DIÁRIO DA REPÚBLICA

2.ª série
N.º 210
29-10-2024

UNIVERSIDADE DE COIMBRA

Regulamento n.º 1243/2024

Sumário: Aprova o Regulamento para a utilização de sistemas de videovigilância na Universidade de Coimbra.

Nos termos da alínea x) do artigo 49.º dos Estatutos da Universidade de Coimbra, homologados pelo Despacho Normativo n.º 43/2008, de 1 de setembro, alterados e republicados pelo Despacho Normativo n.º 11/2024, de 15 de abril, ouvidos o Senado e a Comissão da Trabalhadores e após consulta pública, nos termos do disposto no n.º 3 do artigo 110.º da Lei n.º 62/2007, de 10 de setembro, que aprova o Regime Jurídico das Instituições de Ensino Superior, e no n.º 1 do artigo 101.º do Código do Procedimento Administrativo, aprovado pelo Decreto-Lei n.º 4/2015, de 7 de janeiro, na sua redação atual, aprovo Regulamento para a utilização de sistemas de videovigilância na Universidade de Coimbra, em anexo.

7 de outubro de 2024. — O Reitor, Amílcar Falcão.

ANEXO

Regulamento para a utilização de sistemas de videovigilância na Universidade de Coimbra

Preâmbulo

A proteção de dados pessoais merece consagração na ordem jurídica portuguesa desde a Lei n.º 67/98, de 26 de outubro, que transpôs a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dados pessoais e à livre circulação desses dados.

Contudo, apenas com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD), relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, aplicável a partir de 25 de maio de 2018, e com a respetiva Lei de execução nacional, a Lei n.º 58/2019, de 8 de agosto, se perspetivou o surgimento de uma regulamentação impressivamente marcada pelo conceito de dados pessoais como propriedade do respetivo titular. Neste conspecto, gozam os trabalhadores, estudantes e demais pessoas singulares que contactem com a Universidade de Coimbra (UC), nomeadamente através das suas Unidades e Serviços, incluindo os Serviços de Ação Social, de uma esfera de proteção efetiva, sendo-lhes concedido um poder no tratamento automatizado de dados.

O RGPD veio igualmente alterar o paradigma da intervenção da autoridade de controlo, passando de um regime de autorização prévia para a regra de autorresponsabilização e de autodisciplina no tratamento de dados pessoais. Cabe, assim, aos responsáveis pelo tratamento e aos subcontratantes o dever prévio de verificação do cumprimento do RGPD, dever este impulsionado pela obrigação, em determinados casos, de registo das atividades de tratamento, o qual deve ser disponibilizado à autoridade de controlo quando solicitado, nos termos previstos no artigo 30.º do RGPD.

Complementarmente, o artigo 19.º da Lei n.º 58/2019, de 8 de agosto, prevê as condições e os critérios para a delimitação do âmbito do tratamento de dados pessoais decorrentes dos sistemas de videovigilância.

É neste contexto de maior responsabilidade da Universidade de Coimbra e, também, de grande sofisticação tecnológica, caracterizada pela recolha de quantidades massivas de dados suscetíveis de revelar informações de natureza altamente pessoal, pelo armazenamento, conexão, transmissão e utilização de forma automatizada desses dados, sem que o respetivo titular de imediato os possa controlar ou mesmo disso se aperceber, que se impõe a aprovação e implementação de um regulamento que garanta, simultaneamente, o reconhecimento do direito fundamental à proteção de dados pessoais, à intimidade da vida privada de cada um, incluindo à sua imagem, enquanto parte visível de sentimen-

tos e emoções; e a concordância legal dos direitos em conflito, nomeadamente, a proteção dos dados pessoais e a privacidade das pessoas *versus* a segurança de pessoas e bens nos espaços da UC. Para tanto, as soluções preconizadas na presente regulamentação foram delineadas em consonância com a disciplina plasmada no RGPD e na referida Lei de execução nacional e com as diretrizes da Comissão Nacional de Proteção de Dados.

CAPÍTULO I

Disposições Gerais

Artigo 1.º

Objeto

O presente Regulamento estabelece os princípios, regras e procedimentos aplicáveis à autorização, instalação, utilização e acesso a Sistemas de Videovigilância (SVV), através da utilização de Circuitos Fechados de Televisão (CFTV), instalados nos espaços da Universidade de Coimbra (UC), englobando os espaços dos Serviços de Ação Social (SASUC), para tratamento de imagem e som, incluindo a sua recolha e gravação captação.

Artigo 2.º

Âmbito de aplicação

As disposições constantes do presente Regulamento são aplicáveis:

a) Aos SVV instalados em todos os espaços interiores e exteriores da UC, para os fins previstos no artigo seguinte;

b) Aos trabalhadores, estudantes e demais pessoas singulares que contactem com a UC, nomeadamente através das suas unidades orgânicas, outras unidades e serviços, incluindo os Serviços de Ação Social.

Artigo 3.º

Finalidade

1 — A UC utiliza os SVV exclusivamente para proteção de pessoas e bens, de modo a garantir:

a) A segurança dos trabalhadores, estudantes e demais pessoas singulares que com ela contactem;

b) A segurança dos edifícios, bens e informações que se encontrem nas suas instalações, ou aí estejam armazenados;

c) A prevenção da prática de factos qualificados pela lei como crimes em locais em que exista razoável risco da sua ocorrência.

2 — Os SVV não podem, em caso algum, ser utilizados para a vigilância e avaliação do desempenho dos trabalhadores ou para controlo da assiduidade.

Artigo 4.º

Definições e Abreviaturas

No presente Regulamento, são adotadas as seguintes definições e abreviaturas:

a) «AIPD» — Avaliação de Impacto sobre a Proteção de Dados, é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir riscos para os direitos e liberdades das pessoas decorrentes do tratamento de dados pessoais, avaliando-os e determinando as medidas necessárias para fazer face a esses riscos;

b) «CNPD» — Comissão Nacional de Proteção de Dados;

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

d) «CFTV» — Circuito Fechado de Televisão, do termo inglês *Closed Circuit TeleVision* (CCTV), é um sistema de televisionamento que distribui sinais provenientes de câmaras localizadas em locais específicos, para pontos de supervisão pré-determinados. Os sistemas de CFTV normalmente utilizam câmaras de vídeo, cabos, fibras óticas, transmissores/recetores sem-fio ou redes, processadores de vídeo, monitores e por último os gravadores;

e) «Dados biométricos» — Dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;

f) «Dados pessoais» — 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;

g) «Dados sensíveis» — Dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano, dados relacionados com a saúde, dados relativos à vida sexual ou orientação sexual da pessoa;

h) «EPD-UC» — Encarregado de Proteção de Dados da UC;

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

j) «Identificável» — A pessoa pode ser identificada quando se procede ao registo da imagem e/ou som da pessoa, mas também quando através de meios/recursos/outras informações utilizadas pela pessoa e identificados na imagem e/ou som;

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

l) «Responsável máximo de Unidade ou Serviço» — Órgão superior ou dirigente máximo de cada unidade ou serviço da UC, de acordo com a estrutura orgânica prevista nos Estatutos da Universidade, sendo que, para efeitos do presente Regulamento, são responsáveis máximos:

i) Na Reitoria, o Reitor;

ii) Nas Unidades Orgânicas, os respetivos Diretores;

iii) Nas Unidades de Extensão Cultural e de Apoio à Formação, os respetivos Diretores;

iv) Na Administração, o Administrador da UC;

v) Nos SASUC, o respetivo Administrador.

m) «Responsável pelo tratamento de dados» — A pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais;

n) «RGPD» — Regulamento Geral sobre a Proteção de Dados, Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE;

o) «Salas de Informática» — Os espaços da UC, com material elétrico, eletrónico, componentes ativos ou passivos de suporte ou proteção às infraestruturas de comunicação, informática e multimédia;

p) «SASUC» — Serviços de Ação Social da Universidade de Coimbra;

q) «SVV» — Sistemas de Videovigilância;

r) «Subcontratante» — A pessoa singular ou coletiva, que trate os dados pessoais por conta do responsável pelo tratamento;

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

t) «Tratamento de dados pessoais» — A operação ou o conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição (a simples monitorização, ainda que sem recurso a gravação, basta para constituir um tratamento de dados pessoais);

u) «Tratamento de categorias especiais de dados (dados sensíveis)» — A operação ou o conjunto de operações que envolve/m identificadores que revelem a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, saúde e genética, biometria, vida ou orientação sexual, condenações penais e infrações, aptidões intelectuais e profissionais, traços de personalidade ou desempenho profissional;

v) «UC» — Universidade de Coimbra.

CAPÍTULO II

Instalação de SVV

Artigo 5.º

Princípios Gerais

As unidades orgânicas, outras unidades e serviços da UC, incluindo os SASUC, e/ou o(s) subcontratante(s) responsáveis pela instalação e utilização dos SVV e tratamento de dados pessoais, devem assegurar o cumprimento, a todo o tempo, dos seguintes princípios:

a) Proporcionalidade, necessidade, idoneidade e adequação estrita aos fins da proteção de pessoas e bens, tendo em conta as circunstâncias concretas do local a proteger;

b) Otimização da gestão de equipamentos, objetivando-se a uniformização e centralização de sistemas, sem perda da operacionalidade de cada especificidade local;

c) Privacidade e direito à reserva da intimidade da vida privada e demais direitos de personalidade;

d) Legalidade, por força do qual as operações de tratamento de dados decorrem em conformidade com as normas previstas no RGPD e demais legislação aplicável;

e) Licitude, lealdade, transparência, equidade, limitação das finalidades, minimização dos dados e limitação da conservação, no âmbito do tratamento de dados pessoais.

SECÇÃO I

Implementação dos SVV

Artigo 6.º

Pedido de autorização

1 — A instalação de SVV num espaço da UC está sujeita a autorização do órgão competente em matéria de instalações e património.

2 — O pedido de autorização deve ser apresentado pelo Responsável Máximo de Unidade ou Serviço e instruído com a AIPD, na qual devem constar os seguintes elementos:

a) Justificação da necessidade de instalação do SVV;

b) Localização prevista para a(s) câmara(s) de videovigilância;

c) Área a abranger pela(s) câmara(s) de videovigilância;

d) Atividades desenvolvidas nas áreas indicadas na alínea anterior;

e) Meios adequados e proporcionais aos objetivos que se pretende alcançar;

f) Especificações técnicas e demais elementos necessários para a instrução do procedimento de aquisição de bens e serviços.

3 — A decisão de autorização, emitida no prazo máximo de 30 dias, é precedida de parecer do serviço competente em matéria de instalações e património, de consulta ao serviço competente em matéria de sistemas e infraestruturas de informação e de comunicação ao EDP-UC.

4 — Cabe ao/à requerente efetuar e acompanhar o pedido de aquisição de bens e serviços, observando as regras e procedimentos do serviço competente em matéria financeira.

5 — Após a adjudicação dos bens e serviços indicados no número anterior, deve o/a requerente promover reunião(iões) entre a empresa instaladora do SVV e os serviços competentes em matéria de instalações e património e de sistemas e infraestruturas de informação e comunicação da UC, com vista à apresentação da solução proposta, eventuais esclarecimentos, elaboração de planeamento de execução e indicação de interlocutores para o apoio técnico.

6 — Concluída a instalação, deve o/a requerente promover reunião(iões) entre a empresa instaladora do SVV, os serviços competentes em matéria de instalações e património da UC e de sistemas e infraestruturas de informação e comunicação da UC e o EPD-UC, com vista à elaboração de auto de receção e aprovação da entrada em funcionamento do SVV.

Artigo 7.º

Requisitos para Implementação dos SVV

1 — As unidades orgânicas, outras unidades e serviços da UC, incluindo os SASUC, e/ou o(s) subcontratante(s) responsáveis pela implementação dos SVV devem cumprir os seguintes requisitos gerais:

a) Abster-se de recolher som, salvo em situações previstas na legislação em vigor;

b) Definir a localização das câmaras, os ângulos utilizados e as modalidades de registo de imagens;

c) Reduzir o campo visual em função da finalidade prosseguida;

d) Dispensar grandes planos ou detalhes não relevantes;

e) Não instalar câmaras de videovigilância desproporcionadamente, restringindo ao mínimo a sua quantidade;

f) Manter sempre atualizadas a data e a hora das gravações;

g) Afixar sinalização de existência de videovigilância, nos termos previstos no artigo 19.º

2 — Os responsáveis pela implementação dos SVV devem, cumulativamente, respeitar os seguintes requisitos técnicos:

a) As câmaras de videovigilância só podem incidir sobre os perímetros externos e locais de acesso, e ainda sobre espaços cujos bens e equipamentos requeiram especial proteção, como laboratórios ou salas de informática;

b) As câmaras de videovigilância não podem incidir sobre:

i) Vias públicas, propriedades limítrofes ou outros locais que não sejam do domínio exclusivo da UC, exceto no que seja estritamente necessário para cobrir os acessos aos imóveis da UC;

ii) A zona de digitação de códigos de caixas multibanco ou outros terminais de pagamento ATM;

iii) O interior de áreas reservadas a trabalhadores, estudantes e demais pessoas singulares, designadamente instalações sanitárias, zonas de espera, provadores ou vestiários, zonas de refeição, ginásios ou zonas exclusivamente afetas ao seu descanso.

c) A comunicação entre os componentes do sistema pode ser efetuada com recurso à infraestrutura de cablagem preexistente desde que sejam cumpridos os seguintes requisitos:

i) O responsável pela implementação do SVV valida, sem reservas, a adequação da cablagem à transmissão de dados entre os componentes do sistema por esta interligados;

ii) No caso de ser necessário usar equipamentos ativos de rede para interligar secções distintas da cablagem preexistente, deverão ser usados equipamentos ativos dedicados exclusivamente ao SVV;

iii) A comunicação entre os componentes do SVV deverá, sempre que tecnicamente possível, utilizar comunicações seguras (encriptadas).

d) O acesso físico às áreas técnicas de armazenamento do sistema SVV usadas para suportar as comunicações é restrito a pessoas devidamente autorizadas pela UC, devendo o serviço competente em matéria de sistemas e infraestruturas de informação e de comunicação assegurar que os acessos são auditáveis pela UC.

CAPÍTULO III

Tratamento de dados

SECÇÃO I

Acesso aos dados pessoais recolhidos

Artigo 8.º

Acesso a imagens

1 — O acesso às imagens, gravadas ou visionadas em direto, obtidas de acordo com o presente Regulamento, bem como a arquitetura técnica dos SVV, é restrito a pessoas devidamente autorizadas pela UC.

2 — A autorização a que se refere o número anterior, depende de procedimento que determina as pessoas que, em razão das suas funções, têm acesso às imagens captadas em tempo real e/ou às imagens gravadas, assim como permissões para copiar, descarregar, apagar ou alterar quaisquer imagens filmadas.

3 — As pessoas autorizadas a aceder às imagens, nos termos previstos dos números anteriores devem guardar sigilo, sob pena de procedimento disciplinar e/ou criminal.

Artigo 9.º

Acesso restrito aos dados

1 — Compete à UC encontrar uma solução técnica para que o registo dos dados de videovigilância fique selado, impedindo o acesso fácil.

2 — Em caso de deteção de situações que indiciem a ocorrência de ilícito criminal, durante a captação de imagens, o registo dos dados de videovigilância pode ser aberto, nos termos previstos na lei.

Artigo 10.º

Acesso remoto

Nos casos em que se verifique a necessidade de aceder remotamente a sistemas de visionamento de imagens de videovigilância, compete à UC proteger a informação através de autenticação forte do utilizador, designadamente através da autenticação por dois fatores, da "limitação do número de tentativas" e/ou de métodos adequados de encriptação, com vista a minimizar os riscos de acesso por terceiros não autorizados.

Artigo 11.º

Comunicação de dados a terceiros

1 — Nos casos e termos previstos no RGPD e demais legislação em vigor, a UC pode comunicar dados a terceiros, designadamente às autoridades competentes para o processo penal.

2. As imagens gravadas e outros dados pessoais registados através da utilização de sistemas de vídeo ou outros meios tecnológicos de vigilância à distância, nos termos previstos no artigo 20.º do Código do Trabalho, só podem ser utilizados no âmbito do processo penal.

3 — Nos casos previstos no número anterior, as imagens gravadas e outros dados pessoais podem também ser utilizados para efeitos de apuramento de responsabilidade disciplinar, na medida em que o sejam no âmbito do processo penal.

Artigo 12.º

Salvaguarda de Dados Pessoais

Com vista à salvaguarda dos dados pessoais, a UC adota as seguintes medidas de caráter técnico e organizativo:

a) A aquisição ou instalação de qualquer novo SVV é previamente analisada do ponto de vista da proteção de dados;

b) Os SVV só podem captar som no período em que as instalações vigiadas estejam encerradas, ou mediante a autorização prévia da CNPD;

c) Deve garantir-se que os SVV fazem o registo dos acessos, incluindo a identificação de quem a eles acede, e apresentam garantias de inviolabilidade dos dados relativos à data e hora da recolha;

d) Sem prejuízo do disposto no artigo anterior, a UC não pode copiar nem ceder as gravações a terceiros.

Artigo 13.º

Registo de Operações de Tratamento de Dados Pessoais

1 — A UC procede ao registo do tratamento de dados pessoais, detalhando obrigatoriamente a identificação da pessoa que consulta ou divulga os dados pessoais, o motivo e finalidade do tratamento, bem como a data, hora e identificação de destinatário(s) desses dados pessoais.

2 — A UC regista os acessos aos SVV, para garantia da integridade da informação e para satisfação do exercício do direito de acesso por parte dos titulares dos dados pessoais captados.

3 — A UC, ou a(s) entidade(s) por si subcontratada(s), implementa(m) uma política de análise dos registos e elabora relatórios periódicos de análise, que devem ser mantidos para efeitos de fiscalização pela CNPD.

Artigo 14.º

Auditorias

A UC garante um acesso restrito, tanto físico como remoto, aos servidores do sistema, os quais devem manter registos de acesso à informação, bem como registos da transmissão desses dados, para controlo das operações e para a realização de auditorias internas e externas pelos serviços referidos no n.º 3 do artigo 6.º

SECÇÃO II

Segurança no Tratamento dos dados

Artigo 15.º

Conservação das gravações

1 — As gravações de imagem obtidas pelos SVV e de acordo com o presente regulamento, são conservadas, em registo codificado, pelo prazo de 30 dias contados desde a respetiva captação, findo o qual são destruídas, no prazo máximo de 48 horas.

2 — O prazo a que se refere o número anterior também é aplicável a cada uma das gravações efetuadas por SVV de gravação intermitente.

3 — Sem prejuízo do disposto nos números anteriores, em caso de incidente de segurança, as imagens podem ser conservadas para além dos 30 dias, no âmbito de processo criminal.

Artigo 16.º

Conservação dos registos

Os registos a que se refere o n.º 1 do artigo 13.º são conservados enquanto o sistema estiver ativo, pelo prazo de 120 dias, a contar da data do fim do tratamento.

Artigo 17.º

Direitos do Titular dos Dados

1 — Nos termos da legislação em vigor, a UC assegura ao titular dos dados o direito a:

a) Obter a confirmação de que os dados pessoais que lhe digam respeito são, ou não, objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e a informações nomeadamente as finalidades do tratamento dos dados e o prazo previsto de conservação dos mesmos;

b) Obter a retificação dos dados pessoais inexatos que lhe digam respeito;

c) Obter o apagamento dos seus dados pessoais, excetuando-se no caso de cumprimento de obrigação legal ou outra exceção prevista na legislação em vigor;

d) Limitar o tratamento dos seus dados, incluindo o não apagamento dos mesmos em circunstâncias específicas;

e) Opor-se, a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito;

f) Solicitar junto do EPD-UC o controlo da conformidade com o RGPD;

g) Apresentar uma reclamação junto da entidade de controlo (CNPD).

2 — Se os pedidos apresentados pelo titular dos dados, no âmbito dos direitos previstos no número anterior, forem manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, a UC reserva-se o direito de cobrar custos administrativos ou recusar-se a dar seguimento ao pedido.

3 — O exercício dos direitos previstos no n.º 1 pode ainda ser fundamentadamente recusado:

a) Quando seja suscetível de constituir perigo para a defesa do Estado ou para a segurança pública;

b) Quando esse exercício prejudique investigações, inquéritos, processos judiciais, ou a prevenção, deteção, investigação ou repressão de infrações penais;

c) Para execução de sanções penais, nos termos da legislação em vigor.

Artigo 18.º

Violação dos Dados

1 — Caso ocorra a violação dos dados pessoais obtidos através da utilização de SVV, a UC deve notificar a CNPD, 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 — Caso não seja possível efetuar essa notificação no prazo de 72 horas, a notificação deve ser acompanhada dos motivos do atraso, podendo ainda as informações ser fornecidas por fases, sem demora injustificada.

3 — Sem prejuízo do disposto no n.º 1, compete ao EPD-UC, quando informado de uma violação de dados pessoais, efetuar todas as diligências no sentido da mitigação dos impactos nos titulares e da aplicação de medidas corretivas e emergentes junto do responsável pelo tratamento de dados.

SECÇÃO III

Divulgação dos SVV

Artigo 19.º

Publicidade dos SVV Autorizados

1 — A divulgação pode ser efetuada por transmissão, difusão ou qualquer outra forma de disponibilização.

2 — Nos locais que sejam objeto de vigilância com recurso a câmaras é obrigatória a afixação, em local bem visível, de aviso com a seguinte menção «Para sua proteção, este local é objeto de videovigilância», bem como a informação respeitante à finalidade da captação de imagens e sons, a entidade de segurança que opera o sistema e o responsável pelo tratamento dos dados.

3 — O aviso a que se refere o número anterior, deve conter um pictograma, definido nos termos da legislação em vigor, e constante no Anexo I.

SECÇÃO IV

Controlo dos SVV

Artigo 20.º

Revisões periódicas

1 — Compete ao EPD-UC, em conjunto com os serviços competentes em matéria de instalações e património da UC e em matéria de sistemas e infraestruturas de informação e comunicação da UC, avaliar os SVV em utilização, com uma periodicidade trienal.

2 — A UC pode subcontratar o serviço referido no número anterior.

3 — No âmbito das revisões periódicas, a UC verifica, nomeadamente:

a) A conformidade dos SVV em utilização com o presente Regulamento e demais legislação em vigor;

b) A necessidade do sistema de videovigilância implementado;

c) A possibilidade de substituir o SVV implementado por outro meio/sistema considerado mais adequado;

d) A conformidade do presente Regulamento com as normas em vigor.

Artigo 21.º

Incumprimento

1 — A violação do disposto no presente Regulamento pode dar origem à abertura de procedimento com vista ao apuramento dos factos praticados ou, quando aplicável, à instauração de procedimento disciplinar, nos termos legalmente previstos, sem prejuízo da eventual responsabilidade civil ou criminal.

2 — Sem prejuízo do disposto no número anterior, a violação do disposto no presente Regulamento pode implicar ainda, como medida cautelar ou urgente, a revogação, total ou parcial, de determinadas permissões, na medida e em função do que se mostre necessário, de forma a salvaguardar a segurança e integridade das pessoas e bens ou dos dados pessoais em causa.

3 — Cabe ao Responsável máximo da Unidade ou Serviço tomar a decisão prevista no número anterior, dela cabendo recurso para o Reitor, salvo se este tiver sido o decisor, caso em que apenas há lugar a reclamação ou a impugnação judicial, nos termos gerais.

CAPÍTULO IV

Disposições Finais e Transitórias

Artigo 22.º

Ações de Sensibilização e de Formação

1 — A UC promove ações de sensibilização inicial e/ou ações de atualização, bem como ações de formação, na área da proteção de dados pessoais, especialmente aos trabalhadores que, no âmbito das suas funções, tenham, ou possam vir a ter, contacto com os dados obtidos através da utilização de SVV.

2 — Após o processo de avaliação dos trabalhadores no âmbito da(s) ação(ões) referidas no número anterior, compete aos serviços envolvidos atestar se o trabalhador pode realizar tratamento de dados pessoais em ambiente SVV.

Artigo 23.º

Dúvidas de Interpretação

As dúvidas suscitadas pela aplicação do presente Regulamento são resolvidas por despacho do Reitor, tendo em atenção a legislação em vigor.

Artigo 24.º

Legislação Subsidiária

Em tudo o que não esteja especialmente previsto no presente Regulamento, aplica-se subsidiariamente, na sua redação atual:

a) O RGPD;

b) A Lei n.º 58/2019, de 8 de agosto;

c) O Código do Trabalho, aprovado pela Lei n.º 7/2009, de 12 de fevereiro;

d) A Lei Geral do Trabalho em Funções Públicas, aprovada pela Lei n.º 35/2014, de 20 de junho;

e) A Lei n.º 34/2013, de 16 de maio, na sua atual redação e restante legislação que regula a atividade de segurança privada.

Artigo 25.º

Revisão do Regulamento

O presente Regulamento pode ser objeto de revisão, por iniciativa do Reitor ou sob proposta do EPD-UC.

Artigo 26.º

Norma Transitória

1 — Os responsáveis máximos de cada Unidade ou Serviço procedem, no prazo de 60 dias após a entrada em vigor do presente Regulamento, à revisão ou atualização dos SVV instalados nos edifícios sob sua responsabilidade.

2 — Para efeitos do disposto no número anterior, os responsáveis devem submeter o pedido de análise ao serviço competente em matéria de instalações e património da UC, através de uma AIPD, contendo os seguintes elementos:

a) Finalidade do SVV;

b) Localização da(s) câmara(s) de videovigilância;

c) Área de abrangência de cada câmara de videovigilância;

d) Atividade(s) desenvolvida(s) nas áreas indicadas na alínea anterior;

e) Procedimentos em vigor para a gestão dos sistemas;

f) Identificação da(s) pessoa(s) com acesso ao SVV, diferenciando entre visualização e gravação de imagens;

g) Cópia do(s) contrato(s) celebrados com empresa(s) externa(s), quando aplicável.

Artigo 27.º

Delegação de Competências

As competências previstas no presente Regulamento podem ser exercidas por delegação de competências formais emanadas pelos titulares dos respetivos órgãos.

Artigo 28.º

Norma Revogatória

Com a entrada em vigor do presente Regulamento são revogadas todas as normas internas que contrariem as disposições nele consignadas.

Artigo 29.º

Entrada em vigor

O presente Regulamento entra em vigor no dia seguinte ao da sua publicação no *Diário da República*.

318265658