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

Preâmbulo

O Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679), de 27 de abril de 2016, (em diante também designado RGPD) relativo à proteção de dados pessoais e à livre circulação desses dados, entrou em vigor no dia 25 de maio de 2018. A Lei n.º 58/2019 de 8 de agosto, que assegura a execução na ordem jurídica nacional do RGPD, entrou em vigor no dia 09 de agosto de 2019.

O Município como entidade pública que procede ao tratamento de dados pessoais encontra-se vinculado ao cumprimento do supra indicado regulamento comunitário e lei nacional de execução e demais legislação sobre proteção de dados pessoais.

Considerando o que antecede e para adaptar à realidade municipal as obrigações legais sobre proteção de dados pessoais, o executivo municipal apresenta proposta de aprovação desta (política a aprovar na Câmara Municipal ou Regulamento a aprovar pela Assembleia Municipal).

(Esta política ou Regulamento) tem natureza prática e complementar em relação à citada legislação, concretizando as obrigações legais à realidade do Município e não pode em caso algum contrariar o disposto naquela legislação.

Regulamento de Proteção de Dados do Município de Monforte

Artigo 1º

Lei habilitante

O Regulamento de Proteção de Dados é elaborada(o) ao abrigo do disposto no artigo 241.º da Constituição da República Portuguesa, artigo 135.º e ss do Código do Procedimento Administrativo, artigo 4.º, no n.º 1 do artigo 23.º; alínea g) do n.º 1 do artigo 25.º e alínea k) do n.º 1 do artigo 33.º do Regime Jurídico das Autarquias Locais aprovado pela Lei n.º 75/2013, de 12 de setembro, na sua redação atual, Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679), de 27 de abril de 2016 e Lei n.º 58/2019 de 8 de agosto.

Artigo 2º

Dados pessoais

Considera-se dados pessoais qualquer informação relativa a uma pessoa singular (humano) identificada ou identificável.

Artigo 3º

Dados pessoais sensíveis

Dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

Artigo 4º

Tratamento de dados pessoais

Uma operação ou conjunto de operações efetuadas sobre dados pessoais ou conjuntos de dados pessoais.

Artigo 5º

Responsável pelo tratamento

O Município será responsável pelo tratamento sempre que determine as finalidades e os meios de tratamento de dados pessoais. A competência pela proteção de dados pessoais é da Câmara Municipal podendo esta delegar essa competência no Presidente da Câmara e este em Vereador.

Artigo 6º

Objeto da política

Implementar nas unidades orgânicas e serviços municipais e municipalizados procedimentos e medidas técnicas e organizativas para cumprimento das normas legais em vigor sobre proteção de dados pessoais.

Artigo 7º

Âmbito de aplicação

1. Esta política deve ser aplicada pelas unidades orgânicas dos serviços municipais e municipalizados, por qualquer pessoa que preste nestes serviços funções públicas, pelos prestadores de serviços e avençados, estagiários, colaboradores, e todas as pessoas ou entidades contratadas pelo município sempre que tomem contacto ou efetuem o tratamento de dados pessoais por conta do município.
2. A responsabilidade por gerir e supervisionar a aplicação deste regulamento incumbe especialmente aos dirigentes das respetivas unidades orgânicas.
3. Cada dirigente deve adaptar os procedimentos administrativos das suas unidades orgânicas para que seja garantida, demonstrada e comprovada a execução das regras, medidas técnicas e organizativas indicadas neste regulamento.
4. Os dirigentes das unidades orgânicas devem relativamente aos tratamentos de dados pessoais e à implementação de regras e medidas técnicas e organizativas obter aconselhamento do Encarregado de Proteção de Dados designado pelo município.
5. Nos tratamentos de dados já pendentes devem ser implementadas todas as medidas e alterações necessárias a observar o disposto nesta política e na legislação em vigor.

Artigo 8º

Princípios relativos ao tratamento de dados pessoais

1. No tratamento de dados pessoais devem ser respeitados os seguintes princípios:
a) Princípio da licitude: só pode tratar-se dados pessoais quando se verifique pelo menos um dos fundamentos de licitude previstos na legislação.
b) Princípio da lealdade e transparência: O tratamento deverá ser realizado sempre de forma leal e transparente com os titulares dos dados.
c) Princípio da limitação das finalidades: Os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de forma incompatível com as finalidades de recolha.
d) Princípio da minimização: Só devem ser recolhidos e tratados dados pessoais que sejam adequados, pertinentes e necessários à finalidade estabelecida.
e) Princípio da exatidão: Os dados devem ser exatos e atualizados. Os dados inexatos devem ser apagados ou retificados sem demora.
f) Princípio da limitação da conservação: Os dados pessoais devem ser conservados de forma a permitir a identificação dos titulares dos dados, apenas durante o período estritamente necessário, para as finalidades para as quais são tratados.
g) Princípio da integralidade e confidencialidade: Os dados pessoais devem ser tratados de uma forma que garanta a sua segurança, proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, mediante adoção de medidas técnicas ou organizativas adequadas.
h) Princípio da responsabilidade: responsabilidade por cumprir e comprovar o cumprimento destes princípios.

Artigo 9º

Licitude do tratamento de dados pessoais

1. Só pode ser efetuado o tratamento de dados pessoais caso se verifique pelo menos uma das seguintes condições:
a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
b) O tratamento for necessário para a execução de contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
c) O tratamento for necessário para o cumprimento de obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
f) O tratamento for necessário para 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.
2. O consentimento não deve ser utilizado sempre que coloque em causa ou limite a liberdade do consentimento ou se existirem outros fundamentos.
3. O tratamento necessário para cumprimento de obrigação legal ou para funções de interesse público e autoridade pública é definido pela legislação nacional ou comunitária.
4. Os serviços e respetivos dirigentes devem solicitar e obter informação e aconselhamento do Encarregado de Proteção de Dados.

Artigo 10º
Licitude do tratamento de dados pessoais sensíveis

1. Por regra é proibido o tratamento de dados pessoais sensíveis. Só pode ser efetuado o tratamento de dados pessoais sensíveis caso se verifique pelo menos uma das seguintes condições:

a) Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, exceto se esse consentimento não for permitido por lei.
b) Se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido por lei ou por convenção coletiva que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados;
c) Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento;
d) Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;
e) Se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial;
f) Se o tratamento for necessário por motivos de interesse público importante com base legal, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;
g) Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base legal ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n. 3;
h) Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base legal que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;
i) Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89, n. 1 do RGPD, com base legal, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados.
2. Os dados pessoais referidos no n. 1 podem ser tratados para os fins referidos no n. 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo

profissional, nos termos da lei ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade prevista na lei.
3. Os serviços e respetivos dirigentes devem solicitar e obter informação e aconselhamento do Encarregado de Proteção de Dados.

Artigo 11º
Condições aplicáveis ao consentimento

1. O consentimento do titular dos dados é 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.
2. Quando o tratamento for realizado com consentimento deve ficar assegurada a sua comprovação, devendo ficar devidamente documentado e arquivado.
3. O pedido de consentimento deve ser claramente percetível, inteligível, de fácil acesso e numa linguagem clara e simples.
4. O titular dos dados deve ser informado que pode retirar o consentimento a qualquer momento, a retirada de consentimento não compromete a licitude do tratamento efetuado.
5. O consentimento deve ser tão fácil de retirar quanto de dar.
6. Relativamente aos tratamentos de dados pessoais em curso baseados no consentimento dos titulares, não é necessário obter novo consentimento se o anterior tiver observado as condições previstas na legislação em vigor, caso contrário o consentimento deverá ser renovado.
7. Quando sejam recolhidos dados pessoais de menores o consentimento deve ser prestado pelos titulares das responsabilidades parentais.
8. Os serviços e respetivos dirigentes devem solicitar e obter informação e aconselhamento do Encarregado de Proteção de Dados.

Artigo 12º
Dados pessoais relativos a condenações penais

1.O tratamento de dados pessoais relacionados com condenações penais, infrações e medidas de segurança conexas só pode ser realizado quando previsto em lei.

Artigo 13.º
Transparência do tratamento e o exercício dos direitos

1. Devem ser tomadas medidas adequadas para fornecer aos titulares dos dados as informações relativas ao tratamento dos dados e aos seus direitos de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, por escrito ou por outros meios, incluindo, se aplicável, por meios eletrónicos. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.
2. Deve ser facilitado o exercício dos direitos pelos titulares dos dados e deve dar-se seguimento imediato a pedidos de exercício de direitos, fornecendo informações sobre as medidas tomadas para garantir o exercício dos direitos, devendo a resposta ser dada no prazo de um mês a contar da data de receção do pedido. Para facilitar o exercício dos direitos é disponibilizado formulário de requerimento de exercício de direitos para ser utilizado pelos titulares dos dados.
3. Se o titular dos dados apresentar o pedido por meios eletrónicos, a informação é, sempre que possível, fornecida através de meios eletrónicos, salvo pedido em contrário do titular.
4. O exercício de direitos, as informações prestadas e quaisquer comunicações e medidas tomadas devem ser gratuitas.
5. Se houver dúvidas razoáveis quanto à identidade da pessoa que apresenta o pedido podem ser solicitadas informações adicionais para confirmar a identidade do titular dos dados.
6. Os serviços e respetivos dirigentes devem solicitar e obter informação e aconselhamento do Encarregado de Proteção de Dados.

Artigo 14º
Informações a prestar aos titulares na recolha de dados pessoais

1. Sempre que ocorrer a recolha de dados pessoais devem ser facultadas aos titulares dos dados as seguintes informações:
a) A identidade e os contactos do responsável pelo tratamento;

b) Os contactos do encarregado da proteção de dados;
c) As finalidades do tratamento dos dados pessoais e o fundamento jurídico para o tratamento;
d) Se for esse o fundamento do tratamento indicar os interesses legítimos;
e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
f) O prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;
g) A existência do direito de solicitar ao responsável pelo tratamento 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;
h) Se o tratamento dos dados se basear no consentimento, a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado;
i) O direito de apresentar reclamação a uma autoridade de controlo;
j) 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;
k) A existência de decisões automatizadas, incluindo a definição de perfis e informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para os titulares dos dados.
2. Para que a prestação destas informações ocorra no momento da recolha dos dados e fique devidamente documentada e comprovada, estas informações podem ser prestadas nos formulários dos requerimentos em uso para os diversos procedimentos administrativos ou noutro suporte adequado a documentar e comprovar que as informações foram prestadas.
3. Se os dados pessoais não são recolhidos junto do titular, para além das informações supra indicadas devem também ser prestadas informações sobre as categorias de dados pessoais recolhidos e a origem dos dados, devendo todas as informações ser comunicadas:
a) Num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que estes forem tratados;
b) Se os dados pessoais se destinarem a ser utilizados para fins de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação ao titular dos dados; ou
c) Se estiver prevista a divulgação dos dados pessoais a outro destinatário, o mais tardar aquando da primeira divulgação desses dados.
4. Nos casos de recolha de dados pessoais sem que o titular dos dados apresente o formulário de requerimento em uso, seja por apresentar um requerimento elaborado pelo próprio, seja por simplesmente não apresentar qualquer requerimento, deve ser utilizado outro documento ou suporte para prestação de informações sobre tratamento de dados pessoais.
5. Cada dirigente dos serviços municipais e municipalizados deve adaptar os seus formulários, procedimentos administrativos e práticas para que seja garantida, demonstrada e comprovada a prestação destas informações.
6. Os serviços e respetivos dirigentes devem solicitar e obter informação e aconselhamento do Encarregado de Proteção de Dados.

Artigo 15º

Direitos dos titulares dos dados e o seu exercício

1. Os titulares dos dados pessoais podem exercer os seguintes direitos, nos termos e condições previstos na legislação:
a) Direito de acesso e confirmação do tratamento;
b) Direito de retificação;
c) Direito ao apagamento dos dados;
d) Direito à limitação do tratamento;
e) Direito de portabilidade dos dados;
f) Direito de oposição ao tratamento;
g) Direito de retirar o consentimento se for esse o fundamento de licitude do tratamento, sem comprometer a licitude do tratamento efetuado com base no consentimento até ao exercício deste direito;
h) Direito de apresentar reclamação à autoridade de controlo CNPD;

i) Direito a saber se existem decisões individuais automatizadas incluindo definição de perfis e as informações úteis sobre a lógica subjacente, bem como a importância e as consequências desse tratamento para os titulares dos dados;
2. Sempre que algum titular de dados pretenda exercer algum dos referidos direitos, para facilitar esse exercício, cada unidade orgânica deve disponibilizar formulário de requerimento para exercício de direitos.
3. Sempre que se verifique alguma notificação ou comunicação para o exercício de direitos, o dirigente da unidade orgânica deve encaminhar de forma célere o pedido para o Encarregado de Proteção de Dados através para a respetiva resposta nos termos e prazos legalmente previstos.
4. Se o titular dos dados exercer o direito por meios eletrónicos a resposta deve ser dada por meios eletrónicos, desde que seja possível associar o endereço eletrónico ao titular dos dados e sem prejuízo de solicitar mais informações sobre a identidade do titular.
5. Os serviços e respetivos dirigentes devem solicitar e obter informação e aconselhamento do Encarregado de Proteção de Dados.

Artigo 16º
Responsabilidades no tratamento de dados

1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados pessoais, bem como os riscos para direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, os dirigentes das unidades orgânicas do município relativamente aos tratamentos de dados nas respetivas unidades orgânicas, têm as seguintes obrigações:
a) Aplicar medidas técnicas e organizativas que forem adequadas para assegurar e comprovar que os tratamentos de dados pessoais são realizados em conformidade com este regulamento e com a legislação em vigor.
b) Implementar as políticas e procedimentos adequados, bem como, o cumprir eventuais códigos de conduta ou procedimentos de certificação em matéria de proteção de dados.

c) Aplicar a proteção de dados desde a conceção e por defeito, isto é, no momento da definição dos meios de tratamento e no próprio tratamento, implementar as medidas técnicas e organizativas adequadas, destinadas a cumprir os princípios da proteção de dados, e incluir as garantias necessárias no tratamento de forma a respeitar a legislação em vigor e os direitos dos titulares dos dados.

d) Por defeito deve ser respeitado o princípio da minimização, devendo o tratamento ser limitado aos dados necessários para cada finalidade específica de tratamento, no que toca à quantidade de dados recolhidos, à extensão do tratamento, ao prazo de conservação e no acesso aos dados.
2. Os serviços e respetivos dirigentes devem solicitar e obter o aconselhamento do Encarregado de Proteção de Dados relativamente às medidas técnicas e organizativas a implementar em cada tratamento de dados pessoais.

Artigo 17º
Tratamento de dados pessoais com responsáveis conjuntos

1. Sempre que as finalidades e meios de tratamento de dados pessoais sejam determinadas pelo município conjuntamente com outras entidades, deve ser celebrado um acordo escrito e transparente para determinar as respetivas responsabilidades pelo cumprimento das obrigações legais, nomeadamente, no que diz respeito ao exercício dos direitos dos titulares, obrigações de prestação de informações sobre o tratamento e designação de ponto de contacto para os titulares dos dados.
2. Esse acordo escrito deve refletir devidamente as funções e relações dos responsáveis conjuntos pelo tratamento em relação aos titulares dos dados e a essência do acordo deve constar das informações prestadas aos titulares dos dados.
3. Independentemente dos termos do acordo, os titulares dos dados podem exercer os seus direitos em relação a qualquer um dos responsáveis pelo tratamento conjunto.
4. Os dirigentes em relação às respetivas unidades orgânicas com tratamentos de dados envolvendo responsáveis conjuntos devem dar cumprimento ao previsto neste artigo e na legislação em vigor.
5. Para tratamentos já pendentes devem ser celebrados com os demais responsáveis conjuntos acordos escritos ou adendas a contratos que salvaguardem o cumprimento do previsto neste artigo e na legislação em vigor.

6. Os serviços e respetivos dirigentes devem solicitar e obter o aconselhamento do Encarregado de Proteção de Dados relativamente às condições e ao teor dos acordos e adendas a celebrar.

Artigo 18º

Tratamento de dados pessoais com subcontratados

1. Considerando que o município enquanto responsável pelo tratamento tem a obrigação de celebrar contratos com outras pessoas ou entidades, aqui designadas como subcontratados, se estas efetuarem o tratamento de dados pessoais por conta do município, os dirigentes das respetivas unidades orgânicas devem cuidar de observar as regras previstas neste artigo e na legislação em vigor.
2. Recorrendo a subcontratados que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas a respeitar o previsto neste regulamento e na legislação em vigor e a assegurar a defesa dos direitos dos titulares dos dados.
3. Nos cadernos de encargos, contratos ou por adendas aos contratos, que vinculem os subcontratados deve ficar estabelecido por escrito todas as condições exigidas pelo RGPD em relação ao tratamento de dados pessoais através de subcontratados.
6. Os serviços e respetivos dirigentes devem solicitar e obter aconselhamento do Encarregado de Proteção de Dados relativamente às condições e ao teor dos cadernos de encargos, contratos ou adendas a celebrar com os subcontratados, considerando a natureza do tratamento em causa.

Artigo 19º

Tratamento sob autoridade do Município

1.Qualquer pessoa singular, (trabalhadores) que sob a autoridade do Município tem acesso a dados pessoais efetua o seu tratamento com obrigação de confidencialidade e de acordo com as instruções recebidas respeitando esta política e a legislação em vigor.
2. Nos contratos já celebrados com trabalhadores devem ser realizadas adendas e nos contratos a celebrar com os trabalhadores devem ser inseridas clausulas para vincular os trabalhadores e dar cumprimento a esta obrigação e à legislação em vigor.
3. Os serviços e respetivos dirigentes devem solicitar e obter o aconselhamento do Encarregado de Proteção de Dados relativamente às condições e ao teor das adendas e contratos a celebrar com os trabalhadores, considerando a natureza do tratamento em causa.

Artigo 20º

Registos das atividades de tratamento

1. Considerando que o município enquanto responsável pelo tratamento, tem obrigação de conservar registos de todas as atividades de tratamento sob a sua responsabilidade, os dirigentes das respetivas unidades orgânicas devem observar as regras previstas neste artigo e na legislação em vigor.
2. Manter registos atualizados de todos os tratamentos de dados pessoais das respetivas unidades orgânicas, deles devendo constar todas as seguintes informações:
a) O nome e os contactos do responsável pelo tratamento e, sendo caso disso, de qualquer responsável conjunto 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;
e) Se possível, os prazos previstos para o apagamento das diferentes categorias de dados;
f) Se possível, a descrição geral das medidas técnicas e organizativas no domínio da segurança de dados pessoais referidas no artigo 32º, n. 1 do RGPD.
3. Estes registos podem ser disponibilizados à autoridade de controlo (CNPD) caso tal seja solicitado por essa autoridade.
4. Os serviços e respetivos dirigentes devem solicitar e obter o aconselhamento do Encarregado de Proteção de Dados relativamente aos registos de atividades de tratamento.

Artigo 21º

Cooperação com a autoridade de controlo

1.Considerando que a Comissão Nacional de Proteção de Dados (CNPD) é a autoridade de controlo nacional, o Município deve cooperar com essa autoridade sempre que esta o solicite e na prossecução das suas atribuições.

2. Essa cooperação deve ser estabelecida através do Encarregado de Proteção de Dados considerando as suas funções legais de cooperação e ponto de contacto com a autoridade de controlo.

Artigo 22º

Deliberações da autoridade de controlo

1.Mantêm-se válidos os princípios gerais aplicáveis aos tratamentos de dados pessoais e, nessa medida, as deliberações da CNPD podem continuar a ser usadas como referência em tudo que não contrarie a legislação em vigor.

2. Sempre que seja necessário submeter pedidos junto da CNPD incluindo de parecer, devem ser apresentados pelo Encarregado de Proteção de Dados considerando as suas funções legais.

Artigo 23º

Segurança do tratamento de dados pessoais

1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados pessoais, bem como os riscos para direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, os dirigentes das unidades orgânicas do município relativamente aos tratamentos de dados nas respetivas unidades orgânicas, aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

a) A pseudonimização (deixar de atribuir os dados aos titulares) e a cifragem (tornar os dados ininteligíveis) de 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) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

2. Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

3. Os serviços de informática devem implementar ao nível da segurança informática dos dados pessoais nos sistemas do Município as medidas previstas nos seguintes diplomas:

3.1 Resolução do Conselho de Ministros n.º 41/2018 que estabelece a Arquitetura de segurança das redes e sistemas de informação na Administração Pública;

3.2 As medidas de segurança previstas em regulamentação ou na própria Lei n.º 46/2018 de 13 de agosto que Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

3.3 As medidas preconizadas no Quadro Nacional de Referência para a Cibersegurança emitido pelo Centro Nacional de Cibersegurança.

4. Os serviços e respetivos dirigentes devem solicitar e obter o aconselhamento do Encarregado de Proteção de Dados relativamente às medidas de segurança física e informática mais adequadas a cada tratamento de dados pessoais.

Artigo 24º

Violação de dados pessoais

1. Considera-se violação de dados pessoais uma violação de segurança que provoca de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizados a dados pessoais.

2. Qualquer violação de dados deve ser comunicada internamente aos superiores hierárquicos e ao Encarregado de Proteção de Dados nomeado.

3. Qualquer violação de dados pessoais deve ser documentada, incluindo os factos, os efeitos e as medidas adotadas de modo a permitir à autoridade de controlo verificar o cumprimento da legislação.

4. Se a violação for suscetível de resultar em riscos para os direitos e liberdades dos titulares, deve ser efetuada a notificação nos termos legalmente previstos à autoridade de controlo.

5. Se a violação for suscetível de implicar elevados riscos para os direitos e liberdades dos titulares, deve ser comunicada nos termos legalmente previstos aos titulares dos dados.

6. Os serviços e respetivos dirigentes devem solicitar e obter o aconselhamento do Encarregado de Proteção de Dados relativamente a incidentes sobre dados pessoais incluindo no caso de eventual violação.

Artigo 25º

Avaliação de impacto e consulta prévia

1. Em relação ao tratamento de dados que, utilize novas tecnologias, tendo em conta a sua natureza, âmbito, contexto e finalidades for suscetível de implicar elevado risco para direitos e liberdades dos titulares, antes de iniciado o tratamento deve ser realizada avaliação de impacto sobre a proteção de dados.
2. A autoridade de controlo já elaborou e publicou pelo Regulamento n.º 1/2018, a lista de tratamentos de dados pessoais sujeitos a prévia Avaliação de Impacto sobre a Proteção de Dados (AIPD), que acresce às situações já expressamente previstas no n.º 3 do artigo 35.º do RGPD.
3. A avaliação de impacto deve ser realizada nos termos previstos na legislação em vigor e sob controlo do encarregado de proteção de dados.
4. Se a avaliação de impacto indicar que do tratamento resulta em elevados riscos na ausência das medidas tomadas para atenuar esses riscos, antes de proceder ao tratamento deve ser realizada a consulta prévia à autoridade de controlo nos termos previstos na legislação em vigor.
5. Os serviços e respetivos dirigentes devem solicitar e obter o aconselhamento do Encarregado de Proteção de Dados relativamente a avaliações de impacto e consulta prévia.

Artigo 26º

Encarregado de proteção de dados

1. Foi designado encarregado de proteção de dados e tal foi comunicado interna e externamente, podendo ser contactado através do endereço eletrónico dpo@cm-monforte.pt.
2. Os dirigentes das unidades orgânicas devem envolver o encarregado de proteção de dados de forma adequada e em tempo útil em todas as questões relacionadas com a proteção de dados pessoais, solicitando ao Encarregado de Proteção de Dados aconselhamento e recomendações sobre os tratamentos de dados pessoais.
3. Devem ser disponibilizados os recursos necessários ao desempenho das funções e à manutenção dos conhecimentos e deve ser dado acesso aos dados pessoais e operações de tratamento.
4. Os titulares dos dados podem contactar o encarregado de proteção de dados sobre todas as questões relacionadas com o tratamento de dados pessoais e com o exercício de direitos.
5. Nos termos da legislação em vigor as funções do encarregado de proteção de dados incluem:
a) Informar e aconselhar incluindo os trabalhadores que tratem os dados sobre as obrigações previstas na legislação.
b) Controlar a conformidade com a legislação e com as políticas 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) Prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controlar a sua realização.
d) Cooperação com a autoridade de controlo (CNPD) e ponto de contacto com essa autoridade sobre questões relacionadas com o tratamento de dados, e consulta, sendo caso disso, essa autoridade sobre qualquer outro assunto.
e) Assegurar a realização de auditorias, quer periódicas, quer não programadas.
f) Sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança.
g) Assegurar as relações com os titulares de dados conforme previsto na legislação em matéria de proteção de dados.
6. No desempenho das suas funções, o encarregado de proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.
7. Está vinculado ao dever de sigilo ou de confidencialidade conforme previsto na legislação.
8. Exerce as suas funções com autonomia técnica e não recebe quaisquer instruções relativamente ao exercício dessas funções.
9. Informa diretamente ao mais alto nível.

Artigo 27º

Dados pessoais e acesso a documentos administrativos

1. O artigo 86º do RGPD estabelece que o direito de acesso a documentos administrativos deve ser conciliado com o direito à proteção de dados pessoais.
2. Nos termos do artigo 26.º da Lei n.º 58/2019, de 8 de agosto, o acesso a documentos administrativos que contenham dados pessoais rege-se pelo disposto na Lei n.º 26/2016, de 22 de agosto (Lei de Acesso aos Documentos Administrativos ou LADA).
3. A LADA define «documento nominativo» como o documento administrativo que contenha dados pessoais, definidos nos termos do regime legal de proteção de dados pessoais.
4. A mesma LADA estabelece restrições no acesso aos referidos documentos nominativos pelo que os pedidos de acesso a documentos administrativos que sejam também documentos nominativos, devem ser analisados de forma casuística, considerando as referidas restrições e em caso de dúvida deverá ser solicitado parecer ao Encarregado de Proteção de Dados e se dúvidas subsistirem à Comissão de Acesso aos Documentos Administrativos e à Comissão Nacional de Proteção de Dados.

Artigo 28º

Utilização e reprodução de documentos de identificação

1. Nos termos da Lei n.º 7/2007, de 5 de fevereiro a conferência de identidade que se mostre necessária a qualquer entidade pública ou privada não permite a retenção ou conservação do cartão de cidadão, salvo nos casos expressamente previstos na lei ou mediante decisão de autoridade judiciária.
2. De acordo com a mesma lei é interdita a reprodução do cartão de cidadão em fotocópia ou qualquer outro meio sem consentimento do titular, salvo nos casos expressamente previstos na lei ou mediante decisão de autoridade judiciária.
3. O consentimento do titular tem de ser livre e tal pressupõe que o mesmo não seja exigido como condição para prestação de serviços ou fornecimento de bens e que deve ser disponibilizado mecanismo alternativo para conferir a identidade do titular dos dados.
4. Considerando todas as referidas condicionantes, deve ser evitada a retenção, conservação e reprodução do cartão de cidadão em fotocópia ou qualquer outro meio, exceto nos casos em que tal esteja expressamente previsto na lei, devendo a conferência da identidade do titular dos dados ser realizada pela exibição do original do cartão de cidadão.
5. Os serviços e respetivos dirigentes devem solicitar e obter o aconselhamento do Encarregado de Proteção de Dados relativamente à utilização de documentos de identificação.

Artigo 29º

Tratamento de dados pessoais nas relações laborais

1. Nos termos do artigo 28.º da Lei n.º 58/2019, de 8 de agosto, o Município enquanto empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes setoriais e com as especificidades estabelecidas nesse artigo.
2. O número anterior abrange igualmente o tratamento efetuado por subcontratante ou contabilista certificado em nome do empregador, para fins de gestão das relações laborais, desde que realizado ao abrigo de um contrato de prestação de serviços e sujeito a iguais garantias de sigilo.
3. Salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais.
4. Para além das situações previstas em legislação relativa a segurança e saúde no trabalho, não é permitido para efeitos de admissão ou permanência no emprego, exigir a candidato a emprego ou a trabalhador a realização ou apresentação de testes ou exames médicos, de qualquer natureza, para comprovação das condições físicas ou psíquicas, salvo quando estes tenham por finalidade a proteção e segurança do trabalhador ou de terceiros, ou quando particulares exigências inerentes à atividade o justifiquem, devendo em qualquer caso ser fornecida por escrito ao candidato a emprego ou trabalhador a respetiva fundamentação.
5. Por regra não é permitida a utilização de meios de vigilância a distância no local de trabalho, mediante o emprego de equipamento tecnológico, com a finalidade de controlar o desempenho profissional dos trabalhadores, exceto se tiver por finalidade a proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da atividade o justifiquem. Neste caso os trabalhadores devem ser informados sobre a existência e finalidade dos meios de vigilância utilizados, seguido de símbolo identificativo.

6. As imagens gravadas e outros dados pessoais registados através da utilização de sistemas de vídeo ou outros meios tecnológicos de vigilância à distância, só podem ser utilizados no âmbito do processo penal e neste caso também podem ser utilizadas para efeitos de apuramento de responsabilidade disciplinar.
7. Os serviços e respetivos dirigentes devem solicitar e obter o aconselhamento do Encarregado de Proteção de Dados relativamente ao tratamento de dados pessoais em contexto laboral.

Artigo 30º
Portabilidade e interoperabilidade dos dados

1. O direito de portabilidade dos dados, previsto no artigo 20.º do RGPD, abrange apenas os dados fornecidos pelos respetivos titulares, devendo, sempre que possível, ter lugar em formato aberto.
2. A interoperabilidade dos dados, caso não seja tecnicamente possível, o titular dos dados tem o direito de exigir que os mesmos lhe sejam entregues num formato digital aberto, de acordo com o Regulamento Nacional de Interoperabilidade Digital em vigor.

Artigo 31º
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 para a prossecução da finalidade.
2. Devem ser considerados para efeitos de prazos de conservação os prazos de arquivo previstos no Regulamento Arquivístico para as Autarquias Locais relativamente aos dados pessoais contidos em documentos sujeitos a arquivo.
3. Quando, pela natureza e finalidade do tratamento, designadamente para fins de arquivo e interesse público, fins de investigação científica ou histórica ou fins estatísticos, não seja possível determinar antecipadamente o momento em que o mesmo deixa de ser necessário, é lícita a conservação dos dados pessoais, desde que sejam adotadas medidas técnicas e organizativas adequadas a garantir os direitos do titular dos dados, designadamente a informação da sua conservação.
4. Quando os dados pessoais sejam necessários para 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.
5. Quando cesse a finalidade que motivou o tratamento, inicial ou posterior, de dados pessoais, o responsável pelo tratamento deve proceder à sua destruição ou anonimização.
6. Nos casos em que existe um prazo de conservação de dados imposto por lei, só pode ser exercido o direito ao apagamento previsto no artigo 17.º do RGPD findo esse prazo.
7. 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.
8. Os serviços e respetivos dirigentes devem solicitar e obter o aconselhamento do Encarregado de Proteção de Dados relativamente aos prazos de conservação de dados pessoais.

Artigo 32º
Tratamento de dados pessoais para finalidades diferentes

1. O tratamento de dados pessoais para finalidades diferentes das determinadas pela recolha tem natureza excecional e deve ser devidamente fundamentado com vista a assegurar a prossecução do interesse público que de outra forma não possa ser acautelado, nos termos da alínea e) do n.º 1, do n.º 4 do artigo 6.º e da alínea g) do n.º 2 do artigo 9.º do RGPD.
2. A transmissão de dados pessoais entre entidades públicas para finalidades diferentes das determinadas pela recolha tem natureza excecional, deve ser devidamente fundamentada nos termos referidos no número anterior e deve ser objeto de protocolo que estabeleça as responsabilidades de cada entidade interveniente, quer no ato de transmissão, quer em outros tratamentos a efetuar.
3. Os serviços e respetivos dirigentes devem solicitar e obter o aconselhamento do Encarregado de Proteção de Dados relativamente a tratamento de dados pessoais para finalidades distintas da recolha, designadamente, para arquivo histórico ou de interesse público de dados pessoais.

Artigo 33º
Publicação em jornal oficial

A publicação de dados pessoais em jornais oficiais, designadamente, o Diário da República, deve respeitar os princípios relativos ao tratamento de dados pessoais, nomeadamente os princípios da finalidade e da minimização.
2. Sempre que o dado pessoal «nome» seja suficiente para garantir a identificação do titular e a eficácia do tratamento, não devem ser publicados outros dados pessoais.
3. Os dados pessoais publicados em jornal oficial não podem, em circunstância alguma, ser alterados, rasurados ou ocultados.
4. O direito ao apagamento de dados pessoais publicados em jornal oficial tem natureza excecional e só se pode concretizar nas condições previstas no artigo 17.º do RGPD, nos casos em que essa seja a única forma de acautelar o direito ao esquecimento e ponderados os demais interesses em presença.
5. O disposto no número anterior realiza-se através da desindexação dos dados pessoais em motores de busca, sempre sem eliminação da publicação que faz fé pública.
6. Em caso de publicação de dados pessoais em jornais oficiais, considera-se responsável pelo tratamento a entidade que manda proceder à publicação.
7. Os serviços e respetivos dirigentes devem solicitar e obter o aconselhamento do Encarregado de Proteção de Dados.

Artigo 34º
Publicação de dados no âmbito da contratação pública

1.No âmbito da contratação pública, e caso seja necessária a publicação de dados pessoais, não devem ser publicados outros dados pessoais para além do dado pessoal «nome», sempre que este seja suficiente para garantir a identificação do contraente público e do cocontratante.
2.Os serviços e respetivos dirigentes devem solicitar e obter o aconselhamento do Encarregado de Proteção de Dados.

Artigo 35º
Tratamentos para fins de arquivo de interesse público

1. O tratamento para fins de arquivo de interesse público deve respeitar o princípio da minimização dos dados e incluir a anonimização ou a pseudonimização dos mesmos sempre que tal por possível e os fins visados possam ser atingidos por uma destas vias.
2. Quando os dados pessoais sejam tratados para fins de arquivo de interesse público ficam prejudicados os direitos de acesso, retificação, limitação do tratamento e de oposição previstos nos artigos 15.º, 16.º, 18.º e 21.º do RGPD, na medida do necessário, se esses direitos forem suscetíveis de tornar impossível ou prejudicar gravemente a realização desses fins.
3. Ao tratamento de dados pessoais para fins de arquivo de interesse público é aplicável o Decreto-Lei n.º 16/93, de 23 de janeiro, na sua redação atual.
4. Os serviços e respetivos dirigentes devem solicitar e obter o aconselhamento do Encarregado de Proteção de Dados.

Artigo 36º
Proteção de dados pessoais de pessoas falecidas
1. Os dados pessoais de pessoas falecidas que sejam sensíveis, reportem à intimidade da vida privada, à imagem ou relativos a comunicações têm a proteção prevista na legislação em vigor.
2. Os direitos relativos aos dados indicados no número anterior, são exercidos por quem a pessoa falecida haja designado para o efeito ou, na sua falta, pelos respetivos herdeiros.
3. 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.
4. Os serviços e respetivos dirigentes devem solicitar e obter o aconselhamento do Encarregado de Proteção de Dados.

Artigo 37º
Orientações técnicas
1.Os serviços municipais devem dar cumprimento a todas as orientações técnicas para a aplicação do RGPD pela Administração Pública.

2.Os serviços municipais devem dar cumprimento à Resolução do Conselho de Ministros n.º 41/2018 que aprovou os requisitos técnicos mínimos das redes e sistemas de informação que são exigidos ou recomendados a todos os serviços e entidades da administração direta e indireta do Estado.
3. Os serviços municipais devem dar cumprimento a todas as orientações e deliberações emitidas pela Comissão Nacional de Proteção de Dados que sejam aplicáveis aos tratamentos realizados.
4. Os serviços municipais devem dar cumprimento a todas as orientações e deliberações emitidas pelo Centro Nacional de Cibersegurança e pelo Gabinete Nacional de Segurança sobre segurança física e informática de dados pessoais que se apliquem aos tratamentos realizados.

Artigo 38º
Legislação subsidiária

A tudo o que não esteja especialmente previsto nesta política aplica-se subsidiariamente o Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, a Lei n.º 58/2019, de 8 de agosto e as demais disposições legais e regulamentares em matéria de proteção de dados pessoais ainda que não diretamente aplicáveis à Administração Pública Local.

Artigo 39º
Interpretação e casos omissos

As lacunas, as dúvidas interpretativas e os casos omissos suscitados na aplicação desta política são preenchidos ou resolvidos por despacho fundamentado do órgão hierarquicamente competente ainda que depois de recomendação emitida pelo Encarregado de Proteção de Dados.

Artigo 40º
Entrada em vigor

A presente política (ou regulamento) entra em vigor com a publicação em Diário da República depois da sua aprovação em deliberação da Câmara Municipal (ou Assembleia Municipal).