COMUNIDADE INTERMUNICIPAL DO TÂMEGA E SOUSA

Regulamento n.º 400/2022

Sumário: Regulamento Intermunicipal de Dados Pessoais.

Regulamento Intermunicipal de Dados Pessoais

Nos termos do artigo 139.º do Código do Procedimento Administrativo, aprovado em anexo ao Decreto-Lei n.º 4/2015, de 07/01, publica-se o Regulamento Intermunicipal de Dados Pessoais, aprovado pelo Conselho Intermunicipal na sua reunião ordinária de 2022/02/22, cujo projeto foi submetido pelo Secretariado Executivo da Comunidade Intermunicipal do Tâmega e Sousa (CIM-TS).

Nota Justificativa

Com a celebração da Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108) do Conselho da Europa de 1981, com depósito do instrumento de ratificação por Portugal em 2 de setembro de 1993, pela primeira vez foi feita referência aos princípios que nortearam a elaboração da Diretiva 95/46/CE, de 24 de outubro e ao Regulamento (eu) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

A Diretiva 95/46/CE do Parlamento Europeu e do Conselho visou harmonizar a defesa dos direitos e das liberdades fundamentais das pessoas singulares em relação às atividades de tratamento de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros.

A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. Nessa senda, artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais. O presente Regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares.

Em Portugal, a Diretiva 95/46/CE, foi transposta para a ordem jurídica portuguesa através da Lei n.º 67/98, de 26 de outubro (Lei da Proteção de Dados Pessoais).

O Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril, adiante designado de modo indistinto por RGPD ou Regulamento, foi publicado em 4 de maio de 2016 no Jornal Oficial da União Europeia, entrou em vigor a 25 de maio de 2016, sendo de aplicação direta em todos os Estados-Membros a partir de 25 de maio de 2018, e revogou a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, que com esta mutação jurídica acabou por transformar a proteção de dados pessoais de aplicação direta e imediata, libertando-a da maior ou menor capacidade dos Estados Membros de legislar quanto à sua transposição.

A Comunidade Intermunicipal do Tâmega e Sousa, doravante designada de forma indistinta por CIM do Tâmega e Sousa ou CIM-TS, em conformidade com o artigo 40.º do RGPD, tem de promover a elaboração de um código de conduta, destinado a contribuir para a correta aplicação do mesmo Regulamento e, neste sentido, torna-se necessário elaborar normativo intermunicipal, que discipline a recolha de dados pessoais e, não de menos, o respetivo tratamento.

À luz deste Regulamento, entende-se por dados pessoais, "informação relativa a uma pessoa singular identificada ou identificável (titular dos dados), é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética,

mental, económica, cultural ou social dessa pessoa singular" e por tratamento (de dados pessoais) "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" (cf. o artigo 4.º, n.os 1 e 2 do Regulamento).

Este Regulamento designa-se por "Regulamento Intermunicipal de Dados Pessoais", procurando servir de auxílio aos Colaboradores desta Comunidade Intermunicipal e, do mesmo passo, prestar informação a um número indeterminado de destinatários que interagem com a mesma nas relações jurídico-administrativos na parte de tratamento dos seus dados pessoais.

Com esta proposta, pretende-se criar um lastro jurídico intermunicipal no âmbito da proteção dos dados pessoais, enquanto direito fundamental e, do mesmo passo, estabelecer regras comuns que permitam construir uma estratégia integrada

Resumidamente, no seu Capítulo I (Disposições Gerais) introduzem-se definições nucleares para a compreensão desta temática, com destaque para os conceitos do RGPD o seu devido enquadramento, os princípios base que devem servir de orientação cimeira, a parte respeitante aos direitos dos titulares dos dados pessoais, devidamente caracterizados, o consentimento enquanto manifestação de vontade «livre, específica, informada e inequívoca». O papel a desempenhar pela CIM-TS enquanto responsável pelo tratamento de dados pessoais é densificado no Capítulo II (Responsável pelo Tratamento). No Capítulo III (Medidas de Segurança) são abordadas as metodologias que garantirão o cumprimento do RGPD na recolha, tratamento, limitação da conservação, análise de impacto, de dados pessoais. As políticas de gestão de acessos de utilizadores a sistemas de informação, bem como a gestão de palavras passe (*passwords*) são caracterizados no Capítulo IV (Identidade Eletrónica e gestão de palavras passe). O papel fundamental desempenhado pelo Encarregado de Proteção de Dados (EPD) e a sua designação são descritos no Capítulo V (Encarregado de Proteção de Dados). O Capítulo VI (Situações Especiais) remete para procedimentos a desenvolver no âmbito de tratamento de dados especiais, nomeadamente no que concerne a menores de idade, recolha de imagem/som/vídeo, reuniões dos órgãos de governo da CIM-TS e biometria. No Capítulo VII (Disposições Finais) são efetuadas disposições sobre o regime sancionatório, publicações em jornais oficiais e a entrada em vigor do presente regulamento. Por fim, mas não de menos, acolhendo a sugestão da Comissão Nacional de Proteção de Dados (CNPD), consigna-se no articulado norma teleologicamente orientada para garantir a revisão do presente Regulamento ao fim de três anos.

O presente Projeto de Regulamento tem, nos termos do artigo 136.º do Código do Procedimento Administrativo (CPA), aprovado pelo Decreto-Lei n.º 4/2015, de 7 de janeiro, por normas habilitantes as disposições conjugadas do n.º 7, do artigo 112.º e artigo 241.º, da Constituição da República Portuguesa, bem como o disposto do artigo 90.º, n.º 1, al. *q*), do Anexo I à Lei n.º 75/2013, de 12 de setembro, na redação em vigor, do 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, de 24 de outubro de 1995 (Regulamento Geral sobre a Proteção de Dados) e a Lei n.º 58/2019, de 8 de agosto.

O projeto de Regulamento foi aprovado pela deliberação /2022/42 da CNPD.

Para efeitos do artigo 99.º, parte final, do CPA a nota justificativa do projeto do Regulamento deve ser acompanhada por uma ponderação dos custos e benefícios das medidas projetadas. Dando cumprimento a esta exigência acentua-se que o teor do presente Regulamento visa dar continuidade a um projeto intermunicipal de conformidade com o RGPD, cujo objetivo é promover o seu cumprimento, com critérios e regras uniformes, ao nível da NUT III Tâmega e Sousa., funcionando como instrumento de responsabilização útil e eficaz, apresentando uma descrição circunstanciada do que é o conjunto de comportamentos mais adequados, lícitos e éticos.

CAPÍTULO I

Disposições gerais

Artigo 1.º

Lei habilitante

O presente Regulamento é elaborado ao abrigo e nos termos do artigo 241.º da Constituição da República Portuguesa, do disposto do artigo 135.º do CPA, do artigo 90.º, n.º 1, alínea *q*) do Anexo I à Lei n.º 75/2013, de 12 de setembro, na redação em vigor, do 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 (Regulamento Geral sobre a Proteção de Dados), adiante designado de forma abreviada por RGPD e a Lei n.º 58/2019, de 8 de agosto.

Artigo 2.º

Objeto

O presente Regulamento tem por objeto a elaboração de um código de conduta destinado a disciplinar internamente a recolha e subsequente tratamento de dados pessoais e à livre circulação desses dados por parte da CIM-TS, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de terceiros, em conformidade com o RGPD, bem como da legislação nacional aplicável e orientações da Comissão Nacional de Proteção de Dados (CNPD) e do Comité Europeu para a Proteção de Dados.

Artigo 3.º

Âmbito de aplicação

O presente Regulamento aplica-se a todos os tratamentos de dados pessoais realizados exclusivamente por parte dos órgãos, serviços e colaboradores da CIM-TS.

Artigo 4.º

Definições

Para efeitos do presente Regulamento, entende-se por:

1 — Dados pessoais, informação relativa a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

2 — Tratamento, uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a limitação da 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, o apagamento ou a destruição.

3 — Responsável pelo tratamento, a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro.

4 — Consentimento do titular dos dados, uma manifestação de vontade, livre, específica, informada e inequívoca, 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.

5 — Avaliação de impacto sobre a proteção de dados, um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos.

Artigo 5.º

Princípios base e sua amplitude

1 — Os princípios base do RGPD, e do presente Regulamento, são a licitude do tratamento, a minimização dos dados, a transparência, a finalidade, a exatidão, a limitação da conservação, a integridade e confidencialidade e a responsabilização dos intervenientes no tratamento de dados pessoais no campo de ação das competências legais da CIM-TS. Aplicando-se:

a) A todos os tratamentos de dados pessoais abrangidos pelo presente Regulamento;

b) A todos os colaboradores da CIM-TS, independentemente do seu vínculo;

c) Às interações entre a CIM-TS com os seus colaboradores, Municípios que a compõem, fornecedores, parceiros, assim como todos os cidadãos.

2 — No que se reporta aos princípios acima mencionados, entende-se o seguinte:

a) O princípio da licitude de tratamento significa que o tratamento de dados pessoais apenas é possível se se verificar um fundamento legítimo para tal operação, elencando o artigo 6.º do RGPD as situações em que o tratamento é considerado lícito:

i) Genericamente, sendo a CIM-TS uma entidade pública, os seus tratamentos de dados pessoais assentam em dois fundamentos basilares, a previsão legal (ou regulamentar) e a prossecução do interesse público. Os tratamentos de dados pessoais enquadrados nestes dois fundamentos não carecem de consentimento do titular dos dados nos termos melhor descritos no artigo 8.º do presente regulamento;

ii) Nos casos não incluídos no inciso i. a licitude do tratamento deve basear-se no consentimento do titular dos dados, nomeadamente quando:

I. Tratamento de dados incluídos nas categorias especiais de dados pessoais;

II. Finalidade que não a que originou a recolha dos dados junto do titular dos mesmos;

III. Transferência de dados no âmbito de Acordos relativos a tratamento de dados pessoais.

b) O princípio da minimização significa que os dados a tratar devem ser adequados, pertinentes e limitados ao que é exigido pelas finalidades que determinam o tratamento:

i) Os dados pessoais recolhidos devem corresponder ao “mínimo indispensável” para se satisfazer a finalidade pretendida;

ii) Os dados pessoais apenas devem ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios;

iii) Caso se verifique que foram solicitados dados excessivos, o tratamento passará a ser ilícito.

c) Por princípio da transparência o processamento dos dados pessoais deve ser feito de forma licita, leal e transparente, com respeito pelos direitos do titular dos direitos de personalidade:

i) A CIM-TS manterá um registo das atividades de processamento de dados pessoais sob sua responsabilidade;

ii) O prazo de conservação dos dados pessoais deverá ser dado a conhecer ao titular dos dados pessoais no momento da recolha, ou, se não for possível, os critérios usados para definir esse prazo.

d) O princípio da finalidade determina que os dados devem ser recolhidos para finalidades determinadas, explícitas e legítimas e, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades:

i) Nesta medida, afigura-se que não podem ser recolhidos dados pessoais para finalidades futuras, ainda não determinadas no momento da recolha.

ii) Este princípio assume uma importância fundamental uma vez que só depois de conhecida a finalidade do tratamento é possível apurar se a informação pessoal recolhida é necessária e não excessiva.

e) Por princípio da exatidão os dados pessoais devem ser exatos e atualizados sempre que necessário e quando estejam inexatos devem os mesmos ser retificados, utilizando para tal todas as medidas adequadas:

i) Será dada resposta aos pedidos de retificação do titular dos dados sem demora injustificada, no prazo máximo de um mês e quando for intenção de recusa do pedido do titular dos dados deverá ser apresentada a correspondente justificação.

f) Por princípio da limitação da conservação, o prazo limite da conservação de dados pessoais, não pode exceder o tempo necessário para a concretização da finalidade para as quais os dados pessoais foram recolhidos.

g) Por princípio da integridade e confidencialidade o legislador estabelece o dever de integridade e confidencialidade no tratamento de dados pessoais:

i) Os dados pessoais serão tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando-se as medidas técnicas ou organizativas adequadas.

h) Por princípio da responsabilização dos operacionais do tratamento de dados pessoais, está consagrada a responsabilidade da CIM-TS por qualquer tratamento de dados pessoais realizado por esta ou por sua conta. Em especial, a CIM-TS executará as medidas que forem adequadas e eficazes, e em simultâneo ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o RGPD, incluindo a eficácia das medidas. Essas medidas levarão em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares;

i) A fim de comprovar a observância do RGPD, a CIM do Tâmega e Sousa e seus subcontratantes, nos termos do artigo 30.º do RGPD, deverão conservar registos de atividades de tratamento sob a sua responsabilidade.

Artigo 6.º

Direitos dos titulares dos dados pessoais

1 — De acordo com o disposto no RGPD, constituem direitos dos titulares dos dados pessoais, os seguintes:

a) O direito à informação;
b) O direito de acesso aos dados;
c) O direito à portabilidade e à interoperabilidade dos dados;
d) O direito de retificação;
e) O direito à oposição;
f) O direito ao apagamento e à eliminação (“direito a ser esquecido”);
g) Direito à limitação do tratamento.

2 — No que se reporta aos direitos dos titulares dos dados pessoais acima mencionados, entende-se o seguinte:

a) Direito à informação, no momento em que os dados são recolhidos, ou caso a recolha dos dados não seja feita diretamente junto deste, logo que os dados sejam tratados o titular dos dados, tem o direito de ser informado, designadamente, sobre:

i) A finalidade do tratamento e o prazo de limitação da conservação;
ii) A base jurídica para o tratamento dos seus dados;
iii) A quem podem ser comunicados e/ou transmitidos os seus dados;
iv) Quais as condições em que pode aceder e retificar os seus dados;
v) Quais os dados que tem que fornecer obrigatoriamente e quais são opcionais;
vi) O contacto do responsável pelo tratamento dos dados, bem como do encarregado de proteção de dados;
vii) O direito a apresentar reclamação à CNPD.

b) Direito de acesso aos dados, o titular dos dados pessoais tem o direito de aceder aos dados que sejam registados sobre si, sem restrições e sem demoras, bem como saber quaisquer informações disponíveis sobre a origem desses dados. O exercício do direito de acesso deve ser feito pelo titular dos dados mediante formulário, em suporte digital ou de papel, dirigido ao responsável pelo tratamento dos dados, tendo o direito de obter uma cópia dos dados num formato acessível, desde que não prejudique os direitos e as liberdades de terceiros.

c) Direito à portabilidade e à interoperabilidade dos dados, quando o tratamento de dados pessoais se realize por meios automatizados e se basear no consentimento prévio do titular dos dados ou na necessidade de cumprimento de uma obrigação contratual, o titular dos dados pessoais tem o direito a, quando tal não colida com o cumprimento de obrigação legal ou persecução do interesse público (cf. n.º3 do artigo 20.º do RGPD):

i) Receber os seus dados pessoais que foram objeto de tratamento de forma estruturada, em formato aberto ou através de interoperabilidade de sistemas, sempre que seja tecnicamente possível;
ii) Transmitir esses dados a outro responsável por tratamento de dados, sem que a CIM-TS se possa opor, e desde que o mesmo não prejudique os direitos e as liberdades de terceiros.

d) Direito de retificação, o titular dos dados pessoais tem o direito a solicitar ao responsável pelo tratamento dos dados, mediante formulário, em suporte digital ou de papel, a retificação dos dados pessoais inexatos que lhe digam respeito.

e) Direito à oposição, o titular dos dados pessoais tem o direito de se opor, a seu pedido e gratuitamente, ao tratamento dos seus dados pessoais, nos seguintes casos:

i) Para efeitos de publicidade direta ou de qualquer outra forma de prospeção, sem o seu prévio consentimento, designadamente a publicitação de eventos e ações desenvolvidos pela CIM-TS;
ii) Que sejam comunicados a terceiros, salvo disposição legal em contrário;
iii) A que os seus dados, nalguns casos previstos na lei, não sejam objeto de tratamento, por razões ponderosas e legítimas relacionadas com a sua situação particular, nomeadamente dados pessoais recolhidos no âmbito do Plano Integrado e Inovador de Combate ao Insucesso Escolar do Tâmega e Sousa e Transporte Público rodoviário do Tâmega e Sousa.

f) Direito ao apagamento e à eliminação ("direito a ser esquecido"), o titular dos dados pessoais tem o direito de exigir que os seus dados sejam eliminados:

i) O direito a ser esquecido é definido pelo direito de os titulares dos dados impedirem a continuação do tratamento dos respetivos dados e de os mesmos serem apagados quando deixarem de ser necessários para fins legítimos. Assim, sempre que uma pessoa singular deixe de permitir o tratamento dos seus dados e não haja razões legítimas para a sua limitação da conservação,

os dados deverão obrigatoriamente ser apagados. Designadamente quando a licitude do tratamento por parte da CIM-TS assente no consentimento informado por parte do titular dos dados;

ii) O exercício do direito de apagamento e à eliminação dos dados é exercido diretamente junto do responsável pelo tratamento dos dados, mediante formulário, em suporte digital ou de papel, cf. descrito no ponto 3 do presente artigo.

g) Direito à limitação do tratamento, o titular dos dados pode exigir a limitação do tratamento (durante um certo período de tempo, o tratamento de dados fica limitado na sua utilização, não podendo os dados nomeadamente ser comunicados a terceiros, transferidos internacionalmente, ou apagados) junto do responsável pelo tratamento, nas seguintes situações:

i) Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão;

ii) 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;

iii) O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;

iv) Se tiver oposto ao tratamento nos termos do exercício do direito à oposição, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

3 — O exercício dos direitos referidos nos pontos 1 e 2 do presente artigo será assegurado através de um formulário disponibilizado pela CIM-TS, permitindo ao titular dos dados exercer os direitos que lhe são conferidos, a título gratuito. O formulário preenchido será encaminhado para o Encarregado de Proteção de Dados da CIM-TS, e este remetê-lo-á ao colaborador afeto ao respetivo tratamento de dados para cumprimento do exercício de direitos.

4 — Os direitos de informação e de acesso a dados pessoais não podem ser exercidos quando a lei imponha ao responsável pelo tratamento ou subcontratante um dever de segredo que seja oponível ao próprio titular dos dados, podendo o titular dos dados solicitar à CNPD a emissão de parecer quanto à oponibilidade do dever de segredo.

Artigo 7.º

Consentimento

1 — O consentimento deverá ser solicitado apenas quando a licitude do tratamento não está abrangida pelos pressupostos enunciados no inciso i da alínea *a*) do n.º 2 do artigo 5.º do presente regulamento.

2 — O consentimento deverá abranger as operações de tratamento realizadas com a mesma finalidade, incluídas no conjunto indicado no ponto 1 do presente artigo, devendo igualmente permitir a concessão do consentimento separado para cada uma das operações previstas.

3 — O pedido de consentimento deve ser apresentado de modo inteligível e de fácil acesso, e numa linguagem clara e simples. Não são admitidos consentimentos tácitos nem opções pré-validadas.

4 — Uma declaração de consentimento, previamente formulada, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina.

5 — Da declaração de consentimento deve também constar qual o tratamento realizado sobre os dados, qual a finalidade, se existe partilha ou transferência dessa informação com outras entidades e qual o prazo de conservação.

6 — Quando a licitude do tratamento estiver baseada no consentimento do titular dos dados, a CIM-TS, através do colaborador que efetuou a recolha dos mesmos, deverá ser capaz de demonstrar que o titular deu o seu consentimento. Nomeadamente, através de uma declaração

escrita, onde sejam claras as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e do seu alcance.

7 — O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento, não comprometendo a licitude do tratamento efetuado com base no consentimento previamente dado.

CAPÍTULO II

Responsável pelo tratamento de dados

Artigo 8.º

Responsável pelo tratamento de dados pessoais

1 — O responsável pelo tratamento de dados pessoais é a CIM-TS.

2 — O Secretariado Executivo pode delegar a competência para a assinatura de acordos relativos a tratamento de dados pessoais.

Artigo 9.º

Obrigações do responsável pelo tratamento de dados pessoais

1 — Cabe ao responsável pelo tratamento de dados pessoais o cumprimento das seguintes obrigações:

a) Aplicar as medidas técnicas e organizativas que forem adequadas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento, de forma a poder comprovar que o tratamento é realizado em conformidade com o RGPD, legislação nacional e o presente Regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.

b) Comunicar à CNPD as violações dos dados pessoais, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar risco para os direitos e liberdades das pessoas singulares. Se a notificação à CNPD não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.

c) Comunicar ao titular dos dados pessoais, sem demora injustificada, a violação destes, se a mesma for suscetível de implicar um elevado risco para os seus direitos e liberdades, exceto quando se verifique um dos seguintes casos:

i) O responsável pelo tratamento tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, nomeadamente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem;

ii) O responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados pessoais já não for suscetível de se concretizar; ou

iii) Implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz.

d) Proceder, antes de iniciar o tratamento de dados pessoais, a uma avaliação de impacto sobre a proteção dos referidos dados, a fim de avaliar a probabilidade ou gravidade particulares do elevado risco, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do risco, bem como consultar a CNPD. Essa avaliação de impacto deverá incluir, nomeadamente, as medidas, garantias e procedimentos previstos para atenuar esse risco, assegurar a proteção dos dados pessoais e comprovar a observância do cumprimento do RGPD, legislação nacional e do presente Regulamento.

e) Solicitar pareceres ao encarregado de proteção de dados, no âmbito da avaliação de impacto a que se refere a alínea anterior.

f) Apoiar o encarregado de proteção de dados no exercício das suas funções, fornecendo-lhe os recursos necessários ao desempenho dessas funções e à atualização dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento.

Artigo 10.º

Responsabilidade dos dirigentes e/ou responsáveis das unidades orgânicas

1 — Todos os dirigentes da CIM-TS e/ou responsáveis por unidades orgânicas devem identificar as diferentes atividades que são desenvolvidas nas mesmas, bem como os dados pessoais que são recolhidos e o respetivo tratamento.

2 — Os dirigentes e/ou responsáveis pelas unidades orgânicas devem comunicar ao encarregado de proteção de dados a informação recolhida no ponto anterior e mantê-la atualizada.

CAPÍTULO III

Medidas de segurança

Artigo 11.º

Tratamento de dados pessoais

1 — O acesso ou a consulta aos dados pessoais, assim como a recolha, o registo, a alteração ou a sua eliminação só pode ser realizado pelos colaboradores previamente legitimados e que necessitem de o fazer, no cumprimento das suas funções ou no âmbito de um procedimento administrativo, devendo ser criado um registo, obrigatoriamente eletrónico, onde conste o nome do colaborador, a data e fundamento da operação bem como a identificação do documento ou processo.

2 — Para a concretização das operações a que se refere o número anterior deverá ser criado um perfil de acesso.

3 — No caso dos dados pessoais se encontrarem disponíveis fisicamente, estes devem estar devidamente arquivados em locais fechados, sendo que as chaves devem igualmente estar na posse de colaboradores determinados pelos respetivos dirigentes e/ou responsáveis das unidades orgânicas, devendo, neste caso, ser guardado um registo de acesso aos mesmos, onde conste o nome do trabalhador, o motivo para a consulta, a data e a identificação do documento/processo.

4 — No caso de os dados pessoais constarem de processos arquivados ou a decorrerem em plataformas eletrónicas, os dirigentes e/ou responsáveis pelas unidades orgânicas devem identificar quem tem permissões para aceder aos mesmos e os momentos em que o podem fazer.

Artigo 12.º

Segurança das redes e sistemas de informação

Os sistemas de informação devem estar desenhados e concebidos para abranger qualquer tratamento de dados pessoais garantindo o cumprimento dos seguintes pressupostos:

a) Todas as aplicações e sistemas de informação da CIM-TS deverão cumprir os requisitos técnicos constantes na Resolução do Conselho de Ministros n.º 41/2018, de 28 de março, que define as orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais;

b) É da competência dos dirigentes e/ou responsáveis pelas unidades orgânicas identificar os colaboradores com permissões para o tratamento de dados pessoais no âmbito dos processos que coordenam e ainda solicitar ao dirigente e/ou responsável pelos Serviços de Informática a sua implementação nos sistemas de informação;

c) É da competência dos Serviços de Informática definir e implementar os requisitos específicos indicados na alínea *a*) do presente artigo.

d) Adicionalmente poderão ser acauteladas e desenvolvidas medidas tecnológicas e procedimentais tendentes a aumentar e garantir os níveis e segurança de todos os dados pessoais e restante informação à sua guarda.

Artigo 13.º

Avaliação de impacto sobre a proteção de dados

1 — A avaliação de impacto sobre a proteção de dados (AIPD) consiste num processo que visa estabelecer e demonstrar a conformidade com o RGPD, legislação nacional e o presente Regulamento.

2 — Nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo seu tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco.

3 — Uma avaliação de impacto sobre a proteção de dados deve conter:

a) Uma descrição do tratamento e das suas finalidades;

b) Uma avaliação da necessidade e da proporcionalidade do tratamento medida em mapa de risco; A análise do risco e a adoção de medidas baseadas na mitigação resume o sistema de gestão de riscos da informação a mapear, através dos seguintes procedimentos simplificados:

i) A aceção do Risco será o resultado da conjugação da relação Valor da informação vs Probabilidade de ocorrência;

ii) Identificação dos Ativos de Informação (Tratamentos):

1) São designados ativos da informação, sistemas, portais, servidores, base de dados, equipamentos de comunicação, contratos, etc. que devem ser identificados no âmbito da segurança da informação;

2) Serão identificados qualquer operação ou conjunto de operações efetuados sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, limitação da conservação, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, comparação ou interconexão, bem como a limitação, apagamento ou destruição.

iii) Determinação do Valor da Informação (Criticidade):

1) Para cada ativo de informação identificado, é efetuada a classificação no que se refere à confidencialidade, integridade e disponibilidade.

2) Será determinado o Valor do Ativo da Informação que caracterize o impacto da perda para cada propriedade (confidencialidade, integridade e disponibilidade):

a) Alto: Se a combinação Confidencialidade, Integridade e Disponibilidade for do tipo — Alta | Alta | Alta ou Alta | Alta;

b) Médio: Se a combinação Confidencialidade, Integridade e Disponibilidade for do tipo — Média ou Média | Média ou Média | Média | Média;

c) Baixo: Se a combinação Confidencialidade, Integridade e Disponibilidade for do tipo — Baixa | Baixa ou Baixa | Baixa | Baixa.

iv) Determinação da Probabilidade de Ocorrência de riscos (Vulnerabilidades):

1) Para cada ativo de informação identificado devem ser identificadas as vulnerabilidades e possível impacto, de acordo com as seguintes definições:

a) Vulnerabilidade: É uma condição ou um conjunto de condições que permitem que ameaças afetem os ativos;

b) Impacto: Deve ser classificado na ótica do impacto que a exposição dos dados pessoais pode causar para os titulares dos dados, através da exploração de uma vulnerabilidade:

i) Insignificante — Os titulares não são afetados ou poderão encontrar uns pequenos inconvenientes que conseguem superar sem problema;
ii) Limitado — Os titulares podem encontrar inconvenientes significantes que conseguem superar apesar de algumas dificuldades;
iii) Significante — Os titulares podem enfrentar consequências significantes que devem conseguir superar, embora com dificuldades sérias e reais;
iv) Máximo — Os titulares podem enfrentar consequências significantes ou até irreversíveis que podem não conseguir superar.

c) Probabilidade de Ocorrência: Probabilidade que uma ameaça tem de explorar inerentes ao ativo:

i) Insignificante — Não parece possível que os riscos se materializem através da exploração das vulnerabilidades;
ii) Limitada — Parece difícil que os riscos se materializem através da exploração das vulnerabilidades;
iii) Significante — Parece possível que os riscos se materializem através da exploração das vulnerabilidades;
iv) Máxima — É quase certo que os riscos se materializem através da exploração das vulnerabilidades.

v) Determinação do Risco:

1) O risco será determinado levando em conta uma escala de classificação de probabilidade de ocorrência e impacto (valor) de acordo com uma matriz com graduação de cores, permitindo assim a priorização dos riscos em termos de grau de premência de atuação;
2) Graduação do Risco:

a) Baixo (Verde)
b) Médio (Amarelo)
c) Alto (Laranja)
d) Elevado (Vermelho)

vi) Identificação dos Controlos a Aplicar:

1) O risco associado às ameaças identificadas deverá ser possível de ser eliminado ou reduzido por implementação de metodologias de controlo a identificar.

vii) Implementação do Plano de Ação de Mitigação:

1) Para cada controlo com necessidade de implementação de plano de ação, devem ser estabelecidas um conjunto de ações, responsabilidades e prazos que permitam assegurar a execução dos controlos definidos.

viii) Revisão da Avaliação de Riscos:

1) Dever-se-á efetuar uma reavaliação dos riscos periodicamente, por forma a:

a) Incluir alterações nos ativos de informação;
b) Incorporar mudanças nas prioridades e necessidades;
c) Considerar novas ameaças e vulnerabilidades;
d) Verificar se os controlos permanecem eficazes e apropriados.

ix) O resultado desta avaliação, permite identificar e quantificar os riscos que podem afetar a segurança da informação.

c) Uma apreciação sobre os riscos para os direitos e liberdades do titular;

d) Medidas previstas para diminuir os riscos em conformidade com o RGPD, legislação nacional, orientações da CNPD e o presente Regulamento.

4 — Para além das operações de tratamento sujeitas a uma avaliação de impacto sobre a proteção de dados definidas no RGPD, em legislação nacional, bem como na lista que a CNPD publicou através do Regulamento n.º 798/2018, de 30 de novembro (*Diário da República,* 2.ª série, n.º 231, de 30 de novembro de 2018), da CNPD, deverá a CIM-TS efetuar uma avaliação de impacto sobre a proteção de dados, nas seguintes situações:

a) A celebração de protocolos de geminação com países fora do âmbito territorial do RGPD, quando exista transferência de dados pessoais que implique um elevado risco para os direitos e liberdades das pessoas singulares;

b) Tratamento de dados pessoais, no âmbito de projetos, programas ou eventos realizados, que digam respeito a categorias especiais de dados pessoais.

5 — As transferências de base de dados ou de ferramentas eletrónicas na nuvem/internet ou correio eletrónico devem assegurar que o fluxo de transferência dos dados e seu arquivo ocorra em território da União.

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

7 — O Encarregado de Proteção de Dados (EPD) poderá, caso tal lhe seja solicitado, prestar assistência ao responsável pelo tratamento de dados pessoais na realização de uma AIPD. Aplicando o princípio da proteção de dados desde a conceção, ao efetuar uma AIPD, o responsável pelo tratamento deve solicitar parecer do EPD, sobre as seguintes questões:

a) A necessidade da realização de uma AIPD;

b) Qual a metodologia a seguir na realização de uma AIPD;

c) Se a AIPD deverá ser realizada internamente ou se deverá externalizá-la;

d) As salvaguardas (incluindo medidas técnicas e organizativas) a aplicar no sentido de atenuar os eventuais riscos para os direitos e interesses dos titulares de dados;

e) Se a AIPD foi ou não corretamente efetuada e se as suas conclusões (se o tratamento deve ou não ser realizado e quais as salvaguardas a aplicar) estão em conformidade com o RGPD.

8 — O parecer do EPD e as decisões tomadas pelo responsável pelo tratamento de dados pessoais deverão ser documentadas e integradas na AIPD.

Artigo 14.º

Procedimentos administrativos

1 — Apenas podem ser recolhidos os dados pessoais para efeitos procedimentais que forem estritamente necessários.

2 — A lei ou qualquer outro normativo, previamente definido, determina quais são os dados pessoais que são necessários recolher para efeitos procedimentais.

3 — Aquando da necessidade de recolha de dados pessoais adicionais, cujo fundamento de licitude não assente no disposto do inciso i da alínea *a*) do n.º 2 do artigo 5.º do presente regulamento, deverá ser recolhido o consentimento do titular dos dados.

4 — O exercício dos direitos dos titulares dos dados pessoais, referidos no artigo 6.º, do presente Regulamento, deverá ser feito mediante o preenchimento de formulário, em suporte digital ou de papel.

5 — No exercício do direito ao apagamento e à eliminação ("direito a ser esquecido") por parte do titular dos dados pessoais, referido na alínea *f*) do ponto 2 do artigo 6.º do presente Regulamento, o responsável pelo tratamento dos dados (CIM-TS), deverá proceder à destruição dos dados

pessoais em causa, lavrar o respetivo auto para o efeito e notificar o titular dos dados pessoais. Igualmente deverá notificar os eventuais subcontratantes e terceiros, para que estas procedam em conformidade com o pedido efetuado.

6 — A documentação rececionada no atendimento ao público deverá ser remetida para o *backoffice*, ou quando tal não seja possível não deverá estar visível a pessoas terceiras.

7 — Na receção de documentação via correio eletrónico, o consentimento para a recolha e subsequente tratamento dos dados pessoais, deve ser solicitado pelo dirigente e/ou responsável pela unidade orgânica a que o assunto se reportar, que deverá solicitar junto do titular a recolha do respetivo consentimento.

8 — A resposta relativa aos direitos dos titulares deve ser dada sem demora justificada e no prazo de um mês a contar da data da receção do pedido.

Artigo 15.º

Atendimento

1 — A comunicação de informação que envolva dados pessoais via telefone, serviços eletrónicos ou correio eletrónico só poderá ser realizada se previamente o titular dos dados tiver dado o consentimento expresso nesse sentido.

2 — No atendimento presencial ao público deverá ser reservada e mantida a distância necessária para uma maior salvaguarda e proteção da privacidade no tratamento dos dados pessoais das pessoas singulares.

CAPÍTULO IV

Identidade eletrónica e gestão de palavras passe

Artigo 16.º

Política de atribuição de identidade eletrónica (conta de utilizador)

1 — Entende-se por identidade eletrónica (conta de utilizador) a credencial que permite o acesso às infraestruturas tecnológicas da CIM-TS através da identificação do utilizador em conjunto com uma palavra passe, certificado ou outra forma que garanta a sua identificação.

2 — Todo o utilizador necessita de uma identidade eletrónica para ter acesso aos serviços e recursos da CIM-TS, que mediante o seu tipo de perfil, poderá ser condicionado.

3 — Após validação do registo pelos Recursos Humanos da Comunidade Intermunicipal do Tâmega e Sousa, a Informática processa a criação de conta e os serviços associados.

4 — No caso de situações não suscetível de validação por parte dos Recursos Humanos, cabe à Informática executar esse procedimento.

5 — A autorização de acesso aos sistemas de informação deve manter-se válida enquanto subsistir a situação que justificou a sua emissão.

6 — As autorizações atribuídas são pessoais e intransmissíveis, competindo ao utilizador manter a confidencialidade e proteção das credenciais que lhe sejam atribuídas devendo, para o efeito, tomar as precauções necessárias para manter a palavra passe em segurança e utilizar as suas credenciais apenas em equipamentos de confiança.

Artigo 17.º

Política de mudança periódica de palavra passe

1 — As palavras passe são obrigatoriamente alteradas a cada 6 (seis) meses, com a obrigatoriedade do cumprimento dos seguintes requisitos de qualidade mínimos:

a) Não contenham três ou mais caracteres consecutivos iguais ao nome de utilizador ou nome completo;

b) Contenham pelo menos 13 caracteres;
c) Deverão cumprir pelo menos três das seguintes quatro regras:

i) Caracteres com letras maiúsculas (A…Z);
ii) Caracteres com letras minúsculas (a…z);
iii) Um algarismo (0…9);
iv) Caracteres especiais (!,$,#,&,.).

Os requisitos de qualidade mínimos são igualmente verificados aquando da alteração da palavra passe.

2 — Não é possível reutilizar palavras passe anteriores.

3 — A partir de 15 (quinze) dias antes da data de expiração da palavra passe serão enviados automaticamente avisos informando sobre o final do prazo da palavra passe.

4 — Após a expiração da palavra passe esta terá de ser reativada, através do contacto com os Serviços de Informática.

5 — No caso de 3 (três) erros sucessivos da palavra passe em trinta minutos, a conta ficará automaticamente bloqueada por trinta minutos. Após este período a conta estará novamente disponível. Este mecanismo pretende defender os utilizadores de tentativas de acesso com testes sucessivos de palavras passe associadas ao nome de utilizador.

CAPÍTULO V

Encarregado de proteção de dados

Artigo 18.º

Encarregado de proteção de dados

1 — Compete ao Secretariado Executivo designar o encarregado de proteção de dados.

2 — O encarregado de proteção de dados exerce a sua função com autonomia técnica, não recebe instruções relativamente ao exercício das suas funções, assim como não pode ser destituído nem penalizado pelo responsável pelo tratamento dos dados pessoais, pelo facto de exercer as suas funções.

3 — O encarregado de proteção de dados está obrigado ao dever de sigilo e de confidencialidade durante o exercício de funções, mantendo-se tal dever após o termo das mesmas.

Artigo 19.º

Funções do encarregado de proteção de dados

1 — O encarregado de proteção de dados serve como intermediário entre a CNPD, os titulares dos dados e o responsável pelo tratamento dos dados, exercendo as seguintes funções:

a) Informa e aconselha o responsável pelo tratamento dos dados, bem como os colaboradores que tratem os dados pessoais, a respeito das suas obrigações nos termos do presente Regulamento;
b) Controla de forma contínua a conformidade com o RGPD, legislação nacional, bem como com o presente Regulamento relativo à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados;
c) Assegura a realização de auditorias, quer periódicas, quer não programadas, incidindo estas nos seguintes pontos:

i) Regulamentos, processos e procedimentos internos;
ii) O registo dos tratamentos ou categorias de atividades de tratamentos;
iii) Os dados pessoais recolhidos e respetiva finalidade;
iv) Prazos de retenção dos dados pessoais;
v) As Avaliações de Impacto da proteção de dados realizadas;
vi) Os modelos de recolha do consentimento, caso necessários;

vii) A prova de que os titulares deram o seu consentimento, ou que existe habilitação legal ou contratual;

viii) A informação prestada aos titulares dos dados;

ix) Procedimentos e ferramentas existentes para o exercício dos direitos dos titulares dos dados;

x) Regras de acesso, privilégios aos dados pessoais tratados na entidade;

xi) Registos de acessos aos dados pessoais tratados na entidade;

xii) Contratos com os subcontratantes e respetivas cláusulas sobre a proteção de dados.

d) Assegura a relação com os titulares dos dados pessoais nas matérias abrangidas pelo RGPD, legislação nacional e o presente Regulamento na proteção dos dados;

e) Presta aconselhamento e emite pareceres, quando tal lhe for solicitado pelo responsável pelo tratamento dos dados, no que respeita à avaliação de impacto sobre a proteção de dados, controlando a sua realização;

f) Coopera com a CNPD e assegura a manutenção do *dossier* de conformidade;

g) Ponto de contacto para a CNPD sobre questões relacionadas com o tratamento de dados, incluindo a consulta prévia, cujo poder de decisão de realização é do responsável do tratamento, antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados indicar que do mesmo resultaria um elevado risco;

h) Colabora com o responsável pelo tratamento dos dados pessoais no reporte de qualquer violação de dados pessoais no prazo máximo de 72 horas;

i) Sensibiliza os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança.

2 — No desempenho das suas funções, o encarregado de proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

CAPÍTULO VI

Situações especiais

Artigo 20.º

Consentimento de menores

1 — O tratamento dos dados pessoais de menores relativos à oferta direta de serviços da sociedade de informação disponibilizados pela CIM-TS e especificamente definidos, é lícito, quando as mesmas deem formalmente o consentimento e já tenham completado 13 anos de idade.

2 — Caso a criança tenha idade inferior a 13 anos, o tratamento só é lícito se o consentimento for dado pelos representantes legais desta, de preferência com recurso a meios de autenticação segura, nomeadamente através de assinatura digital qualificada ou Chave Móvel Digital.

Artigo 21.º

Recolha, tratamento e divulgação de imagens, fotografias e/ou vídeos

1 — A recolha, a divulgação e as demais operações de tratamento de imagens, fotografias e/ou vídeos por parte da CIM-TS dependem de consentimento do titular dos dados, a quem deverá ser prestada toda a informação, em linguagem clara e simples, também sobre o destino de arquivamento.

2 — Quando a recolha, tratamento e divulgação de imagens, fotografias e/ou vídeos por parte da CIM-TS, disser respeito a menores deverá ser obtido o prévio consentimento dos seus representantes legais, privilegiando-se, no entanto, os direitos dos menores optando por captação de imagem de longe e de ângulos em que os mesmos não sejam facilmente identificáveis.

Artigo 22.º

Reuniões do Conselho Intermunicipal e Assembleia Intermunicipal *on-line*

1 — Quando os membros do Conselho Intermunicipal ou os eleitos da Assembleia Intermunicipal, dirigentes e outros colaboradores intervierem nas reuniões do Conselho Intermunicipal e/ou nas sessões da Assembleia Intermunicipal, deverá ser solicitado o prévio consentimento dos mesmos para recolha e subsequente tratamento de dados pessoais, quando esta situação se verificar, nomeadamente para a transmissão da sua imagem e o som da sua voz, que resultem das intervenções nestas reuniões para a transmissão *on-line*.

2 — Quando existirem intervenções por parte do público inscrito para participar nas reuniões do Conselho Intermunicipal e/ou sessões da Assembleia Intermunicipal, deverá ser solicitado o prévio consentimento dos mesmos, para recolha e subsequente tratamento de dados pessoais, quando esta situação se verificar, nomeadamente para transmissão da sua imagem e o som da sua voz, que resultem das intervenções nestas reuniões para a transmissão *on-line*.

3 — A recolha e subsequente tratamento dos dados pessoais mencionados nos números anteriores, com ou sem meios automatizados, incluem a recolha, o registo, a organização, a limitação da conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição.

4 — A gravação de som para efeitos de redação de ata não carece de consentimento dos titulares dos dados pessoais, uma vez que o fundamento de licitude para esta recolha assenta no cumprimento de uma obrigação legal.

Artigo 23.º

Videovigilância

1 — Sem prejuízo das disposições legais específicas que imponham a sua utilização, nomeadamente por razões de segurança pública, os sistemas de videovigilância cuja finalidade seja a proteção de pessoas e bens asseguram os requisitos previstos no artigo 31.º da Lei n.º 34/2013, de 16 de maio, na sua versão atual, de onde se destaca o referido no ponto seguinte.

2 — As câmaras não podem incidir sobre:

a) Vias públicas, propriedades limítrofes ou outros locais que não sejam do domínio exclusivo do responsável, exceto no que seja estritamente necessário para cobrir os acessos ao imóvel;

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

c) O interior de áreas reservadas aos colaboradores, designadamente zonas de refeição, vestiários, ginásios, instalações sanitárias e zonas exclusivamente afetas ao seu descanso.

3 — Nos casos em que é admitida a videovigilância, é proibida a captação de som, exceto no período em que as instalações vigiadas estejam encerradas ou mediante autorização prévia da CNPD.

Artigo 24.º

Proteção de dados pessoais de pessoas falecidas

1 — Quando forem recolhidos ou tratados dados de pessoas falecidas, nomeadamente, quando o Conselho Intermunicipal e/ou Assembleia Intermunicipal deliberar sobre votos de pesar, os dados pessoais que corresponderem aos de origem racial ou étnica, sobre opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual, ou quando se reportem à intimidade da vida privada, à imagem ou aos dados relativos às comunicações, torna-se necessário solicitar o consentimento escrito à pessoa que haja sido designada para o efeito pelo titular dos dados em vida ou, na sua falta, aos respetivos herdeiros para divulgar esses mesmos dados pessoais, salvo se o titular dos dados, em vida, tiver manifestamente tornado público os dados acima identificados.

2 — Todos os dados pessoais que não sejam identificados no número anterior, podem ser divulgados sem a necessidade de consentimento.

3 — A notificação da deliberação do Conselho Intermunicipal e/ou Assembleia Intermunicipal sobre o voto de pesar para um determinado endereço postal ou eletrónico, depende sempre do consentimento escrito dos herdeiros do falecido, assim como em situações idênticas que envolva os dados pessoais de pessoas falecidas.

4 — Os direitos de acesso, retificação e apagamento, são exercidos por quem a pessoa falecida haja designado para o efeito ou, na sua falta, pelos respetivos herdeiros.

5 — Os titulares dos dados podem igualmente, nos termos legais aplicáveis, deixar determinada a impossibilidade de exercício dos direitos referidos no número anterior após a sua morte.

Artigo 25.º

Publicação de dados pessoais

1 — A publicação de dados pessoais em jornais oficiais e plataformas eletrónicas, que sejam da responsabilidade da CIM-TS, devem obedecer aos princípios base, mencionados no artigo 5.º do presente Regulamento, nomeadamente ao princípio da finalidade e da minimização.

2 — Sempre que o dado pessoal "nome" seja suficiente para garantir a identificação do titular dos dados e a eficácia do tratamento, não devem ser publicados outros dados pessoais.

Artigo 26.º

Dados biométricos

1 — Consideram-se como 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.

2 — O tratamento de dados biométricos dos colaboradores da CIM-TS só pode ser considerado legítimo por razões de controlo de assiduidade e controlo de acessos às instalações da CIM-TS.

3 — Deve assegurar-se que só são utilizadas representações do dado biométrico (*template*) e que o processo não permita a reversibilidade dos dados.

4 — Os dados biométricos são conservados durante o período necessário para a prossecução das finalidades do tratamento a que se destinam, devendo ser destruídos no momento da transferência do trabalhador para outro local de trabalho ou da cessação do contrato de trabalho.

Artigo 27.º

Tratamento e prazo de conservação de dados pessoais

1 — O tratamento e o prazo de conservação de dados pessoais é o que estiver fixado por norma legal, regulamento intermunicipal ou norma associada à finalidade para a recolha de dados.

2 — O tratamento para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos deve respeitar o princípio da minimização dos dados e incluir a anonimização ou a pseudonimização dos mesmos sempre que os fins visados possam ser atingidos por uma destas vias.

3 — Quando os dados pessoais sejam tratados para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos, ficam prejudicados os direitos de acesso, retificação limitação do tratamento e de oposição, na medida do necessário, se esses direitos forem suscetíveis de tornar impossível ou prejudicar gravemente a realização desses fins.

CAPÍTULO VII

Disposições finais

Artigo 28.º

Responsabilidade civil, criminal, contraordenacional e disciplinar

A violação das normas do RGPD, legislação nacional e do presente Regulamento, pode gerar responsabilidade civil, criminal, contraordenacional e disciplinar.

Artigo 29.º

Publicação em jornal oficial

1 — A publicação de dados pessoais em jornais oficiais deve obedecer ao artigo 5.º do RGPD, nomeadamente aos princípios da finalidade e da minimização.

2 — Sempre que o dado pessoal «nome» seja suficiente para garantir a identificação do titular e a eficácia do tratamento, não devem ser publicados outros dados pessoais.

3 — Os dados pessoais publicados em jornal oficial não podem, em circunstância alguma, ser alterados, rasurados ou ocultados.

4 — O direito ao apagamento de dados pessoais publicados em jornal oficial tem natureza excecional e só se pode concretizar nas condições previstas no artigo 17.º do RGPD, nos casos em que essa seja a única forma de acautelar o direito ao esquecimento e ponderados os demais interesses em presença.

Artigo 30.º

Representação dos titulares dos dados

Sem prejuízo da observância das regras relativas ao patrocínio judiciário, o titular dos dados tem o direito de mandatar um organismo, uma organização ou uma associação sem fins lucrativos constituída em conformidade com o direito nacional, cujos fins estatutários sejam de interesse público e cuja atividade abranja a defesa dos direitos, liberdades e garantias do titular dos dados quanto à proteção de dados pessoais para, em seu nome, exercer os direitos previstos nos artigos 77.º, 78.º, 79.º e 82.º do RGPD.

Artigo 31.º

Dúvidas e omissões

Em tudo o que não se encontrar previsto no presente Regulamento, aplica-se subsidiariamente o RGPD, a legislação nacional e as orientações da CNPD.

Artigo 32.º

O presente Regulamento deverá ser revisto, obrigatoriamente, no prazo máximo de três anos.

Artigo 33.º

Entrada em vigor

O presente Regulamento entra em vigor no prazo de cinco dias após a sua publicação no *Diário da República.*

23 de fevereiro de 2022. — O Primeiro-Secretário da Comunidade Intermunicipal do Tâmega e Sousa, *Telmo Manuel Medeiros Pinto*.

315063621