DIÁRIO DA REPÚBLICA

2.ª série
N.º 26
06-02-2025

MUNICÍPIO DA PRAIA DA VITÓRIA

Aviso n.º 3647/2025/2

Sumário: Regulamento Municipal de Proteção de Dados da Câmara Municipal da Praia da Vitória.

Regulamento Municipal de Proteção de Dados da Câmara Municipal da Praia da Vitória

Vânia Marisa Borges Figueiredo Ferreira, Presidente da Câmara Municipal da Praia da Vitória, faz público, nos termos e para os efeitos do disposto no artigo 56.º, do Anexo I à Lei n.º 75/2013, de 12 de setembro, e nos termos do artigo 139.º do Código do Procedimento Administrativo, aprovado pelo Decreto-Lei n.º 4/2015, de 7 de janeiro, que a Assembleia Municipal da Praia da Vitória, no uso da competência que lhe é conferida pela alínea g) do n.º 1 do artigo 25.º daquele mesmo Anexo I à Lei n.º 75/2013, aprovou, na sua sessão ordinária realizada no dia 19 de dezembro de 2024, sob proposta da Câmara Municipal, aprovada na reunião de Câmara de 2 de outubro de 2024, o Regulamento Municipal de Proteção de Dados da Câmara Municipal da Praia da Vitória.

«Regulamento Municipal de Proteção de Dados da Câmara Municipal da Praia da Vitória

Nota justificativa

O Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679), de 27 de abril de 2016, doravante designado de RGPD, foi publicado a 04 de maio de 2016, tendo entrado em vigor no dia 25 de maio de 2018, aprovado pela Comissão Europeia e relativo à proteção de pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, revogando assim a Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados).

O RGPD estabelece os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais e que estes devam respeitar, independentemente da nacionalidade ou local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção de dados.

Qualquer tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado na União deverá ser feito em conformidade com o RGPD, independentemente de o tratamento em si ser realizado na União.

No âmbito nacional, aplica-se a Lei de Execução Nacional do RGPD (Lei n.º 58/2019, de 08 de agosto), sendo a Comissão Nacional de Proteção de Dados, doravante designada CNPD, a Autoridade de Controlo Nacional para efeitos do RGPD, da Lei de Execução Nacional do RGPD e demais disposições legais e regulamentares aplicáveis, em matéria de proteção de dados pessoais, com o objetivo de defender os direitos, liberdades e garantias das pessoas, no âmbito do tratamento desses mesmos dados pessoais.

A Câmara Municipal da Praia da Vitória, como qualquer entidade pública ou privada que proceda ao tratamento de dados pessoais, encontra-se abrangida pelo RGPD, contudo, existe uma verdadeira lacuna no que concerne a uma política de proteção de dados, no âmbito municipal.

Numa lógica de salvaguarda dos dados pessoais dos cidadãos que interagem com a Câmara Municipal da Praia da Vitória e para auxiliar os serviços municipais, os cidadãos e as empresas na prossecução do disposto no RGPD e na Lei n.º 58/2019, de 08 agosto, a Câmara Municipal da Praia da Vitória elaborou o Regulamento Municipal de Proteção de Dados da Câmara Municipal da Praia da Vitória (RMPD).

O presente Regulamento apresenta-se como complementar à legislação em vigor, sendo considerado fundamental para a atuação da Câmara Municipal da Praia da Vitória, como responsável pelo tratamento de dados pessoais.

O RMPD não substitui o disposto no RGPD, na Lei n.º 58/2019, de 08 agosto, nem em demais legislação especial relativa à proteção de dados pessoais bem como nas demais disposições legais e regulamentares existentes em matéria de proteção de dados pessoais. O que o RMPD pretende é dar

resposta à implementação do RGPD e da Lei n.º 58/2019, de 08 agosto, tendo em conta as especificidades dos serviços do Município, apresentando um conjunto de minutas e documentos necessários ao cumprimento das obrigações do mesmo enquanto responsável pelo tratamento de dados pessoais, em tudo o que não contraria a legislação supramencionada.

As situações não previstas e/ou não contempladas e/ou não referenciadas no presente Regulamento regem-se pelo disposto no RGPD, na Lei n.º 58/2019, de 08 agosto e nas demais disposições legais e regulamentares existentes, no que concerne a proteção de dados pessoais. São igualmente consideradas as Orientações e Diretrizes da CNPD, que se afigurem aplicáveis aos tratamentos de dados realizados pelo Município.

O presente Regulamento, apesar de fazer referência a normas e medidas organizativas internas, excede uma lógica meramente interna, uma vez que estas normas e medidas produzem um efeito externo, isto é, influenciam a relação entre os titulares dos dados pessoais e a Câmara Municipal da Praia da Vitória, enquanto responsável pelo tratamento desses dados. Com base nesta premissa e pelo facto de apresentar uma panóplia de destinatários, considera-se que o RMPD é um regulamento de eficácia externa.

Ponderados os custos e benefícios da elaboração do presente regulamento, é de concluir que o mesmo não implica qualquer aumento significativo de encargos para o município, e que os benefícios resultantes da regulamentação do tratamento dos dados pessoais e a segurança e salvaguarda que proporcionam, claramente justificam e superam os custos da sua implementação.

O projeto de Regulamento foi submetido por 30 dias a consulta pública, mediante publicação do Aviso n.º 16108/2024/2, publicado no *Diário da República*, 2.ª série, n.º 148, de 1 de agosto de 2024, e na página oficial da internet da Câmara Municipal da Praia da Vitória, através do Edital n.º 9181/2024, de 1 de agosto de 2024, nos termos e para os efeitos do artigo 101.º, do Código de Procedimento Administrativo.

Assim e ao abrigo do artigo 241.º da Constituição da República Portuguesa, conjugado com os artigos 25.º, n.º 1, alínea g), 33.º, n.º 1, alínea k), do Anexo I da Lei n.º 75/2013, de 12 de setembro, foi, por deliberação da Assembleia Municipal da Praia da Vitória, datada de 19 de dezembro de 2024, sob proposta da Câmara Municipal, aprovada em reunião de câmara datada de 2 de outubro de 2024, aprovado o Regulamento Municipal de Proteção de Dados da Câmara Municipal da Praia da Vitória.

Regulamento Municipal de Proteção de Dados da Câmara Municipal da Praia da Vitória

CAPÍTULO I

Disposições gerais

Artigo 1.º

Lei habilitante

O Regulamento Municipal de Proteção de Dados da Câmara Municipal da Praia da Vitória é elaborado ao abrigo e nos termos do disposto no artigo 241.º da Constituição da República Portuguesa; nos artigos 98.º e 135.º e seguintes do Código de Procedimento Administrativo; no art. 4.º, no n.º 1 do art. 23.º, na alínea g) do n.º 1 do art. 25.º e na alínea k) do n.º 1 do art. 33.º do Regime Jurídico das Autarquias Locais aprovado pela Lei n.º 75/2013, de 12 de setembro, na sua redação atual; no art. 24.º do Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679), de 27 de abril de 2016 e na Lei n.º 58/2019, de 08 agosto.

Artigo 2.º

Objeto, Âmbito e Objetivos Gerais

1 — O presente Regulamento estabelece as regras, os termos e as condições pelas quais se rege a atuação da Câmara Municipal da Praia da Vitória, enquanto responsável pelo tratamento de dados pessoais, tendo em consideração o disposto na legislação atualmente em vigor.

Aviso n.º 3647/2025/2

2 — O presente Regulamento visa:

a) Disciplinar a recolha e subsequente 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 RGPD, na Lei n.º 58/2019, de 08 agosto e nas demais disposições legais e regulamentares existentes, em matéria de proteção de dados pessoais;

b) Promover, defender e garantir, de forma complementar o regime legal vigente, os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais e os seus direitos enquanto titulares dos dados, aquando da sua interação com a Câmara Municipal da Praia da Vitória, de forma indiscriminada;

c) Consolidar a implementação do RGPD no âmbito da ação e da atuação da Câmara Municipal da Praia da Vitória, enquanto responsável pelo tratamento de dados pessoais;

d) Definir a atuação dos serviços municipais, no âmbito da recolha e do tratamento de dados pessoais.

3 — São destinatários do presente Regulamento:

a) Os serviços municipais inseridos na Estrutura Orgânica Interna da Câmara Municipal da Praia da Vitória;

b) Os funcionários, trabalhadores e outros colaboradores da Câmara Municipal da Praia da Vitória;

c) Os contraentes de aquisições de bens e serviços, empreitadas ou detentores de concessão municipal;

d) Todas as pessoas singulares que, a qualquer título, se relacionem com a Câmara Municipal da Praia da Vitória.

CAPÍTULO II

Política geral de privacidade

Artigo 3.º

Responsável pelo Tratamento

O responsável pelo tratamento é a Câmara Municipal da Praia da Vitória, sita na Praça Francisco Ornelas da Câmara, 9760-851 Santa Cruz, contactável através do *site* https://www.cmpv.pt/, via *e-mail:* geral@cmpv.pt, telefone: +351 295 540 200, e ainda presencialmente.

Artigo 4.º

Encarregado de Proteção de Dados

1 — Nos termos do artigo 37.º do RGPD e dos artigos 9.º e 12.º da Lei n.º 58/2019, de 08 agosto, a Câmara Municipal de Praia da Vitória designou um encarregado de proteção de dados, o qual pode ser contactado através do *e-mail:* epd@cmpv.pt.

2 — O encarregado de proteção de dados deve ser designado com base nas suas qualificações profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito nacional e europeu de proteção de dados, no conhecimento das operações de processamento realizadas, das tecnologias de informação, das práticas de segurança de dados, bem como da estrutura organizacional da Câmara Municipal de Praia da Vitória.

3 — Nos termos dos artigos 37.º a 39.º do RGPD e do artigo 11.º da Lei n.º 58/2019, de 08 agosto, são funções do encarregado de proteção de dados:

a) Informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos da legislação em vigor;

Aviso n.º 3647/2025/2

b) Controlar a conformidade com a legislação em vigor e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados e as auditorias correspondentes;

c) Prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados, controlando a sua realização nos termos do artigo 35.º do RGPD e artigo 7.º da Lei n.º 58/2019, de 08 agosto;

d) Cooperar com a CNPD, sendo o seu ponto de contacto quanto a questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.º do RGPD, consultando ainda esta entidade, quando achar necessário;

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 nas matérias abrangidas pelo RGPD, pela legislação nacional e pelo presente Regulamento, em matéria de proteção de dados.

4 — Nos termos do n.º 2 do artigo 39.º do RGPD, 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 de tratamento.

5 — Nos termos do n.º 5 do artigo 38.º do RGPD e do artigo 10.º da Lei n.º 58/2019, de 08 agosto, o encarregado de proteção de dados, bem como os responsáveis pelo tratamento de dados, incluindo os subcontratantes, e todas as pessoas que intervenham em qualquer operação de tratamento de dados, estão obrigados a um dever de confidencialidade, que se mantém após o termo das funções que lhe deram origem, que acresce aos deveres de sigilo profissional legalmente previstos.

6 — As funções do encarregado de proteção de dados são exercidas com total independência e autonomia em relação à estrutura dos serviços, isenção, distanciamento e não subordinação à hierarquia municipal, não podendo ser prejudicado nem penalizado pelo exercício das mesmas ou pelo teor dos pareceres que emite ou pelas iniciativas que desenvolve no âmbito das suas funções e competências.

7 — No âmbito e na prossecução das suas funções, de forma célere e independente, o encarregado de proteção de dados da Câmara Municipal da Praia da Vitória tem acesso ilimitado ao sistema, à documentação e à informação da organização.

8 — A Câmara Municipal da Praia da Vitória deve providenciar ao encarregado de proteção de dados os meios necessários de ordem logística e tecnológica necessários ao desempenho da sua função e das suas competências.

Artigo 5.º

Definições Relevantes

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

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

Aviso n.º 3647/2025/2

3 — "Limitação do tratamento": a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro.

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

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

6 — "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.

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

8 — "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.

9 — "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.

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

11 — "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.

12 — "Dados biométricos": dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos.

13 — "Dados relativos à 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.

Artigo 6.º

Videovigilância e Autorizações para Tratamento de Dados Pessoais

Após a entrada em vigor do RGPD, não é necessária a autorização da CNPD para a existência de um sistema de videovigilância, não obstante, este deve respeitar os requisitos legais, que podem incluir além do RGPD e a Lei n.º 58/2019, de 8 de agosto, a Lei n.º 34/2013, de 16 de maio, que regula a atividade de segurança privada ou o Código do Trabalho, consoante o que for aplicável à sua situação concreta.

Artigo 7.º

Princípios Relativos ao Tratamento de Dados Pessoais

Nos termos do artigo 5.º do RGPD, são os princípios relativos ao tratamento de dados pessoais:

a) Princípio da licitude: O tratamento de dados pessoais só poderá ser realizado ao abrigo das condições previstas na legislação em vigor, entenda-se o RGPD, a Lei n.º 58/2019, de 8 de agosto, e as demais disposições legais e regulamentares em matéria de proteção de dados pessoais;

Aviso n.º 3647/2025/2

b) Princípio da lealdade e transparência: O tratamento de dados pessoais deverá ser realizado sempre de forma leal e transparente perante os titulares dos dados pessoais;

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, incluindo a 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: O responsável pelo tratamento tem de cumprir todos os princípios indicados e conseguir comprovar esse cumprimento.

Artigo 8.º

Tratamento de Dados Pessoais em Geral

Nos termos do artigo 6.º do RGPD, o tratamento de dados pessoais em geral, por parte da Câmara Municipal da Praia da Vitória, é lícito sempre que se verifique 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 específicas. Porém, de acordo com o disposto no considerando 43 do RGPD, este afirma que o consentimento não pode ser utilizado como fundamento de licitude do tratamento de dados pessoais pela Câmara Municipal da Praia da Vitória, isto porque, a fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública, sendo considerado improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa;

b) Contratos: O tratamento for necessário para a 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, entenda-se competências e atribuições legais da Câmara Municipal da Praia da Vitória;

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

e) Interesse público e autoridade pública: 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) Interesse legítimo: 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.

Aviso n.º 3647/2025/2

Artigo 9.º

Licitude do tratamento de Categorias de Dados Especiais e/ou de Dados Pessoais Sensíveis

1 — As categorias especiais de dados pessoais e/ou dados pessoais sensíveis englobam os dados ou informações que implicam maiores riscos para os direitos e liberdades fundamentais da pessoa humana, como: 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 — Nos termos do n.º 1 do artigo 9.º do RGPD, é proibido o tratamento destes dados pessoais, exceto nos casos previstos nos termos do n.º 2 e do n.º 3 do artigo 9.º do RGPD, a saber:

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 a legislação europeia e nacional previr que a proibição não pode ser anulada pelo titular dos dados;

b) O tratamento é necessário para o 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;

c) O tratamento é necessário para fins de medicina preventiva ou do trabalho, para 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;

d) O tratamento se refira a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;

e) O tratamento é necessário para interesse público importante, legalmente previsto, 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;

f) O tratamento é necessário para arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, previsto na lei, 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, respeitando o disposto no artigo 31.º da Lei n.º 58/2019, de 8 de agosto.

Artigo 10.º

Recolha de Dados Pessoais no *Website* Oficial da Câmara Municipal da Praia da Vitória

O acesso e a utilização do *website* oficial da Câmara Municipal da Praia da Vitória (https://www.cmpv.pt/) não implica, em geral, a disponibilização e recolha de dados pessoais, o que sucederá 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.

Artigo 11.º

Consentimento dos Titulares dos Dados Pessoais no *Website* da Câmara Municipal da Praia da Vitória

Os dados pessoais serão recolhidos através do consentimento dos utilizadores do *website* oficial da Câmara Municipal da Praia da Vitória, considerando-se os 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.

Aviso n.º 3647/2025/2

Artigo 12.º

Finalidades da Recolha de Dados Pessoais no *Website* da Câmara Municipal da Praia da Vitória

1 — Os dados pessoais submetidos no formulário de contacto destinam-se a esclarecer dúvidas, pedidos de informação ou esclarecimentos e em geral qualquer solicitação apresentada no formulário em questão.

2 — A comunicação dos dados pessoais não constitui uma obrigação legal nem contratual. O titular não está obrigado a fornecer os dados pessoais, mas não os fornecendo, não poderá usufruir das respetivas funcionalidades.

Artigo 13.º

Finalidades do Tratamento de Dados Pessoais

Como finalidades do tratamento de dados pessoais, a Câmara Municipal da Praia da Vitória terá:

a) 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.

b) O cumprimento pela Câmara Municipal da Praia da Vitória das suas atribuições ou obrigações legais e das suas funções de interesse público ou autoridade pública enquanto órgão da Administração Pública.

c) O exercício pelos titulares dos dados ou pela Câmara Municipal da Praia da Vitória de direitos e obrigações previstos na legislação.

Artigo 14.º

Transmissão de Dados Pessoais

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

Artigo 15.º

Prazo de Conservação de Dados Pessoais

O prazo de conservação de dados pessoais será o prazo necessário para a tramitação de procedimentos administrativos, duração de contratos, acrescido do prazo legal de arquivo dos documentos onde os dados estão registados, conforme estabelecido no Regulamento para a Classificação e Avaliação da Informação Arquivística da Administração Local, aprovado pela Portaria n.º 112/2023, de 27 de abril.

Artigo 16.º

Direitos dos Titulares dos Dados Pessoais

1 — Nos termos do Capítulo III do RGPD (Direitos do Titular dos Dados), e identificadas as disposições específicas no que à Câmara Municipal da Praia da Vitória diz respeito, os direitos dos titulares são:

a) Confirmação de que os dados pessoais são objeto de tratamento;

b) Direito de informação;

c) Direito de acesso aos dados pessoais;

d) Direito de retificação;

e) Direito ao apagamento;

Aviso n.º 3647/2025/2

f) Direito à limitação do tratamento;

g) Direito de portabilidade dos dados;

h) Direito de oposição ao tratamento;

i) Direito de apresentar reclamação à entidade de controlo, a CNPD.

2 — Relativamente ao consentimento dos titulares dos dados pessoais no *website* oficial da Câmara Municipal da Praia da Vitória, está associado o direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado.

3 — No que diz respeito ao direito ao apagamento dos dados, à portabilidade dos dados e à oposição ao tratamento, estes direitos não poderão ser exercidos nas seguintes situações:

a) Quando o tratamento se revela necessário ao cumprimento de obrigações legais que exigem o tratamento e ao exercício de funções de interesse público e ao exercício da autoridade pública de que esteja investido a Câmara Municipal da Praia da Vitória;

b) Quando o tratamento, baseado no cumprimento de obrigações legais, no exercício de funções de interesse público e/ou no exercício da autoridade pública por parte da Câmara Municipal da Praia da Vitória, não é precedido pelo consentimento do titular dos dados.

Artigo 17.º

Transparência do Tratamento e o Exercício dos Direitos pelos Titulares dos Dados Pessoais

1 — Nos termos do n.º 1 artigo 12.º do RGPD, a Câmara Municipal da Praia da Vitória, enquanto responsável pelo tratamento dos dados pessoais, deve fornecer aos titulares dos dados as informações relativas ao tratamento dos dados e aos direitos dos titulares dos dados 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 — A Câmara Municipal da Praia da Vitória, enquanto responsável pelo tratamento dos dados pessoais, facilita o exercício dos direitos pelos titulares dos dados e fornece aos titulares dos dados as informações sobre as medidas tomadas, para garantir o exercício dos direitos pelos titulares dos dados, no prazo de um mês a contar da data de receção do pedido de exercício dos direitos.

3 — O prazo presente no n.º 2 do presente artigo pode ser prorrogado até dois meses, quando necessário, tendo em conta a complexidade do pedido e o número de pedidos, devendo-se informar o titular dos dados de alguma prorrogação e dos motivos da demora, no prazo de um mês a contar da data de receção do pedido.

4 — 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.

5 — Se não for dado seguimento ao pedido apresentado pelo titular dos dados, este deve ser informado no prazo de um mês, a contar da data de receção do pedido, das razões que o levaram a não tomar medidas e da possibilidade de apresentar reclamação à autoridade de controlo (CNPD) e de intentar a respetiva ação judicial.

6 — As informações fornecidas e quaisquer comunicações e medidas tomadas são fornecidas a título gratuito.

7 — 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 de tomada das medidas solicitadas;

b) Recusar-se a dar seguimento ao pedido.

Aviso n.º 3647/2025/2

8 — Na sequência do n.º 7 do presente artigo, cabe à Câmara Municipal da Praia da Vitória demonstrar o caráter manifestamente infundado ou excessivo do pedido.

9 — Em cumprimento das obrigações de transparência e para facilitar o exercício dos direitos pelos titulares, a Câmara Municipal da Praia da Vitória disponibiliza um formulário de requerimento de exercício de direitos para ser utilizado pelo titular dos dados, presente no Anexo I-A.

Artigo 18.º

Informações sobre o Tratamento e os Direitos dos Titulares no Momento da Recolha dos Dados Pessoais

1 — No momento da recolha dos dados pessoais, a Câmara Municipal da Praia da Vitória, enquanto responsável pelo tratamento, faculta informações sobre o tratamento dos dados pessoais e sobre os direitos dos titulares.

2 — Para que a prestação das informações ocorra no momento da recolha dos dados e fique devidamente documentada e comprovada, estas são prestadas nos formulários dos requerimentos dos diversos procedimentos.

3 — Nos casos em que haja recolha de dados pessoais, sem que o titular dos dados apresente o formulário do requerimento disponibilizado pela Câmara Municipal da Praia da Vitória, seja por apresentar um requerimento elaborado pelo próprio, seja por simplesmente não apresentar qualquer requerimento, é utilizado o formulário presente no Anexo I-C, exclusivamente destinado a comprovar a prestação das informações sobre o tratamento de dados e direitos dos titulares.

Artigo 19.º

Outras Informações sobre o Tratamento de Dados Pessoais

1 — A comunicação dos dados pessoais à Câmara Municipal da Praia da Vitória é em geral necessária para exercício de direitos e cumprimento de obrigações legais ou contratuais.

2 — A não disponibilização dos dados pessoais pelos titulares é, em geral, impeditiva do exercício de direitos e cumprimento de obrigações legais ou contratuais.

3 — Não existem decisões automatizadas, nem a definição de perfis.

4 — Para além do cumprimento da obrigação legal de tratamento para arquivo, não haverá tratamento posterior de dados pessoais para finalidades distintas das que presidiram à recolha.

5 — As informações sobre o tratamento de dados pessoais e direitos dos titulares, de uma forma genérica, estão presentes no Anexo I-C.

Artigo 20.º

Segurança do Tratamento de Dados Pessoais

1 — Nos termos do artigo 32.º do RGPD e tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, a Câmara Municipal da Praia da Vitória, enquanto responsável pelo tratamento, aplica medidas técnicas e organizativas para garantir um nível de segurança adequado ao risco, incluindo, manter a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento e a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada, no caso de um incidente físico ou técnico; bem como, adotar procedimentos para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

2 — Estas medidas técnicas e organizativas estão referenciadas e especificadas no Capítulo III do presente Regulamento, que compreende o intervalo entre o artigo 34.º e o artigo 56.º, inclusive.

Aviso n.º 3647/2025/2

Artigo 21.º

Notificação da Violação de Dados Pessoais à Autoridade de Controlo (CNPD)

Nos termos do artigo 33.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, a Câmara Municipal da Praia da Vitória, enquanto responsável pelo tratamento, notifica desse facto a autoridade de controlo (CNPD) utilizando o procedimento implementado para esse efeito, presente no Anexo I-D.

Artigo 22.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, a Câmara Municipal da Praia da Vitória, enquanto responsável pelo tratamento, comunica a violação de dados pessoais ao titular dos dados sem demora injustificada, utilizando o procedimento implementado para esse efeito, presente no Anexo I-E.

Artigo 23.º

Sigilo Profissional

Os responsáveis pelo tratamento, os subcontratantes, bem como qualquer outra pessoa que, no exercício das suas funções, tenha acesso a dados pessoais, ficam obrigados a sigilo profissional, mesmo após o termo das suas funções.

Artigo 24.º

Tratamento de Dados Pessoais através de Subcontratantes

1 — A Câmara Municipal da Praia da Vitória, enquanto responsável pelo tratamento, só recorre a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de forma que o tratamento satisfaça os requisitos do RGPD e assegure a defesa dos direitos do titular dos dados.

2 — O tratamento em subcontratação é regulado por contrato ou outro ato normativo previsto na lei, que vincula os subcontratantes à Câmara Municipal da Praia da Vitória.

Artigo 25.º

Registos de atividades de tratamento de dados pessoais

A Câmara Municipal da Praia da Vitória, enquanto responsável pelo tratamento, conserva registos de todas as atividades de tratamento de dados pessoais sob a sua responsabilidade, sendo que desses registos das atividades de tratamento constam todos os elementos e informações legalmente exigidos.

Artigo 26.º

Avaliações de Impacto sobre a Proteção de Dados Pessoais

1 — Nos termos do artigo 35.º do RGPD, quando um certo tipo de tratamento, tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, a Câmara Municipal da Praia da Vitória, enquanto responsável pelo tratamento, efetua as necessárias avaliações de impacto sobre a proteção de dados pessoais (AIPD), nos termos e condições legalmente previstos.

Aviso n.º 3647/2025/2

2 — Existem operações de tratamento de dados pessoais realizadas pela Câmara Municipal da Praia da Vitória que se enquadram nas condições previstas no RGPD e no Regulamento n.º 1/2018, de 16 de outubro, relativo à lista de tratamento de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados, da CNPD:

a) Tratamento de dados pessoais através de sistemas de videovigilância: por se enquadrar como uma operação de "Controlo sistemático de zonas acessíveis ao público em grande escala", tipificado no n.º 3 do art. 35.º RGPD, que não foi, contudo, submetido a Avaliação de Impacto Sobre a Proteção de Dados, porque de acordo com as Orientações do Grupo de Trabalho do artigo 29.º, não é necessária a realização da AIPD para operações de tratamento que tenham sido previamente controladas ou autorizadas pela autoridade de controlo (CNPD) e não tenham sofrido alterações nas condições de tratamento;

b) Tratamento de dados biométricos: Por se enquadrar como uma operação de "Tratamento de dados biométricos para identificação inequívoca dos seus titulares, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados", nos termos previstos no Regulamento n.º 1/2018 da CNPD e no considerando 91 do RGPD.

Artigo 27.º

Consulta prévia à Autoridade de Controlo

Nos termos do artigo 36.º do RGPD, a Câmara Municipal da Praia da Vitória enquanto responsável pelo tratamento, consulta a autoridade de controlo (CNPD) antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados indicar que do tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar esse risco.

Artigo 28.º

Cooperação com a autoridade de controlo

Nos termos do artigo 8.º da Lei n.º 58/2019, de 8 de agosto, a Câmara Municipal da Praia da Vitória, enquanto responsável pelo tratamento, coopera e colabora com a autoridade de controlo (CNPD) a pedido desta, na prossecução das suas atribuições e competências.

Artigo 29.º

A Proteção de Dados Pessoais e o Direito de Acesso aos Documentos Administrativos

Nos termos do artigo 86.º do RGPD, do artigo 26.º da Lei n.º 58/2019, de 8 de agosto, e da Lei n.º 26/2016, de 22 de agosto (com as devidas atualizações), os dados pessoais que constem de documentos oficiais na posse da Câmara Municipal da Praia da Vitória, para a prossecução de atribuições de interesse público, podem ser divulgados nos termos da legislação de acesso a documentos administrativos, a fim de conciliar o acesso do público a documentos oficiais com o direito à proteção dos dados pessoais.

Artigo 30.º

Utilização e Reprodução de Documentos de Identificação

A utilização e reprodução dos documentos de identificação dos titulares dos dados pode ser apenas realizada mediante consentimento escrito dos mesmos.

Artigo 31.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, a Câmara Municipal da Praia da Vitória 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.

Aviso n.º 3647/2025/2

CAPÍTULO III

Medidas Técnicas e Organizativas de Proteção de Dados Pessoais

Artigo 32.º

Regras gerais

1 — Criar e manter um registo atualizado de todos os ativos tecnológicos (*hardware, firmware* e *software*).

2 — Garantir um nível de segurança forte dos dados pessoais e dos recursos de tratamento.

3 — Dar formação adequada a todos os utilizadores sobre segurança do sistema e dos dados pessoais.

4 — Implementar diferentes tipos de mecanismos de segurança, criando diferentes camadas de proteção.

5 — Assegurar que cada mecanismo de segurança contribuiu, separadamente e/ou em combinação com outros mecanismos, para atingir os objetivos de segurança.

6 — Anular ou, pelo menos, mitigar quaisquer deficiências na segurança que possam existir, mantendo um risco residual num nível aceitável a cada caso.

7 — Efetuar alterações de hardware, *firmware* e software não devem enfraquecer a segurança do sistema.

8 — 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.

9 — 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.

10 — Sensibilizar todos os utilizadores para as respetivas responsabilidades individuais na segurança do sistema e dos dados pessoais.

11 — Obter a aceitação de todos os utilizadores, que tenham perfis de privilégios de escrita, leitura e eliminação de dados pessoais, das condições definidas num termo de responsabilidade.

12 — Garantir a assistência técnica a todos os utilizadores quando e onde necessário.

13 — Criar e manter registos (*logs*), de modo a permitir o rastreamento das atividades com impacto na segurança dos dados pessoais.

14 — 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*).

15 — Assegurar a manutenção do sistema não deve violar a sua segurança.

16 — Conduzir visitas técnicas para determinar se as medidas de segurança no local são suficientes e adequadas.

17 — Realizar auditorias internas e a entidades subcontratadas, cujos resultados devem ficar versados em relatório.

18 — 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.

19 — Determinar investigações nos casos de violações de segurança ou de suspeitas de violação.

Aviso n.º 3647/2025/2

Artigo 33.º

Medidas Técnicas e Organizativas de Proteção de Dados de Categorias Especiais

1 — Controlo da entrada nas instalações: impedir o acesso de pessoas não autorizadas às instalações utilizadas para o tratamento de dados.

2 — Controlo dos suportes de dados: impedir que suportes de dados possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada.

3 — 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.

4 — Controlo da utilização: impedir que sistemas de tratamento automatizados de dados possam ser utilizados por pessoas não autorizadas.

5 — Controlo de acesso: garantir que pessoas autorizadas só possam ter acesso aos dados abrangidos pela autorização.

6 — Controlo da transmissão: garantir a verificação das entidades a quem possam ser transferidos os dados pessoais através da instalação de transmissão de dados.

7 — Controlo da introdução: garantir que se possa verificar a posteriori, em prazo adequado à natureza do tratamento, quais os dados pessoais introduzidos, quando e por quem.

8 — 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 34.º

Definição de Áreas de Acesso Restrito e Controlado

1 — Definição de áreas de acesso restrito e controlado através de mecanismos que permitam o acesso unicamente a pessoas autorizadas.

2 — Criação e atualização de lista de pessoas autorizadas a aceder às áreas referidas no n.º 1 do presente artigo.

3 — Criação e preservação de registos de acesso às áreas referidas no n.º 1 do presente artigo.

Artigo 35.º

Responsabilidades Coletivas e Individuais

1 — Cada utilizador deve ser individualmente responsável por respeitar as políticas e medidas de segurança implementadas.

2 — Todas as atividades realizadas no sistema devem estar sujeitas a monitorização e auditorias.

3 — Existência de uma política de segregação de funções, de modo a reduzir a probabilidade de erro humano no tratamento de dados pessoais.

4 — Proibição do acesso aos dados pessoais sob o controlo da organização a partir de dispositivos pessoais.

5 — Proibição da utilização de dispositivos da organização fora das instalações, incluindo para fins pessoais.

6 — A proibição expressa no n.º 5 do presente artigo não abrange os chefes de divisão, porém incluí a proibição da sua utilização para fins pessoais.

7 — Utilização de dispositivos de armazenamento removíveis apenas mediante prévia autorização.

8 — Proibição da utilização do correio eletrónico da organização para fins pessoais.

9 — Proibição da modificação de qualquer programa, incluindo a tentativa.

10 — Proibição do acesso a áreas para as quais não tenham sido especificamente autorizados, incluindo a tentativa.

11 — Proibição do uso, acesso e/ou modificação não autorizada a equipamentos informáticos, programas e dados.

Artigo 36.º

Em Caso de Violação de Segurança de Dados Pessoais

1 — Implementação de medidas para deteção, identificação e investigação das circunstâncias.

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 elevado risco.

Artigo 37.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, emails e anexos recebidos de fontes externas e internas.

Artigo 38.º

Identificação e Prevenção de Incidentes de Segurança pelos Utilizadores

1 — Informação imediata ao responsável pela segurança, sempre que for detetado código malicioso.

2 — Comunicação imediata de qualquer alerta do sistema antivírus.

3 — Parar imediatamente qualquer processamento em curso, desconectar o sistema potencialmente infetado da rede e identificar o responsável pela segurança em caso de suspeita.

4 — Entende-se como responsável pela segurança Paulo Leonardo.

Artigo 39.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 através de um formulário próprio, devidamente preenchido e assinado, presente no anexo I-F.

3 — A aprovação concedida para a criação referida no n.º 2 do presente artigo irá despoletar geração de uma nova conta individual para o utilizador e uma palavra -passe inicial que lhe irão permitir aceder às funções do sistema para as quais foi autorizado.

Aviso n.º 3647/2025/2

4 — Não são permitidas contas compartilhadas.

5 — As credenciais de autenticação de cada utilizador devem ser únicas e intransmissíveis.

6 — A palavra-passe de autenticação deve ser alterada, no máximo, a cada 180 dias para perfis de utilizador ou quando for comprometida ou se suspeite que venha a ser comprometida.

7 — A reutilização de palavras-passe anteriores deverá ser evitada, recomendando-se que não seja igual ou semelhante às últimas vinte e quatro palavras-passe utilizadas.

8 — Cada utilizador deve possuir somente os privilégios necessários para realizar a sua função na organização.

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.

10 — A listagem referida no n.º 9 do presente artigo deve ser disponibilizada ao encarregado de proteção de dados, sempre que este assim o solicite, para controlo interno e verificação de conformidade.

Artigo 40.º

Controlo das Contas dos Utilizadores

1 — As contas dos utilizadores são bloqueadas, automaticamente, após três tentativas não sucedidas.

2 — Ocorrerá um bloqueio manual quando houver a suspeita de que a conta está a ser usada incorretamente.

3 — As contas desnecessárias devem ser bloqueadas.

4 — O encarregado de proteção de dados deve ser avisado das situações de bloqueio de contas de forma periódica, no início de cada mês, aviso referente ao mês imediatamente anterior, ou no início de cada mês, de forma intervalada, aviso referente aos dois meses imediatamente anteriores, sempre que se verifiquem estas situações.

5 — O bloqueio da estação de trabalho (Windows+L) deve ser ativado por cada utilizador, em caso de ausência do local de trabalho, sendo apenas desbloqueado com recurso às credenciais de acesso.

6 — No final de cada ciclo de trabalho, a respetiva sessão deve ser encerrada.

Artigo 41.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 do sistema, que permitam a reconstrução do histórico de eventos: quem, onde, quando e ação efetuada sobre o dado pessoal.

3 — Os registos devem abranger qualquer atividade de criação, leitura, alteração, pesquisa, consulta, transmissão de dados a terceiros ou eliminação de dados pessoais, incluindo o registo temporal da ação e o respetivo resultado.

Artigo 42.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 eventos, tanto eventos bem-sucedidos como falhados.

Aviso n.º 3647/2025/2

2 — Os acessos aos registos de atividade dos utilizadores devem ser limitados a pessoas devidamente autorizadas e para os fins legalmente previstos, nomeadamente auditorias.

Artigo 43.º

Controlo dos Sistemas em Produção

1 — As configurações dos sistemas em produção devem estar em conformidade com as regras de segurança para que possam ser aprovadas.

2 — As alterações ao sistema em produção devem ser, logo que possível, comunicadas ao encarregado de proteção de dados, por meio de relatórios.

Artigo 44.º

Instalação de novo hardware e software

1 — Apenas se procede à instalação de novo *hardware* e/ou *software* e/ou componentes de *hardware* e *software* mediante autorização prévia.

2 — A configuração local de hardware e software do sistema não deve ser alterada sem autorização prévia.

3 — As alterações à configuração local de *hardware* e/ou *software* do sistema devem ser, logo que possível, comunicadas ao encarregado de proteção de dados.

4 — Os equipamentos devem ser instalados e protegidos de modo a se reduzir os riscos de ameaças, os perigos ambientais e as oportunidades para acesso não autorizado.

Artigo 45.º

Cópias de Segurança

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.

Artigo 46.º

Computação em Nuvem *(Cloud)*

1 — Determinar os requisitos técnicos (flexível e escalável) e definir 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 de serviço.

3 — As políticas de segurança definidas devem ter em conta que 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 provedor de serviço.

4 — Os centros de dados devem ficar alojados em instalações com as condições de segurança adequadas à proteção dos dados pessoais e serviços contratados.

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.

Aviso n.º 3647/2025/2

6 — Apresentar tecnologias de 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 47.º

Proteção dos Suportes de Dados

1 — A Câmara Municipal da Praia da Vitória disponibiliza os seus próprios suportes de dados eletrónicos.

2 — A utilização dos suportes de dados removíveis deve ser gerida em todas as suas fases, incluindo a aquisição, distribuição, utilização e destruição.

3 — Antes da eliminação ou reutilização de equipamentos que contenham suportes de dados deve verificar-se se todos os dados foram efetivamente removidos ou eliminados.

4 — No caso do suporte de dados em papel, a impressão e/ou cópia de documentos contendo dados pessoais deve ser limitada ao estritamente necessário.

5 — A reprodução dos documentos deve ser efetuada com recurso a um sistema de impressão segura, as máquinas fotocopiadoras pressupõem a autenticação do utilizador.

6 — Os utilizadores devem garantir que nenhuma impressão e/ou cópia fica esquecida na impressora/fotocopiadora.

Artigo 48.º

Eliminação dos Suportes de Dados

1 — Os suportes de dados devem ser eliminados de forma segura.

2 — Devem ser eliminados 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 — No caso de dados pessoais sensíveis, a destruição do suporte de dados (eletrónicos e em papel) deve ser testemunhada presencialmente pelo encarregado de proteção de dados.

6 — A destruição de suportes de dados contendo dados pessoais sensíveis deve ser acompanhada da elaboração de certificados de destruição, que devem ser conservados por um período mínimo de 5 anos.

Artigo 49.º

Interrupções no Fornecimento de Energia Elétrica

1 — Os equipamentos, nomeadamente os componentes críticos do sistema, devem ser protegidos contra eventuais interrupções no fornecimento de energia elétrica.

2 — Deve ser assegurada a continuação do fornecimento de energia elétrica adequada a todos os componentes críticos do sistema.

3 — A redundância energética permite o fornecimento da energia elétrica aos componentes críticos, com base nos respetivos requisitos de disponibilidade.

Aviso n.º 3647/2025/2

Artigo 50.º

Segurança Física

1 — Aplicação de medidas físicas, técnicas e procedimentais de proteção para impedir o acesso não autorizado a informação considerada sensível, incluindo dados pessoais.

2 — Garantir que as ações sobre a informação sensível são efetuadas por pessoas autorizadas, responsáveis e que têm necessidade de conhecer.

3 — Assegurar que os dados pessoais são manuseados e armazenados de forma adequada.

4 — Assegurar que as medidas definidas negam ou dificultam a entrada fraudulenta ou forçada de pessoas não autorizadas.

5 — Assegurar que as medidas definidas segregam o acesso aos dados pessoais com base na necessidade de conhecer.

6 — Assegurar que as medidas definidas dissuadem, impedem e detetam ações não autorizadas.

7 — Assegurar que as medidas definidas permitem detetar e reagir rapidamente a eventuais quebras de segurança.

8 — A exigência das medidas deve ser proporcional ao risco identificado.

Artigo 51.º

Responsabilidades na Segurança Física

Para se obter um grau satisfatório de segurança é necessário que todos conheçam as suas responsabilidades e saibam agir em conformidade, devendo ser elaboradas instruções claras, podendo ser produzidos procedimentos específicos para cada um dos diferentes grupos de utilizadores: Serviços de Segurança; Utilizadores; Visitantes; Pessoal de Manutenção e Limpeza.

Artigo 52.º

Segurança em Relação a Pessoas

1 — Devem ser estabelecidos perímetros visivelmente definidos e protegidos (barreiras físicas).

2 — Sempre que possível, controlar todas as entradas e saídas de pessoas e de veículos de forma visual (efetuado por agente de segurança ou rececionista), eletrónico, eletromecânico e/ou físico.

3 — Acesso é concedido apenas a pessoas devidamente habilitadas e especificamente autorizadas.

4 — As autorizações de acesso devem ser concedidas a pessoas especificamente autorizadas com base no princípio da necessidade de conhecer.

5 — Pessoas não autorizadas e que necessitem aceder às áreas seguras devem:

a) Solicitar previamente uma autorização específica e justificar esta necessidade;

b) Ser identificadas à entrada;

c) Ser sujeitas a uma verificação de segurança;

d) Ser acompanhadas durante toda a sua permanência nas referidas áreas.

Aviso n.º 3647/2025/2

Artigo 53.º

Segurança para Instalações

1 — Deve existir iluminação exterior ao longo de todo o perímetro.

2 — As portas de acesso devem dispor de um sistema de controlo de acessos mecânico e de um sistema lógico, não combinados necessariamente.

Artigo 54.º

Segurança Documental

1 — No interior das áreas seguras devem existir cofres e armários apropriados (fechados com chave, fechadura de segredo ou tranca com cadeado), desejavelmente à prova de fogo, para guardar os dados pessoais mais críticos.

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 envelope duplo selado.

4 — Os envelopes que contêm as combinações de segredo devem também ser sujeitos a uma proteção adequada.

5 — As combinações de segredo deverão ser conhecidas pelo número mais restrito possível de pessoas.

6 — 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.

7 — Devem ser mantidos registos escritos das alterações das combinações de segredo.

8 — Os documentos em papel que contêm dados pessoais, principalmente aqueles localizados em espaços físicos acessíveis aos munícipes e a entidades externas, devem estar devidamente acautelados, não possibilitando a sua visualização.

Artigo 55.º

Segurança Eletrónica

1 — 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, principalmente nos casos em que se tratem de dados pessoais críticos.

3 — Nas ligações entre equipamentos localizadas no interior da mesma área segura, bem como nas ligações entre diferentes áreas seguras dentro do mesmo edifício, deve utilizar-se, preferencialmente, fibra ótica.

4 — Não sendo possível a utilização de fibra ótica, recomenda-se uma separação entre a cablagem das redes e sistemas de informação que processam dados pessoais e a restante cablagem (energia e dados).

Aviso n.º 3647/2025/2

5 — Dentro das áreas seguras apenas devem existir linhas de comunicação e dispositivos eletrónicos autorizados.

CAPÍTULO IV

Disposições Finais

Artigo 56.º

Obrigações Gerais

1 — A Câmara Municipal da Praia da Vitória, os seus serviços e os seus funcionários e colaboradores estão legalmente obrigados a cumprir o disposto no RGPD, na Lei n.º 58/2019, de 8 de agosto, no RMPD da Câmara Municipal da Praia da Vitória e nas demais disposições legais em vigor; recorrendo ainda às orientações da Comissão Nacional de Proteção de Dados.

2 — Devem os funcionários e os colaboradores da Câmara Municipal da Praia da Vitória notificar o respetivo superior hierárquico aquando da deteção de violação e/ou suspeita de violação de dados pessoais, sob pena de sanção prevista nas disposições legais em vigor.

3 — Devem os serviços municipais prestar as informações necessárias e auxiliar o encarregado de proteção de dados no âmbito e na prossecução das suas funções.

4 — A assinatura de requerimentos ou outros documentos, sempre que efetuada perante funcionário da Câmara Municipal da Praia da Vitória, deve ser acompanhada da conferência da identidade com o cartão de cidadão respeitando as normas de utilização deste documento, nos termos da Lei n.º 7/2007, de 5 de fevereiro, e sucessivas atualizações, pela Lei n.º 91/2015, de 12 de agosto, e pela Lei n.º 32/2017, de 1 de junho.

5 — Sempre que seja necessária a conferência da identidade, devem os serviços recorrer a uma de três opções:

a) Exibição do cartão de cidadão para conferência de identidade;

b) Reprodução com o consentimento do titular, que deverá ficar documentado;

c) Reprodução que esteja legalmente prevista.

6 — Sempre que se inicie um procedimento de tratamento de dados, devem obrigatoriamente os serviços municipais, na pessoa dos respetivos funcionários, notificar os titulares dos dados, no que ao RGPD, à Lei n.º 58/2019, de 8 de agosto e ao RMPD diz respeito.

7 — A cláusula presente no Anexo II -A, relativamente à proteção de dados, deve estar presente em todos os formulários e/ou requerimentos dos diversos procedimentos e nos contratos a celebrar pela Câmara Municipal da Praia da Vitória, com exceção dos procedimentos e contratos respeitantes aos serviços municipais referidos no n.º 8 do presente artigo.

8 — Em substituição da cláusula referida no n.º 7 do presente artigo, os serviços municipais concretamente referidos no Capítulo IV do presente Regulamento utilizam cláusulas específicas, referenciadas nos respetivos artigos.

9 — Aquando da criação de novos formulários e/ou requerimentos, deve o encarregado de proteção de dados da Câmara Municipal da Praia da Vitória ser notificado de tal situação.

Artigo 57.º

Legislação subsidiária

A tudo o que não esteja especialmente previsto no presente Regulamento 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 que sejam aplicáveis em razão da matéria.

Aviso n.º 3647/2025/2

Artigo 58.º

Interpretação e casos omissos

1 — As lacunas, as dúvidas interpretativas e os casos omissos suscitados na aplicação do presente Regulamento são preenchidos ou resolvidos, na linha do seu espírito, mediante despacho fundamentado do Presidente da Câmara Municipal da Praia da Vitória.

2 — As menções referentes aos serviços municipais, nomeadamente departamentos, divisões, unidades orgânicas e gabinetes, constantes do presente Regulamento reportam-se, em caso de alteração da estrutura orgânica da Câmara Municipal da Praia da Vitória, àquelas que as sucederem nas respetivas funções.

Artigo 59.º

Entrada em vigor

O presente Regulamento entra em vigor 5 dias após a sua publicação na 2.ª série do *Diário da República*.

ANEXO I

Procedimentos de Notificação e Comunicação

ANEXO I-A

Requerimento para o Exercício de Direito pelos Titulares de Dados Pessoais

Exmo. Sr.
Presidente da Câmara Municipal da Praia da Vitória

Titular dos dados:
Nome:
_____
_____
Morada:
_____
_____
E-mail:
_____
_____
Telemóvel n.º: _____
Documento de identificação: _____
Nº de documento de identificação: _____
Validade de documento de identificação: _____

Representante do titular dos dados (a ser aplicável):
Nome:
_____
_____
Morada:
_____
_____
Email:
_____
_____
Telemóvel n.º: _____
Documento de identificação: _____
Nº de documento de identificação: _____
Validade de documento de identificação: _____
Na qualidade de: _____

Vem, relativamente aos dados pessoais que são objeto de tratamento pela Câmara Municipal da Praia da Vitória, nos seguintes assuntos *(indique qual o assunto, o número do processo e o que pretende)*:
Assunto:
_____
Nº do Registo:
_____
Pretensão:
_____

Direitos que pode exercer (assinalar):
☐ Confirmação de que os dados pessoais são objeto de tratamento.
☐ Direito de acesso aos dados pessoais.
☐ Direito de retificação.
☐ Direito à limitação do tratamento.
☐ Direito ao apagamento dos dados ("direito a ser esquecido").
☐ Direito de portabilidade dos dados.
☐ Direito de oposição.

Informações e direitos sobre o tratamento de dados pessoais neste procedimento:
Responsável pelo tratamento dos dados: Câmara Municipal da Praia da Vitória, sita na Praça Francisco Ornelas da Câmara, 9760-851 Praia da Vitória, contactável através do website: https://www.cmpv.pt/ ou email: geral@cmpv.pt ou telefone: +351 295 540 200 ou presencialmente no nosso horário de atendimento.

Aviso n.º 3647/2025/2

Encarregado de proteção de dados: Encarregado de Proteção de Dados da Câmara Municipal da Praia da Vitória, sita na Praça Francisco Ornelas da Câmara, 9760-851 Praia da Vitória, contactável através do email: epd@cmpv.pt ou telefone: +351 295 540 200 ou presencialmente na morada indicada.
Finalidade do tratamento: O exercício pelo titular dos dados dos direitos e pelo responsável do tratamento das obrigações previstas na legislação de proteção de dados pessoais.

Licitude do tratamento: Cumprimento pela Câmara das suas obrigações legais, e das suas funções de interesse público e autoridade pública enquanto órgão da Administração Pública.
Dados pessoais e categorias: Os dados pessoais dos titulares e legais representantes constantes deste requerimento, não envolvendo a recolha de dados de categorias especiais.
Destinatários dos dados pessoais: Os serviços municipais.
Prazo de conservação dos dados pessoais: o prazo necessário para a tramitação do procedimento acrescido do prazo legal de arquivo dos documentos onde os dados estão registados conforme estabelecido no Regulamento Arquivístico para as Autarquias locais.
Direitos que pode exercer: Confirmação de que os dados pessoais são objeto de tratamento, Direito de acesso aos dados pessoais, Direito de retificação, Direito à limitação do tratamento, Direito ao apagamento dos dados, Direito de oposição e Direito de apresentar reclamação à autoridade de controlo (CNPD).
Outras informações: A comunicação dos dados pessoais neste procedimento é necessária para cumprir uma obrigação legal ou contratual, caso não forneça os dados o seu pedido ou pretensão não poderá ser tratado pela Câmara Municipal. Não existem decisões automatizadas, nem a definição de perfis. Para além do cumprimento da obrigação legal de tratamento para arquivo, não haverá tratamento posterior dos dados pessoais para finalidade distinta das que presidiram à recolha. Qualquer violação de dados pessoais será levada a conhecimento do interessado no prazo legal.

Como pretende apresentar este pedido (assinale e cumpra as indicações):
☐ Verbalmente – Este requerimento deverá ser preenchido pelos serviços municipais de acordo com as informações e pedido do titular dos dados que deverá exibir o documento de identificação e assinar o requerimento.
☐ Em papel – Este requerimento deverá ser preenchido e assinado pelo titular dos dados que no momento da entrega nos serviços municipais deverá exibir o documento de identificação para conferência da assinatura.
☐ Eletronicamente – Este requerimento deverá ser preenchido e convertido em PDF e assinado mediante assinatura eletrónica qualificada do Cartão de Cidadão pelo titular dos dados e remetido através do email indicado.

Como pretende que seja prestada a informação (assinale e cumpra as indicações):
☐ Verbalmente – O requerente deverá dirigir-se aos serviços municipais fazendo-se acompanhar do documento de identificação ou outro documento que ateste a representação, onde serão prestadas as informações de acordo com o seu pedido devendo assinar um documento que comprove que as informações foram prestadas.
☐ Papel presencialmente – O requerente deverá dirigir-se aos serviços municipais fazendo-se acompanhar do documento de identificação ou outro documento que ateste a representação, onde será entregue documento com as informações de acordo com o seu pedido, devendo assinar um duplicado desse documento para comprovar que as informações foram prestadas.
☐ Pelos correios – O requerente receberá na morada indicada documento com as informações de acordo com o seu pedido.
☐ Eletronicamente – O requerente receberá no email indicado o documento com as informações de acordo com o seu pedido.

Pede deferimento,
Praia da Vitória, _____ de _____ de 20____
O(A) Requerente,

(Assinatura conforme documento de identificação verificada por conferência)

Aviso n.º 3647/2025/2

ANEXO I-B

Resposta ao Requerimento de Exercício de direitos dos Titulares

Exmo.(a). Sr.(a)
Nome:
_____
_____
Morada:
_____
_____

Enquanto titular ou representante do titular dos dados pessoais, prestamos informações sobre o exercício dos seguintes direitos:
Confirmação de que os dados pessoais são objeto de tratamento:
☐ SIM ou ☐ NÃO
Se SIM, no exercício do direito de acesso aos dados pessoais, prestamos as seguintes informações:
Dados pessoais em tratamento:
_____
Finalidades do tratamento dos dados:
_____
Destinatários ou categorias de destinatários de dados pessoais:
_____
_____
Prazo previsto para conservação dos dados pessoais ou critérios usados para fixar esse prazo: o prazo necessário para a tramitação do procedimento acrescido do prazo legal de arquivo dos documentos onde os dados estão registados conforme estabelecido no Regulamento Arquivístico para as Autarquias Locais.

Os dados foram recolhidos junto do titular:
☐ SIM ou ☐ NÃO
Se NÃO, foram cedidos à Câmara Municipal da Praia da Vitória por:
_____
_____

Existem decisões automatizadas:
☐ SIM ou ☐ NÃO
Se SIM, prestamos informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados:
_____
_____

Existe a definição de perfis:
☐ SIM ou ☐ NÃO
Se SIM, prestamos informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados:
_____
_____

Tem o direito de solicitar ao responsável pelo tratamento, a retificação, o apagamento ou a limitação do tratamento dos dados pessoais ou o direito de se opor a esse tratamento nos termos previstos na lei.
Tem ainda o direito de apresentar reclamação à autoridade de controlo (CNPD).
Segue em anexo uma cópia dos dados pessoais em fase de tratamento.

Direito de retificação:
☐ SIM ou ☐ NÃO
Se SIM, foram retificados os seguintes dados:
_____
_____

Se NÃO, os fundamentos foram os seguintes:
_____
_____

Aviso n.º 3647/2025/2

Direito à limitação do tratamento:
☐ SIM ou ☐ NÃO
Se SIM, os fundamentos foram os seguintes:
_____
_____

Se NÃO, os fundamentos foram os seguintes:
_____
_____

Comunicação aos destinatários da retificação ou apagamento ou limitação do tratamento dos dados pessoais:
☐ SIM ou ☐ NÃO

Se SIM, quais os destinatários:
_____
_____

Praia da Vitória, _____ de _____ de 20____

O(A) Funcionário(a),
(Assinatura conforme documento de identificação)

ANEXO I-C

Informação sobre o Tratamento de Dados e Direitos dos Titulares

Responsável pelo tratamento dos dados: Câmara Municipal da Praia da Vitória, sita na Praça Francisco Ornelas da Câmara, 9760-851 Praia da Vitória, contactável através do website: https://www.cmpv.pt/ ou email: geral@cmpv.pt ou telefone: +351 295 540 200 ou presencialmente no nosso horário de atendimento.
Encarregado de proteção de dados: Encarregado de Proteção de Dados da Câmara Municipal da Praia da Vitória, sita na Praça Francisco Ornelas da Câmara, 9760-851 Praia da Vitória, contactável através do email: epd@cmpv.pt ou telefone: +351 295 540 200 ou presencialmente na morada indicada.
Finalidade do tratamento: 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. O exercício pelo titular dos dados ou pelo responsável pelo tratamento de direitos e ou obrigações previstas em legislação.
Licitude do tratamento: Cumprimento pela Câmara das suas obrigações legais, e das suas funções de interesse público e autoridade pública enquanto órgão da Administração Pública.
Dados pessoais e categorias: Os dados pessoais dos titulares e legais representantes constantes deste requerimento, não envolvendo a recolha de dados de categorias especiais.
Destinatários dos dados pessoais: Os serviços municipais.
Prazo de conservação dos dados pessoais: O prazo necessário para a tramitação do procedimento acrescido do prazo legal de arquivo dos documentos onde os dados estão registados conforme estabelecido no Regulamento Arquivístico para as Autarquias Locais.
Direitos que pode exercer: Confirmação de que os dados pessoais são objeto de tratamento, Direito de acesso aos dados pessoais, Direito de retificação, Direito à limitação do tratamento, Direito ao apagamento dos dados, Direito de oposição e Direito de apresentar reclamação à autoridade de controlo (CNPD).
Outras informações: A comunicação dos dados pessoais neste procedimento é necessária para cumprir uma obrigação legal ou contratual, caso não forneça os dados o seu pedido ou pretensão não poderá ser tratado pela Câmara Municipal. Não existem decisões automatizadas, nem a definição de perfis. Para além do cumprimento da obrigação legal de tratamento para arquivo, não haverá tratamento posterior dos dados pessoais para finalidade distinta das que presidiram à recolha. Qualquer violação de dados pessoais será levada a conhecimento do interessado no prazo legal.

Tomei conhecimento,
Praia da Vitória, _____ de _____ de 20____

O(A) Requerente,
(Assinatura conforme documento de identificação verificada por conferência)

ANEXO I-D

Formulário de Comunicação da Violação de Dados Pessoais à Autoridade de Controlo (CNPD)

O formulário de comunicação da violação de dados pessoais à autoridade de controlo é preenchido no *website* da Comissão Nacional de Proteção de Dados, através do *link:* https://www.cnpd.pt/DataBreach/

Este formulário é submetido pelo encarregado de proteção de dados da Câmara Municipal da Praia da Vitória, em representação da mesma.

Aviso n.º 3647/2025/2

Aquando do início do preenchimento do formulário, deve ser selecionada uma de duas opções, consoante a tipologia da pretensão:

— Notificar uma nova violação de dados pessoais

ou

— Alterar uma notificação anteriormente submetida

Caso selecione uma nova violação de dados pessoais, deve o encarregado de proteção de dados preencher os campos presentes nos seguintes separadores:

— Dados da entidade

— Dados de contacto

— Informação sobre a violação de dados

— Consequências da violação de dados

— Dados pessoais envolvidos

— Titulares dos dados

— Informação aos titulares

— Medidas preventivas/corretivas

— Tratamentos transfronteiriços

Caso selecione alterar uma notificação anteriormente submetida, deve o encarregado de proteção de dados indicar a referência da notificação anteriormente submetida (referência presente no documento que foi remetido por *e-mail* aquando da notificação). Depois deve alterar os campos que pretende nos respetivos separadores.

ANEXO I-E

Formulário de Comunicação da Violação de Dados Pessoais aos Singulares

Exmo.(a). Sr.(a)
Nome:
_____
_____
Morada:
_____
_____

Enquanto titular ou representante do titular dos dados pessoais, comunicamos a verificação da seguinte violação da segurança:
(descrever em linguagem clara e simples a natureza da violação dos dados pessoais)
_____
_____

Que provocou a:
□ Destruição
□ Perda
□ Alteração
□ Divulgação
□ Acesso, não autorizados

Dos seus dados pessoais:
(descrever)
_____
_____

Que estavam na nossa posse por:
□ Recolha
□ Transmissão
□ Conservação
□ Outro tipo de tratamento:
(descrever o "outro tipo de tratamento")
_____

De modo:
□ Acidental ou □ ilícito

Que é suscetível de implicar um elevado risco para os seus direitos e liberdades. As consequências prováveis da violação de dados pessoais são:
(descrever)
_____
_____

As medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos são:
(descrever)
_____
_____
Poderá contactar o Encarregado de Proteção de Dados da Câmara Municipal da Praia da Vitória através do e-mail: epd@cmpv.pt para obter mais informações.

Praia da Vitória, _____ de _____ de 20____

O(A) Funcionário(a),

(Assinatura conforme documento de identificação)

Aviso n.º 3647/2025/2

ANEXO I-F

Criação ou Modificação de Conta de Utilizador

CRIAÇÃO
Nome do utilizador:
Serviço ao qual está afeto:
Software a utilizar:
Nível de permissão (discriminado por tipo de software):

MODIFICAÇÃO
Nome do utilizador:
Serviço ao qual está afeto:
Nível de permissão a modificar:
Adicionar software a utilizar:

Praia da Vitória, _____ de _____ de 20____

O(A) Funcionário(a),
(Assinatura conforme documento de identificação)

ANEXO II

Minutas e cláusulas

ANEXO II-A

Cláusula genérica

Responsável pelo tratamento dos dados: Câmara Municipal da Praia da Vitória, sita na Praça Francisco Ornelas da Câmara, 9760-851 Praia da Vitória, contactável através do *website:* https://www.cmpv.pt/ ou *e-mail*: geral@cmpv.pt ou telefone: +351 295 540 200 ou presencialmente no nosso horário de atendimento.

Encarregado de proteção de dados: Encarregado de Proteção de Dados da Câmara Municipal da Praia da Vitória, sita na Praça Francisco Ornelas da Câmara, 9760-851 Praia da Vitória, contactável através do *e-mail:* epd@cmpv.pt ou telefone: +351 295 540 200 ou presencialmente na morada indicada.

Finalidade do tratamento dos dados: 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. O exercício pelo titular dos dados ou pelo responsável pelo tratamento de direitos e ou obrigações previstas em legislação.

Licitude do tratamento: Cumprimento pela Câmara Municipal da Praia da Vitória das suas obrigações legais, e das suas funções de interesse público e autoridade pública enquanto órgão da Administração Pública.

Dados pessoais e categorias: Os dados pessoais dos titulares e legais representantes constantes deste requerimento, não envolvendo a recolha de dados de categorias especiais.

Destinatários dos dados pessoais: Os serviços municipais.

Prazo de conservação dos dados pessoais: O prazo necessário para a tramitação do procedimento acrescido do prazo legal de arquivo dos documentos onde os dados estão registados conforme estabelecido no Regulamento Arquivístico para as Autarquias Locais.

Aviso n.º 3647/2025/2

Direitos que pode exercer: Confirmação de que os dados pessoais são objeto de tratamento, Direito de acesso aos dados pessoais, Direito de retificação, Direito à limitação do tratamento, Direito ao apagamento dos dados, Direito de oposição e Direito de apresentar reclamação à autoridade de controlo (CNPD).

Outras informações: A comunicação dos dados pessoais neste procedimento é necessária para cumprir uma obrigação legal ou contratual, caso não forneça os dados o seu pedido ou pretensão não poderá ser tratado pela Câmara Municipal. Não existem decisões automatizadas, nem a definição de perfis. Para além do cumprimento da obrigação legal de tratamento para arquivo, não haverá tratamento posterior dos dados pessoais para finalidade distinta das que presidiram à recolha. Qualquer violação de dados pessoais será levada a conhecimento do interessado no prazo legal.

ANEXO II-B

Cláusula compras

Proteção de Dados Pessoais pela Entidade Adjudicante

Titular dos dados: O(s) adjudicatário(s), seus legais representantes e ou trabalhadores são os titulares dos dados pessoais.

Responsável pelo tratamento: A entidade adjudicante é o responsável pelo tratamento e destinatário dos dados pessoais.

Encarregado de proteção de dados: A entidade adjudicante designou um encarregado de proteção de dados que poderá ser contactado pelos titulares dos dados para esclarecimento de dúvidas e exercício de direitos sobre o tratamento dos seus dados pessoais.

Finalidades do tratamento dos dados: A entidade adjudicante vai tratar os dados pessoais para a tramitação nos serviços municipais, por exigência legal, de procedimentos administrativos, celebração e execução de contratos de contratação pública. O cumprimento das suas atribuições ou obrigações legais e das suas funções de interesse público ou autoridade pública, enquanto órgão da Administração Pública. E para exercício pelo titular dos dados ou pelo responsável pelo tratamento de direito e ou obrigações previstas na legislação.

Licitude do tratamento: O tratamento dos dados pessoais é necessário para execução de contrato no qual o titular dos dados é parte ou diligências pré-contratuais a pedido do titular dos dados. Para cumprimento de obrigações jurídicas a que a entidade adjudicante se encontra sujeita. E ainda necessário para o exercício de funções de interesse público e exercício de autoridade pública em que está investida a entidade adjudicante, enquanto órgão da Administração Pública.

Dados pessoais: De acordo com o princípio da minimização dos dados a entidade adjudicante efetua o tratamento dos dados pessoais que sejam adequados, pertinentes, necessários e previstos na legislação aplicável. Os dados pessoais recolhidos constam de requerimentos, contratos ou documentos anexos e procedimentos administrativos, podendo incluir: nome, data de nascimento, nacionalidade, morada, localidade, código postal, número do documento de identificação, data de emissão, número de identificação fiscal, número de inscrição na segurança social, telefone, telemóvel, endereço eletrónico, as habilitações académicas, experiência profissional, habilitações para condução de veículos ou máquinas.

Transmissão dos dados pessoais: A entidade adjudicante fará a transmissão para outras entidades dos dados pessoais se e quando prevista em disposição legal e/ou para cumprimento de direitos ou obrigações legalmente previstas e ou se absolutamente necessária à prossecução do interesse público ou exercício de autoridade pública. Ocorrerá designadamente para instituições financeiras ou entidades bancárias para pagamento de valores estipulados nos contratos. Para outras entidades de que são exemplo, a Administração Tributária, o Tribunal de Contas, ou outras entidades nos termos previstos na legislação.

Aviso n.º 3647/2025/2

Prazo de conservação dos dados pessoais: Pelo prazo necessário para a tramitação do procedimento, ou duração e execução do contrato, acrescido do prazo legal de arquivo dos documentos onde os dados estão registados conforme estabelecido no Regulamento Arquivístico para as Autarquias Locais.

Direitos dos titulares dos dados: Confirmação de que os dados pessoais são objeto de tratamento, Direito de acesso aos dados pessoais, Direito de retificação, Direito à limitação do tratamento, Direito ao apagamento dos dados, Direito de oposição e Direito de apresentar reclamação à autoridade de controlo (CNPD).

Outras informações: A comunicação dos dados pessoais é necessária para cumprimento de obrigação legal ou contratual. Caso não sejam fornecidos os dados o pedido ou pretensão não poderá ser tratado, nem poderá celebrar contratos. Não existem decisões automatizadas, nem a definição de perfis. Para além do cumprimento da obrigação legal de tratamento para arquivo, não haverá tratamento posterior dos dados pessoais para finalidades distintas das que presidiram à recolha. Qualquer violação de dados pessoais será levada a conhecimento do titular no prazo legal.

Proteção de Dados Pessoais pelo Adjudicatário ou Subcontratante

Se o adjudicatário (aqui também designado por subcontratante) tiver contacto ou conhecimento de dados pessoais que estão sob a responsabilidade da entidade adjudicante (aqui também designada por responsável pelo tratamento) ou efetuar o tratamento de dados pessoais por conta da entidade adjudicante (responsável pelo tratamento) fica obrigado ao cumprimento das seguintes regras:

a) Efetuará o tratamento desses dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito, informando nesse caso o responsável pelo tratamento desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público;

b) Assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;

c) Adota todas as medidas de segurança do tratamento de dados pessoais exigidas nos termos do artigo 32.º do RGPD;

d) Respeita as condições a que se referem os n.os 2 e 4 do artigo 28.º do RGPD para contratar outro subcontratante;

e) Toma em conta a natureza do tratamento, e na medida do possível, presta assistência ao responsável pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos previstos no capítulo III do RGPD;

f) Presta assistência ao responsável pelo tratamento no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32.º a 36.º do RGPD, tendo em conta a natureza do tratamento e a informação ao dispor do subcontratante;

g) Consoante a escolha do responsável pelo tratamento, apaga ou devolve-lhe todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo da legislação;

h) Disponibiliza ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações aqui previstas e facilita e contribui para as auditorias, inclusive as inspeções, conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado;

i) Informa imediatamente o responsável pelo tratamento se, no seu entender, alguma instrução deste violar o RGPD ou outras disposições legais em matéria de proteção de dados;

j) Se o subcontratante contratar outro subcontratante para a realização de operações específicas de tratamento de dados por conta do responsável pelo tratamento, são impostas a esse outro subcontratante, por contrato, as mesmas obrigações em matéria de proteção de dados que as estabelecidas neste contrato, em particular a obrigação de apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento seja conforme com os requisitos do RGPD. Se esse outro subcontratante não cumprir as suas obrigações em matéria de proteção de dados, o aqui subcontratante continua a ser plenamente responsável, perante o responsável pelo tratamento, pelo cumprimento das obrigações desse outro subcontratante;

k) O subcontratante que, em violação deste contrato ou do RGPD, determinar as finalidades e os meios de tratamento, é considerado responsável pelo tratamento no que respeita ao tratamento em questão;

l) O adjudicatário garante que implementou procedimentos internos e medidas técnicas e organizativas adequadas a efetuar o tratamento de dados pessoais e a proteger os direitos dos titulares de dados pessoais de acordo com as condições estabelecidas na legislação em vigor, designadamente, no Regulamento Geral de Proteção de Dados;

m) O adjudicatário obriga-se a durante a vigência do contrato e após a sua cessação a manter confidenciais os dados pessoais de que tenha tomado contacto ou conhecimento ou que lhe tenham sido transmitidos pela entidade adjudicante;

n) O adjudicatário compromete-se, designadamente, a não copiar, reproduzir, adaptar, modificar, alterar, apagar, destruir, difundir, transmitir, divulgar ou por qualquer outra forma colocar à disposição de terceiros os dados pessoais a que tenha acesso ou que lhe sejam transmitidos pela entidade adjudicante ao abrigo do contrato, sem que para tal tenha sido expressamente instruído, por escrito, pela entidade adjudicante;

o) O adjudicatário será responsável por qualquer prejuízo em que a entidade adjudicante venha a incorrer em consequência do tratamento, por parte do mesmo e/ou dos seus colaboradores, de dados pessoais em violação das normas legais aplicáveis e/ou do disposto no contrato;

p) Para efeitos do disposto na alínea (o) entende-se por "colaborador" toda e qualquer pessoa singular ou coletiva que preste serviços ao adjudicatário, incluindo, designadamente, representantes legais, trabalhadores, prestadores de serviços, procuradores e consultores, independentemente da natureza e validade do vínculo jurídico estabelecido entre o adjudicatário e o referido colaborador;

q) O adjudicatário enquanto subcontratante, que tenha 250 ou mais trabalhadores, ou que faça tratamento de dados suscetível de implicar risco para os direitos e liberdades dos titulares, ou que faça tratamentos de dados que não sejam ocasionais, ou que abranja categorias especiais de dados pessoais ou dados pessoais relativos a condenações penais e outras infrações tem de conservar um registo de todas as categorias de atividades de tratamento realizadas em nome da entidade adjudicante enquanto responsável pelo tratamento, do qual consta:

— O nome e contactos do subcontratante e do responsável pelo tratamento em nome do qual o subcontratante atua, bem como, sendo caso disso do representante do responsável pelo tratamento ou do subcontratante e do encarregado de proteção de dados;

— As categorias de tratamentos de dados pessoais efetuados em nome do responsável pelo tratamento;

— Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 49.º, n.º 1, segundo parágrafo, a documentação que comprove a existência das garantias adequadas;

— Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32.º, n.º 1 do RGPD.

Aviso n.º 3647/2025/2

ANEXO II-C

Cláusula recursos humanos

Proteção de Dados Pessoais

Titular dos dados: O Segundo Outorgante é o titular dos dados pessoais.

Responsável pelo tratamento: O Primeiro Outorgante é o responsável pelo tratamento e destinatário dos dados pessoais do Segundo Outorgante.

Encarregado de proteção de dados: O Primeiro Outorgante designou um encarregado de proteção de dados que poderá ser contactado pelo Segundo Outorgante para esclarecimento de dúvidas e exercício de direitos sobre o tratamento de dados pessoais.

Finalidades do tratamento dos dados: O Primeiro Outorgante pode efetuar o tratamento de dados pessoais de categorias especiais do Segundo Outorgante, incluindo dados biométricos, estado de saúde ou incapacidades para o trabalho e filiação sindical para o cumprimento de legislação laboral, de segurança social, proteção social, medicina preventiva ou do trabalho, avaliação da capacidade de trabalho e o diagnóstico médico, neste último caso, por profissionais submetidos a sigilo profissional. O Primeiro Outorgante pode ainda tratar outros dados pessoais do Segundo Outorgante necessários para a celebração e execução de contratos de trabalho e diligências pré-contratuais necessárias à celebração desses contratos, incluindo-se aqui a gestão de recursos humanos, processamento de remunerações, formação profissional, gestão de sanções disciplinares, seleção e recrutamento de trabalhadores e controlo de horário e assiduidade.

Licitude do tratamento: O tratamento pelo Primeiro Outorgante dos dados pessoais de categorias especiais (biométricos, estado de saúde, ou incapacidade para o trabalho e filiação sindical) do Segundo Outorgante é necessário para o cumprimento de legislação laboral, de segurança social, proteção social, e medicina preventiva ou do trabalho, avaliação da capacidade para o trabalho, o diagnóstico médico, neste caso sob responsabilidade de profissional sujeito a obrigação de sigilo profissional ou pessoa sujeita a obrigação de confidencialidade. O tratamento dos demais dados pessoais do Segundo Outorgante é necessário para execução de contrato no qual o titular dos dados é parte ou diligências pré-contratuais a pedido do titular dos dados. Para cumprimento de obrigações jurídicas a que o Segundo Outorgante se encontra sujeito. E ainda necessário para o exercício de funções de interesse público e exercício de autoridade pública em que está investido o Primeiro Outorgante, enquanto responsável pelo tratamento e órgão da Administração Pública.

Dados pessoais: De acordo com o princípio da minimização dos dados, o Primeiro Outorgante efetua o tratamento dos dados pessoais do Segundo Outorgante que sejam adequados, pertinentes, necessários e previstos na legislação aplicável. Os dados pessoais recolhidos constam de requerimentos, contratos ou documentos anexos e procedimentos administrativos podendo incluir: nome, data de nascimento, género, nacionalidade, morada, localidade, código postal, número do documento de identificação, data de emissão, número de identificação fiscal, número de inscrição na segurança social, telefone, telemóvel, endereço eletrónico, as habilitações académicas, situação jurídico-funcional dos trabalhadores, experiência profissional e funções exercidas, categoria ou carreira, constituição de agregado familiar e número de dependentes, capacidade para o exercício da atividade profissional, grau de incapacidade (se aplicável), situação de doença e período de incapacidade próprio ou de familiar, avaliação ou monitorização de desempenho, habilitação para condução de veículos, inscrição em mapas de férias e mapas de pessoal, filiação sindical e impressões digitais.

Transmissão dos dados pessoais: O Primeiro Outorgante fará a transmissão para outras entidades dos dados pessoais do Segundo Outorgante se e quando prevista em disposição legal e ou para cumprimento de direitos ou obrigações legalmente previstas e ou se absolutamente necessária à prossecução do interesse público ou exercício de autoridade pública. Ocorrerá designadamente para instituições financeiras ou entidades bancárias para pagamento de remunerações e outros direitos laborais; Segurança Social ou outras entidades gestoras de Fundos de Pensões ou do Regime de Previdência; Autoridades de controlo das condições de trabalho, Companhias de seguros para celebração

Aviso n.º 3647/2025/2

de seguros de acidentes de trabalho e para Entidades prestadoras de serviços de Segurança, Saúde, Medicina no trabalho e Formação Profissional.

Prazo de conservação dos dados pessoais: O Primeiro Outorgante conservará os dados do Segundo Outorgante pelo prazo necessário para a tramitação do procedimento, ou duração do contrato, acrescido do prazo legal de arquivo dos documentos onde os dados estão registados conforme estabelecido no Regulamento Arquivístico para as Autarquias Locais.

Direitos dos titulares dos dados: O Segundo Outorgante pode exercer perante o Primeiro Outorgante Direitos de confirmação de que os seus dados pessoais são objeto de tratamento, Direito de acesso aos dados pessoais, Direito de Retificação, Direito à limitação do tratamento e Direito de apresentar reclamação à autoridade de controlo (CNPD).

Direitos que não podem ser exercidos e sua justificação: O Segundo Outorgante não pode exercer Direito ao apagamento dos dados ("direito a ser esquecido"), Direito de portabilidade dos dados e Direito de oposição, porque o tratamento se revela necessário: ao cumprimento de uma obrigação legal que exige o tratamento e a que o responsável está sujeito, ao exercício de funções de interesse público e ao exercício da autoridade pública de que esteja investido o Segundo Outorgante.

Outras informações: A comunicação dos dados pessoais pelo Segundo Outorgante ao Primeiro é necessária para cumprimento de obrigação legal ou contratual. Caso o Segundo não forneça os dados o seu pedido ou pretensão não poderá ser tratado, nem poderá celebrar contrato com o Primeiro. Não existem decisões automatizadas, nem a definição de perfis. Para além do cumprimento da obrigação legal de tratamento para arquivo, não haverá tratamento posterior dos dados pessoais para finalidades distintas das que presidiram à recolha. Qualquer violação de dados pessoais será levada a conhecimento do titular no prazo legal.

Confidencialidade ou Sigilo Profissional

a) Ao serviço do Primeiro Outorgante e na execução do contrato de trabalho o Segundo Outorgante pode ter contacto ou acesso a dados pessoais dos titulares de dados que se relacionam com o Primeiro Outorgante;

b) Nos termos da legislação europeia e nacional sobre proteção de dados pessoais o Primeiro Outorgante, enquanto responsável pelo tratamento de dados pessoais, tem obrigação de assegurar que as pessoas autorizadas a tratar dados pessoais o fazem sob sigilo profissional ou confidencialidade;

c) O Segundo Outorgante reconhece a sua obrigação de sigilo profissional ou confidencialidade conforme previsto na legislação aplicável e que decorre ainda do seu dever de lealdade perante o Primeiro Outorgante, obrigando-se a adotar no desempenho das suas funções os procedimentos implementados pelo primeiro outorgante para garantir a proteção de dados pessoais, obrigando-se ainda a não divulgar dados pessoais tratados pelo Primeiro Outorgante, exceto se receber indicações e apenas nas condições indicadas pelo Primeiro Outorgante em cumprimento das suas atribuições legais;

d) Caso o Segundo Outorgante tenha conhecimento direto ou indireto de incidentes de segurança que possam causar a violação de dados pessoais, ou caso esta tenha ocorrido, deve de imediato informar o Primeiro Outorgante de tais factos, contactando o seu superior hierárquico ou o encarregado de proteção de dados designado, devendo também prestar toda a colaboração solicitada;

e) Este dever de sigilo profissional ou confidencialidade mantém-se durante e após a cessação, interrupção e/ou suspensão do contrato de trabalho."

7 de janeiro de 2025. — A Presidente da Câmara Municipal, Vânia Marisa Borges Figueiredo Ferreira.

318536781

Aviso n.º 3647/2025/2