CÂMARA MUNICIPAL DA MARINHA GRANDE

CÓDIGO DE CONDUTA PARA SEGURANÇA DA INFORMAÇÃO

E DADOS PESSOAIS

(RGPD)

Preâmbulo

O presente Código é elaborado ao abrigo do disposto no artigo 40.º 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 (RGPD), com vista à correta aplicação deste mesmo Regulamento.

O Município da Marinha Grande, através dos seus órgãos, trata dados pessoais, quer dos recursos humanos internos da Câmara Municipal, quer de todos os cidadãos que com ele se relacionam e interagem, pelo que, em cumprimento daquele normativo, a Câmara Municipal aprovou em sua reunião de 2 de maio de 2023, o presente Código de Conduta que define o conjunto de regras necessárias para alcançar níveis adequados de eficácia e consistência na proteção daqueles dados.

Artigo 1.º
Objeto e âmbito

1. O presente Código estabelece as regras a aplicar pela Câmara Municipal da Marinha Grande no exercício das suas competências legais, em matéria de tratamento e proteção de dados pessoais.

2. O presente documento aplica-se:
   a) A todos trabalhadores da Câmara Municipal que efetuam recolha, tratamento e utilização de dados pessoais, independentemente da natureza do seu vínculo;
   b) Às relações que se estabelecem entre a Câmara Municipal e os seus trabalhadores, seus subcontratantes e seus parceiros ou fornecedores.

3. Para efeitos do presente Código, entende-se por:
   a) «Dados pessoais», a 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.

Artigo 2.º
Recolha de Dados

1. A recolha de dados pessoais para tratamento é fundamentada no cumprimento de uma obrigação legal ou no consentimento do seu titular e deve processar-se:
a) Nos termos da legislação em vigor;
b) No estrito cumprimento dos direitos, liberdades e garantias dos cidadãos.

2. A Câmara Municipal e os seus subcontratantes devem, previamente à recolha de dados junto dos respetivos titulares, informá-los acerca da finalidade que a determina, adequando o seu tratamento ao estrito cumprimento dessa finalidade.

3. Os trabalhadores da Câmara Municipal, bem como os seus subcontratantes devem impreterivelmente assegurar:
a) Que o tratamento dos dados é efetuado apenas no âmbito das finalidades para as quais os mesmos foram recolhidos;
b) Que a recolha, utilização e conservação é realizada apenas sobre os dados pessoais mínimos, necessários e suficientes para a finalidade respetiva;
c) Que a conservação dos dados pessoais é efetuada apenas pelo período de tempo necessário para o cumprimento da finalidade do tratamento que lhe deu origem, sem prejuízo da sua conservação por período mais longo, desde que tratados exclusivamente para fins de interesse público;
d) Que não existe qualquer transmissão de dados pessoais para fins comerciais ou de publicidade;
e) Que o tratamento dos dados pessoais é realizado para fins legalmente previstos ou para a prossecução de serviços online a seu pedido.

Artigo 3.º
Direito à informação e acesso

1 - Enquanto responsável pelo tratamento, a Câmara Municipal obriga-se a informar os respetivos titulares dos dados pessoais que recolhe e da respetiva finalidade.

2 – O titular dos dados tem o direito à confirmação de que os seus dados pessoais são ou não objeto de tratamento e o direito de aceder aos seus dados pessoais.

Artigo 4.º
Retificação, atualização, portabilidade e apagamento dos dados

1 - Sempre que legalmente permitido, a Câmara Municipal compromete-se a retificar, atualizar, disponibilizar e eliminar os dados pessoais a pedido do seu titular, no mais curto espaço de tempo possível.

2 - A disponibilização dos dados ao seu titular só pode ser efetuada se o tratamento for realizado por meios automatizados.

3 – O direito ao apagamento dos dados não pode ser exercido quando o tratamento se revele necessário ao cumprimento de uma obrigação legal, ao exercício de funções de interesse público ou ao exercício de autoridade pública de que a Câmara Municipal se encontra investida.

Artigo 5.º
Medidas Técnicas e Organizativas

1 - A Câmara Municipal da Marinha Grande cumpre as exigências previstas no artigo 32.º, nºs. 1 e 2 do RGPD.

2 - Consoante o que for adequado às características e sensibilidade de cada tratamento de dados pessoais e às especificidades existentes no Município são adotadas as medidas previstas nos artigos seguintes.

Artigo 6.º
Medidas Organizativas

1 - É definido um plano de resposta a incidentes e recuperação do desastre, com o exercício regular do mesmo, estando previstos os mecanismos necessários para garantir a segurança da informação e a resiliência dos sistemas e serviços, assegurando ainda que a disponibilidade dos dados é restabelecida após a ocorrência de um incidente.

2 - A informação é classificada de acordo com o nível de sensibilidade, sendo adotadas as medidas organizativas e técnicas adequadas à sua classificação.

3 - As políticas de segurança existentes estão devidamente documentadas.

4 - São adotados procedimentos de análise para a monitorização dos fluxos de tráfego na rede.

5 – São escrupulosamente cumpridas as seguintes políticas:

a) Política de gestão de palavras-passe seguras (impostos requisitos para o tamanho, a composição, o armazenamento e a frequência com que a palavra-passe deve ser alterada);
b) Política de gestão de ciclo de vida dos utilizadores, por forma a garantir que cada trabalhador tem apenas acesso aos dados necessários para executar as suas funções, revendo ainda, com a frequência necessária, as permissões dos vários perfis de utilizadores e desativando/revogando os perfis inativos.

6 - É adotada a alarmística necessária que permite identificar situações de acesso, tentativas ou utilização indevida.

7 - Quando aplicável, são adotadas as melhores práticas de segurança de informação, quer em fase de desenvolvimento de *software*, quer em fases de testes de aceitação, considerando em particular:
a) Os princípios de proteção de dados desde a conceção e por defeito;
b) Análises de risco do tratamento e do ciclo de dados;
c) Métodos de pseudonimização e anonimização dos dados, mesmo quando o sistema é desenvolvido e mantido por subcontratantes.

8 - São realizadas auditorias de segurança de Tecnologias de Informação e avaliações de vulnerabilidade (testes de penetração) sistemáticos.

9 – São realizadas auditorias internas e regulares, sobre se as medidas de segurança estão efetivamente em prática, por forma a que as mesmas se mantenham eficazes e atualizadas, procedimentos que são igualmente aplicáveis aos subcontratantes do Município.

10 - Quaisquer vulnerabilidades de segurança detetadas são documentadas e corrigidas, no mais curto período de tempo.

11 - São respeitadas todas as medidas previstas no artigo 33.º do RGPD relativas à notificação de uma violação de dados pessoais à CNPD.

12 – Todas as medidas internas de segurança técnicas e organizativas são avaliadas periodicamente, procedendo-se à sua atualização e revisão, sempre que se considerar necessário.

Artigo 7.º
Medidas Técnicas de Autenticação

1 - É obrigatório utilizar credenciais fortes com palavras-passe longas (pelo menos 12 caracteres), únicas, complexas e com números, símbolos, letras maiúsculas e minúsculas, tendo as mesmas de ser alteradas de 3 em 3 meses.

2 - Face à sensibilidade da informação em causa, são verificados e equacionados os privilégios dos utilizadores ou a sua forma de acesso à informação em causa, aplicando-se a autenticação multifator, caso se entenda necessário.

Artigo 8.º
Medidas Técnicas de Infraestruturas e Sistemas

1 - Os sistemas operativos e terminais devem manter-se sempre atualizados, bem como todas as aplicações utilizadas.

2 - O *firmware* dos equipamentos da rede deve estar sempre atualizado.

3 - Os sistemas, bem como a própria infraestrutura do Município, foram desenhados e organizados, de modo a segmentar ou isolar os sistemas e as redes de dados, prevenindo a propagação de *malware* dentro do Município e para sistemas externos.

4 – Foram implementadas medidas para robustecer a segurança dos postos de trabalho e servidores, tais como:

a) Bloqueio de acesso a sítios que sejam suscetíveis de constituir um risco para a segurança;
b) Bloqueio de redireccionamentos suspeitos através de motores de busca;
c) Bloqueio, imediato, de ficheiros e aplicações infetadas com *malware*;
d) Realização de inspeções periódicas do estado e utilização dos recursos do sistema;
e) Monitorização da utilização do software instalado;
f) Ativação e conservação dos registos de auditoria (*logs*) ;
g) Validação dos acessos por *IP* aos servidores que estão expostos ao público;
h) Alteração do porto configurado por omissão para o protocolo de acessos remotos (RDP).

Artigo 9.º
Medidas Técnicas quanto ao Correio Eletrónico

1 - Devem ser respeitadas as políticas e procedimentos internos sobre o envio de mensagens de correio eletrónico que contenham dados pessoais, tendo em conta que:

a) No caso de múltiplos destinatários, se deve garantir a inserção dos endereços de correio eletrónico dos destinatários, no campo “Bcc ”;
b) Se devem prevenir erros na introdução manual dos endereços de correio eletrónico;
c) Se devem assegurar que os ficheiros enviados em anexo contêm apenas os dados pessoais que se pretendem comunicar;
d) Se devem criar listas de distribuição ou grupos de contacto, apenas com o objetivo de prevenir a divulgação dos endereços dos destinatários, em operações de envio massivo de mensagens de correio eletrónico;
e) Se devem criar regras com o objetivo de adiar/atrasar a entrega de mensagens de correio eletrónico contendo dados pessoais, mantendo-as na “Caixa de Saída ” por

um tempo determinado, permitindo verificações de conformidade, após clicar em "Enviar ";

f) Se devem encriptar com código, ao qual só o destinatário tenha acesso, os emails e/ou anexos enviados que contenham dados pessoais;
g) Se deve confirmar com o destinatário, previamente ao envio de *email* contendo dados pessoais, o endereço de *email* preferencial para contacto.

2 – Devem ser realizadas ações de formação/sensibilização no sentido de capacitar os trabalhadores a operar os mecanismos de envio de mensagens de correio eletrónico, de acordo com os procedimentos definidos, sensibilizando-os para os erros mais comuns, potencialmente suscetíveis de originar violações de dados pessoais, incentivando-os à dupla verificação.

3 - O sistema de alerta da ferramenta da alarmística do Município é reforçado, por forma a assegurar visibilidade imediata sobre a criação de utilizadores de regras de encaminhamento automático de emails para contas externas.

4 - O sistema do Município é reforçado com ferramentas *antiphishing* e *antispam*, para que sejam bloqueadas ligações e/ou anexos com código malicioso.

5 - São adotados os controlos de segurança considerados essenciais, para classificar e proteger as mensagens de correio eletrónico sensíveis.

Artigo 10.º
Medidas Técnicas de Proteção contra *malware*

1 - É utilizada encriptação segura, especialmente no caso de credenciais de acesso, de dados especiais, de dados de natureza altamente pessoal e de dados financeiros.

2 - É utilizado um sistema de segurança (backup) atualizado, seguro e devidamente testado, totalmente separado das bases de dados principais e sem acessibilidade externa.

3 - O sistema do Município é reforçado com ferramentas *antimalware*, com capacidade de o verificar e detetar, bem como de efetuar o bloqueio, em tempo real, de ameaças do tipo *ransomware*.

Artigo 11.º
Medidas técnicas de Utilização de Equipamentos em Ambiente Externo

1 - Os dados são armazenados em sistemas internos, protegidos com medidas de segurança apropriadas e acessíveis remotamente, através de acesso seguro (VPN).

2 - Os acessos a estes equipamentos, em ambiente externo ao Município, apenas são permitidos através de VPN.

3 - Após 5 tentativas inválidas de login, proceder-se-á ao bloqueio da conta.

4 - Para os utilizadores do equipamento, é ativada a autenticação multifator.

5 - É aplicada a cifragem dos dados no sistema operativo.

6 - Sempre que se considerar necessário e aplicável, são ativadas as funcionalidades "*remote wipe* " e "*find my device* ".

7 - Quando o equipamento se encontra ligado à rede do Município, são efetuadas cópias de segurança automáticas das pastas de trabalho.

8 – O Município deve garantir que estas políticas de utilização de equipamentos em ambiente externo são escrupulosamente cumpridas.

Artigo 12.º
Medidas Técnicas de Armazenamento de Documentos em Papel

1 - É utilizado papel que permite a durabilidade da impressão.

2 - A documentação física é conservada em local com controlo de humidade e temperatura.

3 - Os documentos que contenham dados pessoais sensíveis, são armazenados, devidamente organizados, num local fechado, resistente ao fogo e inundação.

4 - Os acessos a essa documentação devem ser controlados, com registo das respetivas data e hora, quem acedeu e qual o documento acedido.

5 - Os documentos físicos são destruídos através de equipamento específico, que garanta a destruição "segura".

Artigo 13.º
Medidas técnicas de transporte de informação que integre dados pessoais

1 - São adotadas as medidas necessárias para impedir que, no transporte de informação com dados pessoais, estes possam ser lidos, copiados, alterados ou eliminados de forma não autorizada.

2 - É utilizada a encriptação segura no transporte, em dispositivos de massa ou arquivo potencialmente permanente, como CD/DVD/PEN e USB.

Artigo 14.º
Equipamentos de segurança

A Câmara Municipal, na prossecução das suas atividades, utiliza um conjunto de tecnologias e procedimentos de segurança adequados à proteção dos dados pessoais, protegendo o acesso ou divulgação não autorizados, nomeadamente através de:

a) Medidas de segurança física, como o controlo de acessos físicos de trabalhadores, colaboradores e visitantes às instalações da sede, mecanismos muito restritos de acesso a centros de dados e de combate à intrusão, medidas de segurança contra incêndios, alojamento de equipamentos em *datacenter* com monitorização 24x7 e controlo de acessos em conformidade com a Política de Controlo de Acessos;
b) Medidas de segurança lógica, na componente de acessos a sistemas e postos de trabalho através de mecanismos de gestão de identidades, autenticação e privilégios; na componente de rede, o uso de *firewalls* e sistemas de deteção de intrusão, segregação de redes (interna, externa, zona desmilitarizada) e ambientes aplicacionais, bem como cifragem de informação através de canais de comunicação seguros.

Artigo 15.º
Utilização de recursos informáticos e tecnologias de informação

1 - Os trabalhadores devem utilizar o material e os recursos informáticos que lhes são disponibilizados pela Câmara Municipal exclusivamente para fins profissionais e de forma diligente zelando pela respetiva manutenção, sendo proibida a troca de periféricos ou a abertura de equipamentos informáticos sem autorização expressa do serviço de Informática;

2 - A Câmara Municipal possui um sistema central de diretório para gestão das contas e estações de trabalho dos utilizadores, sendo atribuído a cada trabalhador uma conta de utilizador e uma palavra-passe, para acesso aos recursos informáticos disponibilizados, de acordo com o respetivo perfil de acesso.

3 - É da responsabilidade de cada utilizador a manutenção segura das suas palavra-passe nos termos da Política de Controlo de Acessos definida globalmente para a Câmara Municipal.

4 - As plataformas eletrónicas cuja gestão ou administração compete à Câmara Municipal dispõem de mecanismos de autenticação segura, podendo os trabalhadores autenticar-se através do certificado de autenticação disponível no Cartão de Cidadão ou da Chave Móvel Digital enquanto mecanismo alternativo com o mesmo grau de segurança.

5 - No que respeita à utilização de *software*, estabelece-se o seguinte:

a) A imagem de base das estações de trabalho disponibilizada pela Câmara Municipal contempla uma suite standard de aplicações de produtividade comuns a todos os utilizadores;

b) As atualizações e alterações à base de *software* são realizadas centralmente e distribuídas automaticamente através de políticas de grupo;

c) A necessidade de *software* adicional para o desempenho de funções específicas deve ser comunicada ao serviço de Informática, estando a respetiva instalação sujeita a autorização;

d) A deteção de avarias no funcionamento do *software* ou suspeita de *malware* deve ser de imediato comunicada ao serviço de Informática.

6 - No que respeita à utilização da Internet:
a) É proibido o acesso a sítios da Internet que contenham mensagens sexualmente explícitas, profanações, obscenidades ou outros;
b) A Câmara Municipal reserva-se o direito de bloquear e impedir o acesso a sítios da Internet em condições de equidade de todos os utilizadores.

7 - No que respeita à utilização do correio eletrónico, estabelece-se o seguinte:
a) É fornecido um endereço de correio eletrónico a cada trabalhador;
b) O endereço de correio eletrónico fornecido pela Câmara Municipal deve ser utilizado exclusivamente para fins profissionais;
c) É expressamente proibida a utilização do correio eletrónico para o envio de:
i. Material que seja considerado ilegal, nomeadamente conteúdos que violem os direitos de autor ou possuam material obsceno ou ofensivo dos bons costumes;
ii. Mensagens de continuação que tenham por fim dar seguimento em cadeia a *emails* ou equivalentes;
d) Após a cessação de funções de um trabalhador, o endereço de correio eletrónico é extinto e o respetivo conteúdo eliminado.

Artigo 16.º
Registo das atividades de tratamento

1 - Os dirigentes de cada unidade orgânica da Câmara Municipal devem conservar um registo de todas as atividades de tratamento de dados pessoais, sob a sua responsabilidade, mantendo-o permanentemente atualizado.

2 – No exercício das suas funções, os trabalhadores das unidades orgânicas que tratam dados pessoais devem reportar ao respetivo dirigente qualquer nova atividade de tratamento de dados pessoais, procedendo este ao seu imediato registo.

Artigo 17.º
Relações institucionais com a Autoridade de Controlo

A Câmara Municipal, através do seu encarregado da proteção de dados, coopera com a autoridade de controlo facultando-lhe as informações, sempre que solicitado.

Artigo 18.º
Encarregado da proteção de dados

1 - Após a sua nomeação, o encarregado da proteção de dados tem como principais funções:
a) Informar e aconselhar a Câmara Municipal ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações;

b) Controlar a conformidade dos tratamentos efetuados ao abrigo do RGPD, com outras disposições de proteção de dados da União Europeia ou nacionais e com as políticas da Câmara Municipal ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;
c) 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) Colaborar com a autoridade de controlo.

2 - No desempenho das suas funções o encarregado da 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.

Artigo 19.º
Segredo profissional

Independentemente do tipo de vínculo laboral, todos os trabalhadores da Câmara Municipal, prestadores de serviços e fornecedores que tratem dados pessoais estão obrigados a manter o segredo sobre os mesmos, ficando impedidos de os revelar ou utilizar, salvo em cumprimento de obrigação legal ou decisão judicial.

Artigo 20.º
Responsabilidade disciplinar

1 - Os trabalhadores da Câmara Municipal são disciplinarmente responsáveis pela violação ou transmissão ilegal dos dados pessoais a que, devida ou indevidamente, tenham acesso, bem como pela violação das normas deste Código.

2 - Os restantes colaboradores, fornecedores ou prestadores de serviços são responsáveis nos termos legais e contratualmente estabelecidos.

Artigo 21º
Violação de dados pessoais

1 - A Câmara Municipal deve notificar a autoridade de controlo, sem demora injustificada e, sempre que possível, no prazo de 72 horas após o conhecimento de uma violação de dados pessoais, suscetível de implicar um risco para os direitos e liberdades das pessoas singulares.

2 - Não sendo possível cumprir o prazo referido no número anterior, a notificação deve ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases, sem demora injustificada.

3 - Sempre que se verifique uma violação de dados pessoais a Câmara Municipal abre um processo de averiguações interno para apurar as respetivas causas.

4 - Todos os trabalhadores que tenham conhecimento de qualquer situação que possa implicar uma violação de dados pessoais devem comunicá-la imediatamente ao seu superior hierárquico que, por sua vez, fica obrigado a comunicá-la, sem demora injustificada, ao encarregado da proteção de dados da Câmara Municipal, através do endereço eletrónico dpo@cm-mgrande.pt, ou qualquer outro meio mais expedito.

Artigo 22.º
Dúvidas e omissões

1 - As dúvidas suscitadas na interpretação e aplicação do presente Código devem ser dirigidas ao encarregado da proteção de dados, que deve responder às mesmas no prazo fixado no contrato que celebrou com o Município da Marinha Grande.

2 -Em tudo o que não se encontre especialmente previsto neste Código é aplicável o RGPD e legislação nacional em vigor sobre esta matéria.

3 - O encarregado da proteção de dados promove a divulgação deste Código de Conduta junto de todos os trabalhadores e efetua ações de sensibilização, formação, e acompanhamento da sua aplicação e respetiva avaliação, em colaboração com a equipa que considere necessária.

Artigo 23º
Entrada em vigor

O presente Código de Conduta entra em vigor no quinto dia útil seguinte à data da sua aprovação pela Câmara Municipal.