subcontratantes, prazos de conservação, medidas de segurança, avaliação de risco e, quando aplicável, referência à avaliação de impacto sobre a proteção de dados.

2 — Nos casos em que os sistemas informáticos usados na UPCoimbra não permitam a criação dos registos previstos, é elaborada uma ficha de registo de tratamento de dados que permita identificar, caracterizar, gerir e monitorizar de forma eficiente a recolha de dados.

3 — Cada Unidade Orgânica e serviço coopera na atualização do registo das atividades de tratamento que desenvolva, de acordo com os mecanismos, responsabilidades e periodicidade definidos pela UPCoimbra.

CAPÍTULO V

Segurança dos Dados Pessoais

Artigo 26.º

Confidencialidade e restrição de acessos

1 — Apenas podem ser autorizados a tratar dados pessoais os trabalhadores e demais colaboradores da UPCoimbra que deles necessitem para cumprimento das suas funções ou tarefas, devendo estes absterem-se de aceder a dados pessoais a que possam indevidamente ter acesso.

2 — É expressamente proibido o tratamento de dados pessoais sem prévia autorização, bem como o tratamento para fins distintos dos enunciados na autorização, em especial fins pessoais ou comerciais.

3 — Os intervenientes no tratamento de dados pessoais, bem como o EPD, estão adstritos à observância de um dever de confidencialidade que acresce aos deveres de sigilo profissional a que estejam já sujeitos, obrigação que se mantém após a cessação de funções na UPCoimbra.

Artigo 27.º

Segurança do tratamento

1 — A UPCoimbra aplica medidas técnicas e organizativas que assegurem um nível de segurança adequado ao risco, de forma a evitar a destruição, perda e alteração acidentais ou ilícitas, a divulgação ou o acesso não autorizados aos dados pessoais, garantindo, designadamente:

a) A pseudonimização — os dados pessoais que tenham sido pseudonimizados são considerados informações sobre uma pessoa singular identificável;

b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;

Despacho n.º 11473/2026

c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico.

2 — Complementarmente ao disposto no número anterior, são implementadas na UPCoimbra um conjunto vasto de boas práticas, compiladas no manual a que alude o artigo 35.º

3 — Em caso algum podem os dados pessoais ser armazenados em equipamentos não protegidos ou em ficheiros sem proteção.

4 — Os ficheiros não automatizados e automatizados com dados pessoais estão equipados com sistemas de segurança que impedem a consulta, modificação, destruição ou acréscimo de dados pessoais por pessoa não autorizada, bem como, mecanismos que garantem a deteção de eventuais desvios intencionais de informação.

5 — O acesso aos sistemas e serviços que tratem dados pessoais é assegurado através de mecanismos de autenticação, autorização, gestão de privilégios, registo de atividade e revisão periódica de acessos adequados ao risco, à criticidade do serviço e à natureza dos dados tratados.

6 — A UPCoimbra define, através de normas técnicas e procedimentos complementares, os requisitos aplicáveis à gestão de credenciais, autenticação multifatorial, acessos privilegiados, acessos remotos, cifragem de dados em repouso e em trânsito, utilização de dispositivos, conservação de registos técnicos, deteção de eventos de segurança e resposta a incidentes.

7 — A transmissão de dados pessoais por correio eletrónico ou por outros meios eletrónicos deve ser realizada através de canais e medidas de segurança adequados à natureza dos dados, aos destinatários, ao contexto de transmissão e ao risco para os direitos e liberdades dos titulares.

8 — As regras técnicas aplicáveis à proteção de ficheiros, à cifragem, à partilha de chaves ou palavras-passe e à utilização de canais alternativos de comunicação constam de norma técnica ou instrução operacional aprovada pela UPCoimbra.

Artigo 28.º

Procedimento para a divulgação de dados pessoais na UPCoimbra

1 — A UPCoimbra, ou quem por ela agir, enquanto responsável pelo tratamento, na determinação das finalidades e dos meios de tratamento de dados pessoais, deve atender à adequada ponderação dos interesses e valores que representam a transparência da administração pública e o exercício do direito à privacidade e, também, acautelar o risco da utilização abusiva da divulgação dos referidos dados por meios digitais, de modo a não comprometer a sua capacidade em cumprir, ou fazer cumprir, o disposto no RGPD e demais legislação aplicável.

2 — O procedimento de divulgação de dados pessoais deve assegurar a definição da finalidade, fundamento jurídico, categorias de dados, destinatários, período de disponibilização, medidas de minimização, condições de acesso e registo das decisões adotadas.

Artigo 29.º

Procedimento para a elaboração de cadernos eleitorais

1 — Os cadernos eleitorais para realização de atos eleitorais na UPCoimbra são elaborados pelos serviços competentes para a eleição em causa, designadamente os responsáveis pela gestão académica ou os responsáveis pelos recursos humanos, com a indicação do nome dos eleitores, podendo ser utilizado um segundo identificador, como critério de diferenciação, nos termos seguintes:

a) No caso de trabalhadores/as, além do nome, pode ser colocado o número mecanográfico, com omissão dos últimos três dígitos (por exemplo, 87654***);

b) No caso dos estudantes, além do nome e do curso, pode constar o número de aluno, com omissão dos cinco primeiros dígitos (por exemplo, *****54321).

Despacho n.º 11473/2026

2 — Os cadernos eleitorais são submetidos a validação do EPD pelo serviço que os elabora, sendo posteriormente remetidos à unidade ou ao serviço requerente para que proceda à respetiva verificação e digitalização.

3 — A digitalização a que se refere o número anterior obriga à passagem para um formato que impeça a extração automática da informação e eventual propagação massiva por meios digitais.

4 — Os cadernos eleitorais são publicitados, no formato referido no número anterior, em intranet e em página única, sendo imediatamente retirados logo que atingida a finalidade que levou à sua publicitação.

5 — Sem prejuízo no disposto nos números anteriores, em situações devidamente fundamentadas, o EPD pode decidir por formatos alternativos.

Artigo 30.º

Notificação da violação de dados pessoais

1 — A UPCoimbra notifica a CNPD de qualquer violação de dados pessoais, sem demora injustificada e, sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido, a menos que seja capaz de demonstrar, em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares.

2 — Na impossibilidade de cumprir o prazo de 72 horas previsto no número anterior, a notificação é acompanhada dos motivos do atraso.

3 — Quando constituir um elevado risco para os direitos e liberdades do titular dos dados, a violação a que alude o n.º 1 é-lhe igualmente comunicada.

4 — Todas as violações ocorridas, os efeitos e as medidas de reparação devem ser documentados, de forma a permitir à CNPD verificar o cumprimento das regras previstas no RGPD.

5 — A UPCoimbra dispõe de procedimento interno de deteção, registo, classificação, triagem, contenção, investigação, recuperação, comunicação e documentação de incidentes de segurança suscetíveis de constituir violações de dados pessoais.

6 — O procedimento previsto no número anterior assegura a articulação atempada entre o EPD, o Responsável de Cibersegurança, os serviços competentes em matéria de tecnologias da informação e comunicação, as Unidades Orgânicas e os demais serviços cuja intervenção se revele necessária.

7 — A triagem interna dos incidentes deve permitir determinar, de forma documentada, a eventual existência de violação de dados pessoais, o nível de risco para os direitos e liberdades dos titulares, as medidas de contenção e reparação, bem como as comunicações e notificações legalmente aplicáveis.

CAPÍTULO VI

Encarregado de Proteção de Dados

Artigo 31.º

Designação e estatuto

1 — Nos termos do artigo 37.º do RGPD e do artigo 9.º da Lei n.º 58/2019, de 8 de agosto, o EPD é designado por despacho da Reitora da UPCoimbra, com base nas suas qualidades profissionais e nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, não carecendo de certificação profissional para o efeito.

2 — Independentemente da natureza da sua relação jurídica, o EPD exerce a sua função com autonomia técnica face à UPCoimbra, não lhe sendo atribuídas funções que possam culminar num conflito de interesses.

Despacho n.º 11473/2026

3 — A UPCoimbra assegura que o EPD é envolvido de forma adequada e em tempo útil nas questões relativas à proteção de dados pessoais, disponibilizando-lhe os recursos humanos, técnicos, financeiros e organizacionais necessários ao exercício efetivo das suas funções, incluindo acesso à informação, aos sistemas, aos registos de tratamento e às operações de tratamento relevantes.

4 _ Sem prejuízo da autonomia do EPD, a UPCoimbra assegura mecanismos de apoio administrativo, técnico e organizacional que permitam a execução das funções de aconselhamento, controlo, auditoria, formação, acompanhamento de incidentes e cooperação com a autoridade de controlo.

Artigo 32.º

Funções do EPD

1 — São funções do EPD:

a) Aconselhar e controlar a realização de avaliação de impacto sobre proteção de dados;

b) Propor e acompanhar a realização de auditorias e ações de verificação, programadas ou extraordinárias, de acordo com plano baseado no risco, sem prejuízo das competências dos órgãos e serviços institucionalmente competentes em matéria de auditoria e controlo interno;

c) Assegurar as relações com os titulares dos dados nas matérias abrangidas pelo RGPD e pela legislação nacional em matéria de proteção de dados;

d) Controlar a conformidade com a lei e com as políticas da UPCoimbra relativamente à proteção de dados pessoais;

e) Cooperar com a CNPD;

f) Informar e aconselhar as unidades orgânicas e serviços da UPCoimbra em matéria de proteção de dados;

g) Sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e cibersegurança;

h) Ser um ponto de contacto com a CNPD sobre questões relacionadas com o tratamento, incluindo a consulta prévia, e consultar, sendo caso disso, esta autoridade de controlo sobre qualquer outro assunto;

i) Outras atribuições que lhe sejam conferidas.

2 — Compete igualmente ao EPD, em conjunto com as unidades orgânicas e serviços, com as partes interessadas e com o responsável pela cibersegurança da UPCoimbra, propor soluções para o tratamento de dados e medidas de segurança dos mesmos.

3 — No desempenho das suas funções, o EPD afere e pondera os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

Artigo 33.º

Contactos

O EPD pode ser contactado por *e-mail,* através do endereço epd@ipc.pt.

Artigo 34.º

Cooperação com o EPD

1 — As Unidades Orgânicas, os Serviços de Ação Social e os demais serviços da UPCoimbra cooperam com o EPD, designadamente através dos interlocutores previstos no n.º 3 do artigo 22.º,

Despacho n.º 11473/2026

respondendo às suas solicitações no prazo por este fixado ou, na falta de indicação, no prazo de cinco dias úteis.

2 — O EPD pode solicitar informações que sejam relevantes para o exercício das suas funções ao dirigente da área a que essa informação respeite, devendo este colaborar de forma oportuna e célere com o EPD.

CAPÍTULO VII

Disposições Finais

Artigo 35.º

Orientações e boas práticas

1 — A UPCoimbra, através do seu EPD, promove ações de sensibilização e divulga, no seu sítio de internet, orientações sobre proteção de dados, nomeadamente sob a forma de pareceres e recomendações.

2 — Adicionalmente, é aprovado um manual de boas práticas, que visa complementar a disciplina plasmada nas presentes normas, objeto de revisão periódica anual pelo EPD, e que consta do Anexo 1.

3 — A UPCoimbra assegura, ainda, a divulgação de um folheto informativo, em suporte físico e/ou eletrónico, contendo síntese das principais boas práticas previstas no manual referido no número anterior, a disponibilizar aos membros da comunidade académica em termos claros, acessíveis e adequados.

4 — As orientações, pareceres, recomendações, o manual de boas práticas e o folheto informativo previstos nos números anteriores são divulgados e atualizados em articulação com os serviços competentes da UPCoimbra, sem prejuízo das competências próprias do EPD.

Artigo 36.º

Dúvidas e omissões

As dúvidas suscitadas pela aplicação do presente Código de conduta e os casos omissos são resolvidos por despacho da Reitora da UPCoimbra, ouvido o EPD.

Artigo 37.º

Norma revogatória

É revogado o Manual de Boas Práticas no Tratamento de Dados Pessoais, aprovado por Despacho de 7 de janeiro de 2025.

Artigo 38.º

Norma transitória

1 — No prazo de 120 dias após a entrada em vigor do presente Código, é aprovado um plano de implementação que identifica as medidas prioritárias, os responsáveis, os instrumentos complementares a elaborar ou rever, os recursos necessários e os mecanismos de acompanhamento.

2 — O plano de implementação deve atribuir prioridade, designadamente, à gestão de incidentes e violações de dados pessoais, à gestão de identidades e acessos, ao registo das atividades de tratamento, à avaliação de fornecedores e subcontratantes, à segurança dos sistemas, à continuidade dos serviços e à capacitação dos intervenientes.

Despacho n.º 11473/2026

3 — As políticas, normas técnicas, procedimentos e instruções operacionais necessários à execução do presente Código são aprovados ou atualizados de forma progressiva, de acordo com critérios de risco, criticidade, proporcionalidade e disponibilidade de recursos.

4 — A execução do plano é objeto de acompanhamento periódico, devendo ser conservadas evidências das medidas adotadas, das ações de formação realizadas, dos incidentes tratados, das avaliações efetuadas e das melhorias implementadas.

Artigo 39.º

Entrada em vigor

1 — O presente Código de Conduta entra em vigor no dia seguinte ao da sua publicação no *Diário da República*.

ANEXO 1

Manual de Boas Práticas

Em cumprimento do disposto no artigo 35.º do Código de Conduta e Boas Práticas na Proteção de Dados Pessoais na Universidade Politécnica de Coimbra, elencam-se no presente anexo as boas práticas a implementar pelos diversos intervenientes nos processos de tratamento de dados pessoais realizados na UPCoimbra.

1 — Objeto, natureza e articulação

1 — O presente Manual de Boas Práticas complementa o Código de Conduta e Boas Práticas na Proteção de Dados Pessoais da Universidade Politécnica de Coimbra, adiante designado por UPCoimbra.

2 — O Manual estabelece orientações práticas dirigidas aos membros da comunidade académica e demais pessoas que, no exercício das respetivas funções, tratem dados pessoais sob responsabilidade da UPCoimbra.

3 — As orientações constantes do presente Manual não substituem as obrigações previstas no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, no Código de Conduta, na legislação aplicável nem nas políticas, normas técnicas, procedimentos e instruções operacionais aprovados pela UPCoimbra.

4 — Os parâmetros técnicos suscetíveis de atualização frequente, designadamente os relativos a autenticação, gestão de credenciais, autenticação multifatorial, cifragem, utilização de dispositivos, retenção de registos técnicos, gestão de vulnerabilidades, cópias de segurança e recuperação de serviços, são definidos em normas técnicas e instruções operacionais próprias.

5 — O presente Manual é objeto de revisão periódica, pelo menos anual, ou sempre que se verifiquem alterações relevantes no enquadramento legal, tecnológico, organizacional ou no perfil de risco da UPCoimbra.

2 — Princípios gerais aplicáveis a todos os utilizadores

1 — Os dados pessoais apenas podem ser tratados no âmbito das funções, competências e autorizações atribuídas e para finalidades determinadas, explícitas e legítimas.

2 — Deve ser recolhida, consultada, utilizada, comunicada e conservada apenas a informação adequada, pertinente e necessária para a finalidade em causa.

3 — É proibido aceder, consultar, copiar, alterar, divulgar, conservar ou utilizar dados pessoais para fins pessoais, comerciais, alheios às funções exercidas ou não autorizados.

Despacho n.º 11473/2026

4 — Quem trate dados pessoais deve respeitar o dever de confidencialidade, que se mantém após a cessação das funções ou da relação com a UPCoimbra.

5 — Sempre que existam dúvidas sobre a legitimidade, necessidade, segurança ou adequação de um tratamento, deve ser solicitada orientação ao superior hierárquico, ao serviço competente ou ao Encarregado de Proteção de Dados, adiante designado por EPD.

6 — Os dados pessoais não devem ser mantidos em cópias paralelas, arquivos pessoais, suportes não autorizados ou locais que não assegurem condições adequadas de segurança e controlo de acesso.

7 — A eliminação, anonimização, bloqueio, arquivamento ou conservação de dados deve obedecer aos prazos e critérios definidos pela UPCoimbra para a atividade de tratamento em causa.

8 — Os utilizadores devem participar nas ações de formação e sensibilização em proteção de dados, segurança da informação, cibersegurança e utilização responsável das tecnologias que lhes sejam destinadas.

3 — Responsabilidades institucionais

3.1 — Reitor da Universidade Politécnica de Coimbra

1 — Compete ao Reitor da UPCoimbra, assegurar a definição e promoção das orientações institucionais em matéria de proteção de dados pessoais, segurança da informação, cibersegurança e utilização responsável das tecnologias.

2 — O Reitor promove, em articulação com o Encarregado de Proteção de Dados, o Responsável de Cibersegurança, os serviços responsáveis pelas tecnologias de informação e comunicação e os Presidentes ou Diretores das Unidades Orgânicas, a definição de diretrizes institucionais relativas à gestão de identidades e acessos, à proteção da informação, à gestão de incidentes, à continuidade dos serviços, à utilização de serviços *cloud*, à contratação de terceiros e à utilização de sistemas de inteligência artificial, quando aplicável.

3 — O Reitor assegura que as responsabilidades atribuídas pelo Código de Conduta são acompanhadas de condições organizacionais, recursos, competências, instrumentos de suporte e mecanismos de acompanhamento adequados ao respetivo exercício.

4 — Compete ao Reitor aprovar ou submeter à aprovação dos órgãos competentes, conforme o regime aplicável, as políticas institucionais, normas, procedimentos e instrumentos complementares necessários à execução do Código de Conduta.

5 — O Reitor assegura a existência de mecanismos de articulação periódica entre o Encarregado de Proteção de Dados, o Responsável de Cibersegurança e as estruturas institucionais competentes em matéria de tecnologias de informação e comunicação e de inteligência artificial, sem prejuízo das competências próprias de cada interveniente.

6 — O Reitor assegura que o Encarregado de Proteção de Dados dispõe dos recursos humanos, técnicos, financeiros e organizacionais necessários ao exercício efetivo das respetivas funções, preservando a sua autonomia funcional.

3.2 — Presidentes ou Diretores das Unidades Orgânicas, Administrador da UPCoimbra e Administrador dos Serviços de Ação Social

1 — Compete aos Presidentes ou Diretores das Unidades Orgânicas, ao Administrador da UPCoimbra e ao Administrador dos Serviços de Ação Social, no âmbito das respetivas atribuições:

a) Assegurar a aplicação do Código de Conduta, das políticas, normas técnicas, procedimentos e instruções operacionais aplicáveis;

b) Promover a formação, sensibilização e informação contínua dos trabalhadores, docentes, investigadores, estudantes e colaboradores sob a sua direção;

Despacho n.º 11473/2026

c) Designar ou assegurar a existência de interlocutores adequados para matérias de proteção de dados, segurança da informação e cibersegurança, nos termos definidos institucionalmente;

d) Comunicar aos serviços competentes as necessidades de recursos, competências, formação, apoio técnico e medidas de segurança necessárias;

e) Garantir que os acessos a dados pessoais são atribuídos, alterados, revistos e revogados em função das necessidades funcionais e das regras institucionais aplicáveis;

f) Assegurar a utilização de sistemas, aplicações, plataformas e serviços institucionais ou expressamente autorizados;

g) Promover o reporte atempado de incidentes, vulnerabilidades, acessos indevidos, utilizações não autorizadas e outras ocorrências suscetíveis de afetar dados pessoais;

h) Cooperar com o EPD, com o Responsável de Cibersegurança e com os serviços responsáveis pelas tecnologias de informação e comunicação;

i) Assegurar a atualização da informação relevante para o Registo das Atividades de Tratamento e para a avaliação de novos tratamentos ou alterações substanciais;

j) Garantir que a contratação, utilização ou renovação de serviços de terceiros que envolvam dados pessoais é submetida aos procedimentos institucionais aplicáveis;

2 — Os responsáveis referidos no número anterior devem assegurar a adoção de medidas proporcionais à natureza dos dados tratados, à criticidade dos serviços, aos riscos identificados e aos recursos disponíveis, sem prejuízo dos requisitos mínimos definidos institucionalmente.

3.3 — Encarregado de Proteção de Dados

1 — O EPD exerce as suas funções com autonomia técnica e nos termos previstos no RGPD, na legislação nacional, no Código de Conduta e nos instrumentos institucionais aplicáveis.

2 — Sem prejuízo das competências legalmente atribuídas, compete ao EPD:

a) Informar e aconselhar a UPCoimbra, as Unidades Orgânicas, os serviços, trabalhadores e demais intervenientes sobre as suas obrigações em matéria de proteção de dados;

b) Acompanhar a conformidade das atividades de tratamento com a legislação e com os instrumentos internos aplicáveis;

c) Aconselhar sobre a necessidade e realização de avaliações de impacto sobre a proteção de dados;

d) Cooperar com a CNPD e atuar como ponto de contacto nas matérias legalmente previstas;

e) Participar nos mecanismos de gestão e triagem de incidentes suscetíveis de constituir violações de dados pessoais;

f) Emitir orientações e recomendações, promover ações de sensibilização e contribuir para a atualização do Manual;

g) Colaborar na definição de requisitos de proteção de dados aplicáveis à contratação de terceiros, à aquisição ou desenvolvimento de sistemas e à adoção de plataformas digitais.

3 — O EPD não substitui os órgãos competentes, os dirigentes, os responsáveis funcionais ou os serviços técnicos na tomada de decisões e na execução das medidas que lhes competem.

3.4 — Responsável de Cibersegurança

1 — O Responsável de Cibersegurança assegura, no âmbito das competências que lhe sejam atribuídas, a coordenação das medidas de cibersegurança adequadas à proteção de dados pessoais e a articulação com as Unidades Orgânicas, os serviços responsáveis pelas tecnologias de informação e comunicação, o EPD e outras estruturas institucionais relevantes.

Despacho n.º 11473/2026

2 — Compete-lhe, designadamente:

a) Apoiar a definição e acompanhamento das medidas de segurança da informação e Cibersegurança;

b) Coordenar ou acompanhar a gestão de incidentes de cibersegurança, sem prejuízo da intervenção do EPD quando estejam em causa dados pessoais;

c) Promover a articulação com as entidades externas competentes em matéria de cibersegurança, quando aplicável;

d) Contribuir para a gestão de vulnerabilidades, monitorização, continuidade, recuperação, gestão de fornecedores e sensibilização dos utilizadores;

e) Participar na definição e revisão das normas técnicas de segurança aplicáveis aos sistemas que tratem dados pessoais.

3 — A intervenção do Responsável de Cibersegurança não prejudica a autonomia, as funções e as responsabilidades próprias do EPD.

3.5 — Serviços responsáveis pelas tecnologias de informação e comunicação

1 — Os serviços responsáveis pelas tecnologias de informação e comunicação asseguram, no âmbito das respetivas competências, a execução e manutenção das medidas técnicas aprovadas pela UPCoimbra para proteção dos sistemas, redes, aplicações, equipamentos, identidades digitais e dados pessoais.

2 — Compete-lhes, designadamente:

a) Colaborar na gestão de identidades, acessos, privilégios, autenticação e revogação de acessos;

b) Apoiar a proteção de sistemas, dispositivos, redes e aplicações que tratem dados pessoais;

c) Implementar e manter medidas técnicas de segurança, registo, monitorização, cópias de segurança, recuperação e continuidade, de acordo com as normas institucionais aplicáveis;

d) Participar na deteção, análise, contenção, recuperação e documentação de incidentes;

e) Apoiar o inventário de ativos, sistemas, serviços e dependências tecnológicas relevantes;

f) Colaborar na avaliação técnica de fornecedores, plataformas *cloud*, integrações, sistemas de IA e outras soluções que envolvam tratamento de dados pessoais;

g) Contribuir para a definição, atualização e divulgação de normas técnicas e instruções operacionais.

3 — Os serviços responsáveis pelas tecnologias de informação e comunicação devem colaborar com o EPD e com o Responsável de Cibersegurança sempre que estejam em causa medidas de proteção de dados, incidentes, avaliações de impacto, fornecedores, novos tratamentos ou alterações relevantes de sistemas.

3.6 — Trabalhadores, docentes, investigadores, estudantes e demais colaboradores

1 — Os trabalhadores, docentes, investigadores, estudantes e demais colaboradores que tratem dados pessoais devem:

a) Tratar dados exclusivamente no âmbito das respetivas funções, atividades autorizadas e finalidades legítimas;

b) Utilizar apenas sistemas, contas, plataformas e ferramentas institucionais ou autorizadas;

c) Manter a confidencialidade dos dados a que tenham acesso;

d) Proteger os documentos, equipamentos, contas e credenciais sob a sua responsabilidade;

e) Comunicar imediatamente acessos indevidos, incidentes, vulnerabilidades, mensagens suspeitas, erros de envio, perdas de informação ou outras ocorrências relevantes;

f) Colaborar com os serviços e estruturas competentes na resposta a pedidos de titulares, atualização do Registo das Atividades de Tratamento (*ROPA — Record of Processing Activities*), realização de Avaliação de Impacto sobre a Proteção de Dados (AIPD), gestão de incidentes e avaliação de fornecedores, quando chamados a intervir;

g) Participar nas ações de formação e sensibilização que lhes sejam dirigidas.

2 — A atribuição de deveres aos utilizadores não prejudica a responsabilidade institucional da UPCoimbra enquanto responsável pelo tratamento nem as responsabilidades próprias dos órgãos, dirigentes, serviços e estruturas competentes.

4 — Tratamento quotidiano de dados pessoais

4.1 — Recolha, utilização e consulta

1 — Antes de recolher dados pessoais, deve ser confirmada a necessidade da recolha, a finalidade do tratamento e a existência de fundamento de licitude aplicável.

2 — Devem ser recolhidos apenas os dados estritamente necessários à atividade, procedimento ou serviço em causa.

3 — Os dados pessoais devem ser utilizados exclusivamente para as finalidades que justificaram a sua recolha ou para finalidades posteriores legalmente compatíveis.

4 — O tratamento de categorias especiais de dados, dados relativos a infrações penais, dados de menores ou outros dados particularmente sensíveis exige especial cuidado e o cumprimento das regras e procedimentos aplicáveis.

5 — Sempre que adequado, devem ser utilizadas técnicas de pseudonimização, anonimização, agregação ou outras medidas de minimização de dados, nos termos das orientações técnicas e procedimentais aprovadas pela UPCoimbra.

6 — Os utilizadores não devem criar listas, bases de dados, ficheiros de controlo ou cópias locais contendo dados pessoais sem necessidade funcional, autorização ou enquadramento no tratamento institucional aplicável.

4.2 — Documentos em papel e segurança física

1 — Os documentos em papel que contenham dados pessoais devem ser mantidos em locais protegidos e com acesso condicionado às pessoas autorizadas.

2 — Após a utilização, os processos, dossiers e documentos com dados pessoais devem ser arquivados, guardados em armário, gaveta ou outro local seguro, ou destruídos de modo irrecuperável quando não devam ser conservados.

3 — Os postos de trabalho devem cumprir os princípios de secretária limpa e ecrã protegido, evitando que documentos ou informação pessoal fiquem acessíveis a pessoas não autorizadas.

4 — As impressões, fotocópias e digitalizações que contenham dados pessoais devem ser recolhidas sem demora dos equipamentos partilhados.

5 — A impressão ou reprodução de documentos com dados pessoais deve limitar-se ao estritamente necessário.

6 — Os documentos que já não sejam necessários e cuja conservação não seja obrigatória devem ser destruídos através de métodos que impeçam a sua recuperação ou reconstituição.

Despacho n.º 11473/2026

7 — O transporte físico de documentos com dados pessoais deve ser autorizado quando necessário e efetuado com medidas de proteção adequadas à natureza da informação e ao risco de acesso, perda ou divulgação indevida.

4.3 — Sistemas, contas e acessos

1 — As contas de acesso são pessoais e intransmissíveis e só podem ser utilizadas pelo respetivo titular, salvo mecanismos institucionais de acesso delegado expressamente autorizados.

2 — Os utilizadores devem proteger as suas credenciais de autenticação, não as partilhando, divulgando ou guardando em locais acessíveis a terceiros.

3 — Os utilizadores devem bloquear o respetivo posto de trabalho sempre que se ausentem e terminar a sessão ou desligar o equipamento quando deixem de o utilizar, de acordo com as instruções técnicas aplicáveis.

4 — Os acessos concedidos devem corresponder às necessidades funcionais do utilizador. Qualquer acesso excessivo, indevido ou já desnecessário deve ser comunicado sem demora.

5 — Os acessos a dados pessoais em equipamentos, aplicações, plataformas e serviços devem ser realizados através de soluções institucionais ou expressamente autorizadas.

6 — É proibido instalar, utilizar ou ligar aos sistemas institucionais software, extensões, aplicações, serviços *cloud*, ferramentas de inteligência artificial ou equipamentos não autorizados, quando possam envolver tratamento de dados pessoais ou afetar a segurança dos recursos da UPCoimbra.

7 — Os requisitos aplicáveis a palavras-passe, autenticação multifatorial, acessos privilegiados, acessos remotos, proteção de dispositivos, cifragem e gestão de suportes amovíveis constam de normas técnicas e instruções operacionais próprias.

4.4 — Correio eletrónico, partilha e comunicações

1 — O correio eletrónico institucional deve ser utilizado de forma prudente, exclusivamente para fins profissionais, académicos, científicos, administrativos ou institucionais legítimos.

2 — Não devem ser utilizadas contas de correio eletrónico pessoais para transmitir, receber, conservar ou tratar dados pessoais no âmbito das atividades da UPCoimbra.

3 — Antes do envio de uma mensagem ou ficheiro, deve ser verificada a identidade, endereço e legitimidade dos destinatários, bem como a adequação dos dados e anexos a transmitir.

4 — Nas comunicações dirigidas a múltiplos destinatários externos entre si, devem ser utilizados mecanismos que evitem a divulgação indevida dos respetivos endereços eletrónicos, designadamente o campo de cópia oculta, quando adequado.

5 — Os ficheiros ou mensagens que contenham dados pessoais devem ser transmitidos através de canais e com medidas de segurança adequadas à natureza dos dados, aos destinatários e ao risco da comunicação, nos termos das normas técnicas aplicáveis.

6 — Quando uma mensagem ou ficheiro seja recebido por engano, o destinatário deve abster-se de utilizar o respetivo conteúdo, eliminá-lo quando adequado e informar o remetente ou os serviços competentes.

7 — Não devem ser abertas hiperligações, anexos, pedidos de autenticação ou mensagens cuja origem, conteúdo ou contexto suscitem dúvidas razoáveis de segurança. Estas situações devem ser reportadas através dos canais definidos pela UPCoimbra.

8 — É proibido transmitir por correio eletrónico credenciais, palavras-passe, códigos de autenticação ou outros elementos de segurança, salvo através de mecanismos institucionais especificamente aprovados.

Despacho n.º 11473/2026

4.5 — Atendimento presencial e telefónico

1 — Os dados pessoais apenas podem ser comunicados presencialmente, por telefone ou por outros meios de contacto quando o interlocutor esteja legitimado a recebê-los e a sua identidade seja adequadamente confirmada.

2 — Não devem ser prestadas informações pessoais a terceiros sem confirmação do fundamento legal, autorização aplicável ou enquadramento funcional da comunicação.

3 — Nas comunicações internas, apenas devem ser partilhados os dados necessários ao exercício das funções do destinatário.

4 — As conversas que envolvam dados pessoais devem decorrer em condições que impeçam a audição por pessoas não autorizadas.

5 — Não devem ser divulgadas a terceiros informações sobre a localização, ausências, estado de saúde ou circunstâncias pessoais de trabalhadores, estudantes ou outros membros da comunidade académica, salvo quando exista fundamento legal, necessidade funcional e autorização aplicável.

4.6 — Teletrabalho, mobilidade e dispositivos pessoais (BYOD)

1 — O tratamento de dados pessoais fora das instalações da instituição, seja em regime de teletrabalho ou em mobilidade, exige a adoção de medidas de segurança equivalentes às aplicadas no posto de trabalho físico.

2 — Sempre que os utilizadores acedam a redes, ficheiros ou sistemas de gestão internos a partir do exterior, devem utilizar obrigatoriamente a ligação por rede privada virtual institucional (VPN) e os métodos de autenticação forte homologados.

3 — A utilização excecional de dispositivos pessoais (*Bring Your Own Device* — BYOD) para o tratamento de dados pessoais no âmbito de atividades institucionais está sujeita a:

a) Existência de bloqueio automático por palavra-passe, PIN ou biometria robustos;

b) Cifragem ativa do disco rígido ou dos suportes de armazenamento do equipamento;

c) Atualização contínua do sistema operativo, aplicações e antivírus;

d) Segregação absoluta entre ficheiros institucionais e ficheiros pessoais, sendo proibida a sincronização com contas pessoais de serviços *cloud* de terceiros;

e) Eliminação imediata dos ficheiros locais logo que concluída a tarefa ou transferida a informação para os repositórios institucionais.

4 — É expressamente proibida a realização de ligações a redes sem fios públicas ou não encriptadas sem a ativação prévia da VPN institucional.

4.7 — Videovigilância e controlo de acessos físicos

1 — O sistema de videovigilância em circuito fechado (CCTV) dos *campi*, edifícios e instalações tem por finalidade exclusiva a segurança de pessoas e bens e a prevenção da criminalidade, não podendo ser utilizado para o controlo de assiduidade ou desempenho de trabalhadores ou estudantes.

2 — É proibida a visualização, gravação ou partilha de imagens de CCTV fora das funções estritamente atribuídas ao pessoal de segurança autorizado e aos órgãos competentes.

3 — As imagens recolhidas são conservadas pelo prazo máximo legal de 30 dias contados da respetiva captação, findo o qual são destruídas de forma segura e automática, salvo se existirem processos judiciais, disciplinares ou de investigação criminal em curso.

4 — Todos os locais abrangidos por videovigilância devem dispor de avisos informativos visíveis e adequados, identificando o responsável pelo tratamento e os canais de contacto.

Despacho n.º 11473/2026

5 — Plataformas digitais, ensino e gravações

1 — As atividades de ensino, avaliação, reuniões, eventos ou prestação de serviços em ambiente digital devem utilizar plataformas institucionais ou expressamente autorizadas pela UPCoimbra.

2 — As plataformas utilizadas devem ser configuradas, sempre que tecnicamente possível, para limitar o acesso às pessoas autorizadas e para assegurar a adequação dos participantes, permissões, partilhas, gravações, conservação e eliminação de conteúdos.

3 — A captação, gravação, armazenamento, partilha ou divulgação de imagem e som apenas pode ocorrer quando exista fundamento legítimo, finalidade determinada, necessidade comprovada e cumprimento dos procedimentos aplicáveis.

4 — As gravações não devem ser utilizadas para finalidades distintas das que justificaram a respetiva recolha e devem ser eliminadas, anonimizadas ou arquivadas de acordo com o prazo aplicável.

5 — É proibida a realização de capturas de ecrã, fotografias, gravações ou cópias de conteúdos que incluam dados pessoais, salvo quando tal seja necessário, autorizado e realizado nos termos das regras aplicáveis.

6 — A publicação de imagens, som ou outros conteúdos que permitam identificar pessoas depende de fundamento jurídico adequado e do cumprimento das regras institucionais sobre informação aos titulares, autorizações, conservação e divulgação.

7 — As regras específicas sobre gravação de aulas, conservação de conteúdos pedagógicos, videoconferência, avaliação digital e plataformas de ensino são definidas em procedimento ou norma técnica complementar.

6 — Publicação de classificações e pautas de avaliação

1 — A publicitação de classificações e pautas de avaliação, sumários e listas de frequência deve ocorrer preferencialmente em áreas reservadas do portal académico ou da plataforma de gestão da aprendizagem (*LMS*), com controlo de autenticação individual.

2 — Quando seja legal ou regulamentarmente admissível a publicação de listas em suporte físico ou em áreas de consulta coletiva, devem ser adotadas medidas de minimização e pseudonimização, designadamente a identificação dos estudantes exclusivamente através do respetivo número de estudante (número mecanográfico), suprimindo o nome completo, o número de identificação civil, o NIF ou quaisquer outros dados suscetíveis de identificação direta.

3 — É estritamente vedada a publicação, afixação ou divulgação pública de pautas e resultados de avaliação associados a:

a) Circunstâncias pessoais ou motivos justificativos de faltas;

b) Estatutos especiais, designadamente de trabalhador-estudante ou necessidades educativas específicas;

c) Situação de regularização de propinas, taxas ou emolumentos.

4 — O cruzamento interno dos dados referidos no número anterior com o aproveitamento escolar é reservado exclusivamente aos órgãos, serviços de apoio psicopedagógico, ação social e docentes expressamente autorizados, na estrita medida do necessário para:

a) A monitorização do insucesso e prevenção do abandono escolar;

b) A aplicação de planos pedagógicos individualizados ou adaptações curriculares;

c) O acompanhamento tutorial e a concessão de apoios institucionais.

Despacho n.º 11473/2026

5 — O tratamento previsto no número anterior rege-se pelo princípio da necessidade e confidencialidade, mediante perfis de acesso restritos no sistema de gestão académica, sem prejuízo do registo das operações de tratamento efetuadas.

7 — Utilização responsável de sistemas de inteligência artificial (IA)

1 — É expressamente proibido inserir, carregar ou submeter dados pessoais, categorias especiais de dados, informação confidencial, dados de processos disciplinares, dados de saúde ou trabalhos e elementos de avaliação de estudantes em plataformas ou ferramentas públicas de inteligência artificial generativa não homologadas institucionalmente.

2 — A utilização de sistemas de IA para apoio a processos de decisão académica, administrativa ou de triagem que afetem os direitos dos titulares depende de validação prévia pelo EPD e pelos serviços de TIC, sendo vedada a sujeição a decisões baseadas exclusivamente no tratamento automatizado sem intervenção humana significativa.

8 — Investigação científica, projetos de I&D e ciência aberta

1 — As atividades de investigação científica, teses, dissertações e projetos de I&D desenvolvidos na ou pela instituição que envolvam dados pessoais devem reger-se pelos princípios da licitude, minimização, limitação da conservação e confidencialidade.

2 — Antes do início da recolha de dados junto de participantes humanos, os investigadores e docentes responsáveis devem:

a) Submeter o protocolo do projeto à Comissão de Ética competente e, quando aplicável, proceder à triagem prévia de proteção de dados;

b) Disponibilizar aos participantes um documento claro de consentimento informado ou nota informativa detalhando as finalidades, a duração do estudo, a equipa de investigação e o tratamento conferido aos dados recolhidos;

c) Implementar, desde a conceção (*privacy by design*), mecanismos de anonimização ou pseudonimização precoce dos registos.

3 — As categorias especiais de dados recolhidas em contexto de investigação (nomeadamente saúde, dados genéticos, biométricos ou dados relativos a menores) devem ser mantidas

4 — cifradas e segregadas de qualquer tabela de correspondência identificativa (*chave de decifra*), mantendo-se esta sob custódia restrita do investigador principal.

5 — No quadro de iniciativas de Ciência Aberta (*Open Science*) e partilha de repositórios de dados (*Open Data*), apenas podem ser disponibilizados conjuntos de dados efetiva e irreversivelmente anonimizados, assegurando-se que não existe risco residual de reidentificação por via de cruzamento de variáveis com bases de dados externas.

9 — Direitos dos titulares e pedidos de informação

1 — Os pedidos de informação, acesso, retificação, apagamento, limitação, portabilidade, oposição ou não sujeição a decisões automatizadas devem ser encaminhados, sem demora, através do canal institucional definido para o exercício dos direitos dos titulares.

2 — Os serviços e Unidades Orgânicas devem colaborar atempadamente com o EPD e com os serviços competentes na identificação da informação necessária para responder aos pedidos dos titulares.

3 — Não devem ser prestadas respostas informais, parciais ou não verificadas a pedidos de titulares quando a matéria exija apreciação nos termos do procedimento institucional aplicável.

4 — Os utilizadores devem assegurar que os dados sob a sua responsabilidade são mantidos tão exatos e atualizados quanto necessário para as finalidades do tratamento.

Despacho n.º 11473/2026

5 — Sempre que seja solicitada retificação, apagamento, limitação ou comunicação a destinatários, devem ser seguidas as instruções emitidas no âmbito do procedimento de gestão dos direitos dos titulares.

6 — A eliminação, destruição ou expurgo de documentos e suportes que contenham dados pessoais, em formato físico ou digital, está condicionada ao estrito cumprimento das tabelas de seleção e prazos de conservação previstos na legislação e regulamentação arquivística. O exercício do direito ao apagamento (*direito a ser esquecido*) ou de limitação do tratamento não prejudica a conservação de registos biográficos, termos de avaliação, pautas finais, certidões e demais registos de arquivo de interesse público ou de conservação permanente previstos na lei, nos termos do n.º 3 do artigo 17.º do RGPD.

10 — Registo e avaliação de tratamentos

1 — As Unidades Orgânicas e serviços devem colaborar na identificação, atualização e validação das atividades de tratamento que desenvolvam para efeitos do Registo das Atividades de Tratamento da UPCoimbra.

2 — Qualquer novo projeto, sistema, plataforma, integração, contratação, alteração substancial ou iniciativa que envolva tratamento de dados pessoais deve ser comunicado atempadamente aos intervenientes definidos no procedimento institucional de triagem prévia.

3 — A triagem prévia deve permitir determinar, designadamente, a necessidade de atualização do Registo das Atividades de Tratamento, a realização de avaliação de impacto sobre a proteção de dados, a definição de medidas de segurança, a intervenção do EPD e a aprovação de condições específicas de utilização.

4 — Sempre que um tratamento seja suscetível de implicar elevado risco para os direitos e liberdades das pessoas singulares, deve ser promovida a realização de Avaliação de Impacto sobre a Proteção de Dados antes do início do tratamento ou da alteração relevante, nos termos da legislação e do procedimento aplicável.

5 — Nenhum projeto ou alteração sujeito a avaliação prévia deve entrar em funcionamento sem que sejam adotadas as medidas e decisões definidas no respetivo processo.

11 — Fornecedores, terceiros e subcontratantes

1 — A contratação, renovação ou alteração de serviços que impliquem tratamento de dados pessoais, acesso a sistemas, alojamento de informação ou utilização de plataformas digitais deve ser comunicada atempadamente aos serviços competentes, de acordo com o procedimento institucional de gestão de fornecedores e terceiros.

2 — Os trabalhadores e colaboradores não devem contratar, utilizar ou disponibilizar a terceiros serviços que envolvam dados pessoais da UPCoimbra sem observância dos procedimentos de contratação, avaliação de risco e validação aplicáveis.

3 — Os contratos, ajustes, protocolos ou outros instrumentos que envolvam tratamento de dados pessoais por terceiros devem incluir as cláusulas de proteção de dados, segurança, confidencialidade, reporte de incidentes, devolução ou eliminação de dados e demais garantias aplicáveis.

4 — A avaliação de terceiros deve ser proporcional à natureza e criticidade do serviço, às categorias de dados tratadas, ao nível de acesso, à utilização de subcontratantes, à localização do tratamento e à dependência institucional do serviço.

5 — Os serviços utilizadores devem comunicar qualquer alteração relevante na prestação, nos acessos, nos subcontratantes, nos fluxos de dados ou nas condições de segurança de um fornecedor ou terceiro.

Despacho n.º 11473/2026

12 — Associações de Estudantes, núcleos e entidades autónomas

As Associações de Estudantes, os núcleos autónomos de curso, as secções culturais ou desportivas e as estruturas académicas congéneres constituem entidades terceiras e responsáveis pelo tratamento autónomos quanto às atividades que promovam em nome próprio. É expressamente vedada a cedência, extração ou partilha em massa de dados de contacto, dados académicos ou identificadores de estudantes ou trabalhadores a favor destas entidades sem prévia base de licitude, protocolo institucional homologado e parecer favorável do EPD. As comunicações de manifesto interesse institucional ou associativo articuladas com a Associação de Estudantes devem ser veiculadas através dos canais de difusão oficiais da instituição, evitando a transmissão direta de bases de dados.

13 — Transferências internacionais de dados para fora do EEE

1 — O envio, partilha, alojamento ou disponibilização de acesso a dados pessoais geridos pela UPCoimbra para entidades, servidores ou plataformas localizadas em países terceiros (fora da União Europeia/Espaço Económico Europeu) depende da prévia verificação das garantias adequadas nos termos do RGPD.

2 — A utilização de serviços ou fornecedores sediados em países sem decisão de adequação da Comissão Europeia exige a celebração de Cláusulas Contratuais — Tipo (SCC) aprovadas pela Comissão Europeia e a realização de uma avaliação de impacto da transferência (TIA), em articulação com o EPD.

3 — No âmbito de programas de mobilidade académica internacional (e.g., programas de cooperação para além do EEE) ou projetos com consórcios internacionais de investigação, a transmissão de dados de estudantes, docentes ou investigadores deve limitar-se ao estritamente necessário à execução do respetivo protocolo ou mobilidade, informando-se expressamente o titular sobre os eventuais riscos decorrentes do nível de proteção do país de destino.

14 — Incidentes e violações de dados pessoais

1 — Qualquer pessoa que tenha conhecimento ou suspeita de uma ocorrência suscetível de afetar dados pessoais deve comunicá-la de imediato (preferencialmente nas primeiras horas após a deteção) através do canal institucional de reporte de incidentes. A urgência da comunicação interna é determinante para habilitar a instituição a cumprir a obrigação legal inultrapassável de notificar a autoridade de controlo (CNPD) no prazo máximo de 72 horas após ter tido conhecimento da violação, sempre que exista risco para os direitos e liberdades das pessoas singulares (artigo 33.º do RGPD). Qualquer demora injustificada no reporte interno compromete a avaliação atempada do incidente e a adoção de medidas urgentes de mitigação.

2 — Constituem exemplos de ocorrências suscetíveis de reporte a perda ou furto de equipamento, envio de informação para destinatário errado, acesso indevido, divulgação não autorizada, comprometimento de conta, *malware*, *phishing*, indisponibilidade de sistema, eliminação acidental de informação, falha de cópias de segurança ou utilização não autorizada de uma plataforma.

3 — A comunicação deve incluir, sempre que disponível, informação sobre a data e hora da ocorrência, os sistemas ou dados envolvidos, os titulares potencialmente afetados, as medidas já adotadas e os elementos que permitam apoiar a avaliação da situação.

4 — A identificação de uma ocorrência não exige que o comunicante determine se existe violação de dados pessoais ou se é necessária notificação à Comissão Nacional de Proteção de Dados. Essa apreciação é efetuada no âmbito do procedimento institucional de gestão e triagem de incidentes.

5 — A gestão de incidentes deve assegurar, de forma articulada, a deteção, registo, classificação, contenção, investigação, recuperação, avaliação de impacto sobre dados pessoais, decisão sobre comunicações e notificações aplicáveis, documentação e análise posterior.

6 — O procedimento de gestão de incidentes deve assegurar a articulação atempada entre o EPD, os serviços responsáveis pelas tecnologias de informação e comunicação, o Responsável de Cibersegurança, as Unidades Orgânicas e os demais serviços cuja intervenção seja necessária.

Despacho n.º 11473/2026

7 — Os utilizadores devem preservar, sempre que possível e sem colocar em risco a segurança, os elementos necessários à análise da ocorrência e cumprir as instruções transmitidas pelos responsáveis pela resposta ao incidente.

15 — Documentação, evidências e formação

1 — As políticas, normas técnicas, procedimentos, instruções operacionais, formulários, registos, relatórios, atas, avaliações e evidências associados à proteção de dados devem ser conservados e geridos de acordo com as regras institucionais aplicáveis.

2 — A existência de uma política ou procedimento não dispensa a necessidade de produzir evidência da respetiva execução, designadamente através de registos de formação, revisões

3 — de acessos, avaliações de fornecedores, incidentes tratados, atualizações de registos de tratamento, avaliações de impacto e testes de continuidade.

4 — Cada instrumento documental deve identificar, quando aplicável, a entidade responsável, o responsável pela elaboração ou atualização, a entidade competente para aprovação, a versão, a data de entrada em vigor, a periodicidade de revisão e a relação com outros instrumentos.

5 — As Unidades Orgânicas e serviços devem divulgar as orientações relevantes aos respetivos trabalhadores, colaboradores, docentes, investigadores, estudantes e outros utilizadores abrangidos.

6 — A UPCoimbra promove ações regulares de formação e sensibilização diferenciadas em função dos perfis de utilizador, das responsabilidades exercidas, da natureza dos dados tratados e dos riscos identificados.

16 — Disposição final

1 — As dúvidas de aplicação do presente Manual são apreciadas nos termos do Código de Conduta e dos procedimentos institucionais aplicáveis, sem prejuízo da consulta ao EPD e aos serviços competentes.

2 — O presente Manual deve ser divulgado em formato acessível à comunidade académica e integrado nos processos de acolhimento, formação e sensibilização dos utilizadores dos recursos e serviços da UPCoimbra.

320042116

Despacho n.º 11473/2026