Politécnico de Coimbra

Código de Conduta e Boas Práticas na Proteção de Dados Pessoais no Instituto Politécnico de Coimbra

CÓDIGO DE CONDUTA E BOAS PRÁTICAS NA PROTEÇÃO DE DADOS PESSOAIS NO INSTITUTO POLITÉCNICO DE COIMBRA

O Instituto Politécnico 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 o Politécnico 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 do Instituto Politécnico 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 do Instituto Politécnico de Coimbra (IPC), 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 no IPC, nomeadamente através das suas unidades orgânicas e dos Serviços de Ação Social (SASIPC).

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. "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;

b) "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;

c) "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;

d) "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;

e) "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;

f) "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;

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

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

i) "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;

j) "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, o IPC 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.

Artigo 5.º

Princípios e regras gerais

1 - O tratamento de dados pessoais no IPC 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 o IPC 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 ao IPC o dever de comprovar o cumprimento dos princípios elencados nas alíneas anteriores.

2 - O IPC 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 do IPC, 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.

Artigo 6.º

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

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 as plataformas Inforgestão, Infordocente, Inforestudante, Moodle, cloud.ipc.pt, forms.ipc.pt, ou outras que inequivocamente cumpram com o preceituado no RGPD quanto à privacidade de dados e que sejam validadas pelo IPC, nomeadamente:

i) As definições de segurança devem limitar o acesso apenas a utilizadores pré-definidos e autorizados pela direção da respetiva Unidade/Serviço;

ii) Cada utilizador apenas tem acesso aos dados de que necessita para as sessões a realizar em ambiente digital ou a distância.

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 o IPC esteja sujeito;

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 o IPC;

e) Tratamento necessário para prossecução dos interesses legítimos do IPC 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.

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 ter várias formas: escrita, oral ou através da validação numa plataforma eletrónica licenciada.

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.

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, o IPC, 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;

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.

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 no IPC.

2 - O tratamento de dados pessoais sensíveis no IPC, 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, o IPC 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;

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 ao IPC;

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 - Qualquer outro reporte de informação do IPC que implique a divulgação de dados pessoais relativos a docentes, investigadores, corpo técnico, outros colaboradores e estudantes, em ambiente de intranet, internet ou noutros circuitos de comunicação, que não decorra de uma obrigação jurídica, tem de ser previamente visado pelo EPD.

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 o IPC esteja sujeito.

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, o IPC trata os dados pessoais de um conjunto alargado de titulares, incluindo, nomeadamente:

a) Estudantes;

b) Trabalhadores;

c) Bolseiros;

d) Investigadores;

e) Candidatos;

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

g) Utentes ou beneficiários de apoios concedidos pelo IPC;

h) Colaboradores que atuem no âmbito de projetos, centros ou unidades de investigação do IPC;

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

j) Titulares de contactos para partilha e divulgação de eventos no IPC.

Artigo 13.º

Direitos

Ao titular dos dados pessoais tratados pelo IPC 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.

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 o IPC 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;

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 - O IPC 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 ao IPC 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) O IPC 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 do IPC prevalecem sobre os seus.

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, o IPC 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 ao IPC, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o IPC 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 o IPC;

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.

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 o IPC, através do endereço de correio eletrónico epd@ipc.pt.

2 - O IPC 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, o IPC 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 - O responsável pelo tratamento dos dados a que se reporta o presente Código de Conduta é sempre o IPC e quem a representa.

2 - Os trabalhadores que, no desempenho das suas funções, estejam nomeados ou equiparados a responsáveis pelo tratamento, ou sejam intervenientes no tratamento dos dados, apesar de agirem por conta do órgão ou do serviço, são responsabilizados por eventuais incumprimentos, quando tal resultar inequivocamente da sua ação.

Artigo 23.º

Contratos com terceiros

1 - Toda a contratação com terceiros que implique o acesso a dados pessoais sob a responsabilidade do IPC é precedida de uma análise das garantias de cumprimento dos normativos legais aplicáveis à proteção de dados pessoais e da implementação de medidas de segurança por parte dos referidos terceiros.

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 do IPC, 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 ao IPC e destrói todas as cópias dos mesmos, salvo se, comprovadamente, existir uma obrigação legal ou contratual que exija a sua conservação.

4 - Quanto aos contratos já celebrados, o IPC procede, no prazo de 30 dias a contar da entrada em vigor do presente Código de conduta, ao inventário dos terceiros que têm acesso direto ou indireto aos dados pessoais sob a sua responsabilidade, à revisão dos contratos e à sua alteração, quando tal se revele necessário para assegurar a sua conformidade com os normativos legais aplicáveis à proteção de dados pessoais.

Artigo 24.º

Subcontratantes

1 - Quando o IPC 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 ao IPC 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 pelo IPC 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 do IPC.

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

Artigo 25.º

Registo das atividades de tratamento

1 - O IPC mantém registos internos das atividades de tratamento sob a sua responsabilidade, deles constando os elementos previstos no n.º 1 do artigo 30.º RGPD, designadamente o tipo de dados tratados, as finalidades do tratamento, a descrição das categorias de titulares de dados e dos destinatários dos mesmos, as medidas de segurança e o prazo de conservação.

2 - Nos casos em que os sistemas informáticos usados no IPC 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.

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 do IPC 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 no IPC.

Artigo 27.º

Segurança do tratamento

1 - O IPC 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;

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 no IPC 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 automatizados está dependente de palavras-passe robustas, individuais e intransmissíveis, conforme previsto no Anexo 1 e no Regulamento de Utilização, Segurança e Gestão dos Recursos de Tecnologias da Informação e Comunicação do IPC.

6 - A transmissão de ficheiros contendo dados pessoais através do sistema de correio eletrónico institucional está dispensada de cifragem, encriptação ou proteção por código, desde que a comunicação ocorra exclusivamente entre caixas de correio oficiais da instituição e no âmbito da rede interna segura.

7 - Para efeitos do disposto no número anterior, assume-se que a infraestrutura tecnológica interna assegura, por si mesma, os níveis necessários de confidencialidade e integridade dos dados em circulação.

8 - A dispensa prevista no n.º 6 não se aplica, sendo estritamente obrigatória, a cifragem do ficheiro e a transmissão da respetiva chave de acesso por canal distinto, sempre que:

a) O destinatário seja uma entidade externa ou utilize um domínio de correio eletrónico não institucional;

b) A mensagem contenha categorias especiais de dados (dados de saúde, filiação sindical, dados biométricos ou registos criminais/contraordenacionais), cuja sensibilidade exija proteção acrescida na transmissão, independentemente do canal utilizado.

Artigo 28.º

Procedimento para a divulgação de dados pessoais no IPC

1 - O IPC, 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 - A divulgação de dados pessoais relativos a docentes, investigadores, corpo técnico, outros colaboradores e estudantes, em ambiente de intranet, internet ou noutros circuitos de comunicação, que não decorra explicitamente de uma obrigação jurídica a que o IPC esteja sujeito,

deve ser sempre previamente aprovada pelo EPD, através do endereço de correio eletrónico epd@ipc.pt.

Artigo 29.º

Procedimento para a elaboração de cadernos eleitorais

1 - Os cadernos eleitorais para realização de atos eleitorais no IPC 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 dígito (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).

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 - O IPC 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.

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 do Presidente do IPC, 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 ao IPC, não lhe sendo atribuídas funções que possam culminar num conflito de interesses.

3 - O IPC assegura que o EPD é envolvido, de forma adequada e em tempo útil, em todas as questões relacionadas com a proteção de dados pessoais, fornecendo-lhe os recursos necessários ao desempenho dessas funções e à manutenção dos seus conhecimentos e dando-lhe acesso aos dados pessoais e às operações de tratamento.

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) Assegurar a realização de auditorias periódicas e não programadas;

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 do IPC relativamente à proteção de dados pessoais;

e) Cooperar com a CNPD;

f) Informar e aconselhar as unidades orgânicas e serviços do IPC 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 do IPC, 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 e serviços do IPC cooperam com o EPD, respondendo às suas solicitações deste, no prazo por este determinado ou, na ausência 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 - O IPC, 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 - O IPC 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 do IPC, 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 do Presidente do IPC, 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

Entrada em vigor

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 no Instituto Politécnico de Coimbra, elencam-se no presente anexo as boas práticas a implementar pelos diversos intervenientes nos processos de tratamento de dados pessoais realizados no IPC.

1 – Presidente do IPC

Promover, em articulação com o Encarregado de Proteção de Dados do IPC (EPD), com o responsável da área das tecnologias da informação e comunicação do IPC e com os Diretores/Presidentes, diretrizes da política de acessos comuns, incluindo os critérios de atribuição e revogação dos mesmos, para cada perfil funcional

2 – Presidentes/Diretores de Unidades Orgânicas, Administrador do IPC e Administrador dos SASIPC

a) Definir políticas de acesso comum compatíveis com as diretrizes existentes.
b) Promover a formação permanente e contínua dos colaboradores sobre proteção de dados e procedimentos de segurança da informação.
c) Definir e sensibilizar os colaboradores para o seu papel e responsabilidades em matéria de segurança da informação, nomeadamente ao nível da proteção dos acessos e das credenciais que lhes são atribuídos.
d) Definir, em articulação com o EPD, políticas de acesso específicas, quando tal se afigure necessário para complementar ou ajustar a política de acessos comuns a algum contexto particular da unidade/serviço.
e) Assegurar os meios para reagir adequada e atempadamente em caso de violação dos dados.
f) Definir a política dos sistemas de videovigilância e garantir ao EPD o acesso aos sistemas de controlo e gravação das imagens.

3 - Técnicos de sistemas

a) Usar preferencialmente equipamentos que assegurem a encriptação dos discos rígidos e outros suportes de armazenamento de ficheiros.

b) Fazer cópias de segurança (*backups*), contra o risco de perda acidental.

c) Guardar as cópias de segurança em localização física distinta da localização dos sistemas. Definir e implementar políticas de *disaster recovery*.

d) Proteger os sistemas contra software malicioso (vírus, *malware, phishing, ransomeware, adware*, etc.).

e) Proteger os sistemas por *firewall* contra acessos indevidos.

f) Restringir e controlar os acessos ao *datacenter*.

g) Restringir e controlar o acesso físico aos equipamentos (utilização de cadeados, por exemplo).

h) Definir as medidas que os utilizadores devem adotar para proteção dos acessos e das credenciais que lhes são atribuídas.

i) Efetuar o acesso remoto aos Recursos de TIC do IPC apenas através de ligações seguras por VPN ou equivalente.

j) Colaborar na definição e implementar a política de acessos, incluindo a atribuição e revogação dos mesmos, para cada perfil funcional, em articulação com o EPD.

k) Garantir que as credenciais de autenticação (utilizador/palavra-passe) são únicas.

l) Sempre que as passwords sejam guardadas em ficheiros, deve ser usado *software* que assegure a respetiva encriptação.

m) Garantir a seguinte composição das *passwords* (com padrão de autenticação do tipo 2FA): a palavra-passe dos administradores deve ter no mínimo 13 caracteres e ser complexa; a sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a ... z), letras maiúsculas (A ... Z), números (0 ... 9) e caracteres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : “ ; ‘ < > ? , . /).

n) Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem carácter de "espaço".

4 - Trabalhadores e demais colaboradores

4.1 - Deveres procedimentais

4.1.1 - Gerais

a) Não tratar dados pessoais fora das situações legal e regulamentarmente previstas.
b) Tratar os dados exclusivamente para as finalidades para que foram recolhidos, no âmbito das suas funções.
c) Ter especial cuidado no tratamento de documentos com informações críticas, como é o caso de dados médicos, de registos criminais ou de menores.
d) Realizar avaliações de impacto sobre a proteção de dados (AIPD), de acordo com o procedimento do SIGQ do IPC, para identificar e mitigar riscos associados ao tratamento de dados pessoais em novos projetos.
e) Fazer o registo das operações de tratamento de dados de acordo com o procedimento do SIGQ do IPC, definindo procedimentos para todo o ciclo de vida dos dados.
f) Sempre que necessário, aplicar técnicas de anonimização ou pseudonimização robustas e manter registos detalhados dos métodos e justificações para a sua escolha.
g) Sempre que os dados forem anonimizados, certificar-se de que os mesmos não podem ser revertidos ou combinados.
h) Eliminar os dados após o tratamento ou após os prazos de conservação legalmente definidos, consoante os casos.
i) Dar conhecimento imediato ao superior hierárquico, da existência de acesso a dados pessoais não necessários ao desempenho das suas funções, em virtude, designadamente, de lapso na definição e atribuição do respetivo perfil. Informar o EPD, por correio eletrónico (epd@ipc.pt), sobre qualquer violação de dados pessoais, efetiva ou potencial, de que tome conhecimento.
j) Não guardar dados sensíveis localmente no computador.
k) Não utilizar o verso de fotocópias com dados pessoais como folhas de rascunho ou com qualquer outra finalidade.
l) Guardar todas as pastas, *dossiers*, processos e documentos com dados pessoais em local seguro e de acesso condicionado (armários com portas fechadas à chave, por exemplo).

m) Retirar da mesa de trabalho qualquer documento ou processo que contenha dados pessoais imediatamente após a sua utilização.

n) Manter o posto de trabalho arrumado e cumprir o princípio de "*clean desk*".

o) Não deixar documentos soltos em cima das secretárias, arquivá-los numa pasta e colocar no armário ou numa gaveta com chave.

p) Limitar ao estritamente necessário as impressões e/ou cópias de documentos que contenham dados pessoais.

q) Recolher as impressões, fotocópias ou digitalizações da impressora de rede o mais rapidamente possível após o seu processamento, de forma a evitar que sejam acedidas por terceiros.

r) Destruir de forma definitiva os documentos que contenham dados pessoais que não seja necessário arquivar, garantindo que não possam ser recuperados.

s) Transportar documentos que contenham dados pessoais de forma devidamente protegida, utilizando um envelope apropriado para o efeito e explicitamente identificado como "confidencial".

t) Não retirar das instalações do IPC qualquer documento ou processo que contenha dados pessoais sem estar previamente e devidamente autorizado para o efeito.

u) Não criar cópias ou arquivos que contenham dados pessoais sem autorização expressa. Não tratar (incluindo aceder) dados pessoais sem estar para isso autorizado.

v) Não tratar dados pessoais sem as devidas medidas de segurança.

w) Não divulgar dados pessoais a terceiros, salvo a outros trabalhadores do IPC e só dentro do estritamente necessário ao exercício de funções e para as finalidades autorizadas.

x) Recolher apenas os dados pessoais que sejam estritamente necessários para o exercício da respetiva atividade profissional e observando sempre os procedimentos em vigor.

y) Guardar sigilo sobre os dados a que tenham acesso no exercício das suas funções.

z) Abster-se de, por qualquer modo, aceder a dados pessoais fora do exercício de funções.

4.1.2 - Dados de identificação

a) Não tratar dados pessoais dos estudantes ou dos trabalhadores do IPC fora das situações previstas no presente regulamento interno e outras regras que venham a ser aprovadas pelo IPC.

b) Esta proibição inclui nome, morada, contactos, números de identificação, características pessoais, resultados escolares e dados de saúde, exceto quando tal seja necessário para o desenvolvimento de atividades educativas do IPC, para o cumprimento de obrigações legais pelo IPC, e estiver autorizado pelo IPC e/ou o pelos titulares dos dados.
c) Tratar os dados exclusivamente para as finalidades para que foram recolhidos.
d) Eliminar os dados pessoais após o tratamento, ou após os prazos de conservação legalmente definidos.

4.1.3 - Captação de imagens e som

a) Não recolher imagens ou som, por meio de fotografia, vídeo ou gravação de som, em qualquer contexto, designadamente aulas, avaliações, visitas de estudo, afixação de pautas, listas de alunos, horários, eventos institucionais ou reuniões de trabalho, salvo se estiverem verificados os seguintes requisitos: imprescindibilidade para o desenvolvimento de atividades enquadradas na missão e fins do IPC devidamente fundamentada por despacho do Presidente do IPC e instruída com parecer favorável do EPD (ou autorização dos órgãos competentes); ou consentimento informado prévio, livre, específico e esclarecido de todos os titulares dos dados a recolher e tratar, ou, tratando-se de menores, dos respetivos representantes legais.
b) Não fazer capturas de ecrã ou tirar fotografias de ecrãs que contenham dados pessoais.
c) As imagens ou sons recolhidos terão apenas o tratamento para que foram captadas e, após tal tratamento, serão eliminadas exceto se o seu arquivo tiver sido autorizado. Não publicar imagens ou som de terceiros em sítios da Internet ou nas redes sociais, sem que tal esteja devida e previamente autorizado pelos titulares dos dados em causa.

4.2 - Cuidados ao nível dos sistemas informáticos e autenticações

4.2.1 - No posto de trabalho e armazenamento

a) Bloquear o computador sempre que se ausentar do seu posto de trabalho, utilizando obrigatoriamente a combinação de teclas (*Windows*+L), e desligá-lo no final do dia de trabalho.
b) Proteger os ficheiros de trabalho digitais que contenham dados pessoais com passwords específicas para abertura e edição.

c) Utilizar sempre a rede informática institucional para a criação das pastas e ficheiros de trabalho, evitando a utilização de pastas e discos locais do computador.

d) Utilizar as ferramentas recomendadas pela instituição para encriptar dados sensíveis tanto em repouso (armazenados) quanto em trânsito (enviados pela rede).

e) Não utilizar discos externos e/ou *pens* USB para o trabalho regular. Sempre que o transporte de dados em suportes amovíveis for estritamente necessário, garantir que o mesmo é feito de modo seguro (por exemplo, com *pens* encriptadas). Não instalar *software* não autorizado em qualquer computador ou outro dispositivo da instituição.

4.2.2 - No correio eletrónico (*e-mail*)

a) Utilizar o *e-mail* de forma prudente e ponderada.

b) Não partilhar ou conceder acesso a terceiros ao correio eletrónico utilizado para fins profissionais. Usar o endereço institucional apenas para assuntos profissionais.

c) Não usar endereço de *e-mail* pessoal para transmitir ou receber informação da organização.

d) Não utilizar dispositivos pessoais partilhados para aceder ao endereço institucional.

e) Verificar sempre com rigor os endereços dos destinatários antes do envio, garantindo que estes devem efetivamente ter acesso à informação.

f) Assegurar que os ficheiros enviados em anexo contêm apenas e exclusivamente os dados pessoais que se pretendam comunicar.

g) Efetuar o envio de correio eletrónico de âmbito geral ou massivo (ex.: *newsletters*, convocatórias, comunicados, informações de carácter geral) para múltiplos destinatários utilizando obrigatoriamente o campo Bcc (*Blind carbon copy*), por forma a ocultar e não expor os endereços dos destinatários.

h) Encriptar com código (ao qual só o destinatário legítimo tenha acesso) ou proteger com password os ficheiros com dados pessoais enviados por correio eletrónico.

i) Não enviar *passwords*, credenciais de acesso ou outros dados pessoais em mensagens de correio eletrónico (em especial em resposta a *e-mails* suspeitos de "*phishing*").

j) Caso receba uma mensagem por engano e não seja o destinatário legítimo da mesma, não utilizar o seu conteúdo, proceder à sua eliminação imediata e notificar o remetente sobre o facto.

k) Abrir apenas as mensagens de origem fidedigna e que não indiciem ser *phishing* ou *malware*.

l) Não executar anexos ou seguir ligações em mensagens de correio eletrónico com origem desconhecida.

m) É expressamente proibido abrir anexos que tenham extensões executáveis (tais como: .exe, .bat, .com, .dll) vindos de fontes não validadas.

n) Não dar seguimento a mensagens do tipo "correntes", devendo eliminar de imediato todo o correio eletrónico que se enquadre nessa categoria.

o) Manter-se alerta e desconfiar sistematicamente de mensagens de correio eletrónico caso o endereço ou telefone do remetente não seja conhecido, ou se a mensagem apresentar erros gramaticais e ortográficos invulgares.

4.2.3 - Nas passwords

a) Utilizar passwords de acesso e cuidar que terceiros não visualizam o *log-on*.

b) Não partilhar e manter totalmente protegidas e confidenciais as credenciais, *passwords* e os códigos de acesso às instalações e aos Recursos de TIC do IPC, não os deixando em locais visíveis ou de fácil acesso.

c) Alterar as *passwords* recebidas de forma automática por outras com grau de complexidade elevado.

d) Garantir que as *passwords* de uso geral possuem um comprimento mínimo de 9 caracteres (em consonância com as regras de segurança digital), incluindo a combinação de letras maiúsculas, letras minúsculas, algarismos e caracteres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : “ ; ‘ < > ? , . /).

4.3 - No atendimento telefónico

a) Não fornecer qualquer informação com dados pessoais por telefone a interlocutores externos.

b) Caso sejam solicitados dados pessoais do exterior, estes apenas devem ser transmitidos nas situações legalmente permitidas e após a receção de um pedido formalizado por escrito.

c) Não transmitir informações pessoais sobre os colegas de trabalho a terceiros (incluindo sobre a sua localização exata ou o motivo detalhado da sua ausência do edifício), limitando-se apenas a informar sobre a respetiva disponibilidade. No caso de indisponibilidade, deve ser solicitado que o interlocutor deixe recado.

d) No ambiente interno da Instituição, os colaboradores apenas devem transmitir dados pessoais por telefone no estrito cumprimento das suas funções, certificando-se previamente de que o interlocutor interno tem perfil e autorização para receber essa informação, e assegurando sempre a total confidencialidade da conversa telefónica de modo que esta não seja audível por terceiros não autorizados.

Ficha Técnica

Título

Código de Conduta e Boas Práticas na Proteção de Dados Pessoais no IPC

Emissor

Pró-Presidente para a área de Modernização e Reestruturação Normativa e Jurídica

Versão 01
Editado em 02.07.2026

Aprovado por

Data de Aprovação

www.ipc.pt
ipc@ipc.pt
qualidade@ipc.pt