Código de Conduta para Proteção de Dados Pessoais

matosinhos

Índice

Preâmbulo

Tendo em consideração que a conduta ética na execução das atribuições municipais se apresenta como elemento crucial da atividade administrativa, considera-se que a Câmara Municipal de Matosinhos, enquanto responsável pelo tratamento de dados pessoais de munícipes, trabalhadores e demais colaboradores e afins, reconhece a legalidade e transparência em todas as suas interações, bem como assegura o exercício de direitos relativos à proteção de dados de todos os titulares de dados pessoais, garantindo para tal, a aplicação de um Código de Conduta.

O presente Código de Conduta, cujo objetivo primordial é disciplinar internamente a recolha/tratamento de dados pessoais e a livre circulação dos mesmos nas atividades da Câmara Municipal de Matosinhos, destina-se a todos os trabalhadores e demais colaboradores, fornecedores, prestadores de serviços e demais entidades que possuem vínculo contratual com o Município. Tal código visa a correta aplicação da legislação de proteção de dados (composta pelo Regulamento Geral de Proteção de Dados, aprovado pelo 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, doravante RGPD, e pela Lei nº 58/2019, de 8 de agosto) e das correspondentes orientações da autoridade de controlo nacional e europeia, servindo por isso, como um instrumento de defesa de valores éticos e deontológicos, de promoção e aumento dos níveis de confiança no seio do Município (a qual constitui elemento demonstrativo do cumprimento das obrigações em matéria de proteção dos dados e correspondentes medidas técnicas e organizativas) e de efetiva defesa dos direitos dos titulares dos dados.

Ademais, considera-se crucial a adoção do elenco normativo apresentado, não só para garantir que os procedimentos são realizados da forma mais sigilosa e confidencial possível, como também assegurar que:

- os princípios da limitação das finalidades, de minimização e limitação da conservação dos dados (abaixo descritos ao pormenor) são efetivamente aplicados, permitindo assim uma necessária execução da privacidade desde a conceção (início do tratamento);
- os procedimentos de segurança e privacidade tecnológicos, como por exemplo as técnicas de anonimização e pseudonimização, são aplicados;
- os direitos dos titulares dos dados, consoante o fundamento de licitude a aplicar, são assegurados pelos funcionários e respetivos subcontratantes dos serviços municipais;
- as partilhas de informação são realizadas de forma mais prudente e lícita possível.

CAPÍTULO I
OBJETO E ÂMBITO DE APLICAÇÃO

Artigo 1º
Objeto e âmbito de aplicação

1. O presente Código de Conduta estabelece as regras, os termos e as condições pelas quais se rege a atuação do Município de Matosinhos, enquanto responsável pelo tratamento de dados pessoais, tendo em conta os direitos e os legítimos interesses dos titulares dos dados, em conformidade com o Regulamento (UE)2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (doravante designado abreviadamente por RGPD), com a legislação nacional aplicável (Lei nº 58/2019, de 8 de agosto) e com as orientações da Autoridade de Controlo Nacional (Comissão Nacional de Proteção de Dados).
2. São destinatários do presente documento:
   a) Os serviços municipais inseridos na Estrutura Orgânica da Câmara Municipal de Matosinhos;
   b) Os trabalhadores e demais colaboradores do Município de Matosinhos, independentemente da natureza do seu vínculo;
   c) Os prestadores de serviços, fornecedores, parceiros e demais entidades que possuam vínculo contratual com o Município.
3. É obrigação de todos os destinatários do presente código de conduta, concorrer para a proteção dos dados pessoais de acordo com o disposto nas disposições legais em vigor relativas à proteção de dados pessoais, não podendo nomeadamente, utilizar os dados pessoais para fins ilegítimos ou comunicá-los a pessoas não autorizadas ao respetivo acesso ou tratamento.
4. Na seleção e contratação dos subcontratantes, a Câmara Municipal de Matosinhos certifica-se que estes cumprem as regras no tratamento de dados pessoais, constantes do artigo 28º do RGPD.

Artigo 2º
Natureza

1. O Código reveste a natureza de regulamento administrativo, sendo aplicável ao tratamento de dados pessoais e, subsidiariamente, aos procedimentos legalmente tipificados que interajam com a matéria versada naquele.

2. A observância das regras aqui vertidas não dispensa os trabalhadores e demais colaboradores do município do conhecimento e cumprimento das restantes normas internas, disposições legais e demais regulamentos em vigor.

Artigo 3º

Definições

1. Para efeitos do presente manual de procedimentos e de acordo com o disposto no RGPD, 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, morada, email, vencimento, património, números de cartões, número de identificação, dados de localização, IP, vídeos, imagem, raça, dados biométricos, folhas de presença, avaliações, curriculum vitae, etc.

Tratamento, uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

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.

Subcontratante, uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

Destinatário, uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro.

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;

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.

Avaliação de Impacto sobre a Proteção de Dados (DPIA), 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.

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;

Dados genéticos, os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que transmita informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa.

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 dactiloscópicos.

Dados de saúde, dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde.

Ficheiro, qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico.

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

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.

CAPÍTULO II
PRINCÍPIOS GERAIS

Artigo 4º
Princípios Base

1. **Princípio da licitude, lealdade e transparência** - O tratamento dos dados pessoais deve ser objeto de tratamento lícito, leal e transparente em relação ao titular dos dados.
2. **Princípio da limitação das finalidades** – Os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de forma contraditória ou incompatível com as finalidades iniciais.
3. **Princípio da minimização dos dados** - Os dados pessoais devem ser os adequados, pertinentes e limitados ao que é necessário para o fim em vista.
4. **Princípio da exatidão** - Os dados pessoais devem ser exatos e atualizados sempre que necessário, sendo que, caso se verifique inexatidão, serão apagados ou retificados no mais curto espaço de tempo.
5. **Princípio da limitação da conservação** – O prazo de conservação dos dados pessoais não pode exceder o tempo necessário para a concretização da finalidade para as quais foram recolhidos.
6. **Princípio da integridade e confidencialidade** - Os dados pessoais devem ser 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 ou deliberada.

Artigo 5º
Licitude do tratamento dos dados pessoais

1. O tratamento de dados só é lícito quando se encontre preenchida pelo menos uma das seguintes condições:

a) Obtenção do consentimento do titular dos dados, o qual deve ser livre, específico, informado e inequívoco;

b) O tratamento seja necessário para a execução de um contrato ou para diligências pré-contratuais;

c) O tratamento seja necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito, ao exercício de funções de interesse

público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento;

d) O tratamento seja necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;

e) O tratamento seja necessário para efeito de prossecução dos interesses legítimos do responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Artigo 6º

Consentimento

1. O consentimento do titular dos dados deve ser dado de forma escrita (em suporte de papel ou via eletrónica, e sempre que possível, em formulário próprio), e fazer prova de que foi obtido de forma livre, específica e informada.
2. Da declaração de consentimento deve 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 dos dados.
3. A declaração de consentimento deve ficar registada e arquivada no serviço que a solicitou, de forma a ser possível ao responsável pelo tratamento de dados pessoais, demonstrar a licitude do tratamento.
4. O consentimento para o tratamento de dados pessoais de menores deve ser obtido junto dos responsáveis parentais (pais ou encarregados de educação).
5. O consentimento prestado para o envio de newsletters ou informação não institucional deve ser renovado de 3 em 3 anos.
6. A utilização e/ou cópia de documento de identificação pessoal só pode ser realizada mediante o consentimento escrito do titular.
7. À retirada do consentimento aplicar-se-ão com as devidas adaptações, as mesmas disposições procedimentais para a obtenção do consentimento.

Artigo 7º

Dados Sensíveis

1. Os dados de saúde recolhidos, nomeadamente para efeitos de medicina do trabalho, avaliação da capacidade de trabalho do trabalhador, diagnóstico médico, prestação de cuidados ou tratamentos de saúde, gestão de sistemas e serviços de saúde ou de ação

social devem ser encriptados e só poderão ser tratados por profissional sujeito à obrigação de sigilo profissional ou por pessoa igualmente sujeita a dever de confidencialidade.

2. Estão obrigados ao dever de sigilo, os titulares dos órgãos, os trabalhadores e demais colaboradores e prestadores de serviços do responsável pelo tratamento de dados de saúde, o encarregado de proteção de dados e todos os profissionais de saúde que tenham acesso aos dados.

Artigo 8º

Direitos dos titulares dos dados pessoais

1. Os titulares dos dados pessoais têm, a qualquer momento, o direito de acesso, retificação, atualização limitação e apagamento dos seus dados pessoais (sempre que legalmente aplicável), o direito de oposição à utilização dos mesmos fora do âmbito da finalidade do registo, bem como o direito à portabilidade dos seus dados.
2. O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento, sem prejuízo da licitude do tratamento efetuado com base no consentimento previamente dado.

Artigo 9º

Prazo de conservação de dados pessoais

1. O prazo de conservação de dados pessoais é o que estiver fixado por norma legal ou regulamentar ou, na falta desta, o que se revele necessário à prossecução da finalidade.
2. Quando os dados pessoais sejam necessários para o responsável pelo tratamento, ou o subcontratante comprovar o cumprimento de obrigações contratuais ou de outra natureza, os mesmos podem ser conservados enquanto não decorrer o prazo de prescrição dos direitos correspetivos.
3. Os dados relativos a declarações contributivas para efeitos de aposentação ou reforma podem ser conservados sem limite de prazo, a fim de auxiliar o titular na reconstituição das carreiras contributivas, desde que sejam adotadas medidas técnicas e organizativas adequadas a garantir os direitos do titular dos dados.

CAPÍTULO III

RESPONSÁVEL PELO TRATAMENTO E ENCARREGADO DE PROTEÇÃO DE DADOS

Artigo 10º

Responsável pelo tratamento

1. O responsável pelo tratamento de dados é a Câmara Municipal de Matosinhos.
2. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos que potencialmente poderão decorrer para os direitos e liberdades dos titulares dos dados, incumbe ao responsável pelo tratamento a determinação e aplicação das medidas técnicas e organizativas mais adequadas por forma a assegurar e comprovar que o tratamento é realizado em conformidade com o estipulado no RGPD. Essas medidas são revistas e atualizadas consoante as necessidades.
3. O responsável pelo tratamento adotará as medidas técnicas e organizativas, nomeadamente de recolha, tratamento e segurança do mesmo, restrições de acesso, anonimização, apagamento de dados, que em cumprimento com o princípio da transparência e informação serão devidamente explicadas aos trabalhadores e demais colaboradores através de ações de formação adequadas.
4. São, de igual modo, competências do responsável pelo tratamento:
    a) Comunicar à autoridade de controlo, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, as violações de dados pessoais que impliquem risco para os direitos e liberdades fundamentais dos titulares dos dados.
    b) Caso o responsável não respeite o prazo de comunicação anteriormente indicado, a mesma deverá fazer-se acompanhar pelos motivos de atraso.
    c) Caso seja suscetível de resultar num elevado risco para os seus direitos e liberdades fundamentais, comunicar ao titular dos dados a violação dos mesmos.
5. Excetuam-se do anteriormente referido, as situações em que:
    a) Implique um esforço desproporcionado por parte do responsável pelo tratamento – situação em que é realizada uma comunicação pública;
    b) O responsável tenha aplicado medidas técnicas e organizativas adequadas de proteção de dados pessoais, que impossibilitem o acesso por parte de pessoas não autorizadas. Apresenta-se como exemplo destas medidas, a cifragem de dados;
    c) O responsável tenha tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados não é suscetível de se concretizar.

6. Realizar, antes de iniciar o tratamento de dados, uma avaliação de impacto da realização de tal tratamento na privacidade dos titulares dos dados. Deverão avaliar-se a natureza, o âmbito, o contexto, as finalidades do tratamento e as fontes do risco, bem como a necessidade de consultar a autoridade de controlo.
7. Solicitar pareceres ao encarregado de proteção de dados, para os efeitos anteriormente indicados.
8. Apoiar o encarregado de proteção de dados no exercício das suas funções, fornecendo-lhe não só os recursos necessários ao seu desempenho e à manutenção dos seus conhecimentos, como também o acesso aos dados pessoais e às operações de tratamento.
9. O responsável pelo tratamento recorre a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas e asseverem os direitos do titular dos dados.

Artigo 11º

Encarregado de Proteção de Dados

1. São funções do encarregado de proteção de dados:
   a) Informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores e demais colaboradores que tratem os dados, a respeito das suas obrigações;
   b) Controlar a conformidade dos tratamentos efetuados ao abrigo do RGPD com outras disposições de proteção de dados da União ou nacionais e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados e as auditorias correspondentes;
   c) Assegurar a realização de auditorias, quer periódicas, quer programadas;
   d) Prestar aconselhamento e emitir pareceres, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados;
   e) Sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança;
   f) Considerar os riscos referentes aos tratamentos de dados, tendo em conta a sua natureza, âmbito, contexto e finalidade;

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

h) Colaborar com a autoridade de controlo.

Artigo 12º

Medidas técnicas e organizativas para proteção de dados

1. Cada responsável pelo tratamento e, sendo caso disso, o seu representante conserva um registo de todas as atividades de tratamento sob a sua responsabilidade, sendo que dele constam:

a) O nome e os contactos do responsável pelo tratamento;

b) As finalidades do tratamento dos dados;

c) A descrição das categorias de titulares de dados e das categorias de dados pessoais;

d) Se possível, os prazos previstos para o apagamento das diferentes categorias de dados;

e) Descrição geral das medidas técnicas e organizativas no domínio da segurança;

2. O responsável pelo tratamento e o subcontratante devem aplicar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

f) A pseudonimização e a cifragem dos dados pessoais;

g) A garantia de que o acesso à informação é realizado apenas pelos trabalhadores e demais colaboradores que possuam intervenção no procedimento/processo e que o nome, motivo para consulta, data e número do processo ou documento consultado se encontram registados aquando do acesso. Caso tal acesso seja realizado de modo físico e não lógico (mediante a consulta de arquivos em papel que ainda possam existir), tal registo deverá obedecer às instruções referidas no 1º período, uma vez que os documentos se deverão encontrar arquivados em locais fechados e as respetivas chaves na posse de trabalhadores e demais colaboradores designados para o efeito, pelos dirigentes/responsáveis da unidade orgânica;

h) A salvaguarda da segurança dos titulares dos dados, não só através do cumprimento dos requisitos técnicos previstos na Resolução do Conselho de Ministros nº 41/2018, de 28 de março (a qual confere orientações técnicas para a atuação da Administração Pública no domínio da arquitetura de segurança de redes e sistemas de informação referentes à proteção de dados), como também da definição das permissões no que à consulta e alterações dos processos diz respeito. Tais permissões deverão ser estipuladas pelos dirigentes/ responsáveis das respetivas unidades orgânicas, que

deverão articular diretamente com o responsável da Divisão de Sistemas de Informação e Comunicação (divisão competente para a aplicação dos requisitos inicialmente referidos);

i) A realização de avaliações de impacto das operações de tratamento sobre a proteção de dados pessoais, sempre que tais operações resultem ou possam resultar num elevado risco para os direitos e liberdades das pessoas singulares;

j) A garantia de que a recolha apenas versa sobre os dados estritamente necessários para o tratamento em causa;

k) A garantia de confidencialidade, integridade e disponibilidade dos sistemas e dos serviços de tratamento, com particular atenção às categorias de dados sensíveis que possam ser recolhidos no âmbito da atividade da Organização;

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

3. Neste sentido, deverá consultar-se a Política de Privacidade e os demais procedimentos relativos à segurança de tratamentos dos dados pessoais, disponíveis no endereço eletrónico do Município.

Artigo 13º

Procedimentos, Competências e Responsabilidades

1. Todos os trabalhadores e demais colaboradores estão obrigados a cumprir e a fazer cumprir as presentes regras e o dever de zelar pela sua proteção.
2. Os dirigentes da câmara municipal e/ou responsáveis pelas restantes unidades orgânicas da câmara municipal, devem identificar as atividades do município em que se encontram envolvidos, bem como os respetivos dados e forma de tratamento de dados pessoais, através do registo detalhado e circunstanciado no Mapa de Registo de Atividades de Tratamento.
3. Da mesma forma, devem identificar e registar todos os contratos com subcontratantes que tratem dados pessoais em nome da Câmara Municipal de Matosinhos no Mapa de Registo de Contratos/Subcontratantes/Terceiros.
4. Os dirigentes e/ou responsáveis pelas unidades orgânicas devem comunicar ao encarregado da proteção de dados a informação recolhida nos pontos anteriores e mantê-la atualizada.
5. Na elaboração de Cadernos de Encargos e/ou na formalização dos Contratos com Subcontratantes que tratem dados pessoais em nome da Câmara Municipal de Matosinhos deverá estar prevista uma cláusula de proteção de dados.

6. O acesso a documentos que contenham dados pessoais deve estar claramente definido e registado, podendo apenas ser efetuado pelo trabalhador ou colaborador para tal autorizado pelo seu superior hierárquico.

Artigo 14º

Subcontratantes

1. Na seleção e contratação dos Subcontratantes, a Câmara Municipal de Matosinhos certifica-se que estes cumprem as regras legais no tratamento de dados pessoais, devendo as mesmas constar dos contratos a celebrar.
2. Para avaliar a conformidade com o RGPD, os fornecedores a contratar deverão preencher o "Questionário de Fornecedores" (Pasta T) relativo ao Tratamento de Dados.

Artigo 15º

Procedimentos e condutas a adotar pelos trabalhadores e demais colaboradores municipais

1. Só podem ser recolhidos os dados pessoais para os efeitos processuais ou procedimentais que forem estritamente necessários.
2. Caso exista a necessidade por parte dos serviços de recolher dados pessoais adicionais que não se encontrem previstos na lei ou em qualquer outro normativo, torna -se sempre necessário obter o consentimento escrito do titular dos dados.
3. A recolha de dados pessoais junto dos respetivos titulares, deve ser precedida de informação aos mesmos sobre a finalidade que a determinou e processar-se em estrita adequação e pertinência a essa finalidade.
4. Os trabalhadores e demais colaboradores da Câmara Municipal de Matosinhos devem impreterivelmente assegurar:
   a) Que o tratamento é efetuado apenas no âmbito das finalidades para as quais os mesmos foram recolhidos;
   b) Que a recolha, utilização e conservação é realizada apenas sobre os dados pessoais mínimos, necessários e suficientes para a finalidade respetiva;
   c) Que a conservação dos dados pessoais é efetuada apenas pelo período necessário para o cumprimento da finalidade do tratamento que lhe deu origem;
   d) Que o tratamento dos dados pessoais é realizado para fins legalmente previstos ou para a prossecução de serviços online a seu pedido.
5. A documentação rececionada no atendimento ao público (*FrontOffice*) deverá ser remetida para o serviço respetivo (*BackOffice*), e não deverá estar visível a pessoas terceiras.

6. A transmissão de procedimentos que contenham dados pessoais sensíveis e dados constantes de participações e processos disciplinares via gestão documental não deve permitir a identificação do titular dos referidos dados.
7. 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.
8. Apenas serão transmitidos dados a terceiros quando o titular o solicite ou autorize por escrito.
9. Não pode ser fornecida qualquer informação com dados pessoais pelo telefone, a menos que seja possível certificar a identidade da pessoa que solicita a informação.
10. As comunicações realizadas via email deverão ser remetidas individualmente ou em "cópia cega" de forma a ocultar os diferentes endereços.
11. Os trabalhadores e demais colaboradores devem garantir que nenhuma impressão e/ou cópia que contenha dados pessoais fica esquecida na impressora/fotocopiadora.
12. Os documentos em papel que contenham dados pessoais devem ser destruídos em máquinas próprias.

CAPÍTULO IV
REGRAS ESPECÍFICAS

Artigo 16º
Medidas de segurança - Acesso e arquivamento

1. O acesso aos dados pessoais recolhidos deve estar devidamente acautelado, no sentido de apenas poderem aceder aos mesmos os trabalhadores e demais colaboradores que em determinado momento processual estejam a desenvolver algum procedimento que os legitime.
2. Devem estar previstas e definidas áreas de acesso restrito e controlado através de mecanismos que permitam o acesso unicamente a pessoas autorizadas.
3. Em cada serviço deve ser criado um registo que confirme o acesso, onde conste o nome do trabalhador ou colaborador, o motivo para a consulta, a data e a identificação do documento ou processo.
4. 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 trabalhadores 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 ou colaborador, o motivo para a consulta, a data e a identificação do documento/processo.

5. 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 17º

Publicação de dados pessoais

Quaisquer publicações de dados pessoais exigidas ao município, nomeadamente publicações em Diário da República ou plataformas de contratação pública deverão obedecer aos princípios elencados no artigo 4º do presente código. Daqui se destaca o princípio da minimização dos dados, o qual implica a utilização dos dados absolutamente necessários para garantir a transparência da administração pública.

Artigo 18º

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

1. A recolha, tratamento e divulgação de imagens, fotografias e vídeos por parte do município deverá ser sujeita ao prévio consentimento do titular dos dados, devendo ser prestada toda a informação, em linguagem clara e simples (conforme minuta colocada na pasta partilhada).
2. Quando a recolha, tratamento e divulgação de imagens, fotografias e/ou vídeos por parte do município, compreender menores, deverá ser obtido o prévio consentimento dos seus representantes legais. Caso não seja possível, impõe-se que tal captação seja realizada de costas e incida sobre planos afastados, de forma que os seus titulares não sejam identificáveis.
3. Caso se preveja a organização de eventos públicos, em que tal captação não seja proibida, impõe se ao município o dever de informar pelos meios adequados o respetivo público.

Artigo 19º

Especificidades aplicáveis ao consentimento

1. Relativamente à oferta de serviços da sociedade de informação disponibilizados pelo Município, mormente envio de newsletter, deverá atender-se à especificidade do

tratamento de dados realizados a menores, uma vez que o seu consentimento só será lícito quando o mesmo apresente pelo menos 13 anos de idade.

2. Caso o menor não apresente idade igual ou superior a 13 anos, deverá ser solicitado o consentimento aos respetivos representantes legais, de preferência com recurso a meios de autenticação segura.
3. Tal pedido de consentimento deverá redigir-se numa linguagem clara e simples que o menor compreenda facilmente.

Artigo 20º

Reuniões online

1. Sempre que necessário, e com exceção das situações em que haja obrigatoriedade legislativa, deverá ser solicitado o prévio consentimento a todos aqueles que intervierem nas reuniões da câmara municipal e/ou sessões da assembleia municipal para proceder à gravação das suas intervenções na ata e/ou transmissões da sua imagem/som.
2. Para efeitos deste tratamento de dados, deverão ser tomadas todas as medidas técnicas e organizativas adequadas para assegurar a privacidade dos intervenientes. Porém, haverá sempre risco perante a circulação em rede sem condições de segurança e a respetiva visualização/atualização dos dados pessoais por terceiros não autorizados.

Artigo 21º

Violação de dados pessoais

1. A violação de dados pessoais é definida como 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.

São incidentes de privacidade, designadamente:

a) A divulgação não autorizada ou acidental de informações confidenciais;
b) O roubo ou perda de informações ou equipamentos sensíveis;
c) Os incidentes de segurança que levem a um incidente de privacidade que cause divulgação acidental e ilegal de informações pessoais (ataques de códigos maliciosos, acessos não autorizados ou intrusões ao sistema, recolha e divulgação não autorizada de dados, utilização não autorizada de serviços ou equipamentos do sistema)

2. É dever de todos os trabalhadores e demais colaboradores dar conhecimento ao seu superior hierárquico, de qualquer situação que possa implicar uma violação de dados

pessoais, bem como comunicá-la, com carácter de urgência, ao Encarregado de Proteção de Dados, através do endereço eletrónico dpo@cm-matosinhos.pt ou qualquer outro meio mais expedito.

3. As notificações de violação de dados pessoais aos titulares dos dados e à CNPD são da competência do responsável pelo tratamento de dados (câmara municipal) que notifica desse facto a autoridade de controlo, 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 num risco para os direitos e liberdades das pessoas singulares.
4. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.
5. Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento de dados comunica a violação de dados pessoais ao titular dos dados sem demora injustificada.
6. Neste sentido, dever-se-á remeter para a Política de Gestão de Incidentes de violação de dados pessoais aplicável ao Município.

Artigo 22º

Segredo Profissional

1. Os trabalhadores e demais colaboradores da Câmara Municipal de Matosinhos, independentemente do vínculo existente, bem como prestadores de serviços e fornecedores que tratem dados pessoais, encontram-se, salvo obrigação legal ou decisão judicial, sujeitos ao segredo profissional.
2. Os trabalhadores e demais colaboradores da Câmara Municipal de Matosinhos são responsáveis a título civil, disciplinar e penal pela violação ou disseminação ilegal dos dados pessoais a que tenham acesso devido ou indevido, a apurar em procedimento disciplinar próprio.
3. Os restantes trabalhadores e demais colaboradores, fornecedores ou prestadores de serviços são responsáveis nos termos contratuais e legalmente estabelecidos.
4. Esta obrigação de confidencialidade manter-se-á em vigor mesmo após a cessação das funções ou dos contratos celebrados, seja qual for a causa da cessação dos mesmos e por todo o tempo que seja necessário ao cumprimento da lei.

Artigo 23º

Receção de reclamações

Quaisquer reclamações referentes a operações de recolha, tratamento e arquivo de dados pessoais, são imediatamente encaminhadas para o encarregado de proteção de dados para apreciação, decisão e resposta a comunicar ao reclamante.

Artigo 24º

Videovigilância

1. Sem prejuízo da legislação que imponha a utilização de câmaras de videovigilância, mormente por questões de segurança pública, considera-se legítima a sua utilização para proteção de pessoas e bens, a qual deverá respeitar os requisitos estabelecidos no artigo 31º da Lei nº 34/2013, de 16 de maio, na sua versão atualizada.
2. De notar que, segundo o previsto no artigo 19º nº2 da Lei nº 58/2019, de 8 de agosto, as câmaras não poderão 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 a clientes ou utentes onde deva ser respeitada a privacidade, designadamente instalações sanitárias, zonas de espera e provadores de vestuário;
   d) O interior de áreas reservadas aos trabalhadores e demais colaboradores, designadamente zonas de refeição, vestiários, ginásios, instalações sanitárias e zonas exclusivamente afetas ao seu descanso.
3. Nos estabelecimentos de ensino, 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.
4. 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 25º

Dados biométricos

1. Como se encontra estabelecido no artigo 28º nº6 da Lei nº 58/2019, de 8 de agosto, o tratamento de dados biométricos só é considerado legítimo para controlo de assiduidade e controlo de acessos às instalações do município, devendo assegurar-se a utilização de apenas representações que não permitam a sua reversão.
2. O processo de recolha destes dados deverá ser devidamente documentado e acompanhado pelo encarregado de proteção de dados.

Artigo 26º

Esclarecimentos e aplicação do código

1. Os pedidos de esclarecimento, dúvidas de interpretação ou aplicação do presente Código de Conduta deverão ser dirigidos ao Encarregado de Proteção de Dados que responderá ou reencaminhará para o departamento competente para responder.

2. As eventuais omissões no Código de Conduta serão supridas pelo estipulado no RGPD, na respetiva Lei de Execução Nacional (Lei nº 58/2019, de 8 de agosto) e em demais legislação aplicável.

Artigo 27º

Entrada em vigor

O presente Código entra em vigor no 3º dia útil subsequente à sua publicitação.