REGULAMENTO MUNICIPAL

Regulamento Interno de Segurança na Utilização de Sistemas de Informação e do Tratamento de Dados Pessoais do Município de Santa Cruz da Graciosa

Introdução

O Regulamento Geral de Proteção de Dados (RGPD) - Regulamento (EU) 2016/679 do Parlamento Europeu, de 27.04.2016, que entrou em vigor em maio de 2016 com aplicação a partir de 25 de maio de 2018, estabelece as regras relativas à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, aplicando-se a todas as entidades que realizem operações que envolvam dados pessoais e à livre circulação desses dados, aplicando-se a todas as entidades que realizem operações que envolvam dados pessoais, incluindo as autarquias locais; e, bem assim, a Lei n.º 58/2019, de 8 de agosto (que pretendeu assegurar a execução, na ordem jurídica nacional, do referido Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016).

Nestes termos, tem-se presente, desde logo, o que se entende por "Dados pessoais" (seguimos de perto, quer o RGPD, quer as referências publicamente disponíveis em ec.europa.eu): são

informações relativas a uma pessoa viva, identificada ou identificável. Também constituem dados pessoais o seu tratamento. Dados pessoais reportam-se ao conjunto de informações distintas que podem levar à identificação de uma determinada pessoa. Dados pessoais que tenham sido descaracterizados, codificados ou pseudonimizados, mas que possam ser utilizados para reidentificar uma pessoa, continuam a ser dados pessoais e são abrangidos pelo âmbito de aplicação do RGPD. Dados pessoais que tenham sido tornados anónimos de modo a que a pessoa não seja ou deixe de ser identificável deixam de ser considerados dados pessoais. Para que os dados sejam verdadeiramente anonimizados, a anonimização tem de ser irreversível. O RGPD protege os dados pessoais independentemente da tecnologia utilizada para o tratamento desses dados – é neutra em termos tecnológicos e aplica-se tanto ao tratamento automatizado como ao tratamento manual, desde que os dados sejam organizados de acordo com critérios pré-definidos (por exemplo, por ordem alfabética). Também é irrelevante o modo como os dados são armazenados — num sistema informático, através de videovigilância, ou em papel; em todos estes casos, os dados pessoais estão sujeitos aos requisitos de proteção previstos no RGPD.

Estipulam os nºs 1 e 2 do artigo 4º do RGPD que:

Para efeitos do presente regulamento, entende-se por:

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;

O RGPD institui duas situações de “intervenientes", refiramos deste modo, para simplificação de

análise, distintos:

A) A pessoa jurídica a quem se aplica o RGPD - no caso, o Município. O RGPD aplica-se aos organismos públicos (e, embora este conceito seja lato, no mesmo contemplam-se ou integram-se, como é consabido, também as autarquias locais - cfr. o art. 2º do RGPD) - nesta perspectiva:

A.1) O Município é o responsável pelo tratamento de dados.

Estipula o artigo 4º/ nº 7 do RGPD: «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 da 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;

E, veja-se, tb., o artigo 5º do RGPD, que estipula:

"Artigo 5º

Princípios relativos ao tratamento de dados pessoais

1. Os dados pessoais são:

a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);

b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 («limitação das finalidades»);

c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);

d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);

e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para

fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.o 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»);

f) 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, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»);

2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no nº 1 e tem de poder comprová-lo («responsabilidade»).”

Cfr., igualmente, do RGPD, os artigos acima referidos e ainda os artigos 30º, 31º, 35º, 36º, 37º, 40º e 42º.

A.2) O “responsável” pelo tratamento de dados pode também ser um subcontratante, um representante do Município, PORÉM atuando sempre por conta e em nome deste, conforme resulta do artigo 28º do RGPD, que assim estatui:

“Artigo 28º

Subcontratante

1. Quando o tratamento dos dados for efetuado por sua conta, o responsável pelo tratamento recorre apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos dados.

2. O subcontratante não contrata outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral. Em caso de autorização geral por escrito, o subcontratante informa o responsável pelo tratamento de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros subcontratantes, dando assim ao responsável pelo tratamento a oportunidade de se opor a tais alterações.

3. O tratamento em subcontratação é regulado por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento. Esse contrato ou outro ato normativo estipulam, designadamente, que o subcontratante:

a) Trata os 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 exigidas nos termos do artigo 32º;

d) Respeita as condições a que se referem os nºs 2 e 4 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;

f) Presta assistência ao responsável pelo tratamento no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32º a 36º, 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 do direito da União ou dos Estados-Membros; e

h) Disponibiliza ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no presente artigo e facilita e contribui para as auditorias, inclusive as inspeções, conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado.

No que diz respeito ao primeiro parágrafo, alínea h), o subcontratante informa imediatamente o responsável pelo tratamento se, no seu entender, alguma instrução violar o presente regulamento ou outras disposições do direito da União ou dos Estados-Membros em matéria de proteção de dados.

4. 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 ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, as mesmas obrigações em matéria de proteção de dados que as estabelecidas no contrato ou outro ato normativo entre o responsável pelo tratamento e o subcontratante, referidas no nº 3, 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 presente regulamento. Se esse outro subcontratante não cumprir as suas obrigações em matéria de proteção de dados, o subcontratante inicial continua a ser plenamente responsável, perante o responsável pelo tratamento, pelo cumprimento das obrigações desse outro subcontratante.

5. O facto de o subcontratante cumprir um código de conduta aprovado conforme referido no artigo 40º ou um procedimento de certificação aprovado conforme referido no artigo 42º pode ser utilizado como elemento para demonstrar as garantias suficientes a que se referem os n.ºs 1 e 4 do presente artigo.

6. Sem prejuízo de um eventual contrato individual entre o responsável pelo tratamento e o

subcontratante, o contrato ou outro ato normativo, referidos nos nºs 3 e 4 do presente artigo podem ser baseados, totalmente ou em parte, nas cláusulas contratuais-tipo referidas nos nºs 7 e 8 do presente artigo, inclusivamente quando fazem parte de

uma certificação concedida ao responsável pelo tratamento ou ao subcontratante por força dos artigos 42º e 43º.

7. A Comissão pode estabelecer cláusulas contratuais-tipo para as matérias referidas nos nºs 3 e 4 do presente artigo pelo procedimento de exame a que se refere o artigo 93º, nº 2.

8. A autoridade de controlo pode estabelecer cláusulas contratuais-tipo para as matérias referidas nos nºs 3 e 4 do presente artigo e de acordo com o procedimento de controlo da coerência referido no artigo 63º.

9. O contrato ou outro ato normativo a que se referem os nºs 3 e 4 devem ser feitos por escrito, incluindo em formato eletrónico.

10. Sem prejuízo do disposto nos artigos 82º, 83º e 84º, o subcontratante que, em violação do presente regulamento, determinar as finalidades e os meios de tratamento, é considerado responsável pelo tratamento no que respeita ao tratamento em questão."

Ainda assim, e tal como reiterado na DIRETRIZ/2023/1, da Comissão Nacional de Proteção de Dados, sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais, disponível em https://www.cnpd.pt/decisoes/diretrizes/, "o recurso à subcontratação não altera o facto de o responsável pelo tratamento deter a responsabilidade global pela proteção dos dados pessoais, sendo que os subcontratantes atuam apenas por conta do responsável, mediante as suas instruções (cf. artigo 4.º). No que diz respeito ao tratamento de dados pessoais, impõe o RGPD que a sua atuação resulte estritamente do que lhes for prescrito pelo responsável pelo tratamento (cf. artigo 28.º, n.º 3, alínea a), do RGPD). Isto sem prejuízo de, caso o responsável pelo tratamento dê instruções que violem o RGPD ou outras disposições do direito da União ou dos Estados-Membros, o subcontratante dever informar imediatamente o responsável pelo tratamento de tal facto (cf. artigo 28.º, n.º 3, alínea h), segundo parágrafo, do RGPD)./Com efeito, independentemente das propostas feitas pelos subcontratantes, a decisão última sobre as operações de tratamento de dados compete ao responsável pelo tratamento, que não pode eximir-se de desempenhar o seu papel e de cumprir as suas obrigações legais, eventualmente diferindo para subcontratantes responsabilidades que são apenas suas."

B) Por seu turno, o responsável pelo tratamento de dados (Município) designa, obrigatoriamente, um encarregado da protecção de dados.

Estipula o art. 37º/ nº 1 do RGPD que:

“Artigo 37º

Designação do encarregado da proteção de dados

1. O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que:

a) O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional; (...)”

Por seu turno, o artigo 39º do RGPD diz-nos quais são as funções do DPO:

“Artigo 39º

Funções do encarregado da proteção de dados

1. O encarregado da proteção de dados tem, pelo menos, as seguintes funções:

a) Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;

b) Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros 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) Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de

dados e controla a sua realização nos termos do artigo 35.o;

d) Coopera com a autoridade de controlo;

e) Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.o, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.

2. No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.”

No entretanto, através da Lei n.º 58/2019, de 8 de agosto, o Estado Português procurou assegurar

a execução, na ordem jurídica nacional, do referido Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016.

De acordo com os artigos 9º a 11º daquele diploma:

"Artigo 9.º

Disposição geral

1 — O encarregado de proteção de dados é designado com base nos requisitos previstos no nº 5 do artigo 37.º do RGPD, não carecendo de certificação profissional para o efeito.

2 — Independentemente da natureza da sua relação jurídica, o encarregado de proteção de dados exerce a sua função com autonomia técnica perante a entidade responsável pelo tratamento ou subcontratante.

Artigo 10.º

Dever de sigilo e confidencialidade

1 — De acordo com o disposto no n.º 5 do artigo 38.º do RGPD, o encarregado de proteção de dados está obrigado a um dever de sigilo profissional em tudo o que diga respeito ao exercício dessas funções, que se mantêm após o termo das funções que lhes deram origem.

2 — 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 acresce aos deveres de sigilo profissional previsto na lei.

Artigo 11.º

Funções do encarregado de proteção de dados

Para além do disposto nos artigos 37.º a 39.º do RGPD, são funções do encarregado de proteção de dados:

a) Assegurar a realização de auditorias, quer periódicas, quer não programadas;

b) Sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança;

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

No artigo 12º daquele diploma, estipula-se, no que às autarquias especialmente importa, o seguinte:

"Artigo 12.º

Encarregados de proteção de dados em entidades públicas

1 — Nos termos da alínea a) do n.º 1 do artigo 37.º do RGPD, é obrigatória a designação de encarregados de proteção de dados nas entidades públicas, de acordo com o disposto nos números seguintes.

2 — Para efeitos do número anterior, entende-se por entidades públicas:

a) O Estado;

b) As regiões autónomas;

c) As autarquias locais e as entidades supranacionais previstas na lei;

d) As entidades administrativas independentes e o Banco de Portugal;

e) Os institutos públicos;

f) As instituições de ensino superior públicas, independentemente da sua natureza;

g) As empresas do setor empresarial do Estado e dos setores empresariais regionais e locais;

h) As associações públicas.

3 — Independentemente de quem seja responsável pelo tratamento, existe pelo menos um encarregado de proteção de dados:

a) Por cada ministério ou área governativa, no caso do Estado, sendo designado pelo respetivo ministro, com faculdade de delegação em qualquer secretário de Estado que o coadjuvar;

b) Por cada secretaria regional, no caso das regiões autónomas, sendo designado pelo respetivo secretário regional, com faculdade de delegação em dirigente superior de 1.º grau;

c) Por cada município, sendo designado pela câmara municipal, com faculdade de delegação no presidente e subdelegação em qualquer vereador;

d) Nas freguesias em que tal se justifique, nomeadamente naquelas com mais de 750 habitantes, sendo designado pela junta de freguesia, com faculdade de delegação no presidente;

e) Por cada entidade, no caso das demais entidades referidas no número anterior, sendo designada pelo respetivo órgão executivo, de administração ou gestão, com faculdade de delegação

no respetivo presidente.

4 — Nos termos do n.º 3 do artigo 37.º do RGPD, pode ser designado o mesmo encarregado de proteção de dados para vários ministérios ou áreas governativas, secretarias regionais, autarquias locais ou outras pessoas coletivas públicas.

5 — Cabe a cada entidade a designação do encarregado de proteção de dados, não sendo

obrigatório o exercício de funções em regime de exclusividade.

6 — O encarregado de proteção de dados de uma entidade pública que tenha atribuições de

regulação ou controlo não pode exercer essas funções simultaneamente em entidade sujeita ao

controlo, ou inserida no perímetro regulatório daquela entidade."

A Comissão Nacional de Proteção de Dados, através da sua deliberação nº 2019/494, de 3 de setembro de 2019, disponível em www.cnpd.pt, veio a decidir como inaplicáveis no ordenamento jurídico interno de Portugal os seguintes artigos da mencionada Lei nº 58/2019, de 8 de agosto:

i. Artigo 2.º, n.ºs 1 e 2

ii. Artigo 20.º, n.º 1

iii. Artigo 23.º

iv. Artigo 28.º, n.º 3, alínea a)

v. Artigo 37.º, n.º 1, alíneas a), h) e k), e n.º 2

vi. Artigo 38.º, n.º 1, alínea b), e n.º 2

vii. Artigo 39.º, n.ºs 1 e 3

viii. Artigo 61.º, n.º 2

ix. Artigo 62.º, n.º 2

Com efeito, considerou e fixou a CNPD que aqueles normativos "(...) são manifestamente incompatíveis com o direito da União, centrando, por ora, a sua atenção sobre aquelas disposições

que, pela sua relevância e frequência de aplicação, suscitam a premência da adoção formal de tal entendimento(...);" e que, "(...) com fundamento no princípio do primado do direito da União Europeia, e nos demais argumentos (...)" por si expostos na mencionada deliberação, "(...) desaplicará em casos futuros que venha a apreciar, relativos a tratamentos de dados e às condutas dos respetivos responsáveis ou subcontratantes (...)", as supra identificadas disposições da Lei n.º 58/2019, de 8 de agosto.

Assim, afigura-se pertinente que o Município introduza internamente na sua organização a aplicação das medidas incluídas no Regulamento Geral de Proteção de Dados (RGPD).

Desde logo no que respeita à normalização das atividades relativas à utilização dos recursos informáticos, atribuindo responsabilidades e definindo direitos e deveres dos utilizadores dos sistemas de informação do Município, *assegurando a segurança* na utilização do seu sistema informático.

Por outro lado, sendo certo que o RGPD tem aplicação imediata, não é menos verdade que o mesmo possui normas cuja aplicação carece de ser adaptada à realidade do Município de modo a que internamente – uma vez que os dados pessoais interagem com as unidades orgânicas da Câmara Municipal e devem ser devidamente salvaguardados - os serviços municipais possam dar uma resposta eficaz e eficiente à "nova realidade" relativa à proteção de dados que o RGPD trouxe para o panorama normativo.

Finalmente, leva-se em consideração as orientações que têm vindo a ser emanadas da Comissão Nacional de Proteção de Dados, nomeadamente as plasmadas na sua DIRETRIZ/2023/1, sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais, disponível em https://www.cnpd.pt/decisoes/diretrizes/

Também se tem presente a matéria relacionada com o tratamento de dados em centrais telefónicas, o controlo de e-mail e do acesso à internet por parte dos trabalhadores (v.g. no que se relaciona com o direito à privacidade dos trabalhadores no contexto da relação laboral, o tratamento de dados, as condições de legitimidade, as interconexões e comunicações de dados a terceiros, o direito de acessos e retificação e eliminação), porém sem prejuízo da (demais) possibilidade de regulamentação interna específica, nos termos legais e que se afigurar pertinente, matéria a que se aplicam, em especial, as orientações da Comissão Nacional de Proteção de Dados plasmadas

na sua DELIBERAÇÃO n.º 1638// 2013, in www.cnpd.pt, e considerando-se o estabelecido nos seguintes corpos normativos:

- A Convenção 108 do Conselho da Europa, de 28 de janeiro de 1981, para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal, e o seu Protocolo Adicional, de 8 de novembro de 2001;

- A Carta Social Europeia (revista) do Conselho da Europa (CETS n.º163), aprovada em Estrasburgo em 3 de maio de 1996;

- O artigo 8.º da Convenção Europeia dos Direitos do Homem, do Conselho da Europa, de 4 de novembro de 1950;

- Os artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia;

- O artigo 16.º do Tratado sobre o Funcionamento da União Europeia;

- A Declaração sobre privacidade no trabalho da Organização Internacional do Trabalho, de 18 de junho de 1998;

- Os artigos 26.º, n.º 1, 32.º, n.º 8, 34.º e 35.º da Constituição da República Portuguesa;

- A Lei nº 58/2019, de 8 de agosto, em tudo quanto não desaplicado pela Deliberação nº 2019/494, de 3 de setembro de 2019, da Comissão Nacional de Proteção de Dados, disponível em www.cnpd.pt;

- O artigo 80.º do Código Civil;

O Código de Trabalho, aprovado pela Lei n.º 7/2009, de 12 de fevereiro, com a sua atual redação, designadamente os seus artigos 10.º, 16.º, 17.º, 22.º, 97.º, 99.º, 106.º e 107.º;

Do mesmo modo, remete-se para a legislação específica e ainda para a DELIBERAÇÃO n.º 7680/ 2014, in www.cnpd.pt, da Comissão Nacional de Proteção de Dados, a disciplinação de tudo quanto importe aos tratamentos de dados pessoais decorrentes da utilização de tecnologias de geolocalização no contexto laboral, nomeadamente decorrente do estabelecido no seguinte corpo normativo:

- A Convenção 108 do Conselho da Europa, de 28 de janeiro de 1981, para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal, e o seu Protocolo Adicional, de 8 de novembro de 2001;

- A Carta Social Europeia (revista) do Conselho da Europa (CETS n.º 163), aprovada em Estrasburgo em 3 de maio de 1996;

- O artigo 8.º da Convenção Europeia dos Direitos do Homem, do Conselho da Europa, de 4 de novembro de 1950;

- Os artigos 7.º, 8.º, 27.º e 31.º da Carta dos Direitos Fundamentais da União Europeia;

- O artigo 16.º do Tratado sobre o Funcionamento da União Europeia;

- Os artigos 26.º, n.º 1, 32.º, n.º 8, e 35.º da Constituição da República Portuguesa;

- A Lei nº 58/2019, de 8 de agosto, em tudo quanto não desaplicado pela Deliberação nº 2019/494, de 3 de setembro de 2019, da Comissão Nacional de Proteção de Dados, disponível em www.cnpd.pt;

- O artigo 80.º do Código Civil;

- O Código do Trabalho, aprovado pela Lei n.º 7/2009, de 12 de fevereiro, com a sua atual redação, designadamente os seus artigos 10.º, 16.º, 17.º, 20.º, 21.º, 97.º, 99.º, 106.º e 107.º, e

- A alínea b) do n.º 1 do artigo 4.º da Lei Geral do Trabalho em Funções Públicas, aprovada pela Lei nº 35/2014, de 20 de junho;

Em conformidade, o presente é um regulamento operacional que visa criar auto-vinculações internas na aplicação do RGPD e que procura responder às vertentes da segurança na utilização do sistema de informação e ao tratamento dos dados pessoais no MUNICÍPIO DE SANTA CRUZ DA GRACIOSA.

Assim, ao abrigo do poder regulamentar conferido às autarquias locais pelo artigo 241.º da Constituição da República Portuguesa e pela parte final da alínea k) do número 1 do artigo 33.º da Lei n.º 75/2013, de 12 de setembro, com a redação atualizada, foi elaborado o presente REGULAMENTO INTERNO DE SEGURANÇA NA UTILIZAÇÃO DOS SISTEMAS DE INFORMAÇÃO E DO TRATAMENTO DE DADOS PESSOAIS DO MUNICÍPIO DE SANTA CRUZ DA GRACIOSA.

Atenta, como se evidencia, a evidente natureza *interna* do presente regulamento, não está o mesmo sujeito às regras de publicitação ou discussão públicas prévias, nos termos gerais do artigo 100.º do CPA, nem, por maioria de razão, à análise de "custos benefícios" prevista no seu artigo 99.º (a matéria objeto do presente regulamento não é, de modo nenhum, mensurável *a priori*, porquanto, além do mais, do ponto de vista dos custos, não há "histórico", apenas podendo acentuar-se, no caso, os potenciais benefícios, todos relacionados com a disciplinação regulamentar interna-administrativa da atividade objeto da presente proposta).

Sem embargo, deve publicitar-se o Regulamento na Internet, no sítio institucional da autarquia.

Capítulo I

DISPOSIÇÕES GERAIS

Artigo 1.º

Lei Habilitante,

Objeto e âmbito de aplicação

1. O Regulamento Interno de Segurança na Utilização dos Sistemas de Informação e do tratamento de Dados Pessoais do MUNICÍPIO DE SANTA CRUZ DA GRACIOSA é elaborado ao abrigo do artigo 241.º da Constituição da República Portuguesa e da alínea k) do n.º 1 do artigo 33.º da Lei 75/2013, de 12 de setembro.

2. O presente Regulamento visa assegurar, no contexto das atividades do Município, a execução das normas referentes ao tratamento de dados pessoais constantes no RGPD e estabelecer um conjunto de normas de utilização e regras de segurança da informação com o intuito de possibilitar o processamento, a partilha e o armazenamento de informação, através do recurso à sua infraestrutura tecnológica.

3. As regras constantes do presente regulamento abrangem todo o tratamento de dados pessoais e a livre circulação desses dados, em defesa dos direitos e das liberdades fundamentais dos seus titulares, quando a responsabilidade do tratamento seja do Município ou seu subcontratante.

4. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.

5. São destinatários do presente Regulamento os trabalhadores municipais das unidades orgânicas da Câmara Municipal, sem prejuízo de o mesmo também se aplicar a qualquer pessoa com vínculo contratual ao Município, ou colocada à disposição do Município por órgãos ou entidades da administração central ou regional, nomeadamente em regime de colaboração, independentemente do regime jurídico a que esteja submetida, e, bem assim, os prestadores de serviços que utilizem os sistemas de informação do Município para o desenvolvimento das suas atividades profissionais.

6. Em tudo quanto não resultar do presente regulamento, nomeadamente em tudo quanto se relaciona com o tratamento de dados em centrais telefónicas, o controlo de e-mail e do acesso à internet por parte dos trabalhadores, v.g. no que respeita, nesse específico âmbito, ao direito à privacidade dos trabalhadores no contexto da relação laboral, tratamento de dados, condições de

legitimidade, interconexões e comunicações de dados a terceiros, direito de acessos e retificação e eliminação, e sem prejuízo da demais regulamentação municipal interna específica complementar e da lei, aplicam-se, em especial, as orientações da Comissão Nacional de Proteção de Dados plasmadas na sua DELIBERAÇÃO n.º 1638// 2013, in www.cnpd.pt, e considerando-se o estabelecido nos seguintes corpos normativos:

- Convenção 108 do Conselho da Europa, de 28 de janeiro de 1981, para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal, e o seu Protocolo Adicional, de 8 de novembro de 2001;

- Carta Social Europeia (revista) do Conselho da Europa (CETS n.º 163), aprovada em Estrasburgo em 3 de maio de 1996;

- Artigo 8.º da Convenção Europeia dos Direitos do Homem, do Conselho da Europa, de 4 de novembro de 1950;

- Artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia;

- Artigo 16.º do Tratado sobre o Funcionamento da União Europeia;

- Declaração sobre privacidade no trabalho da Organização Internacional do Trabalho, de 18 de junho de 1998;

- Artigos 26.º, n.º 1, 32.º, n.º 8, 34.º e 35.º da Constituição da República Portuguesa;

- O artigo 80.º do Código Civil;

- Lei nº 58/2019, de 8 de agosto, em tudo quanto não desaplicado pela Deliberação nº 2019/494, de 3 de setembro de 2019, da Comissão Nacional de Proteção de Dados, disponível em www.cnpd.pt;

- Código de Trabalho, aprovado pela Lei n.º 7/2009, de 12 de fevereiro, com a sua atual redação, designadamente os seus artigos 10.º, 16.º, 17.º, 22.º, 97.º, 99.º, 106.º e 107.º.

7. Do mesmo modo, remete-se para a regulamentação municipal complementar, para as leis gerais e para a legislação específica e ainda para a DELIBERAÇÃO n.º 7680/ 2014, in www.cnpd.pt, da Comissão Nacional de Proteção de Dados, a disciplinação de tudo quanto importe aos tratamentos de dados pessoais decorrentes da utilização de tecnologias de geolocalização no contexto laboral, nomeadamente o decorrente do estabelecido nos seguintes corpos normativos:

- Convenção 108 do Conselho da Europa, de 28 de janeiro de 1981, para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal, e o seu Protocolo Adicional, de 8 de novembro de 2001;

- Carta Social Europeia (revista) do Conselho da Europa (CETS n.º 163), aprovada em Estrasburgo em 3 de maio de 1996;

- Artigo 8.º da Convenção Europeia dos Direitos do Homem, do Conselho da Europa, de 4 de novembro de 1950;

- Artigos 7.º, 8.º, 27.º e 31.º da Carta dos Direitos Fundamentais da União Europeia;

- Artigo 16.º do Tratado sobre o Funcionamento da União Europeia;

- Artigos 26.º, n.º 1, 32.º, n.º 8, e 35.º da Constituição da República Portuguesa;

- Lei nº 58/2019, de 8 de agosto, em tudo quanto não desaplicado pela Deliberação nº 2019/494, de 3 de setembro de 2019, da Comissão Nacional de Proteção de Dados, disponível em www.cnpd.pt;

- Artigo 80.º do Código Civil;

- Código do Trabalho, aprovado pela Lei n.º 7/2009, de 12 de fevereiro, com a sua atual redação, designadamente os seus artigos 10.º, 16.º, 17.º, 20.º, 21.º, 97.º, 99.º, 106.º e 107.º, e

- Alínea b) do n.º 1 do artigo 4.º da Lei Geral do Trabalho em Funções Públicas, aprovada pela Lei nº 35/2014, de 20 de junho;

Artigo 2.º

Definições

Para efeitos do presente regulamento e sem prejuízo das definições legais, nomeadamente as previstas no artigo 4º do RGPD, entende-se por:

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;

3. 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;

4. 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;

5. Pseudonimização: o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;

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

7. Informação: informação digital que pode ser de carácter estratégico, técnico, financeiro, legal, de recursos humanos, ou de qualquer outra natureza, não importando se protegida ou não por normas de confidencialidade, desde que se encontre armazenada e/ou manuseada na infraestrutura tecnológica do Município e que se constitui como património do mesmo;

8. Informação particular: ficheiros, arquivos e documentos pessoais dos utilizadores, entendidos como aqueles que não são de interesse, uso ou propriedade do Município;

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

10. Responsável pelo tratamento de dados: o responsável pelo tratamento de dados é o Município (em conformidade com o estabelecido no nº 7 do artigo 4º do RGPD);

11. Encarregado da proteção de dados: é a pessoa, designada pelos competentes órgãos do Município, conforme alínea c) do nº 3 do artigo 12º da Lei nº 58/2019, de 8 de agosto, que, no âmbito das finalidades e dos meios de tratamento de dados pessoais, desempenha e assegura as

funções consultivas e de fiscalização quanto aos tratamentos de dados pessoais realizados dentro da organização municipal, em conformidade com o disposto nos artigos 32º a 34º do RGPD e nos artigos 9º a 11º da referida Lei nº 58/2019, de 8 de agosto;

12. Subcontratante: uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do Município (sem prejuízo de continuar a ser este a entidade responsável pelo tratamento dos dados pessoais);

13. 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 Município ou do subcontratante, estão autorizadas a tratar os dados pessoais;

14. Registos Log: Processo de registo de eventos relevantes num sistema de informação, geralmente num arquivo de log, o qual pode ser utilizado para auditoria e diagnóstico - esse registo pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça comportamentos dos sistemas no passado;

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

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

17. 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;

18. 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;

8. Utilizador: os trabalhadores municipais das unidades orgânicas da Câmara Municipal e qualquer pessoa com vínculo contratual ao Município, ou colocada à disposição do Município por órgãos ou entidades da administração central ou regional, nomeadamente em regime de colaboração, independentemente do regime jurídico a que esteja submetida, e, bem assim, os prestadores de serviços que utilizem os sistemas de informação do Município para o desenvolvimento das suas atividades profissionais.

19. Rede interna, hardware e software: todas as máquinas, tais como, desktops, laptops, micro PC's, tablets, telemóveis, software licenciado, cabos de rede, equipamentos ativos de rede (routers,

switchs e hubs), servidores, firewalls, proxies, impressoras, digitalizadores, ou qualquer outro equipamento pertencente à infraestrutura tecnológica do Município.

Capítulo II

FUNCIONAMENTO E UTILIZAÇÃO DOS SISTEMAS DE INFORMAÇÃO

Artigo 3.º

Atribuições específicas dos serviços de informática

1. Nos termos da lei e das disposições regulamentares municipais aplicáveis e em vigor, os serviços de informática (Sector de Informática) funcionam na dependência da Divisão Administrativa e Financeira e têm por função a gestão e manutenção dos meios informáticos existentes, a sua ligação ao exterior e o apoio aos Utilizadores na utilização dos meios informáticos disponíveis.

2. Para o efeito do nº 1, os serviços de informática devem:

2.1 - **Em matéria organizativa:**

a) Submeter à aprovação dos competentes órgãos do Município de uma proposta de plano de resposta a incidentes e recuperação do desastre, prevendo os mecanismos necessários para garantir a segurança da informação e a resiliência dos sistemas e serviços, bem como assegurar que a disponibilidade dos dados é restabelecida atempadamente após um incidente;

b) Submeter à aprovação dos competentes órgãos do Município de medidas concretas de Classificação da informação de acordo com o nível de confidencialidade e sensibilidade e, na sequência, adotar as medidas organizativas e técnicas adequadas à classificação;

c) Documentar as políticas de segurança aprovadas pelo Município;

d) Adotar procedimentos de análise para a monitorização dos fluxos de tráfego na rede;

e) Propor aos competentes órgãos do Município a aprovação de um plano de desenvolvimento dos sistemas de informação do Município, para sua gestão, tendo em vista a desburocratização e simplificação de procedimentos técnico-administrativos;

f) Assegurar quando necessário a interligação entre as aplicações informáticas instaladas e outros programas desenvolvidos por outras entidades;

g) Manter de forma permanente e atualizada toda a informação relativa a procedimentos da sua responsabilidade;

h) Promover e organizar levantamentos periódicos de carências ao nível de hardware e software;

i) Acompanhar os processos relativos à dotação de equipamentos informáticos que se revelem imprescindíveis ao desenvolvimento das atividades municipais;

j) Prestar o apoio técnico necessário aos utilizadores;

k) Manter o software de exploração em condições operacionais, de acordo com o âmbito de responsabilidades que vier a ser atribuído;

l) Zelar pelas condições de funcionamento de equipamento, executar os procedimentos de manutenção que lhes vierem a ser cometidos e controlar a execução daqueles que competirem a outras entidades externas;

m) Assegurar a atualização da informação constante na intranet, extranet e no sítio oficial da Câmara Municipal;

n) Submeter à aprovação dos competentes órgãos do Município de modos concretos de definição de palavras-passe seguras, incluindo os requisitos para o tamanho, a composição, o armazenamento e a frequência com que uma palavra-passe precisa de ser alterada;

o) Submeter à aprovação dos competentes órgãos do Município dos critérios técnicos destinados a garantir que cada trabalhador tem acesso apenas aos dados necessários para executar as suas funções e rever com frequência as permissões dos vários perfis de utilizadores, se possível, bem como da desativação/revogação de perfis inativos;

p) Submeter à aprovação dos competentes órgãos do Município dos critérios técnicos destinados a garantir a adoção de alarmística que permita identificar situações de acesso, tentativas ou utilização indevida;

q) Submeter à aprovação dos competentes órgãos do Município dos critérios técnicos destinados a garantir a definição das melhores práticas de segurança de informação a adotar, quer em fase de desenvolvimento de software, quer em fase de testes de aceitação, considerando em particular os princípios de proteção de dados desde a conceção e por defeito, análises de risco do tratamento e do ciclo de vida dos dados, métodos de pseudonimização e anonimização dos dados, mesmo quando o sistema é desenvolvido e mantido por subcontratante(s);

r) Propor aos competentes órgãos do Município a realização de auditorias de segurança de TI (Transmissão da Informação) e de avaliações de vulnerabilidade (testes de penetração) sistemáticos, para que os utilizadores possam ter conhecimento das próprias fragilidades e para que o Município consiga monitorizar os alvos mais frágeis e investir em formação com conteúdo específico e direcionado, de acordo com as vulnerabilidades detetadas e, sempre que habilitados para tanto, concretizar essas ações;

s) Verificar se as medidas de segurança definidas estão em prática, garantindo que são eficazes e propondo aos competentes órgãos do Município a sua atualização regular, especialmente

quando o processamento ou as circunstâncias se alteram, incluindo as que são implementadas pelos subcontratantes nos tratamentos de dados;

t) Documentar e corrigir as vulnerabilidades de segurança detetadas sem demora;

u) Propor aos competentes órgãos do Município a tomada das medidas necessárias para garantir o pleno cumprimento do artigo 33.º do RGPD, em particular no que diz respeito ao desenvolvimento de uma política interna para lidar e documentar eventuais violações de dados pessoais;

v) Avaliar periodicamente as medidas de segurança, técnicas e organizativas, internas e propor aos competentes órgãos do Município aprovar a sua atualização e revisão sempre que necessário.

2.2 – Em matéria de autenticação:

a) Utilizar credenciais fortes com palavras-passe longas (pelo menos 12 caracteres), únicas, complexas e com números, símbolos, letras maiúsculas e minúsculas, alterando-as com frequência;

b) Equacionar, designadamente face à sensibilidade da informação, aos privilégios dos utilizadores ou à forma de acesso (v.g. remota), a aplicação de autenticação multifator;

2.3 – Em matéria de Infraestrutura e sistemas:

a) Garantir que os sistemas operativos de servidores e terminais se encontram atualizados, bem como todas as aplicações (por exemplo, browser e plugins);

b) Manter atualizado o firmware dos equipamentos de rede;

c) Desenhar e organizar os sistemas e a infraestrutura por forma a segmentar ou isolar os sistemas e as redes de dados para prevenir a propagação de malware dentro da organização e para sistemas externos;

d) Robustecer a segurança dos postos de trabalho e servidores, nomeadamente:

i. bloquear o acesso a sítios que sejam suscetíveis de constituir um risco para a segurança;

ii. bloquear os redireccionamentos suspeitos através de motores de busca;

iii. bloquear de imediato os ficheiros e aplicações infetadas com malware;

iv. realizar inspeção periódica do estado e utilização dos recursos do sistema;

v. monitorizar a utilização do software instalado;

vi. ativar e conservar os registos de auditoria (log);

vii. validar os acessos por IP aos servidores que estão expostos ao público;

viii. alterar o porto configurado por omissão para o protocolo de acessos remotos (RDP).

2.4 – Em matéria de ferramenta de correio eletrónico:

a) Propor aos competentes órgãos do Município a definição de forma clara e inequívoca de políticas e procedimentos internos sobre o específico envio de mensagens de correio eletrónico contendo dados pessoais, que introduzam as verificações adicionais necessárias, no sentido de:

i. garantir a inserção dos endereços de correio eletrónico dos destinatários no campo 'Bcc:', nos casos de múltiplos destinatários;

ii. prevenir erros na introdução manual de endereços de correio eletrónico;

iii. assegurar que os ficheiros enviados em anexo contêm apenas os dados pessoais que se pretendem comunicar;

b) Equacionar a criação de listas de distribuição ou grupos de contacto, com o objetivo de prevenir a divulgação dos endereços dos destinatários em operações de envio massivo de mensagens de correio eletrónico;

c) Equacionar a criação de regras com o objetivo de adiar/atrasar a entrega de mensagens de correio eletrónico contendo dados pessoais, mantendo-as na 'Caixa de Saída' por um tempo determinado, permitindo verificações de conformidade, após clique em 'Enviar';

d) Encriptar com código, ao qual só o destinatário tenha acesso, os emails e/ou anexos enviados que contenham dados pessoais;

e) Confirmar com o destinatário, antes de envio de e-mail contendo dados pessoais, o endereço de email preferencial para contacto;

f) Propor aos competentes órgãos do Município a realização de ações de formação no sentido de capacitar os trabalhadores a operar os mecanismos de envio de mensagens de correio eletrónico de acordo com os procedimentos definidos, sensibilizando-os para os erros mais comuns, potencialmente suscetíveis de originar violações de dados pessoais e incentivando-os à dupla verificação;

g) Propor para aprovação dos competentes órgãos do Município os critérios técnicos de reforço do sistema de alerta da ferramenta de alarmística utilizada pelo Município, para assegurar visibilidade imediata sobre a criação por utilizadores de regras de encaminhamento automático de e-mails para contas externas;

h) Reforçar o sistema com ferramentas antiphishing e antispam, que permitam bloquear ligações e/ou anexos com código malicioso;

i) Adotar controlos de segurança que permitam classificar e proteger as mensagens de correio eletrónico sensíveis;

2.5 – Em matéria de Proteção contra malware:

a) Utilizar encriptação segura, especialmente no caso de credenciais de acesso, de dados especiais (os dados pessoais elencados no n.º 1 do artigo 9.º do RGPD, de dados de natureza altamente pessoal (grosso modo, os dados pessoais relacionados com condenações penais e infrações - cf. artigo 10.º do RGPD - ou com dimensões da vida privada e familiar) ou de dados financeiros;

b) Criar um sistema de cópias de segurança (backup) atualizado, seguro e testado, totalmente separado das bases de dados principais e sem acessibilidade externa;

c) Reforçar o sistema com ferramentas antimalware que inclua a capacidade de o verificar e detetar, bem como o bloqueio em tempo real de ameaças do tipo ransomware;

2.6 – Em matéria de Proteção utilização de equipamentos em ambiente externo:

a) Armazenar dados em sistemas internos, protegidos com medidas de segurança apropriadas, e acessíveis remotamente através de mecanismos de acesso seguro (VPN);

b) Permitir acessos apenas por VPN;

c) Bloquear as contas após várias tentativas inválidas de login;

d) Ativar a autenticação multifator para os utilizadores dos equipamentos;

e) Aplicar cifragem dos dados no sistema operativo;

f) Sempre que for aplicável, ativar a funcionalidade de “remote wipe” e “find my device”;

g) Efetuar cópias de segurança automáticas das pastas de trabalho, quando o equipamento se encontra ligado à rede da entidade;

h) Propor para aprovação dos competentes órgãos municipais os critérios de definição de regras claras e adequadas para a utilização de equipamentos em ambiente externo;

i) Propor para aprovação dos competentes órgãos municipais a aprovação as medidas técnicas destinadas a impedir que, no transporte de informação com dados pessoais, estes possam ser lidos, copiados, alterados ou eliminados de forma não autorizada;

j) Utilizar encriptação segura no transporte, em dispositivos de massa ou arquivo potencialmente permanente (CD/DVD/PEN USB).

Artigo 3.º-A

Atribuições específicas dos demais serviços municipais que tenham acessos a documentos que contenham dados pessoais

1. Nos termos da lei e das disposições regulamentares municipais aplicáveis e em vigor, **quaisquer serviços municipais** devem:

a) Em matéria de Transporte de informação que integre dados pessoais:

a.1) Adotar as medidas técnicas aprovadas e destinadas a impedir que, no transporte de informação com dados pessoais, estes possam ser lidos, copiados, alterados ou eliminados de forma não autorizada;

a.2) Utilizar encriptação segura no transporte, em dispositivos de massa ou arquivo potencialmente permanente (CD/DVD/PEN USB);

b) Em matéria de Transporte de Armazenamento de documentos em papel que contenham dados pessoais:

b.1) Nomeadamente os serviços do arquivo municipal, cuidar pelo armazenamento de documentos em papel que contenham dados pessoais;

b.2) Utilizar papel e impressão que seja durável;

b.3) Nomeadamente os serviços do arquivo municipal, conservar documentação em local com controlo de humidade e temperatura;

b.4) Nomeadamente os serviços do arquivo municipal, armazenar, devidamente organizados, os documentos que contêm dados pessoais sensíveis em local fechado, resistente ao fogo e inundação;

b.5) Controlar os acessos, com registo das respetivas data e hora, de quem acede e do(s) específico(s) documento(s) acedido(s);

b.6) Nomeadamente os serviços de ambiente municipais, providenciar pela destruição dos documentos através de equipamento específico que garanta a destruição “segura”.

Artigo 4.º

Utilização do hardware e do software

1. O Município coloca à disposição dos seus trabalhadores recursos tecnológicos nomeadamente equipamentos (hardware) e programas informáticos licenciados (software).

2. O Utilizador não poderá instalar e/ou executar outro software distinto daquele facultado ou autorizado pelo Município.

3. A utilização de software não licenciado é uma conduta ilícita que pode implicar graves responsabilidades de tipo penal e civil, para além de colocar em risco evidente os equipamentos informáticos e a informação contida nos mesmos.

4. Caso o Utilizador necessite de um software adicional para o desempenho das suas tarefas, deverá solicitá-lo, fundamentadamente, ao seu responsável hierárquico imediato que, após apreciação, proporá a melhor solução, submetendo o assunto, sendo o caso, à consideração do responsável hierárquico com poder final decisório,

5. O Utilizador deve utilizar os equipamentos e sistemas informáticos colocados à sua disposição sem incorrer em atividades que possam ser consideradas ilícitas ou ilegais, que infrinjam ou possam infringir os direitos do Município ou de terceiros ou ponham em risco a segurança e estabilidade dos equipamentos e sistemas, assim como da informação neles contidos.

6. São expressamente proibidas as atividades que constituam infração prevista na legislação em vigor, nomeadamente:

a) Aceder, ler, apagar, copiar ou modificar as mensagens de correio eletrónico ou arquivos de outros Utilizadores, exceto com o consentimento do titular, em função de circunstâncias concretas e nos limites da lei;

b) Aceder a áreas restritas dos sistemas informáticos do Município, de outros utilizadores ou de terceiros;

c) Destruir, alterar, inutilizar ou de qualquer forma danificar os dados, programas ou documentos eletrónicos do Município, dos seus Utilizadores, ou de eventuais terceiros;

d) Distorcer ou falsear registos LOG do sistema;

e) Aumentar o nível de privilégios de um Utilizador no sistema;

f) Decifrar as chaves, sistemas ou algoritmos de codificação e qualquer outro elemento de segurança que intervenha nos processos do Municípo;

g) Obstaculizar voluntária ou involuntariamente os acessos de outros Utilizadores aos equipamentos e sistemas do Município pelo consumo massivo de recursos informáticos, assim como realizar ações que danifiquem, interrompam ou gerem erros;

h) Introduzir ou propagar programas, vírus, applets, controlos Active X ou qualquer outro dispositivo lógico ou sequência de caracteres que causem ou sejam suscetíveis de causar qualquer tipo de alteração nos sistemas informáticos da entidade ou de terceiros;

i) Introduzir, descarregar da Internet, reproduzir, utilizar ou distribuir programas informáticos não autorizados expressamente pelo Município ou qualquer outro tipo de obra ou material cujos direitos de propriedade intelectual ou industrial pertençam a terceiros, quando não se disponha de autorização para o efeito;

j) Instalar cópias ilegais de qualquer programa, incluindo os estandardizados de facto e apagar, eliminar, modificar ou alterar qualquer dos programas instalados legalmente;

k) Instalar software ou aplicativos de qualquer espécie cuja licença tenha sido adquirida pelo Município, em equipamentos diversos daqueles fornecidos para tal efeito (o que inclui a título enunciativo, equipamentos ou dispositivos privados do Utilizador).

7. O Utilizador responsabiliza-se por qualquer alteração ou instalação realizada nos equipamentos fornecidos com acesso aberto que pela sua natureza carecem de privilégios de administração.

8. O Utilizador não tem permissão para executar aplicações cujo objetivo seja o acesso remoto por parte de terceiros à infraestrutura Municipal.

9. O Utilizador que pretenda aceder remotamente à infraestrutura do município terá de solicitar o acesso correspondente aos Serviços de Informática.

10. O Utilizador não tem permissão para copiar, alterar ou eliminar arquivos que tenham sido criados por terceiros, sem prévio consentimento do seu autor e/ou dos competentes órgãos do Município, designadamente do presidente Câmara Municipal, de acordo e nos termos das limitações legais.

11. Os equipamentos e sistemas municipais não podem utilizar-se para transmitir ou armazenar conteúdos estranhos ao desenvolvimento das atribuições do município e competências dos seus órgãos.

12. O Utilizador deve informar ou alertar o serviço de informática sempre que detetar qualquer tipo de atividade ou comportamento anormal dos recursos disponibilizados pelo Município, nomeadamente questões de segurança e/ou sistemas desatualizados, quer seja pelo aproveitamento de falhas de segurança, quer pela simples tentativa e erro de acerto de palavra-passe.

13. A utilização de quaisquer equipamentos que não sejam de propriedade do Município, para conexão à sua infraestrutura informática, nomeadamente os computadores portáteis, tablets,

smartphones ou outros, deve ser normalizada e configurada pelo Serviço de Informática, de modo a acautelar a segurança da informação.

14. A alteração de quaisquer componentes internos nos equipamentos não é permitida, ficando vedada aos utilizadores a realização de qualquer modificação ou manutenção que, sempre que necessárias, serão efetuadas pelos Serviços de Informática.

15. Toda a rede interna, hardware e software está sujeita a monitorização, podendo o Município manter o histórico de acessos realizados aos seus sistemas, porém sem prejuízo do direito ao anonimato e à eliminação de dados, nos termos legais aplicáveis.

Artigo 5.º

Palavras passe e chaves de acesso

1. As palavras passe e chaves de acesso são meios utilizados pelos Utilizadores e administradores para salvaguardar a confidencialidade da informação disponível nos equipamentos e sistemas do Município.

2. O responsável pelo Serviço de Informática deterá, mediante prévia autorização e conhecimento dos competentes órgãos municipais as palavras passe e chaves de administração.

3. O Utilizador compromete-se a fazer um uso diligente das palavras passe e chaves de acesso atribuídas e a manter as mesmas confidenciais, responsabilizando-se por qualquer atividade que se realize ou tenha lugar mediante a utilização das mesmas.

4. Após qualquer perda ou suspeita de acesso não autorizado por parte de terceiros às palavras passe e chaves de acesso o Utilizador deverá informar o responsável pelos Serviços de Informática de forma imediata, o qual dará também imediatamente conhecimento ao encarregado da proteção de dados e aos competentes órgãos municipais

5. Se o Utilizador suspeitar que outra pessoa conhece os seus dados de identificação e de acesso deve proceder à alteração imediata da mesma e comunicar o facto aos Serviços de Informática, com o fim de que estes lhe permitam gerar de imediato nova(s) chave(s), sem prejuízo de dever também comunicar o facto ao encarregado da proteção de dados e aos competentes órgãos municipais

6. Nos casos de baixa ou ausência temporal do Utilizador ou perante a inacessibilidade por parte do mesmo aos equipamentos e sistemas atribuídos, este pode, por escrito e indicando a finalidade, solicitar aos competentes órgãos municipais com conhecimento ao encarregado da proteção de dados, que autorize os Serviços de Informática a proceder à alteração da palavra passe e chaves.

7. É proibida a utilização de técnicas de encriptação ou codificação de informação não autorizadas e/ou não facultadas pelo Município.

Artigo 6.º

Correio eletrónico

1. O Município disponibilizará ao Utilizador, sempre que se revele necessário em função das suas responsabilidades laborais, uma conta de correio eletrónico do Município.

2. Em casos pontuais e por solicitação ou necessidade específica de um qualquer serviço, poderão ser criadas contas de e-mail por serviço, partilhadas por vários utilizadores, que deverão respeitar as regras em vigor para as contas de e-mail por utilizador.

3. O Utilizador deve utilizar o correio eletrónico em nome do Município para fins exclusivamente laborais.

4. Sempre que um correio eletrónico pelo seu conteúdo ou pelos anexos, seja relevante para efeitos de um processo que decorra no Município ou contiver informação relevante para o Município, o Utilizador deve gravar o correio eletrónico recebido, enviando para a pasta de trabalho definida para o efeito ou tramitando para o serviço de gestão documental.

5. O Utilizador deve respeitar a predefinição do aspeto gráfico do correio eletrónico da autarquia.

6. O Utilizador não deve enviar, distribuir, dar a conhecer e comunicar informação confidencial ou classificada do Município.

7. É proibida a transmissão de correio cujo conteúdo seja ilegal, difamatório, obsceno, ofensivo, denegatório ou imoral.

8. Cessada a colaboração ou relação laboral de um Utilizador com o Município, e após comunicação dos serviços competentes e mediante prévia decisão dos competentes órgãos municipais será desativada ou encerrada a conta de correio eletrónico do mesmo, podendo ser gerada uma mensagem automática.

9. O Município pode manter, se o entender e nos limites da lei, uma cópia de segurança do correio eletrónico de contas encerradas.

10. O Utilizador, em caso de ausência, deve ativar o mecanismo de mensagem automática *out-of-office* (fora-do-escritório), ou reencaminhar o correio eletrónico para outra conta ativa do Município, de forma a assegurar o normal funcionamento dos serviços.

11. A monitorização será realizada, a qualquer momento e de forma automática, através da utilização de diversos sistemas informáticos existentes para tal finalidade e mantidos na infraestrutura tecnológica do Município.

12. Na sequência de tal monitorização e/ou filtragem, as mensagens enviadas para um e-mail do Município poderão ser redirecionadas para outro e-mail interno, na sequência de fundada suspeita de conter conteúdo malicioso que ponha em causa a segurança da informação, sem necessidade de qualquer aviso prévio e sem conhecimento do emissor e do recetor da mensagem.

Artigo 7.º

Acesso e utilização da Internet

1. O Município disponibiliza ao Utilizador o acesso à Internet, em função das responsabilidades laborais ou tarefas que lhe sejam atribuídas.

2. A Internet é uma ferramenta de trabalho para uso estritamente profissional.

3. O Utilizador tem consciência de que a Internet é uma rede a nível mundial com conteúdos que podem resultar ilícitos, ofensivos ou em geral inapropriados.

4. Sem prejuízo do disposto no número anterior, e estando todo o tráfego sujeito a monitorização e filtragem automática, está bloqueada, a navegação nos sites com a seguinte categorização, excetuando-se os de, ou para, as funções desempenhadas pelo utilizador em questão:

a) Pornografia;

b) Partilha de ficheiros (exemplo.: peer to peer);

c) Terrorismo;

d) Drogas;

e) Hackers e qualquer tipo de pirataria informática;

f) Jogos;

g) Violência e agressividade (racismo, xenofobia, etc.);

h) Vídeo e Áudio;

i) Música on-line;

j) Outros, que se considerem desadequados para as funções do utilizador.

5. O Município monitoriza e controla, de forma automática, os sistemas e tecnologias de informação, e demais meios, validando se cumprem em todo o momento as medidas de segurança necessárias.

6. Os conteúdos de natureza não profissional que os Utilizadores enviem a outrem são passíveis de sancionamento disciplinar, nos termos legais.

7. Nenhum software, ficheiro executável ou base de dados que se descarregue da Internet ou que se receba por correio eletrónico ou através de qualquer suporte material (CD, Pen USB, outros) necessário para o desempenho das tarefas profissionais pode ser instalado no terminal ou dispositivo propriedade do Município sem se comprovar previamente, com os Serviços de Informática, que está devidamente licenciado e limpo de vírus.

8. Os competentes órgãos municipais podem limitar a utilização de dispositivos removíveis de armazenamento, tais como Pens USB, CDs, entre outros.

Artigo 8.º

Utilização da informação

1. Todos os documentos eletrónicos, dados e informações resultantes das atividades exercidas pelos utilizadores e serviços, devem estar armazenados em servidor, nas pastas afetas a cada utilizador ou serviço.

2. Os dados dos serviços constantes nas Bases de Dados utilizadas pelos diversos sistemas aplicacionais em utilização pelo Município são propriedade deste e devem ser mantidos íntegros e invioláveis.

3. Sempre que o Utilizador aceda a dados pessoais incorporados nos ficheiros, por motivos diretamente relacionados com a função desempenhada deve este tratá-los, única e exclusivamente, em conformidade com o âmbito de autorização expressamente comunicada pelos competentes órgãos municipais.

4. O Utilizador não deve usar dados pessoais com fins ou efeitos ilícitos, proibidos ou lesivos de direitos ou interesses de terceiros, ou contrários às finalidades para os quais foram recolhidos.

5. Ao Utilizador é expressamente proibido aceder ou tratar dados pessoais para os quais não tenha obtido expressa autorização legal por parte dos competentes órgãos do Município.

6. O Utilizador não pode criar qualquer base de dados com dados pessoais sem que a mesma seja legal e previamente autorizada e enquadrada pelos competentes órgãos do Município.

7. Quaisquer questões sobre proteção de dados pessoais e sobre o exercício de quaisquer direitos relativos aos mesmos devem ser colocadas aos competentes órgãos do Município, sem prejuízo de também poderem sê-lo, concomitantemente, ao encarregado da proteção de dados do

Município e sem prejuízo de qualquer prerrogativa legal deste e, bem assim, da Comissão Nacional de Proteção de Dados.

Capítulo III

NORMAS E PROCEDIMENTOS INTERNOS A OBSERVAR PELOS SERVIÇOS RELATIVAMENTE AO TRATAMENTO DOS DADOS PESSOAIS

Secção I

Princípios

Artigo 9.º

Princípios relativos ao tratamento de dados pessoais

Os dados pessoais são:

a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados;

b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades;

c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados;

d) Exatos e atualizados sempre que necessário, devendo ser adotadas todas as medidas adequadas para que os dados inexatos, sejam apagados ou retificados sem demora;

e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados;

f) 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, adotando as medidas técnicas ou organizativas adequadas.

Artigo 10.º

Licitude do tratamento

1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;

b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;

c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o Município esteja sujeito;

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

e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o Município;

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

Artigo 11.º

Condições aplicáveis ao consentimento

1. Quando o tratamento for realizado com base no consentimento, o Município, através dos seus competentes órgãos, deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.

2. Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples, não sendo vinculativa qualquer parte dessa declaração que constitua violação da lei geral ou do presente regulamento.

3. O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento, sendo, antes de dar o seu consentimento, o titular dos dados informado desse facto e devendo o consentimento ser tão fácil de retirar quanto de dar.

Artigo 12.º

Consentimento de menores

1. Nos termos do artigo 8.º do RGPD, os dados pessoais de crianças só podem ser objeto de tratamento com base no consentimento previsto na alínea a) do n.º 1 do mesmo artigo 6.º do

RGPD e relativo à oferta direta de serviços da sociedade de informação quando as mesmas já tenham completado treze anos de idade.

2. Caso a criança tenha idade inferior a treze anos, o tratamento só é lícito se o consentimento for dado pelos representantes legais desta, preferencialmente com recurso a meios de autenticação segura, como o Cartão de Cidadão ou a Chave Móvel Digital.

Artigo 13.º

Tratamento de categorias especiais de dados pessoais

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

2. O disposto no n.º 1 não se aplica se se verificar um dos seguintes casos:

a) Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades lícitas específicas, exceto se existir norma legal que previna que a proibição a que se refere o n.º 1 não pode ser infirmada pelo titular dos dados;

b) Se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do Município ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido por norma legal ou ainda por uma convenção coletiva;

c) Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento, sempre nos limites da lei;

d) Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;

e) Se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito, nomeadamente num processo judicial, ou sempre que os tribunais atuem no exercício da sua função jurisdicional;

f) Se o tratamento for necessário por motivos de interesse público importante, com base em norma legal, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;

g) Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, para diagnóstico médico, prestação de cuidados ou tratamentos de saúde ou de ação social ou para a gestão de sistemas e serviços de saúde ou de ação social, com base em norma legal ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.º 3;

h) Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no em norma legal que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;

i) Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, do RGPD com base em norma legal, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados.

3. Os dados pessoais referidos no n.º 1 podem ser tratados para os fins referidos no n.º 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos legais ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade nos termos legais ou de regulamentação estabelecida pelas autoridades nacionais competentes.

Artigo 14.º

Proteção de dados pessoais de pessoas falecidas

1. Os dados pessoais de pessoas falecidas são protegidos nos termos do RGPD quando se integrem nas categorias especiais de dados pessoais a que se refere o n.º 1 do artigo 9.º do RGPD, ressalvados os casos previstos no n.º 2 do mesmo artigo.

2. Os direitos previstos no RGPD relativos a dados pessoais de pessoas falecidas, abrangidos pelo número anterior, nomeadamente os direitos de acesso, retificação e apagamento, são exercidos por quem a pessoa falecida haja legalmente designado para o efeito ou, na sua falta, pelos respetivos herdeiros, nos termos da lei.

Secção II

Responsável pelo tratamento e subcontratante

Artigo 15.º

Responsável e responsabilidade do responsável pelo tratamento

1. O Responsável pelo tratamento de dados é o Município.

2. O responsável pelo tratamento aprova e aplica, através dos seus competentes órgãos e serviços, as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o RGPD, com a demais legislação aplicável e com o presente regulamento.

3. As medidas incluem a adoção e o modo de aplicação das políticas adequadas em matéria de proteção de dados, códigos de conduta, políticas de privacidade e procedimentos de certificação os quais constituem evidências do cumprimento das obrigações legais e regulamentares por parte do Município e norteiam-se, entre outras, pelas orientações emanadas da Comissão Nacional de Proteção de Dados, nomeadamente as previstas na sua DIRETRIZ/2023/1 sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais, disponível em https://www.cnpd.pt/decisoes/diretrizes/, permitindo ao Município, nomeadamente:

a) Acompanhar o desenvolvimento da sociedade da informação, propondo ações e capitalizando as oportunidades daí decorrentes;

b) Assegurar a organização e gestão da rede de comunicações, voz e dados do Município;

c) Promover a adequada formação dos trabalhadores do Município, nas áreas associadas aos sistemas de informação;

d) Fomentar junto dos trabalhadores uma cultura de privacidade e segurança da informação, para que cada um esteja capacitado para reconhecer potenciais ameaças e agir em conformidade, e como forma de reduzir a ocorrência e o impacto do erro humano;

e) Dar a conhecer aos trabalhadores o dever de confidencialidade a que estão sujeitos pelo facto de tratarem dados pessoais;

f) Aprovar e adotar tudo quanto necessário para a cabal implementação do RGPD, designadamente no âmbito das atuações dos serviços municipais apontadas nos artigos 3º e 3º-A do presente regulamento;

g) Nas condições legais, v.g. as previstas no artigo 35º do RGPD, quando um certo tipo de tratamento, em particular que utilize novas tecnologias e 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, o Município procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais, solicitando previamente o parecer do encarregado da proteção de dados.

4. As medidas referidas nas alíneas a) a f) do número anterior são revistas e atualizadas consoante as necessidades, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade de ocorrência e gravidade podem ser variáveis.

Artigo 16.º

Proteção de dados desde a conceção e por defeito

1. Incumbe ao Município determinar a aplicação de medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento, bem como não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

2. A obrigação referida no número anterior aplica-se:

a) À quantidade de dados pessoais recolhidos;

b) À extensão do seu tratamento;

c) Ao seu prazo de conservação;

d) À sua acessibilidade;

Artigo 17.º

Subcontratante

1. Quando o tratamento dos dados for efetuado por sua conta, o Município recorre apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos da lei e do presente regulamento e assegure a defesa dos direitos do titular dos dados.

2. O tratamento em subcontratação é regulado por contrato que vincule o subcontratante ao Município, o qual, entre outras previsões legalmente possíveis, deve estabelecer o objeto, a duração, a natureza e finalidade do tratamento, o tipo de dados pessoais, as categorias dos titulares dos dados e as obrigações e direitos do Município.

Artigo 18.º

Tratamento sob a autoridade do responsável pelo tratamento ou do subcontratante

O subcontratante ou qualquer pessoa que, agindo sob a autoridade do Município ou do subcontratante, tenha acesso a dados pessoais, só pode proceder ao tratamento destes dados mediante clara instrução do Município ou do subcontratante nesse sentido, salvo se o contrário resultar expressamente da lei ou de cominação judicial.

Artigo 19.º

Registos das atividades de tratamento

1. No Município é assegurada a conservação de um registo de todas as atividades de tratamento sob a responsabilidade municipal, constando desse registo as seguintes informações:

a) O nome e os contactos do Município, enquanto entidade responsável pelo tratamento e, sendo caso disso, de qualquer responsável conjunto pelo tratamento e do encarregado da proteção de dados;

b) As finalidades do tratamento dos dados;

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

d) As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais;

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

f) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança.

Secção III

Segurança dos dados pessoais

Artigo 20.º

Segurança do tratamento

1. 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, o Município e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

a) A pseudonimização e a cifragem dos dados pessoais;

b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;

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

d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

2. O Município e o subcontratante tomam medidas para assegurar que qualquer pessoa singular que, agindo sob a autoridade municipal ou do subcontratante, tenha acesso a dados pessoais, só procede ao seu tratamento mediante instruções do Município, nos termos legais aplicáveis, salvo se o contrário resultar expressamente da lei ou de cominação judicial.

Artigo 21.º

Notificação de uma violação de dados pessoais à autoridade de controlo

1. Em caso de violação de dados pessoais, o Município, através dos seus competentes órgãos, notifica desse facto a Comissão Nacional de Proteção de Dados, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares.

2. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.

3. O subcontratante notifica o Município sem demora injustificada após ter conhecimento de uma violação de dados pessoais.

4. A notificação referida no n.º 1 deve, pelo menos:

a) Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;

b) Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações;

c) Descrever as consequências prováveis da violação de dados pessoais;

d) Descrever as medidas adotadas ou propostas pelo Município para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos;

4. Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, estas podem ser fornecidas por fases, sem demora injustificada.

5. O Município documenta quaisquer violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada, devendo essa documentação permitir à Comissão Nacional de Proteção de Dados verificar o cumprimento do disposto no presente artigo.

Artigo 22.º

Comunicação de uma violação de dados pessoais ao titular dos dados

1. Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o Município comunica a violação de dados pessoais ao titular dos dados sem demora injustificada.

2. A comunicação ao titular dos dados a que se refere o n.º 1 do presente artigo descreve em linguagem clara e simples a natureza da violação dos dados pessoais e fornece, pelo menos, as informações e medidas previstas no artigo 21.º, n.º 3, alíneas b), c) e d).

3. Sem prejuízo das prerrogativas legais da Comissão Nacional de Proteção de Dados, a comunicação ao titular dos dados a que se refere o n.º 1 não é exigida se for preenchida uma das seguintes condições:

a) O Município tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados

pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem;

b) O Município tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados a que se refere o n.º 1 já não é suscetível de se concretizar; ou

c) Implicar um esforço desproporcionado, sendo que, neste caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz.

Secção IV

Direitos do titular dos dados

Artigo 23.º

Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados

1. O Município toma as medidas adequadas para que possa fornecer ao titular as informações a que se referem os artigos 24.º e 25.º e qualquer comunicação prevista nos artigos 22.º, 26.º, 28.º e 29.º a 34.º a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças.

2. As informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos.

3. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.

4. O Município facilita o exercício dos direitos do titular dos dados nos termos dos artigos 26.º, 28.º e 29.º a 34.º exceto se demonstrar que não está em condições de identificar o titular dos dados.

5. O Município fornece ao titular as informações sobre as medidas tomadas, mediante pedido apresentado nos termos dos artigos 26.º e 29.º a 33.º, sem demora injustificada e no prazo de um mês a contar da data de receção do pedido, prazo este que pode ser prorrogado até dois meses, quando for comprovada e fundamentadamente necessário, tendo em conta a complexidade do pedido e o número de pedidos.

6. O Município informa 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, sendo que, caso o titular dos dados apresente o pedido por meios eletrónicos, a informação é, sempre que possível, fornecida por meios eletrónicos, salvo pedido em contrário do titular.

7. Se o Município não der seguimento ao pedido apresentado pelo titular dos dados, informa-o sem demora e, o mais tardar, 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 a uma autoridade de controlo e intentar ação judicial.

8. As informações fornecidas nos termos dos artigos 24.º e 25.º e quaisquer comunicações e medidas tomadas nos termos dos artigos 22.º, 26.º, 28.º e 29.º a 34.º são fornecidas a título gratuito.

9. Se os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, o Município pode:

a) Exigir o pagamento de uma taxa legalmente fixada pelos seus competentes órgãos;

b) Recusar-se a dar seguimento ao pedido, demonstrando o caráter manifestamente infundado ou excessivo do mesmo.

8. Quando o Município tiver dúvidas razoáveis quanto à identidade do titular que apresenta o pedido a que se refere o n.º 1 pode solicitar que lhe sejam fornecidas as informações adicionais que forem necessárias para confirmar a identidade do titular dos dados.

Secção V

Informação e acesso aos dados pessoais

Artigo 24.º

Informações a facultar quando os dados pessoais são recolhidos junto do titular

1. Quando os dados pessoais forem recolhidos junto do titular, o Município faculta-lhe, aquando da recolha desses dados pessoais, as seguintes informações:

a) A identidade e os contactos do Município;

b) Os contactos do encarregado da proteção de dados, se for caso disso;

c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;

d) Se o tratamento dos dados se basear no artigo 10.º, n.º 1, alínea f), os interesses legítimos do Município ou de um terceiro;

e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;

2. Para além das informações referidas no n.º 1, aquando da recolha dos dados pessoais, o Município fornece ao titular as seguintes informações adicionais, necessárias para garantir um tratamento equitativo e transparente:

a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;

b) A existência do direito de solicitar o acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;

c) Se o tratamento dos dados se basear no artigo 10.º, n.º 1, alínea a), ou no artigo 13.º, n.º 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;

d) O direito de apresentar reclamação à Comissão Nacional de Proteção de Dados;

e) Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está legalmente obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;

f) A existência de decisões automatizadas, incluindo a definição de perfis, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

3. Quando o Município tiver a intenção de proceder ao tratamento posterior dos dados pessoais para fins legalmente previstos que não sejam aqueles para os quais os dados tenham sido recolhidos, antes desse tratamento fornece ao titular dos dados informações sobre esses fins e quaisquer outras informações pertinentes, nos termos do n.º 2.

Artigo 25.º

Informações a facultar quando os dados pessoais não são recolhidos junto do titular

1. Quando os dados pessoais não forem recolhidos junto do titular, o Município fornece-lhe as seguintes informações:

a) A identidade e os contactos do Município;

b) Os contactos do encarregado da proteção de dados, se for caso disso;

c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;

d) As categorias dos dados pessoais em questão;

e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver.

2. Para além das informações referidas no n.º 1, o Município fornece ao titular as seguintes informações, necessárias para lhe garantir um tratamento equitativo e transparente:

a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para fixar esse prazo;

b) Se o tratamento dos dados se basear no artigo 10.º, n.º 1, alínea f), os interesses legítimos do Município ou de um terceiro;

c) A existência do direito de solicitar o acesso aos dados pessoais que lhe digam respeito, e a retificação ou o apagamento, ou a limitação do tratamento no que disser respeito ao titular dos dados, e do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;

d) Se o tratamento dos dados se basear no artigo 10.º, n.º 1, alínea a), ou no artigo 13.º, nº 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;

e) O direito de apresentar reclamação à Comissão Nacional de Proteção de Dados;

f) A origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público;

g) A existência de decisões automatizadas, incluindo a definição de perfis e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

3. O Município comunica as informações referidas nos n.^{os} 1 e 2:

a) Num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que estes forem tratados;

b) Se os dados pessoais se destinarem a ser utilizados para fins de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação ao titular dos dados; ou

c) Se estiver prevista a divulgação dos dados pessoais a outro destinatário, o mais tardar aquando da primeira divulgação desses dados.

4. Quando o Município tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados pessoais tenham sido obtidos, antes desse tratamento fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes referidas no n.º 2.

5. Os n.^{os} 1 a 4 não se aplicam quando e na medida em que:

a) O titular dos dados já tenha, comprovadamente, conhecimento das informações;

b) Se comprove a impossibilidade de disponibilizar a informação, ou que o esforço envolvido seja desproporcionado, nomeadamente para o tratamento para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, sob reserva das condições e garantias previstas no artigo 89.º, n.º 1 do RGPD, e na medida em que a obrigação referida no n.º 1 do presente artigo seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento, sendo que, nestes casos, o Município toma as medidas adequadas para defender os direitos, liberdades e interesses legítimos do titular dos dados, inclusive através da divulgação da informação ao público;

c) A obtenção ou divulgação dos dados esteja expressamente prevista em normativos legais ao qual o Município estiver sujeito, prevendo medidas adequadas para proteger os legítimos interesses do titular dos dados; ou

d) Os dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional regulamentada por norma legal, inclusive uma obrigação legal de confidencialidade.

Artigo 26.º

Direito de acesso do titular dos dados

1. O titular dos dados tem o direito de obter do Município a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:

a) As finalidades do tratamento dos dados;

b) As categorias dos dados pessoais em questão;

c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;

d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;

e) A existência do direito de solicitar ao Município a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento;

f) O direito de apresentar reclamação à Comissão Nacional de Proteção de Dados;

g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;

h) A existência de decisões automatizadas, incluindo a definição de perfis, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

2. O Município fornece uma cópia dos dados pessoais em fase de tratamento.

3. Para fornecer outras cópias solicitadas pelo titular dos dados, o Município pode exigir o pagamento de taxa legal ou regulamentarmente fixada.

4. Se o titular dos dados apresentar o pedido por meios eletrónicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrónico de uso corrente.

Artigo 27.º

Prazo de conservação de dados pessoais

1. O prazo de conservação de dados pessoais é o que estiver fixado por norma legal ou regulamentar ou, na falta desta, o que se revele comprovadamente necessário para a prossecução da finalidade.

2. Quando, pela natureza e finalidade do tratamento, designadamente para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos, não seja possível determinar antecipadamente o momento em que o mesmo deixa de ser necessário, é lícita a conservação dos dados pessoais.

3. Quando os dados pessoais sejam necessários para o Município, ou o subcontratante, comprovar o cumprimento de obrigações, os mesmos podem ser conservados enquanto não decorrer o prazo de prescrição dos direitos correspetivos.

4. Quando cesse a finalidade que motivou o tratamento, inicial ou posterior, de dados pessoais, o Município deve proceder à sua destruição ou anonimização.

5. Nos casos em que existe um prazo de conservação de dados imposto por lei, só pode ser exercido o direito ao apagamento previsto no artigo 30.º findo esse prazo.

Secção VI

Oposição, retificação e apagamento

Artigo 28.º

Direito de oposição

1. O titular dos dados tem o direito de, em qualquer momento, se opor, nomeadamente por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 10.º, n.º 1, alínea e) ou f), ou no artigo 10.º, n.º 4, incluindo a definição de perfis com base nessas disposições.

2. Salvo razões ponderosas, legais e comprovadas que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo, nomeadamente judicial, o Município faz cessar o tratamento de dados pessoais

Artigo 29.º

Direito de retificação

1. O titular tem o direito de obter do Município, sem demora injustificada, a retificação dos dados pessoais inexatos que lhe digam respeito.

2. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.

Artigo 30.º

Direito ao apagamento dos dados

1. O titular tem o direito de obter do Município o imediato apagamento dos seus dados pessoais, sem demora injustificada, designadamente nas seguintes situações:

a) Os dados pessoais deixem de ser necessários para a finalidade que motivou a sua recolha ou tratamento;

b) O titular retire o consentimento em que se baseia o tratamento dos dados nos termos do artigo 10.º, n.º 1, alínea a), ou do artigo 13.º, n.º 2, alínea a) e se não existir outro fundamento jurídico-legal para o referido tratamento;

c) O titular se oponha ao tratamento nos termos do artigo 28.º e não existam interesses legítimos prevalecentes que justifiquem o tratamento;

d) Os dados pessoais forem tratados ilicitamente;

e) Os dados pessoais tenham de ser apagados para o cumprimento de uma obrigação legal a que o Município esteja sujeito.

2. Quando o Município tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.º 1, toma as medidas que forem ajustadas, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos.

3. Os n.^{os} 1 e 2 não se aplicam na medida em que o tratamento se revele necessário:

a) Ao exercício da liberdade de expressão e de informação;

b) Ao cumprimento de uma obrigação legal que exija o tratamento a que o Município esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja legalmente investido o município;

c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 13.º, n.º 2, alíneas h) e i), bem como do artigo 13.º, n.º 3;

d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.º, n.º 1 do RGPD na medida em que o direito referido no n.º 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou

e) Para efeitos de declaração, exercício ou defesa de um direito, nomeadamente num processo judicial.

Artigo 31.º

Direito à limitação do tratamento

1. O titular dos dados tem o direito de obter do Município a limitação do tratamento, se se aplicar uma das seguintes situações:

a) Contestar a exatidão dos dados pessoais, durante um período que permita ao Município verificar a sua exatidão;

b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização;

c) O Município já não necessitar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito, nomeadamente no âmbito de um processo judicial;

d) Se tiver oposto ao tratamento nos termos do artigo 28.º, até se verificar que os motivos legítimos do Município prevalecem sobre os do titular dos dados.

2. Quando o tratamento tiver sido limitado nos termos do n.º 1, os dados pessoais só podem, à exceção da conservação, ser objeto de tratamento com o consentimento do titular, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos ponderosos de interesse público.

3. O titular que tiver obtido a limitação do tratamento nos termos do n.º 1 é informado pelo Município antes de ser removida a limitação ao referido tratamento.

Artigo 32.º

Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento

1. O Município comunica a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento a que se tenha procedido em conformidade com os artigos 29.º, o artigo 30.º, n.º 1, e 31.º, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado.

2. Se o titular dos dados o solicitar, o Município fornece-lhe informações sobre os referidos destinatários.

Artigo 33.º

Direito de portabilidade dos dados

1. O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido ao Município, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se:

a) O tratamento se basear no consentimento dado nos termos do artigo 10.º, n.º 1, alínea a), ou do artigo 13.º, n.º 2, alínea a), ou num contrato referido no artigo 10.º, n.º 1, alínea b); e

b) O tratamento for realizado por meios automatizados.

2. Ao exercer o seu direito de portabilidade dos dados nos termos do n.º 1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, e na medida do tecnicamente possível.

3. O exercício do direito a que se refere o n.º 1 do presente artigo aplica-se sem prejuízo do disposto no artigo 30.º.

4. O direito previsto no nº 1 não se aplica ao tratamento, nos termos da lei, necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está legalmente investido o Município.

5. O direito a que se refere o n.º 1 não prejudica os direitos e as liberdades e os legítimos interesses de terceiros.

Artigo 34.º

Decisões individuais automatizadas, incluindo definição de perfis

1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

2. O n.º 1 não se aplica se a decisão:

a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e o Município, nos termos legas;

b) For autorizada por norma legal a que o Município estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou

c) For baseada no consentimento explícito do titular dos dados.

3. Nos casos a que se referem o n.º 2, alíneas a) e c), o Município aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, o titular obter intervenção humana por parte do Município e de manifestar o seu ponto de vista e contestar a decisão.

4. As decisões a que se refere o n.º 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9.º, n.º 1, a não ser que o n.º 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

Capítulo IV

DISPOSIÇÕES FINAIS

Artigo 35.º

Política de Proteção de Dados

O Município deve elaborar e manter atualizado e disponível ao público na sua página oficial um documento sobre Política de Proteção de Dados.

Artigo 36.º

Deveres complementares municipais

O Município deve, sem prejuízo d outras incumbências legais:

a) Incrementar um sistema permanente e dinâmico de verificação da conformidade com o RGPD;

b) Provar, mediante evidências, o respeito pelo RGPD;

c) Promover auditorias no âmbito de um controlo contínuo e sistemático para aferir da efetividade e eficácia das medidas implementadas, modificando-as, sempre que necessário em conformidade com o RGPD;

d) Orientar-se pelas competentes diretrizes emanadas da Comissão Nacional de Proteção de Dados.

Artigo 37.º

Encarregado da Proteção de dados

1. O Município, através dos seus competentes órgãos, nos termos previstos no nº 3, e, quando aplicável, o subcontratante, designa um encarregado da proteção de dados (EPD), com base nos requisitos previstos no nº 5 do artigo 37.º do RGPD, não carecendo o EPD de certificação profissional para o efeito.

2. O Município e, quando aplicável, o subcontratante, assegura que:

a) O encarregado da proteção de dados seja envolvido, de forma adequada e em tempo útil, em todas as questões relacionadas com a proteção de dados pessoais;

b) O encarregado da proteção de dados é apoiado no exercício das funções, v.g. a que se referem os artigos 32º a 34º do RGPD, e os artigos 9º a 11º da Lei nº 58/2019, de 8 de agosto, fornecendo-

lhe os recursos necessários ao desempenho dessas funções e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento;

c) São cumpridas todas as demais obrigações legais instituídas, nomeadamente as previstas no RGPD e na Lei nº 58/2019, de 8 de agosto

3. Nos termos do disposto na alínea c) do nº 3 do artigo 12º da Lei n.º 58/2019, de 8 de agosto, **a designação** do Encarregado da Proteção de Dados (*EPD*) **é obrigatória** e **é deliberada pela executivo camarário**, com faculdade de delegação no presidente e subdelegação em qualquer vereador.

4. O Encarregado da Proteção de Dados é uma pessoa singular, à qual incumbe, designadamente:

a) Informar e aconselhar o Município ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do RGPD e de outras disposições de proteção de dados da União ou dos Estados-Membros;

b) Controlar a conformidade com o RGPD, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do Município ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;

c) Prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controlar a sua realização nos termos do artigo 35º do RGPD;

d) Cooperar com a autoridade de controlo (Comissão Nacional de Proteção de Dados);

e) Ser um *ponto de contacto* para a autoridade de controlo (Comissão Nacional de Proteção de Dados) sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36º do RGPD, e consulta, sendo caso disso, dessa autoridade sobre qualquer outro assunto;

f) Para além do disposto nos artigos 37.º a 39.º do RGPD:

f.1) Assegurar a realização de auditorias, quer periódicas, quer não programadas;

f.2) Sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança,

nomeadamente o responsável pelos serviços informáticos do Município;

f.3) Assegurar as relações com os titulares dos dados nas matérias abrangidas pelo RGPD e pela legislação nacional em matéria de proteção de dados.

5. No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

6. O encarregado de proteção de dados é designado com base nos requisitos previstos no nº 5 do artigo 37.º do RGPD, não carecendo de certificação profissional para o efeito.

7. Independentemente da natureza da sua relação jurídica, o encarregado de proteção de dados exerce a sua função com autonomia técnica perante o Município ou subcontratante.

8. De acordo com o disposto no n.º 5 do artigo 38.º do RGPD, o encarregado de proteção de dados está obrigado a um dever de sigilo profissional em tudo o que diga respeito ao exercício dessas funções, que se mantêm após o termo das funções que lhes deram origem.

9. O encarregado de proteção de dados, bem como o Município, incluindo o subcontratante, e todas as pessoas que intervenham em qualquer operação de tratamento de dados, estão obrigados a um dever de confidencialidade que acresce aos deveres de sigilo profissional previsto na lei.

10. O encarregado da proteção de dados pode ser um elemento do pessoal do Município responsável pelo tratamento ou do subcontratante, ou exercer as suas funções com base num contrato de prestação de serviços (neste caso, a contratar pelo Município mediante o recurso às regras gerais do Código dos Contratos Públicos).

11. O Município ou o subcontratante publica os contactos do encarregado da proteção de dados e comunica-os à autoridade de controlo (Comissão Nacional de Proteção de Dados.)

12. Os titulares dos dados podem contactar o encarregado da proteção de dados sobre todas as questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos direitos que lhe são conferidos pelo presente regulamento, pela lei geral e pelo RGPD.

13. O encarregado da proteção de dados está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com o direito da União ou dos Estados-Membros.

14. O encarregado da proteção de dados pode exercer outras funções e atribuições, nos limites da lei.

15. O Município ou o subcontratante assegura que essas funções e atribuições não resultam num conflito de interesses.

Artigo 38.º

Visita à página oficial do MUNICÍPIO

1. A visita ao sítio Web institucional do Município é feita anonimamente.

2. Quem acede apenas deve fornecer os dados pessoais necessários para a prestação do serviço solicitado, nomeadamente para ser capaz de aceder a qualquer um dos serviços no sítio que possuam gestão de processos específicos dependentes do utilizador.

3. Os dados referidos no número anterior serão incorporados nos arquivos correspondentes do Município e serão tratados em conformidade com o regulamento e com a lei e apenas serão objeto de transferência, sempre que apropriado e com o consentimento do titular, nos termos legal ou regulamentarmente previstos.

4. As pessoas cujos dados pessoais estejam contidos nos ficheiros dos serviços municipais, podem exercer os seus direitos de acesso, retificação, cancelamento e oposição, na forma prevista pela lei e no presente regulamento, antes do envio para o arquivo.

Artigo 39.º

Controlo e supervisão

No respeito pela lei, o Município reserva-se o direito de controlar e supervisionar, sem prévio aviso, o correto e lícito uso dos recursos e dispositivos do Município por parte dos Utilizadores e, em concreto, o cumprimento do presente regulamento, prevenindo atividades que possam afetar o Município.

Artigo 40.º

Entrada em Vigor

O presente regulamento interno entra em vigor no primeiro dia útil a seguir à sua aprovação pela Câmara Municipal, será publicitado nos termos legais e revoga qualquer outro anterior com o mesmo objeto.

Aprovado em *Reunião Ordinária* da Câmara Municipal de Santa Cruz da Graciosa de *31 de agosto de 2023*.

O Presidente da Câmara Municipal,

Assinado com Assinatura Digital Qualificada
por:
ANTÓNIO MANUEL RAMOS DOS REIS
Presidente
Município de Santa Cruz da Graciosa
Para efeitos de representação do Município de
Santa Cruz da Graciosa - artº 34º e 35º da Lei
75/2013, de 12 de setembro
Data: 06-09-2023 19:01:12

António Manuel Ramos dos Reis