DIÁRIO DA REPÚBLICA

2.ª série
N.º 74
15-04-2024

MUNICÍPIO DE MÉRTOLA

Edital n.º 503/2024

Sumário: Aprovação do projeto do Regulamento de Proteção de Dados Pessoais do Município de Mértola.

Projeto de Regulamento de Proteção de Dados Pessoais do Município de Mértola

Mário José Santos Tomé, Presidente da Câmara Municipal de Mértola,

Torna público, que em reunião ordinária de 20 de março de 2024, o órgão executivo deliberou aprovar o Projeto de Regulamento de Proteção de Dados Pessoais do Município de Mértola, e que de acordo com o estabelecido no artigo 101.º do Código do Procedimento Administrativo, se encontra para consulta pública, para recolha de sugestões, pelo prazo de 30 dias a contar da data da publicação do presente edital no *Diário da República*, 2.ª série.

Mais se informa que o presente Projeto de Regulamento Municipal está disponível para consulta dos/as interessados/as junto do Gabinete de Atendimento, na Rua Dr. Afonso Costa, n.º 45 ou no sítio do Município em www.cm-mertola.pt.

Poderão os/as interessados/as dirigir as suas sugestões à Câmara Municipal de Mértola, podendo estas ser enviadas por carta registada com aviso de receção para Praça Luís de Camões, 7750-329 Mértola, ou aí entregues pessoalmente, bem como remetidas através do e-mail geral@cm-mertola.pt.

A presente proposta será sujeita a aprovação da Assembleia Municipal, nos termos da alínea g) do n.º 1 do artigo 25.º da Lei n.º 75/2013, de 12 de setembro.

Para constar e devidos efeitos se publica este e outros de igual teor que vão ser afixados nos lugares de estilo.

21 de março de 2024. — O Presidente da Câmara Municipal, Mário José Santos Tomé.

317532542

MÉRTOLA
CÂMARA MUNICIPAL

PROJETO DE REGULAMENTO DE PROTEÇÃO DE DADOS PESSOAIS DO MUNICÍPIO DE MÉRTOLA

2024

Preâmbulo

O Regulamento Geral de Proteção de Dados(UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, doravante designado por RGPD, estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, o referido diploma 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, revogando a Diretiva 95/46/CE do Parlamento Europeu e do Conselho.

Considerando que a conduta ética na execução das atribuições municipais se apresenta como elemento crucial da atividade administrativa, o Município de Mértola, enquanto entidade responsável pelo tratamento de dados pessoais elaborou o presente regulamento, cujo objetivo primordial é disciplinar internamente a recolha e tratamento de dados pessoais e a livre circulação dos mesmos nas atividades municipais.

O presente regulamento destina-se a todos os trabalhadores e demais colaboradores, fornecedores, parceiros, prestadores de serviços e demais entidades que possuem vínculo contratual com o Município de Mértola e 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, 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, e de efetiva defesa dos direitos dos titulares dos dados.

Considera-se crucial a adoção do elenco normativo apresentado, por forma a garantir:

- Que os procedimentos são realizados da forma mais sigilosa e confidencial possível;
- Que os princípios da minimização, limitação da finalidade e conservação dos dados são efetivamente aplicados, permitindo assim uma necessária execução da privacidade desde o início do tratamento;
- Que os procedimentos de segurança e privacidade, são aplicados;
- Que os direitos dos titulares dos dados, consoante o fundamento de licitude a aplicar, são assegurados pelos funcionários e respetivos subcontratantes.

O presente regulamento, apesar de fazer referência a normas e medidas organizativas internas, excede o âmbito de aplicação meramente interno uma vez que estas normas e medidas estabelecem uma relação e âmbito de aplicação com titulares de dados pessoais externos.

Com base nesta premissa e pelo facto de apresentar uma panóplia de destinatários, considera-se que o presente regulamento tem eficácia externa.

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 e seguintes do Código do Procedimento Administrativo, do n.º 1 e 2 do artigo 23.º, da alínea g), do n.º 1 do artigo 25.º, da alínea k), do n.º 1, do artigo 33.º do Anexo I à Lei n.º 75/2013, de 12 de setembro, na sua atual redação, 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) e da Lei n.º 58/2019, de 8 de agosto.

Artigo 2.º

Objeto

O presente regulamento estabelece as regras, os termos e as condições pela quais se rege a atuação do Município de Mértola, enquanto responsável pela recolha e tratamento de dados pessoais e à livre circulação desses dados por parte do Município, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de terceiros, 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, bem como da legislação nacional aplicável e orientações das autoridades de controlo.

Artigo 3.º

Âmbito de aplicação

1. O presente regulamento aplica -se a todos os tratamentos de dados pessoais realizados por parte do Município de Mértola, com recurso a meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.
2. São destinatários do presente regulamento:
    a) Os serviços municipais inseridos na estrutura orgânica da Câmara Municipal de Mértola;
    b) Os trabalhadores e demais colaboradores do Município de Mértola, independentemente da natureza do seu vínculo;
    c) Os prestadores de serviços, fornecedores, parceiros e demais entidades que possuam vínculo contratual com o município;

d) Todas as pessoas singulares, que a qualquer título, se relacionem com o Município de Mértola.

3. O presente regulamento aplica-se também aos titulares de órgãos municipais, e aos membros dos respetivos gabinetes em tudo o que não seja incompatível com o estatuto normativo a que se encontram especialmente vinculados.

Artigo 4º

Deveres gerais

1. É obrigação de todos os destinatários do presente regulamento, 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.
2. Quando o tratamento dos dados pessoais for efetuado por subcontratantes, o Município de Mértola certifica-se que estes cumprem as regras no tratamento de dados pessoais, constantes no RGPD e asseguram a defesa dos direitos dos titulares dos dados.
3. 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.
4. Os titulares dos dados devem exercer os seus direitos com respeito ao princípio da boa-fé, prestando informações adequadas, claras, corretas e precisas ao responsável pelo tratamento de dados, por forma a viabilizar um tratamento lícito, leal e transparente dos dados pessoais.

Artigo 5.º

Definições

1. Para efeitos do presente regulamento, entende -se por:
    a) **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.
    b) **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.

c) **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.

d) **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.

e) **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;

f) **Responsável pelo tratamento**, a pessoa singular ou coletiva, no caso do presente regulamento, o Município de Mértola, representado pelo presidente da Câmara Municipal que determina as finalidades e os meios de tratamento de dados pessoais;

g) **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.

h) **Avaliação de impacto sobre a proteção de dados** (PIA) Diligência e estudo prévio no âmbito da proteção de dados cujo tratamento seja suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares

i) **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;

j) **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.

k) **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.

l) **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.

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

n) **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.

CAPÍTULO II
PRINCÍPIOS

Artigo 6.º
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.

Artigo 7.º
Princípio da limitação das finalidades

1. Os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas, claras e legítimas, não podendo ser tratados posteriormente de forma contraditória ou incompatível com as finalidades iniciais.
2. O tratamento posterior de dados para fins de arquivo de interesse público, de investigação científica ou histórica, bem como para fins estatísticos não se considera incompatível com as finalidades iniciais e com o princípio referido no número anterior.

Artigo 8.º
Princípio da minimização dos dados

Os dados pessoais devem ser os adequados, pertinentes e limitados ao que é necessário para a finalidade estabelecida.

Artigo 9.º

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.

Artigo 10.º

Princípio da limitação da conservação

1. Os dados pessoais devem ser conservados somente durante o tempo necessário para as finalidades para as quais são tratados.
2. Os dados pessoais podem ser conservados durante períodos mais longos do que os exclusivamente necessários à prossecução da respetiva finalidade, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica bem como para fins estatísticos.

Artigo 11.º

Princípio da integridade e confidencialidade

Os dados pessoais devem ser tratados de uma forma que garanta a sua segurança, incluindo todas as medidas organizacionais ou tecnicamente adequadas, que os protejam contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental ou deliberada.

Artigo 12.º

Princípio de responsabilidade

O responsável pelo tratamento é responsável pelo cumprimento do disposto nos princípios constantes nas alíneas anteriores bem como a respetiva comprovação.

CAPÍTULO III

RESPONSÁVEL PELO TRATAMENTO DE DADOS

Artigo 13.º

Responsável pelo tratamento de dados pessoais

1. O responsável pelo tratamento de dados é o Município de Mértola, o qual, nos termos da lei, é representado pelo Presidente da Câmara Municipal.
2. O responsável pelo tratamento determina a aplicação das medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o RGPD, legislação nacional e o presente regulamento.

Artigo 14.º

Competências do responsável pelo tratamento de dados pessoais

1. Sem prejuízo das demais competências previstas no RGPD, são competências do responsável pelo tratamento de dados pessoais:
    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 especifica do tratamento, de forma a poder comprovar que o tratamento é realizado em conformidade com o RGPD, legislação nacional e o presente regulamento.
    b) Comunicar à autoridade de controlo as violações dos dados pessoais que lhe sejam comunicadas pelo encarregado da proteção de dados, 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 autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada da justificação com os 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 a que se refere a alínea c) já não for suscetível de se concretizar;
        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.
2. O responsável pelo tratamento de dados deve conservar um registo de todas as atividades de tratamento sob a sua responsabilidade do qual conste as seguintes informações:
    a) O nome e os contactos do responsável pelo tratamento e do encarregado da proteção de dados;
    b) As finalidades do tratamento dos dados;
    c) A descrição das categorias de titulares de dados e das categorias de dados pessoais;

d) As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais;
e) Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais;
f) Se possível, os prazos previstos para o apagamento das diferentes categorias de dados;
g) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança.

3. O responsável pelo tratamento de dados deve proceder, antes de iniciar o tratamento de dados pessoais, a uma avaliação de impacto (PIA) sobre a proteção dos referidos dados, quando o mesmo for suscetível de resultar num elevado risco para os direitos, liberdades e garantias das pessoas. 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.
4. Solicitar pareceres ao encarregado da proteção de dados, nos termos do número anterior.
5. Incumbe ao responsável pelo tratamento de dados consultar previamente ao tratamento a autoridade de controlo sempre que no âmbito de uma avaliação de impacto (PIA) se concluir que o mesmo, na ausência de garantias e de medidas e procedimentos de segurança para atenuar os riscos, implica um elevado risco para os direitos e liberdades das pessoas singulares que não pode ser atenuado através de medidas razoáveis, atendendo à tecnologia disponível e aos custos de aplicação.
6. Apoiar o encarregado da proteção de dados no exercício das suas funções, fornecendo-lhe os recursos necessários ao desempenho dessas funções e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento.

CAPÍTULO IV
ENCARREGADO DA PROTEÇÃO DE DADOS

Artigo 15.º
Encarregado da proteção de dados

1. Compete ao Município de Mértola, enquanto órgão público e responsável pelo tratamento dos dados pessoais, a designação do Encarregado da Proteção de Dados (EPD), que deverá ser designado com base nas suas qualidades profissionais e, em especial, nos seus

conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como nas suas capacidades para desempenhar as suas funções por forma a promover uma cultura de proteção de dados no Município.

2. As funções de EPD são exercidas com total independência, autonomia em relação à estrutura dos serviços, isenção, distanciamento e não subordinação à hierarquia municipal, não podendo o seu titular ser prejudicado, penalizado pelo exercício das mesmas, ou do teor dos pareceres que emite ou das iniciativas que desenvolve no âmbito das suas competências.
3. O EPD encontra-se sujeito ao dever de sigilo e confidencialidade durante o exercício das suas funções, mantendo-se tal dever após o termo das mesmas.
4. O Encarregado da proteção de dados, quando exerça outras funções ou atribuições, não deve estar sujeito a qualquer conflito de interesses e, na eventualidade de tal se verificar em momento superveniente à sua nomeação, deve optar entre as mesmas.

Artigo 16.º

Funções do encarregado da proteção de dados

1. O EPD serve como intermediário entre a autoridade de controlo, os titulares dos dados e o responsável pelo tratamento dos dados, exercendo as seguintes funções:
   a) Informar e aconselhar o responsável pelo tratamento dos dados, bem como os trabalhadores que tratem os dados pessoais, a respeito das suas obrigações nos termos do presente regulamento;
   b) Controlar 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 e as auditorias correspondentes;
   c) Assegurar a realização de auditorias, quer periódicas, quer não programadas;
   d) Assegurar as relações com os titulares dos dados pessoais nas matérias abrangidas pelo RGPD, pela legislação nacional e pelo presente regulamento na proteção dos dados;
   e) Prestar aconselhamento e emitir 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) Cooperar com a autoridade de controlo, sendo o seu ponto de contacto quanto a questões relacionadas com o tratamento, incluindo a consulta prévia quando a avaliação de impacto sobre a proteção de dados indicar que do mesmo resulta um elevado risco;
   g) Colaborar com o responsável pelo tratamento dos dados pessoais no reporte de qualquer violação de dados pessoais no prazo máximo de 72 horas;

h) 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 EPD deve ter em consideração os riscos associados às operações de tratamento, observando a sua natureza, o âmbito, o contexto e as finalidades do tratamento.

Artigo 17.º

Direitos

1. O Encarregado da Proteção de Dados tem direito a:
   a) Dispor dos recursos financeiros e humanos necessários ao desempenho das suas funções;
   b) Dispor do tempo suficiente para o desempenho das suas tarefas;
   c) Ter acesso a todas as informações existentes nos serviços que lhe permitam exercer a sua função de forma célere e independente;
   d) Dispor dos meios necessários de ordem logística e tecnológicos necessários ao desempenho das suas funções.

CAPÍTULO V
PROTEÇÃO DE DADOS

SECÇÃO I
DIREITOS E TRATAMENTO DOS DADOS PESSOAIS

Artigo 18.º

Licitude do tratamento de dados pessoais

1. O tratamento de dados pessoais só é lícito na medida em que se verifique pelo menos uma das seguintes situações:
   a) Consentimento: O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades especificas; o qual deve ser livre, específico, informado e inequívoco;
   b) Execução de um contrato: O tratamento for necessário para execução de um contrato no qual o titular dos dados é parte, ou para diligências pré- contratuais a pedido do titular dos dados;
   c) Obrigação Jurídica: O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

d) Defesa de Interesse Vital: O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de qualquer pessoa singular;
e) Interesse Público e autoridade Pública: O tratamento for necessário ao exercício de funções de interesse público ou ao exercício de autoridade pública de que está investido o responsável pelo tratamento;
f) Interesse Legítimo: O tratamento for necessário para o efeito dos interesses legítimos prosseguidos pelo 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 19º

Consentimento

1. O consentimento previsto na al. a) do artigo anterior não deve ser dado, via de regra, de forma oral e não poderá revestir a forma de consentimento tácito.
2. O Consentimento por parte do titular dos dados deve ser dado de forma escrita, expressa, livre especifica e informada por ato inequívoco (em suporte de papel ou via eletrónica, e sempre que possível, em formulário próprio), permitindo ao responsável pelo tratamento poder demonstrar que obteve o consentimento do titular dos dados para o tratamento dos seus dados pessoais.
3. Na 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.
4. 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.
5. 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.
6. O consentimento dado tem que ser tão fácil de retirar quanto foi de dar.

Artigo 20.º

Licitude do tratamento de categorias especiais de dados pessoais

1. As categorias especiais de dados pessoais englobam os dados ou informações que implicam maiores riscos para os direitos e liberdades fundamentais de uma pessoa, que revelem a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação

sindical, dados genéticos, dados biométricos que permitam identificar uma pessoa de forma inequívoca, dados relativos à saúde, dados relativos à vida sexual ou orientação sexual.

2. É proibido o tratamento dos dados pessoais referidos no número anterior, salvo nos casos previstos no nº2 do artigo 9º do RGPD.

Artigo 21.º

Registos de atividades de tratamento de dados pessoais

1. O Município de Mértola, enquanto responsável pelo tratamento, conserva registos de todas as atividades de tratamento de dados pessoais sob a sua responsabilidade.
2. Dos registos das atividades de tratamento devem constar todos os elementos e informações legalmente exigidos.

Artigo 22.º

Finalidades do tratamento de dados pessoais

1. Consideram-se como finalidades do tratamento de dados pessoais no Município de Mértola:
   a) As previstas para o seu normal funcionamento;
   b) As previstas na alínea b) do n.º 1 do artigo 5.º do RGPD;
   c) A tramitação nos serviços municipais, por exigência legal, de procedimentos administrativos ou a celebração de contratos, seja oficiosamente ou a requerimento dos titulares dos dados;
   d) O cumprimento pelo Município de Mértola das suas atribuições ou obrigações legais e das suas funções de interesse público ou autoridade pública enquanto órgão da Administração Pública;
   e) O exercício pelos titulares dos dados ou pelo Município de Mértola de direitos e obrigações previstos na lei.
2. É vedada qualquer recolha e tratamento de dados pessoais que não seja determinada, explícita e legítima.

Artigo 23.º

Transmissão de dados pessoais

A transmissão de dados pessoais é permitida quando prevista em disposição legal, para cumprimento de direitos ou obrigações legalmente previstas e/ou se absolutamente necessária à prossecução do interesse público ou exercício de autoridade pública.

Artigo 24.º

Direito de informação

1. Aquando da recolha dos dados pessoais junto do seu titular este tem direito a que lhe seja facultada a seguinte informação:
   a) A identidade e contactos do responsável pelo tratamento e do seu representante;
   b) Os contactos do Encarregado da Proteção de dados;
   c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
   d) Se o tratamento de dados se basear no artigo 6º nº1 al. f) do RGPD, os interesses legítimos do responsável pelo tratamento ou de um terceiro;
   e) Os destinatários ou categorias de destinatários de dados pessoais, se os houver;
   f) Prazo de conservação dos dados, ou os critérios para definir esse prazo;
   g) Se os dados pessoais serão transferidos a país terceiro ou organização internacional conforme disposto no artº 13º nº1 al. f) do RGPD;
   h) A existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;
   i) A existência do direito de retirar o consentimento em qualquer altura;
   j) O direito de apresentar reclamação a uma autoridade de controlo;
   k) Se a comunicação de dados pessoais constitui, ou não, uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;
   l) A existência de decisões automatizadas;
   m) Para que a prestação da referida informação possa ser demonstrada e comprovada, a mesma será prestada nos formulários aplicáveis aos diversos procedimentos existentes no Município;
   n) Sempre que os dados pessoais não sejam recolhidos junto do seu titular, este tem ainda o direito a ser informado sobre as categorias dos dados pessoais em questão, a origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público,

Artigo 25.º

Direito de acesso

1. O titular dos dados tem direito de obter do responsável pelo tratamento confirmação de que os seus dados pessoais são, ou não, objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados e às seguintes informações:
   a) As finalidades a que se destina o tratamento dos dados;
   b) As categorias dos dados pessoais em questão;
   c) Os destinatários, ou categorias de destinatários a quem são comunicados os dados pessoais;
   d) O prazo previsto para conservação dos dados pessoais, ou os critérios utilizados para fixar esses prazos;
   e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou o direito de se opor a esse tratamento;
   f) O direito de apresentar reclamação a uma autoridade de controlo;
   g) As informações disponíveis sobre as origens dos dados, caso não tenham sido recolhidos junto do seu titular;
   h) A existência de decisões automatizadas.

Artigo 26.º

Direito de retirar o consentimento

1. Nas situações em que o tratamento de dados se baseia no consentimento, o titular dos dados tem o direito de o retirar a qualquer momento.
2. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado.
3. O consentimento deverá ser retirado de forma simples, semelhante àquela como foi prestado.

Artigo 27.º

Direito de retificação

1. O titular dos dados tem o direito de obter, sem demora injustificada, a retificação dos dados pessoais inexatos que lhe digam respeito.
2. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, mediante manifestação expressa e formal nesse sentido.

Artigo 28.º

Direito ao apagamento

1. O titular dos dados tem o direito de solicitar ao responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, quando se verifique alguma das seguintes circunstâncias:
   a) Os dados pessoais deixaram de ser necessários para a finalidade que sustentou a sua recolha ou tratamento;
   b) O titular dos dados retira o consentimento em que se baseia o tratamento dos dados pessoais, e não existe outro fundamento jurídico, para o tratamento dos mesmos;
   c) O titular dos dados opõe -se ao tratamento dos dados e o responsável pelo tratamento não demonstra que existem interesses legítimos prevalecentes que justifiquem o tratamento;
   d) Os dados foram tratados ilicitamente;
   e) O apagamento dos dados seja necessário para o cumprimento de uma obrigação legal a que o responsável pelo tratamento esteja sujeito.
2. O responsável pelo tratamento tem obrigação de apagar os dados pessoais, sem demora injustificada.
3. Quando o responsável pelo tratamento tenha tornado públicos os dados pessoais e for obrigado a apaga -los, por força do disposto nos números anteriores, deverá tomar as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos, salvo as exceções previstas no artº17 nº3 do RGPD.

Artigo 29.º

Direito à limitação do tratamento

1. O titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento nos seguintes casos:
   a) Tenha contestado a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão;
   b) O tratamento seja ilícito e o titular dos dados se tenha oposto ao apagamento dos dados pessoais, solicitando, em contrapartida, a limitação da sua utilização;
   c) O responsável pelo tratamento já não necessite dos dados pessoais para fins de tratamento, mas os mesmos sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;

d) Tenha exercido o direito de oposição, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

Artigo 30.º

Direito de portabilidade dos dados

1. O titular dos dados tem o direito de receber, do responsável pelo tratamento dos dados, os seus dados pessoais, num formato seguro, de uso corrente e de leitura automática, e transferi los para outro responsável pelo tratamento.
2. O direito referido no número anterior só pode ser exercido nas seguintes situações:
   a) Em caso de tratamento automatizado de dados (estão excluídos os registos de papel);
   b) Relativamente a dados fornecidos pelo titular ao responsável pelo tratamento;
   c) Caso em que o tratamento seja baseado no consentimento, ou em que o tratamento seja necessário para a execução de um contrato ou para diligências pré -contratuais.
3. O titular dos dados apenas poderá exigir que os seus dados sejam transmitidos diretamente entre os responsáveis pelo tratamento se tal for tecnicamente possível.

Artigo 31.º

Direito de oposição

1. O titular dos dados tem o direito de se opor, a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito.
2. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Artigo 32.º

Decisões individuais automatizadas

O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete, significativamente, de forma similar, com as exceções constantes no artº22º nº2 al a.), b.); e c.). do RGPD

Artigo 33.º

Tratamento de dados pessoais através de subcontratantes

1. O Município de Mértola recorre a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas por forma a salvaguardar que o

tratamento cumpre as exigências do RGPD assegurando a defesa dos direitos do titular dos dados.

2. O tratamento de dados através da subcontratação é regulado por contrato, ou outro ato normativo previsto na lei.

Artigo 34.º

Recolha de dados pessoais no sítio eletrónico do Município de Mértola

1. O acesso e a utilização do sítio eletrónico do Município de Mértola não implicam, em geral, a disponibilização e recolha de dados pessoais, o que sucede apenas através da utilização de funcionalidades pontuais, designadamente as que impliquem submissão de formulários, mediante o preenchimento dos dados pessoais solicitados e a submissão do formulário.
2. Quando os dados pessoais são recolhidos através do sítio eletrónico do Município de Mértola, considera-se que os utilizadores estão a dar o seu consentimento ao preencherem os seus dados pessoais e ao submeterem os respetivos formulários para cada finalidade em concreto.
3. A comunicação dos dados pessoais não constitui uma obrigação legal nem contratual.
4. O titular não está obrigado a fornecer os dados pessoais, mas não os fornecendo, não pode usufruir das respetivas funcionalidades oferecidas pelo sítio eletrónico do Município

Artigo 35.º

Participação nas reuniões dos órgãos autárquicos

1. Os titulares dos dados pessoais que, na qualidade de membros ou participantes, quer façam intervenções, que facilmente resultam na exposição da sua vida privada e familiar, ou que apenas intervenham através da mera presença, em reuniões dos órgãos autárquicos, devem prestar o seu consentimento livre, específico e informado, para o tratamento dos seus dados pessoais incluindo a captação, tratamento e respetiva difusão de voz e imagem, sem prejuízo das referidas transmissões, poderem circular em rede, correndo o risco de serem vistos e utilizados por terceiros não autorizados.
2. A recolha e tratamento dos dados pessoais mencionados no número anterior, com ou sem meios automatizados, incluem a recolha, o registo, a organização, a 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.

Artigo 36.º

Outras informações sobre o tratamento de dados pessoais

1. Em geral, a comunicação dos dados pessoais ao Município de Mértola é necessária para o exercício de direitos e cumprimento de obrigações legais ou contratuais.
2. A não disponibilização dos dados pessoais pelos titulares é impeditiva do exercício de direitos e do respetivo cumprimento de obrigações legais ou contratuais.

SECÇÃO II

PROCEDIMENTOS ADMINISTRATIVOS PARA EXERCÍCIO DOS DIREITOS DO TITULAR DOS DADOS PESSOAIS

Artigo 37.º

Forma de exercício dos direitos pelos titulares dos dados pessoais

1. O titular dos dados inicia o processo de exercício dos seus direitos, com o preenchimento de um formulário, a ser disponibilizado pelo Município de Mértola em formato digital ou papel, dirigido ao responsável pelo tratamento, o qual solicita um parecer ao EPD.
2. No âmbito do pedido, o titular dos dados deve identificar-se com rigor e comprovar a sua identidade ao Município de Mértola, sem fornecer mais dados do que aqueles que estão a ser tratados pelo responsável pelo tratamento.
3. O titular dos dados deve justificar e fundamentar o seu pedido de exercício de direitos.
4. O Município de Mértola deve facultar aos titulares dos dados as informações solicitadas, quer os dados tenham sido ou não recolhidos junto dos mesmos.
5. Sempre que o titular dos dados pretenda exercer o direito ao apagamento e à eliminação, o Município de Mértola deve notificar todas as entidades para onde os respetivos dados tenham sido partilhados, para que estas procedam em conformidade com o pedido efetuado.
6. O Município de Mértola facilita o exercício de direitos pelos titulares dos dados e fornece-lhes as informações sobre as medidas tomadas por forma a garantir o exercício dos referidos direitos no prazo de 30 (trinta) dias a contar da data de receção do pedido de exercício de direitos.
7. Relativamente ao pedido de exercício dos direitos do titular dos dados são, preferencialmente, utilizados os meios eletrónicos e as comunicações do Município com os requerentes, ao longo do procedimento, só podem processar-se através dos meios indicados no formulário disponibilizado, mediante seu prévio consentimento, prestado por escrito.
8. As informações prestadas e quaisquer comunicações e medidas tomadas são facultadas a título gratuito, sem prejuízo do exposto no n.º 10 do presente artigo.

9. Se o titular dos dados o solicitar a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.
10. Se os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, o responsável pelo tratamento pode:
    a. Exigir o pagamento de uma taxa razoável, tendo em conta os custos administrativos do fornecimento das informações, ou da comunicação, ou da tomada das medidas solicitadas;
    b. Recusar-se a dar seguimento ao pedido, devendo-se notificar o interessado/titular dos dados sobre os motivos de recusa.
11. Nos casos referidos no número anterior, cabe ao Município de Mértola demonstrar o caráter manifestamente infundado ou excessivo do pedido.

Artigo 38.º

Procedimentos administrativos

1. Apenas podem ser recolhidos os dados pessoais estritamente necessários para os efeitos processuais que forem estritamente necessários.
2. Caso os serviços identifiquem a necessidade de recolher dados pessoais adicionais que não se encontrem legitimados pelo artigo 6.º do RGPD, deve-se obter o consentimento do titular dos dados.
3. A documentação rececionada no atendimento ao público deve ser imediatamente remetida para os serviços competentes ou, quando tal não seja possível, deve ser mantida de modo a não estar visível a terceiros.
4. Na receção de documentação via correio eletrónico, o consentimento para a recolha e tratamento dos dados pessoais, deve ser assegurado junto do titular.

SECÇÃO III

CONSERVAÇÃO DOS DADOS PESSOAIS

Artigo 39.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, regulamentar, ou na falta desta, o que se revele necessário à prossecução da finalidade.
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. Ao prazo necessário para a tramitação de procedimentos administrativos, bem como o da duração de contratos, acresce o prazo legal de arquivo dos documentos onde os dados estão registados conforme estabelecido no Regulamento Arquivístico para as Autarquias Locais, aprovado pela Portaria n.º 112/2023, de 27 de abril, ou outra que lhe venha a suceder.
4. 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 VI
MEDIDAS DE SEGURANÇA

Artigo 40.º
Segurança do tratamento de dados pessoais

1. O Município de Mértola, enquanto responsável pelo tratamento de dados pessoais, aplica medidas técnicas e organizativas para garantir um nível de segurança adequado ao risco, incluindo, consoante se afigure adequado:
   a) A pseudonimização e a cifragem dos dados pessoais;
   b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
   c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
   d) A adoção de procedimentos para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Artigo 41.º
Segurança das redes e sistemas de informação

1. A recolha, tratamento e salvaguarda dos dados pessoais, deve estar assente numa conceção que tenha a segurança como principal objetivo, por forma a garantir, nomeadamente, o seguinte:
   a) Devem ser cumpridos, em todas as aplicações e sistemas de informação do Município de Mértola, os requisitos técnicos constantes na Resolução do Conselho de Ministros n.º 41/2018, de 28 de março de 2018, ou outra que lhe venha a suceder, 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 determinar os requisitos gerais indicados no número anterior, nomeadamente, quem tem permissões para recolher e tratar dados pessoais, no âmbito dos processos que coordenam, e o momento em que cada um o pode fazer e solicitar ao responsável dos serviços competentes em Tecnologia da Informação a implementação das medidas.

2. É da competência do Núcleo de Comunicação e Informática em articulação com o responsável pela cibersegurança definir e implementar os requisitos específicos indicados na al.a)
3. Adicionalmente, podem ser acauteladas e desenvolvidas medidas tecnológicas e procedimentais tendentes a aumentar e garantir os níveis de segurança de todos os dados pessoais e restante informação à sua guarda.

Artigo 42.º

Notificação da violação de dados pessoais à autoridade de controlo

Nos termos do artigo 33.º do RGPD, caso se verifique uma violação da segurança que provoque, de modo acidental ou ilícita, 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, o Município de Mértola, enquanto responsável pelo tratamento, notifica esse facto à autoridade de controlo, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma.

Artigo 43.º

Comunicação da violação de dados pessoais aos seus titulares

Nos termos do artigo 34.º do RGPD, caso se verifique 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, suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o Município de Mértola, enquanto responsável pelo tratamento, comunica a violação de dados pessoais ao titular dos dados sem demora injustificada.

Artigo 44.º

Acesso e arquivamento

1. O acesso aos dados pessoais recolhidos deve estar devidamente acautelado, no sentido de apenas poderem aceder aos mesmos os trabalhadores que em determinado momento processual estejam a desenvolver algum procedimento que os legitime.
2. Sempre que os dados pessoais se encontrem 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 pelo serviço.
3. Sempre que os dados pessoais constem de processos arquivados fisicamente, ou em plataformas eletrónicas, os dirigentes e/ou responsáveis pelas unidades orgânicas devem identificar quem tem permissões para aceder aos mesmos.

Artigo 45.º

Dever de sigilo e confidencialidade

1. Os titulares dos órgãos municipais, encarregado da proteção de dados, bem como os responsáveis pelo tratamento de dados, incluindo os subcontratantes, trabalhadores e demais colaboradores que intervenham em qualquer operação de tratamento de dados, estão obrigados a um dever de confidencialidade que acresce ao dever de sigilo profissional previsto na lei, que se mantém após o termo do exercício das funções que lhe deram origem.
2. Assim, os trabalhadores e demais colaboradores do Município:
    a) Não devem divulgar ou usar, por si ou por interposta pessoa, informações obtidas no desempenho das suas funções ou em virtude desse desempenho, com preponderância para a proteção dos dados pessoais, e que, pela sua efetiva importância, por legítima decisão dos órgãos decisores da respetiva hierarquia ou por força da legislação em vigor, não devam ser do conhecimento geral;
    b) Que tenham a seu cargo o tratamento de dados pessoais ou que, no exercício das suas funções, tomem conhecimento de dados pessoais, devem estrito respeito à reserva da vida privada dos respetivos titulares e às normas aplicáveis em matéria de proteção das pessoas singulares relativamente ao tratamento de dados pessoais pelas entidades públicas;
    c) Não devem, por si ou por interposta pessoa, utilizar informação que não tenha sido tornada pública ou não seja acessível ao público para promover interesses próprios ou de terceiros.

Artigo 46.º

Avaliação de impacto sobre a proteção de dados

1. A avaliação de impacto sobre a proteção de dados 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 deve encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação da origem, natureza, particularidade e gravidade desse risco.
3. A 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;
   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 das autoridades de controlo e o presente regulamento.
4. 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 autoridade de controlo antes de se proceder ao tratamento de dados pessoais.

Artigo 47.º

Atendimento

1. A comunicação de informação que envolva dados pessoais via telefone, serviços eletrónicos ou correio eletrónico só pode ser realizada se o titular dos dados tiver dado previamente o consentimento expresso nesse sentido.
2. No atendimento presencial ao público deve ser reservada e mantida a salvaguarda e proteção da privacidade no tratamento dos dados pessoais das pessoas singulares.

Artigo 48.º

Política de privacidade

O Município de Mértola deve elaborar e manter atualizado e disponível ao público, na sua página oficial na Internet, um documento sobre política de privacidade.

CAPÍTULO VII

SITUAÇÕES ESPECIAIS

Artigo 49.º

Dever de cooperação

O Município de Mértola, enquanto responsável pelo tratamento, coopera e colabora com a autoridade de controlo, a pedido desta, na prossecução das suas atribuições e competências.

Artigo 50.º

Tratamento de dados pessoais no contexto laboral

Nos termos do artigo 88.º do RGPD e do artigo 28.º da Lei n.º 58/2019, de 8 de agosto, o Município de Mértola pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho, na Lei Geral do Trabalho em Funções Públicas e respetiva legislação complementar, ou noutros regimes setoriais.

Artigo 51.º

Utilização e reprodução de documentos de identificação

A utilização e reprodução dos documentos de identificação dos titulares dos dados só pode ser realizada mediante consentimento escrito dos mesmos e nos termos legalmente previstos.

Artigo 52.º

Consentimento de menores

1. O tratamento dos dados pessoais de menores é lícito quando os mesmos deem formalmente o consentimento e já tenham completado 13 (treze) anos de idade.
2. Caso a criança tenha idade inferior a 13 (treze) anos, o tratamento só é lícito se for dado pelos representantes legais desta e, de preferência, com recurso a meios de autenticação segura.

Artigo 53.º

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

1. O titular dos dados deve dar o prévio consentimento para a recolha, tratamento e divulgação de imagens, fotografias e/ou vídeos por parte do Município, devendo-lhe ser prestada toda a informação em linguagem clara e simples e qual o destino de arquivamento.
2. Quando a recolha, tratamento e divulgação de imagens, fotografias e/ou vídeos por parte do Município disser respeito a menores, deve 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 sobre planos afastados em que os mesmos não sejam facilmente identificáveis.

3. Sempre que existam eventos organizados pelo Município de Mértola, onde não seja proibida a recolha de imagens, som e vídeo, deve o mesmo ser informado aos titulares dos dados pessoais.

Artigo 54.º

Proteção de dados pessoais de pessoas falecidas

1. Quando forem recolhidos ou tratados dados pessoais de pessoas falecidas, os dados pessoais relativos à 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, 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, podendo colocar-se duas situações:
   a) Se o titular dos dados, em vida, tiver manifestamente tornado público os dados acima mencionados, não é necessário o consentimento;
   b) Caso contrário, tem de ser obtido o consentimento escrito e expresso.
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 da Câmara Municipal 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 envolvam 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 55.º

Publicação de dados pessoais

1. A publicação de dados pessoais em jornais oficiais e plataformas eletrónicas, que sejam da responsabilidade do Município, devem obedecer aos princípios base mencionados no presente regulamento, nomeadamente ao princípio da finalidade e 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 56.º

Dados biométricos

O tratamento de dados biométricos dos trabalhadores da Câmara Municipal de Mértola só pode ser considerado legítimo por razões de controlo de assiduidade e controlo de acessos às instalações do Município.

Artigo 57º

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 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, 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.

CAPÍTULO VIII

MEDIDAS TÉCNICAS E ORGANIZATIVAS DE PROTEÇÃO DE DADOS PESSOAIS

Artigo 58.º

Regras gerais

1. O Município deve garantir a adoção de medidas técnicas e organizativas para a proteção de gados, designadamente:
    a) Criar e manter um registo atualizado de todos os ativos tecnológicos (hardware, e software).
    b) Garantir um nível de segurança forte dos dados pessoais e dos recursos de tratamento.
    c) Dar formação adequada a todos os utilizadores sobre segurança do sistema e dos dados pessoais.
    d) Implementar diferentes tipos de mecanismos de segurança, criando diferentes camadas de proteção.
    e) Assegurar que cada mecanismo de segurança contribui, separadamente e/ou em combinação com outros mecanismos, para atingir os objetivos.
    f) Anular ou, pelo menos, reduzir quaisquer deficiências na segurança que possam existir, mantendo um risco residual num nível aceitável a cada caso.
    g) As alterações ou atualizações de hardware, firmware e software não devem enfraquecer a segurança do sistema.
    h) Definir políticas e procedimentos relativos à gestão do ciclo de vida dos utilizadores, incluindo a criação, atribuição, manutenção e atualização das contas de utilizadores do sistema.
    i) Definir e manter atualizados os procedimentos e políticas de segurança que visem a operação segura do sistema e garantir a sua divulgação por todos os utilizadores.
    j) Sensibilizar todos os utilizadores para as respetivas responsabilidades individuais na segurança do sistema e dos dados pessoais.
    k) Garantir a assistência técnica a todos os utilizadores quando e onde necessário.
    l) Criar e manter registos (logs), de modo a permitir o rastreamento das atividades com impacto na segurança dos dados pessoais.
    m) Garantir a salvaguarda e a capacidade de recuperação de informações relevantes para a reposição total do sistema, incluindo os dados pessoais (backups e disaster recovery).
    n) Assegurar que a manutenção do sistema não deve violar a sua segurança.
    o) Conduzir visitas técnicas para determinar se as medidas de segurança no local são suficientes e adequadas.
    p) Realizar auditorias internas, cujos resultados devem ficar registados em relatório.

q) Procurar a melhoria contínua da segurança do sistema, através do planeamento e implementação de novas medidas, monitorização e verificação da adequação das mesmas e adoção de medidas corretivas sempre que necessário.

Artigo 59.º

Medidas de controlo de proteção de dados

1. O Município deve adotar medidas de controlo que garantam a proteção dos dados, designadamente:
   a) Controlo da entrada nas instalações: impedir o acesso de pessoas não autorizadas às instalações utilizadas para o tratamento de dados.
   b) Controlo dos suportes de dados: impedir que suportes de dados possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada.
   c) Controlo da inserção: impedir a introdução não autorizada, bem como a tomada de conhecimento, a alteração ou a eliminação não autorizadas de dados pessoais inseridos.
   d) Controlo da utilização: impedir que sistemas de tratamento automatizados de dados possam ser utilizados por pessoas não autorizadas.
   e) Controlo de acesso: garantir que pessoas autorizadas só possam ter acesso aos dados abrangidos pela autorização.
   f) Controlo da transmissão: garantir a verificação das entidades a quem possam ser transferidos os dados pessoais através da rede de transmissão de dados.
   g) Controlo da introdução: garantir que se possa verificar em data posterior, em prazo razoável, quais os dados pessoais introduzidos, quando e por quem.
   h) Controlo do transporte: impedir que, na transmissão de dados pessoais, bem como no transporte do seu suporte, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada.

Artigo 60.º

Responsabilidades coletivas e individuais

1. Cada utilizador deve ser individualmente responsável pelo cumprimento das políticas e medidas de segurança implementadas.
2. Todas as atividades realizadas no sistema devem estar sujeitas a monitorização e auditorias.
3. Proibição do acesso aos dados pessoais sob o controlo do Município a partir de dispositivos pessoais.
4. Proibição da utilização de dispositivos do Município fora das instalações, incluindo para fins pessoais

5. A proibição expressa no nº4 não abrange os membros do executivo municipal e as chefias e trabalhadores autorizados, porém incluí a proibição da sua utilização para fins pessoais.
6. Utilização de dispositivos de armazenamento removíveis apenas mediante prévia autorização.
7. Proibição da utilização do correio eletrónico profissional para fins pessoais.
8. Proibição da modificação de equipamentos e programas informáticos.
9. Proibição do acesso a áreas para as quais não tenham sido especificamente autorizados, incluindo a tentativa.
10. Proibição do uso, acesso e/ou modificação não autorizada a equipamentos informáticos, programas e dados.

Artigo 61.º

Violação de segurança de dados pessoais

1. Implementação de medidas para deteção, identificação e investigação das circunstâncias, em que ocorreu a Violações de Dados.
2. Adoção de medidas mitigadoras, de um circuito de informação entre responsáveis e subcontratante, e apuramento de responsabilidades.
3. Notificação à Autoridade de Controlo Nacional (CNPD).
4. Comunicação aos titulares dos dados nos casos em que possa resultar num risco elevado.

Artigo 62.º

Proteção dos dados e dos recursos de tratamento contra código malicioso (malware)

1. Existência de controlos de deteção e prevenção.
2. Existência de software antivírus e antispam, devidamente licenciados e de atualização preferencialmente automática, em todas as estações de trabalho e servidores.
3. Verificação regular da presença de código malicioso em dados, sistema operativo instalado, pacotes de software e aplicações, dispositivos de armazenamento removíveis, correio eletrónico e respetivos anexos recebidos quer de fontes internas ou externas.

Artigo 63.º

Identificação e prevenção de incidentes de segurança pelos utilizadores

1. O responsável pela segurança é o Núcleo de Comunicação e Informática o qual deve ser informado sempre que:
    a) For detetado código malicioso.
    b) Seja detetado qualquer alerta do sistema antivírus.

2. Em caso de suspeita deverá parar imediatamente qualquer processamento em curso, desconectar o sistema potencialmente infetado da rede e informar o responsável pela segurança.

Artigo 64.º

Privilégios de acesso, utilização do sistema e credenciais de autenticação

1. O acesso ao sistema deve ocorrer apenas mediante prévio procedimento de registo.
2. Os pedidos de criação ou modificação de uma conta de utilizador, nomeadamente relativa a permissões, devem ser efetuados por escrito, através de email ou criação de ticket na plataforma de Helpdesk.
3. Não são permitidas contas compartilhadas entre utilizadores.
4. As credenciais de autenticação de cada utilizador devem ser pessoais e intransmissíveis.
5. A palavra passe deve ser complexa e tem que ter no mínimo 12 caracteres devendo ser composta pela inclusão de letras maiúsculas, letras minúsculas, números e caracteres especiais.
6. A reutilização de palavras-passe anteriores deverá ser evitada, exigindo-se que não seja igual ou semelhante às últimas oito palavras-passe.
7. A palavra-passe de autenticação deve ser alterada, no máximo, a cada 90 dias.
8. Cada utilizador deve possuir somente os privilégios necessários para realizar as suas funções.
9. Deve existir e ser mantida uma listagem atualizada das pessoas autorizadas a utilizar o sistema, incluindo quais os softwares autorizados, e a extensão da respetiva autorização.

Artigo 65.º

Contas dos utilizadores

1. Compete à respetiva chefia do serviço em causa, solicitar por escrito, utilizando a plataforma de Helpdesk, a criação de conta para novos utilizadores, bem como, definir os respetivos privilégios/permissões aos mesmos.
2. As contas dos utilizadores são bloqueadas automaticamente após três tentativas mal sucedidas.
3. Ocorrerá um bloqueio manual quando houver a suspeita de que a conta está a ser usada incorretamente.
4. As contas desnecessárias devem ser bloqueadas/desativadas.
5. O Encarregado da Proteção de Dados deve ser avisado das situações de bloqueio de contas de forma periódica, no início de cada mês referente ao mês imediatamente anterior.

6. O bloqueio da estação de trabalho deve ser ativado por cada utilizador sempre que o mesmo se ausente do local de trabalho, sendo apenas desbloqueado com recurso às credenciais de acesso.
7. No final de cada ciclo de trabalho, a respetiva sessão deve ser encerrada.
8. No final do dia de trabalho o equipamento deverá ser encerrado.
9. Sempre que um trabalhador deixe de ter relação contratual com o município o responsável pelo serviço deverá informar o Núcleo de Comunicação e Informática, através da plataforma de Helpdesk ou email solicitando a desativação da respetiva conta e demais permissões/ acessos associados.

Artigo 66.º

Registo e monitorização das atividades dos utilizadores

1. Devem ser criados, atualizados e analisados periodicamente os registos de atividade (logs).
2. Os registos devem conter detalhes suficientes sobre as atividades dos utilizadores, que permitam a reconstrução do histórico de ações: quem, onde, quando e ação efetuada sobre o dado pessoal.

Artigo 67.º

Proteção dos registos da atividade dos utilizadores

1. A gravação, os backups e a manutenção dos registos de atividade são obrigatórios e devem incluir todo o tipo de ações.
2. Os acessos aos registos de atividade dos utilizadores devem ser limitados a pessoas devidamente autorizadas e para os fins legalmente previstos, designadamente para realização de auditorias.

Artigo 68.º

Instalação de novo hardware e software

1. Apenas os técnicos de informática podem proceder à instalação e alteração de hardware e/ou software.
2. Os equipamentos devem ser instalados e protegidos de modo a garantir a redução dos riscos de ameaças e o acesso não autorizado.

Artigo 69.º

Cópias de segurança

1. A realização de cópias de segurança (backups) dos dados e do software é feita periodicamente para a proteção contra perdas e danos, bem como para garantir, quando necessário, uma rápida e correta recuperação do sistema.
2. A realização de backups incrementais é feita diariamente.
3. Os backups são efetuados numa primeira instância para disco/storage e posteriormente para tapes.
4. As tapes são guardadas em local físico diferente do local dos backups, dentro de armário fechado e com acesso restrito.

Artigo 70.º

Computação em nuvem (Cloud)

1. No que respeita à computação em nuvem deverão ser determinados os requisitos técnicos (flexível e escalável) e definidos os requisitos de segurança.
2. No caso das redes e sistemas de informação que utilizem os serviços de computação em nuvem públicos ou híbridos, devem ser avaliados o regime de responsabilidade e os níveis de serviço - Service Level Agreement (SLA) - particularmente no que respeita à disponibilidade do sistema, à segurança dos dados e à reposição do sistema.
3. A segurança na computação em nuvem também compreende a segurança da infraestrutura de rede, a segurança das aplicações em nuvem, a segurança das instalações físicas onde se encontram os dados e a possibilidade de realização de auditorias (periódicas e esporádicas) ao fornecedor do serviço.
4. Os centros de dados devem ficar alojados em instalações com as condições de segurança adequadas à proteção dos dados pessoais.
5. Os prestadores de serviços devem possuir referenciais internacionais de segurança, demonstrar a conformidade com o RGPD (subcontratantes), possuir servidores físicos dentro do território nacional e/ou da União Europeia e possuir a opção por nuvens controladas por entidades públicas.
6. Apresentar tecnologias para melhoria da privacidade, favorecendo a aplicação de tecnologias Privacy Enhancing Technologies (PET).
7. Reforçar a segurança de dados pessoais sensíveis através de controlos de acesso mais rígidos, do uso de técnicas de cifragem, da opção pelo sistema de gestão de identidades e acessos (Identity and Access Management) e da adoção de medidas tecnológicas para assegurar que dados específicos não são enviados (e recebidos) para a (e da) nuvem se não estiverem cifrados.

Artigo 71.º

Proteção dos suportes de dados

1. O Município de Mértola gere a utilização dos suportes de dados removíveis em todas as suas fases, incluindo a aquisição, distribuição, utilização e destruição.
2. Antes da eliminação ou reutilização de equipamentos que contenham suportes de dados deve-se verificar se todos os dados foram efetivamente removidos ou eliminados.
3. No caso do suporte de dados em papel, a impressão e/ou cópia de documentos contendo dados pessoais deve ser limitada ao estritamente necessário.
4. A reprodução dos documentos através de fotocópia deve ser efetuada com recurso a um sistema de autenticação que permita a impressão segura.
5. Os utilizadores devem garantir que nenhuma impressão e/ou cópia fica esquecida na impressora/fotocopiadora.

Artigo 72.º

Eliminação dos suportes de dados

1. Os suportes de dados devem ser eliminados de forma segura.
2. Deve ser garantida a eliminação de todos os dados armazenados nos equipamentos em fim de vida.
3. Os equipamentos em fim de vida devem ser desmagnetizados e/ou fisicamente destruídos.
4. Os documentos em papel devem ser destruídos com recurso a máquinas trituradoras próprias.
5. A destruição de suportes de dados contendo dados pessoais sensíveis deve ser acompanhada da elaboração de declarações de destruição, que devem ser conservados por um período mínimo de 5 anos.

Artigo 73.º

Segurança física

1. O Município deverá implementar medidas físicas, de proteção para impedir o acesso não autorizado a informação considerada sensível, incluindo dados pessoais.
2. Assegurar que as medidas definidas impedem ou dificultam a entrada de pessoas não autorizadas.
3. As medidas devem ser proporcionais ao risco identificado.

Artigo 74.º

Segurança documental

1. No interior das instalações municipais deve existir cofres e armários apropriados (fechados com chave, fechadura de segredo ou tranca com cadeado) que garantam a segurança e privacidade dos processos.
2. As chaves dos cofres e armários não deverão ser levadas para fora do perímetro de segurança.
3. As chaves e as combinações de segredo devem ser memorizadas pelas pessoas que precisam de as conhecer e devem ser guardadas em cofre em envelope duplo selado.
4. As combinações de segredo deverão ser conhecidas por um número restrito de pessoas.
5. As combinações deverão ser modificadas:
    a) Quando usadas pela primeira vez;
    b) Sempre que haja uma mudança de pessoal;
    c) Sempre que tenha ocorrido ou haja suspeita de ter ocorrido uma fuga de informação;
    d) Quando sujeitos a manutenção;
    e) No mínimo, de seis em seis meses.
6. Os documentos em papel que contêm dados pessoais, principalmente aqueles localizados em espaços físicos acessíveis aos munícipes e a entidades externas, devem estar devidamente guardados em armários fechados ou em local que não permitam a sua visualização.

Artigo 75.º

Segurança eletrónica

1. Os servidores, sistemas de gestão de redes, controladores de rede e de comunicações, routers, firewalls referentes a redes e sistemas de informação que tratam dados pessoais devem ser acomodados em áreas seguras.
2. Os terminais dos utilizadores devem estar, desejavelmente, localizados em áreas seguras.
3. Dentro das áreas seguras apenas devem existir linhas de comunicação e dispositivos eletrónicos autorizados.

CAPÍTULO IX

RESPONSABILIDADES

Artigo 76.º

Responsabilidade dos dirigentes e/ou responsáveis das unidades orgânicas

1. Todos os dirigentes do Município e/ou responsáveis por unidades orgânicas respondem subsidiariamente ao responsável pelo tratamento de dados, face aos atos e omissões que em concreto, violem os direitos e liberdades de pessoas singulares e devem identificar as diferentes atividades que são desenvolvidas nas mesmas, bem como os dados pessoais que são recolhidos e o respetivo tratamento, e manter atualizado o registo de atividades de tratamento.
2. Os dirigentes e/ou responsáveis pelas unidades orgânicas devem comunicar ao encarregado da proteção de dados a informação recolhida no ponto anterior e mantê-la atualizada.

Artigo 77.º

Responsabilidade civil, criminal ou disciplinar

A violação das normas do RGPD, legislação nacional, orientações das autoridades de controlo e do presente regulamento, pode gerar responsabilidade civil, criminal, contraordenacional e disciplinar.

Artigo 78.º

Cumprimento do dever omitido

Sempre que a contraordenação resulte de omissão de um dever, o pagamento da coima não dispensa o infrator de dar cumprimento ao dever omitido, se este ainda for possível.

CAPÍTULO X

DISPOSIÇÕES FINAIS

Artigo 79.º

Dúvidas e omissões

1. Às situações não previstas no presente regulamento, aplica -se subsidiariamente o Regulamento Geral Sobre a Proteção de Dados (Regulamento (UE) 2016/679, Do Parlamento Europeu e do Conselho, de 27 de abril de 2016, a Lei nº58/2019, de 8 de agosto e as demais disposições legais que sejam aplicáveis em razão da matéria.
2. As menções referentes aos serviços municipais, nomeadamente, Unidades Orgânicas, constantes do presente regulamento reportam-se, em caso de alteração da estrutura orgânica da Câmara Municipal de Mértola, àquelas que se sucederem nas respetivas funções.

Artigo 80.º

Entrada em vigor

O presente regulamento entra em vigor no dia seguinte após a sua publicação no Diário da República.