



MUNICÍPIO DE VILA VELHA DE RÓDÃO

CÂMARA MUNICIPAL

Aprovado,

O Presidente da Câmara



Assinado por: Luis Pereira
Data: 16-09-2022 16:20:25

CADERNO DE ENCARGOS

AQUISIÇÃO DE SERVIÇOS PARA UTILIZAÇÃO E GESTÃO DA
APLICAÇÃO PARA GESTÃO *ONLINE* DE OCORRÊNCIAS

PARTE I

Cláusulas Jurídicas

Artigo 1.º

Entidade pública contratante

A entidade pública contratante é o Município de Vila Velha de Ródão, pessoa coletiva 506642798 sito na Rua de Santana 6030-230 Vila Velha de Ródão, com o número de telefone 272540300, de fax 272540301 e com o e-mail geral@cm-vvrodao.pt.

Artigo 2.º

Objeto

O objeto do procedimento consiste, de acordo com as especificações técnicas descritas na Parte II do presente Caderno de Encargos, **na Aquisição de serviços para utilização e gestão da aplicação online para gestão de ocorrências.**

Artigo 3.º

Local da entrega

Os serviços deverão estar **acessíveis em qualquer lugar através de uma ligação à internet**, permitindo a sua utilização através de *browser web*, aplicação iOS e aplicação Android.

Artigo 4.º

Prazo

O serviço terá uma duração de 24 meses a contar da adjudicação.

Artigo 5.º

Condições de pagamento

- 1- A **utilização da aplicação** no âmbito do presente procedimento deverá ser **faturada mensalmente** no mês seguinte ao da sua efetiva prestação, sendo o pagamento efetuado num **prazo de 30 dias** relativamente à data de apresentação da fatura.
- 2- Em caso de discordância dos valores indicados nas faturas por parte da **entidade adjudicante**, deverá esta comunicar ao adjudicatário, por escrito, os respetivos fundamentos, ficando o adjudicatário obrigado a prestar os esclarecimentos necessários ou a proceder à emissão de nova fatura corrigida.

Artigo 6.º

Valor

- 1- Pelos serviços objeto do presente procedimento, bem como pelo cumprimento das demais obrigações constantes do Caderno de Encargos, a entidade adjudicante deve pagar ao adjudicatário **o preço constante da proposta adjudicada**, que se estima ser **4.440,00€** (quatro mil, quatrocentos e quarenta euros) acrescido de IVA à taxa legal em vigor, que corresponde a um valor estimado de 185,00€ em 24 prestações mensais de igual valor;
- 2- O preço referido no número 1 inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à entidade adjudicante.
- 3- O montante estimado referido no número 1 do presente artigo que deve considerar-se o preço base, nos termos do art.º 47 do CCP como montante máximo que a entidade adjudicante se dispõe a pagar pela execução de todas as prestações que constituem o objeto do procedimento.

Artigo 7.º**Prazo de manutenção da proposta**

O Prazo de manutenção da proposta é de 66 dias.

Artigo 8.º**Obrigações do adjudicatário**

- 1- O adjudicatário obriga-se a cumprir os requisitos e obrigações constantes das especificações técnicas descritas na parte II do presente Caderno Encargos e de acordo com o prazo referido no artigo 4.º.
- 2- O adjudicatário obriga-se a cumprir os suportes e garantias conforme previsto no artigo 14.º.
- 3- O adjudicatário obriga-se a faturar mensalmente, no mês seguinte ao da prestação.

Artigo 9.º**Obrigações do adjudicante**

- 1- A entidade adjudicante compromete-se, através dos seus serviços, a fornecer todo o apoio necessário ao adjudicatário, para o bom funcionamento das soluções propostas por este;
- 2- Disponibilizar as condições físicas, materiais e humanas necessárias ao correto funcionamento dos sistemas propostos;
- 3- A entidade adjudicante compromete-se a pagar as faturas dentro do prazo.

Artigo 10.º**Contrato**

Não há lugar a celebração de contrato escrito, de acordo com o disposto na alínea a) do n.º 1 do art.º 95.º do Decreto-Lei n.º 18/2008, de 29 de janeiro na redação do Decreto Lei n.º 111-B/2017 de 31 de agosto.

Artigo 11.º**Prevalência**

- 1- Fazem parte integrante do contrato os seguintes documentos:
 - a) Os esclarecimentos e as retificações ao caderno de encargos identificados pelo adjudicatário, desde que esses esclarecimentos e as retificações tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
 - b) O caderno de encargos;
 - c) A proposta adjudicada;
 - d) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.
- 2- Em caso de dúvida ou divergência entre os documentos referidos no número anterior, a prevalência é determinada pela ordem pela qual são indicados nesse número.

Artigo 12.º**Objeto do dever de sigilo**

- 1- O adjudicatário deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à entidade adjudicante, de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato;
- 2- A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato;
- 3- Exclui-se o dever de sigilo previsto na informação e na documentação que sejam comprovadamente do domínio público à data da respetiva obtenção pelo adjudicatário ou que este esteja legalmente obrigado a revelar, por força da lei, de

processo judicial ou a pedido de autoridades reguladoras ou de outras entidades administrativas competentes.

Artigo 13.º

Penalidades

- 1- No caso de incumprimento dos prazos fixados no art.º 4 para a **operacionalização dos serviços** e, por causa imputável ao adjudicatário, poderá ser aplicada uma penalidade, calculada de acordo com a seguinte fórmula: $P = V \times A/75$, em que:
P corresponde ao montante da penalidade;
V corresponde ao valor previsto a pagar;
A corresponde ao número de dias em atraso.
- 2- No caso de incumprimento no **fornecimento** por período superior ao previsto no artigo 14º, aplicar-se-á uma penalização de 100% sobre o valor dos serviços inoperacionais.

Artigo 14.º

Suporte e garantias

Em caso de falha ou mau funcionamento da aplicação, a sua **reparação ou configuração** deverá ser efetuada **num prazo máximo de três dias úteis** a contar da participação da entidade adjudicante.

Artigo 15.º

Casos fortuitos ou de força maior

- 3- Não podem ser impostas penalidades ao prestador de serviços, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.
- 4- Podem constituir motivos de força maior, caso se venha a verificar os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.
- 5- Não constituem força maior, designadamente:
 - a) Circunstâncias que não constituam força maior para os subcontratados do prestador de serviços, na parte em que intervenham;
 - b) Greves ou conflitos laborais limitados às sociedades do prestador de serviços ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
 - c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo prestador de serviços de deveres ou ónus que sobre ele recaiam;
 - d) Manifestações populares devidas ao incumprimento pelo prestador de serviços de normas legais;
 - e) Incêndios ou inundações com origem nas instalações do prestador de serviços cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
 - f) Avarias nos sistemas informáticos ou mecânicos do prestador de serviços não devidas a sabotagem;
 - g) Eventos que estejam ou devam estar cobertos por seguros.

- 6- A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
- 7- A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

Artigo 16.º

Comunicações e notificações

- 1- Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas nos termos do Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma das partes identificada no contrato.
- 2- Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Artigo 17.º

Resolução de litígios - Foro competente

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Administrativo e Fiscal de Castelo Branco.

Artigo 18.º

Proteção de dados pessoais

O adjudicatário obriga-se a cumprir a Lei de Proteção de Dados Pessoais (Lei n.º 67/98, de 26 de outubro), ou diploma legal que sobrevier, o Regulamento Geral sobre a Proteção de Dados (Regulamento EU 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016), assim como, o Anexo RGPD do presente Caderno de Encargos.

Artigo 19.º

Legislação aplicável

O procedimento é regulado pela legislação portuguesa, nomeadamente o Código dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro na redação do Decreto-lei n.º 111-B/2017 de 31 de agosto e legislação conexa.

PARTE II

Especificações Técnicas

Artigo 1º

Condições de disponibilização da aplicação

O presente procedimento visa a aquisição de serviços para utilização e gestão da aplicação *online* para gestão de ocorrências no modelo “*software as a service*” (SaaS) pelo período de 2 anos. O objeto do procedimento enquadra-se na categoria SaaS, visto que, o adjudicatário é responsável por toda a estrutura necessária à disponibilização do sistema e a entidade adjudicante utiliza-o através da internet, mediante um pagamento mensal. Esta aplicação deve ser configurada de acordo com o formato organizacional e *layouts* de apresentação da entidade adjudicante, tendo em conta as seguintes condições:

1. Garantia de 99,9% de operacionalidade anual, com exclusão de interrupções planeadas. O adjudicatário deverá, num período de tempo razoável, informar a entidade adjudicante sobre o planeamento de atualizações antes destas terem lugar, isto caso estas atualizações possam afetar o uso da aplicação;
2. Garantia de nível elevado de segurança na estrutura da aplicação, no *datacenter* de alojamento e nas comunicações até aos clientes, bem como o cumprimento escrupuloso do RGPD, com possibilidade de monitorizar todas as ações realizadas;
3. Possibilidade de eliminação da informação da base de dados ou exportação para ficheiros XLS;
4. O adjudicatário deverá incluir melhoramentos e atualizações regulares sem custos adicionais;
5. Para resolução de problemas e outras questões, o adjudicatário, deverá disponibilizar um serviço de suporte ao cliente durante os dias de úteis entre as 08h00 e as 18h00, com 1h mensal no mínimo;
6. A aplicação deverá permitir o envio de notificações relativas às ocorrências por SMS e/ou e-mail para os cidadãos e funcionários, sem que o envio resulte em acréscimo de custos para a entidade adjudicante;
7. O adjudicatário é responsável pela manutenção dos portais *web* e registo nas lojas oficiais Google e Apple, mediante credenciais fornecidas pela entidade adjudicante.

Artigo 2º

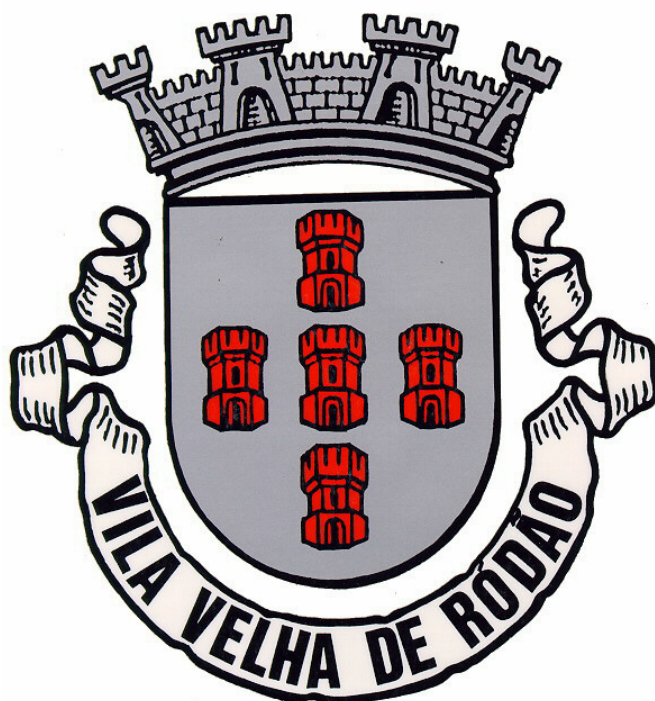
Especificações técnicas

A aplicação de gestão de ocorrências deverá reunir as seguintes características:

1. Utilização sem limites de quantidade de categorias/sub-categorias e utilizadores internos;
2. Acesso à aplicação para gestão de ocorrências, contemplando:
 - a) Função de mapas através de material cartográfico Google Maps;
 - b) Formulário *web* para reporte de ocorrências que possa funcionar autonomamente ou integrado no *website* e perfil Facebook da entidade adjudicante;
 - c) Aplicação de *smartphone* para gestão de ocorrências para uso dos utilizadores internos;
 - d) Aplicação de *smartphone* para reporte de ocorrências para os cidadãos.
3. Permitir o registo de ocorrências pelos cidadãos selecionando entre diversas categorias/sub-categorias;
4. Permitir que o cidadão adicione fotos elucidativas da ocorrência que regista e da sua localização exata através de coordenadas GPS;

5. As versões para *smartphone* devem permitir comunicar imediatamente a realização de ações no próprio local da ocorrência.
6. Múltiplas possibilidades de visualização dependendo do perfil do utilizador;
7. Aplicação com vários écrans possíveis para introdução: participações *web*; ordem de trabalho interna; formulário interno; entre outros;
8. Aplicação com possibilidade de ter diversos registadores e utilizadores, com separação integral das temáticas;
9. Permitir configuração de ações e tarefas associadas às ocorrências, como sejam, enviar para a área do responsável por cada categoria as ocorrências nelas classificadas. A aplicação deverá permitir que todas notificações das ocorrências sejam enviadas rapidamente por meio de uma simples mensagem de texto SMS e/ou por e-mail para o funcionário correspondente para que sejam tomadas as medidas necessárias para a sua resolução;
10. Através de estatísticas e relatórios, a aplicação deve possibilitar que as chefias tenham uma perspetiva real dos pedidos dos cidadãos, bem como do desempenho das equipas;
11. A disponibilização das estatísticas deve contemplar visualização *online* e a possibilidade de exportação para XLS, como sejam por exemplo:
 - a) Número de ocorrências por período de tempo e por tipologia;
 - b) Tempo de resolução médio das ocorrências;
 - c) Tipo de ocorrências mais frequentes.
12. Desmaterialização da manutenção operacional das infraestruturas, espaços públicos e património, permitindo a integração numa filosofia de "*smart city*".

Doc. Ref. N.º:	15.20.PT_CLAUS_RGPD_IC_MVVR
N.º de Páginas	46
Data:	14.09.2022



DE:	Município de Vila Velha de Ródão
PARA:	Infracontrol – ICP Infraestruturas Control Portugal Lda
ASSUNTO:	Cláusulas Contratuais para RGPD

ÍNDICE

Introdução	4
Clausulado-Tipo Contratual	5
1. Preâmbulo	6
2. Os direitos e obrigações do responsável pelo tratamento.....	7
3. O subcontratante atua de acordo com instruções	7
4. Confidencialidade	8
5. Segurança do tratamento.....	8
6. Recurso a subsubcontratantes.....	10
7. Transferências de dados pessoais para países terceiros ou organizações internacionais.....	11
8. Assistência ao responsável pelo tratamento	13
9. Notificação de uma violação de dados pessoais	14
10. Apagamento e devolução de dados	15
11. Auditoria e inspeção	16
12. Acordo entre as partes relativamente a outros termos.....	16
13. Início e término	17
14. Pontos de contacto do responsável pelo tratamento e do subcontratante.....	19
Anexo A: Informação sobre o Tratamento.....	20
A.1. A finalidade do tratamento realizado pelo subcontratante em nome do responsável pelo tratamento é:.....	20

A.2. O tratamento de dados pessoais realizado pelo subcontratante em nome do responsável pelo tratamento deverá maioritariamente limitar-se a (natureza do tratamento):.....	20
A.3. O tratamento inclui os seguintes tipos de dados pessoais relativamente aos titulares dos dados:.....	21
A.4. O tratamento inclui as seguintes categorias de titulares dos dados:.....	21
A.5. O tratamento de dados pessoais realizado pelo subcontratante em nome do responsável pelo tratamento poderá ser realizado quando as cláusulas tenham início. O tratamento tem a seguinte duração:	21
Anexo B: Instrução relativa ao tratamento de dados pessoais.....	22
B.1. Objecto de instrução de tratamento.....	22
B.2. Segurança do tratamento	22
Requisitos técnicos mínimos das redes e sistemas de informação (conforme a Resolução de Ministros n.º 41/2018).....	24
B.3. Prestação de assistência ao responsável pelo tratamento.....	45
B.4. Período de armazenamento/procedimentos de apagamento.....	45
B.5. Localização do tratamento	46
B.6. Instrução para a transferência de dados pessoais para países terceiros.....	46
B.7. Procedimentos para a realização de auditorias pelo responsável pelo tratamento, incluindo inspeções, do tratamento de dados pessoais realizados pelo subcontratante em nome do responsável pelo tratamento	46

INTRODUÇÃO

No contexto europeu e nacional têm vindo a ser criados/reforçados mecanismos de salvaguarda dos indivíduos, no que à proteção de dados diz respeito.

Desde logo, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados - RGPD) traz consigo novas obrigações para os responsáveis pelo tratamento de dados e novos e reforçados direitos para os titulares.

No contexto nacional, a Lei n.º 58/2019, de 8 de agosto, que assegura a execução do RGPD, tem também disposições específicas no que ao tratamento de dados diz respeito.

Finalmente, a Resolução do Conselho de Ministros n.º 41/2018, contém requisitos técnicos mínimos aplicáveis à Administração direta e indireta do Estado, servindo como modelo para o setor privado.

O Município de Vila Velha de Rodão tem como objetivo assegurar o cumprimento de todas as disposições legais que lhe são aplicáveis no contexto da proteção de dados.

Neste sentido, o presente documento oferece as cláusulas-tipo de proteção de dados, conforme adotadas pela Autoridade de Controlo Dinamarquesa e revistas pelo Comité Europeu de Proteção de Dados, com acrescento das disposições constantes na Resolução do Conselho de Ministros n.º 41/2018, relativas aos requisitos técnicos mínimos das redes e sistemas de informação que são exigidos ou recomendados a todos os serviços e entidades da Administração direta e indireta do Estado, servindo também como um modelo para o setor empresarial do Estado e para o setor privado.

CLAUSULADO-TIPO CONTRATUAL

Para os fins definidos no Artigo 28, n.º 3 do Regulamento 2016/679 (RGPD)

Entre o

Município de Vila Velha de Ródão

NIPC 506.642.798

Rua Santana,

6030-230 Vila Velha de Rodão

(o responsável pelo tratamento)

E a

Infracontrol – ICP Infraestruturas Control Portugal Lda

NIPC 513137653

Rua Tenente Valadim N.º17 2.ºF

2560-275 Torres Vedras

(o subcontratante)

Designadas como “parte”; no seu conjunto como “as partes”

CONCORDAM nas seguintes cláusulas contratuais (as cláusulas) de modo a cumprir os requisitos do RGPD e assegurar a proteção dos direitos do titular de dados.

1. Preâmbulo

1. Estas cláusulas contratuais (as cláusulas) estipulam os direitos e obrigações do responsável pelo tratamento bem como do subcontratante, quando este trata dados pessoais em nome do responsável pelo tratamento.
2. As cláusulas foram desenhadas para assegurar a conformidade das partes relativamente ao Art.28º, n. º3 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados - RGPD).
3. No contexto do fornecimento de software como serviços, bem como apoio técnico e manutenção preventiva e corretiva do respetivo software, o subcontratante irá processar dados pessoais em nome do responsável pelo tratamento, de acordo com as cláusulas.
4. As cláusulas devem ser prioritárias face a quaisquer outras disposições contidas em acordos entre as partes.
5. Dois Anexos são adicionados às cláusulas e são parte integrante das mesmas.
6. O Anexo A contém detalhes relativamente ao tratamento de dados pessoais, incluindo as finalidades e a natureza do tratamento, tipo de dados pessoais, categorias de titulares de dados e duração do tratamento.
7. O Anexo B contém as instruções do responsável pelo tratamento relativamente ao tratamento de dados pessoais, as medidas de segurança mínimas que devem ser implementadas pelo subcontratante e como as auditorias do subcontratante e de outros subcontratantes ulteriores devem ser realizadas.
8. As cláusulas, bem como os anexos, devem ser mantidos na forma escrita, incluindo a forma eletrónica, pelas partes.

9. As cláusulas não isentam o subcontratante de obrigações a que este esteja sujeito relativamente ao RGPD ou outra legislação.

2. Os direitos e obrigações do responsável pelo tratamento

1. O responsável pelo tratamento é responsável por assegurar que o tratamento de dados pessoais se encontra em conformidade com o RGPD (ver Art.24º do RGPD), com as disposições de proteção de dados europeias ou dos Estados-Membros que lhe sejam aplicáveis e com as cláusulas.

2. O responsável pelo tratamento tem o direito e a obrigação de tomar decisões sobre as finalidades e os meios do tratamento de dados pessoais.

3. O responsável pelo tratamento deverá ser responsável, entre outros, por assegurar que o tratamento de dados pessoais que é realizado pelo subcontratante em seu nome, através de instruções definidas por si, tem um fundamento legal.

3. O subcontratante atua de acordo com instruções

1. O subcontratante deve tratar dados pessoais apenas mediante instruções documentadas fornecidas pelo responsável pelo tratamento, a menos que tal seja requerido pela legislação aplicável ao subcontratante. Tais instruções devem ser especificadas nos Anexos A e B. Instruções posteriores podem ser fornecidas pelo responsável pelo tratamento durante o tratamento de dados pessoais, mas tais instruções deverão sempre ser documentadas e mantidas na forma escrita, incluindo o formato eletrónico, em relação com as cláusulas.

2. O subcontratante deverá imediatamente informar o responsável pelo tratamento se as instruções fornecidas pelo responsável pelo tratamento, na opinião do subcontratante, contrariam o RGPD ou outra disposição legal aplicável relativa à proteção de dados.

3. No caso de se verificar a emissão de instruções potencialmente desconformes fornecidas pelo responsável pelo tratamento, sendo estas identificadas pelo

subcontratante, este deve proceder a uma comunicação relativamente a este facto ao responsável pelo tratamento, para que este possa proceder à sua retificação. Caso este facto não seja identificado pelo subcontratante ou pelo responsável pelo tratamento, mas sim por terceiros, as mesmas serão consideradas inválidas no momento da sua identificação, tendo efeitos retroativos. As partes deverão acordar entre si quais serão as ações necessárias a tomar, atendendo à situação contextual.

4. Confidencialidade

8

1. O subcontratante deverá conceder acesso a dados pessoais tratados em nome do responsável pelo tratamento a pessoas que estejam sob a autoridade do subcontratante que se tenham comprometido a assegurar a confidencialidade ou estejam sob estatutos apropriados que garantam o dever de sigilo e confidencialidade, seguindo o princípio da necessidade de conhecer. A lista de pessoas a quem o acesso foi concedido deverá ser alvo de revisão periódica. Nesta revisão, o acesso a dados pessoais pode ser removido, se tal acesso não for mais necessário, sendo que tais dados pessoais consequentemente não deverão ser mais acessíveis a tais pessoas.

2. O subcontratante deverá, a pedido do responsável pelo tratamento, demonstrar que as pessoas sob sua autoridade estão sujeitas à obrigação de confidencialidade e sigilo.

5. Segurança do tratamento

1. O Art.32º do RGPD estipula que, considerando o estado da arte, os custos da implementação e a natureza, âmbito, contexto e finalidades do tratamento, bem como o risco de probabilidade e gravidade variável para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante deverão implementar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança apropriado ao risco.

O responsável pelo tratamento deverá avaliar os riscos para os direitos e liberdades das pessoas singulares inerentes ao tratamento e implementar medidas para mitigar tais riscos.

Dependendo da sua relevância, as medidas podem incluir:

- a. Pseudonimização e 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. De acordo com o Art.32º do RGPD, o subcontratante deverá também – independentemente do responsável pelo tratamento – avaliar os riscos para os direitos e as liberdades das pessoas singulares inerentes ao tratamento e implementar medidas para mitigar tais riscos. Para este efeito, o responsável pelo tratamento deverá fornecer ao subcontratante toda a informação necessária para identificar e avaliar tais riscos.
3. O subcontratante deverá auxiliar o responsável pelo tratamento a garantir a conformidade com as obrigações do responsável pelo tratamento no que ao Art.32º do RGPD diz respeito por, nomeadamente, fornecer ao responsável pelo tratamento informação relativa a medidas técnicas e organizativas já implementadas pelo subcontratante no cumprimento deste mesmo artigo, bem como outra informação necessária para que o responsável pelo tratamento esteja em conformidade com as suas obrigações no cumprimento do já citado Art.32º do RGPD.

Se subsequentemente – na avaliação realizada pelo responsável pelo tratamento – a mitigação dos riscos identificados requerer medidas adicionais a serem aplicadas pelo subcontratante, além das que já foram implementadas pelo mesmo no cumprimento do Art.32º do RGPD, o responsável pelo tratamento deverá especificar tais medidas adicionais a serem implementadas no Anexo B.

6. Recurso a subsubcontratantes

10

1. O subcontratante deverá cumprir os requisitos especificados no Art.28º, n.º 2 e n.º 4 do RGPD quando contratar outro subcontratante (um subsubcontratante).
2. O subcontratante não deverá, portanto, contratar outro subcontratante (um subsubcontratante) para o cumprimento das cláusulas sem a prévia autorização geral escrita do responsável pelo tratamento.
3. O subcontratante tem uma autorização geral escrita para contratar subsubcontratantes. O subcontratante deverá informar, por escrito, o responsável pelo tratamento de quaisquer mudanças relativamente quanto ao aumento do número ou à substituição de outros subcontratantes pelo menos com a antecedência de 30 dias, fornecendo assim ao responsável pelo tratamento a possibilidade de se opor a tais alterações antes de os subsubcontratantes serem contratados.
4. Quando o subcontratante contratar um subsubcontratante para realizar um atividades de tratamento de dados específicas em nome do responsável pelo tratamento, as mesmas obrigações relativas à proteção de dados, conforme definidas nas cláusulas, devem ser impostas a esse mesmo subsubcontratante, sob a forma de um contrato ou outro ato legal conforme o direito europeu ou lei de Estado-Membro, em particular fornecendo garantias suficientes para implementar medidas técnicas e organizativas adequadas, de um modo que o tratamento cumpra os requisitos das cláusulas e do RGPD.

O subcontratante deverá, portanto, ser responsável para requerer que esse subsubcontratante pelo menos cumpra com as obrigações às quais o subcontratante se encontra sujeito relativamente às cláusulas e ao RGPD.

5. Uma cópia de tal acordo com o subsubcontratante e as subsequentes adendas deverão – face a um pedido do responsável pelo tratamento – ser submetidas ao responsável pelo tratamento, oferecendo-lhe assim a oportunidade de assegurar que as mesmas obrigações no contexto da proteção de dados definidas nas cláusulas são impostas ao subsubcontratante. Cláusulas relacionadas com questões de negócio que não afetem o conteúdo legal relativo a proteção de dados do acordo com o subsubcontratante não são submetidas para envio ao responsável pelo tratamento.

6. O subcontratante deverá realizar um contrato a favor de terceiro com o subsubcontratante onde – no caso da falência do subcontratante – o responsável pelo tratamento deverá ser a parte beneficiária do contrato com o subsubcontratante e deverá ter o direito a fazer cumprir o contrato com o subsubcontratante em que o subcontratante era parte, por exemplo, permitindo ao responsável pelo tratamento a instruir o subsubcontratante a eliminar ou devolver dados pessoais que eram objeto do contrato referido.

7. Caso o subsubcontratante não cumpra as suas obrigações no contexto da proteção de dados, o subcontratante deverá ser plenamente responsável face ao responsável pelo tratamento no que diz respeito ao cumprimento das obrigações do subsubcontratante. Isto não afeta os direitos dos titulares de dados no que ao RGPD diz respeito - em particular os que se encontram previstos nos Artigos 79.º e 82.º do RGPD – face ao responsável pelo tratamento e subcontratante, incluindo o subsubcontratante.

7. Transferências de dados pessoais para países terceiros ou organizações internacionais

1. Qualquer transferência de dados pessoais para países terceiros ou organizações internacionais pelo subcontratante deverão apenas ocorrer tendo por base instruções documentadas do responsável pelo tratamento e deverão sempre ser realizadas em conformidade com o Capítulo V do RGPD.
2. No caso de transferências para países terceiros ou organizações internacionais, realizadas pelo subcontratante sem instruções documentadas por parte do responsável pelo tratamento, que são requeridas pelo direito da União ou de Estado-Membro a que o subcontratante se encontre sujeito, o subcontratante deverá informar o responsável pelo tratamento dessa obrigação jurídica antes de iniciar o tratamento, a menos que essa lei proíba tal informação tendo por base motivos de interesse público.
3. Sem instruções documentadas por parte do responsável pelo tratamento, o subcontratante não pode, no âmbito das cláusulas:
 - a. transferir dados pessoais para outro responsável pelo tratamento ou para um subcontratante num país terceiro ou numa organização internacional;
 - b. transferir o tratamento de dados pessoais para um subsubcontratante num país terceiro;
 - c. ter dados pessoais tratados por si num país terceiro.
4. As instruções do responsável pelo tratamento relativas à transferência de dados pessoais para um país terceiro incluindo, se aplicável, o mecanismo de transferência previsto no Capítulo V do RGPD no qual são baseadas, deverão ser definidas no Anexo B.6.
5. As cláusulas não devem ser confundidas com cláusulas standard de proteção de dados conforme o significado do Art.46º, n.º 2, al. c) e d) do RGPD e as cláusulas não podem ser encaradas pelas partes como um mecanismo de transferência previsto no Capítulo V do RGPD.

8. Assistência ao responsável pelo tratamento

1. Considerando a natureza do tratamento, o subcontratante deverá auxiliar o responsável pelo tratamento por medidas técnicas e organizativas adequadas, na medida do possível. No cumprimento das obrigações do responsável pelo tratamento para responder aos pedidos relativos ao exercício de direitos dos titulares de dados descritos no Capítulo III do RGPD.

Isto implica que o subcontratante deverá, na medida do possível, prestar assistência ao responsável pelo tratamento na conformidade com:

- a. o direito a ser informado quando haja recolha de dados pessoais do titular dos dados;
- b. o direito a ser informado quando dados pessoais não tenham sido recolhidos junto do titular dos dados;
- c. o direito do acesso do titular de dados;
- d. o direito de retificação;
- e. o direito ao apagamento dos dados ("direito a ser esquecido");
- f. o direito à limitação do tratamento;
- g. a obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento;
- h. o direito de portabilidade dos dados;
- i. o direito de oposição;
- j. o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis.

2. O subcontratante deverá, considerando a natureza do tratamento e a informação disponível para o subcontratante, prestar assistência ao responsável pelo tratamento, de modo a assegurar conformidade com:

- a. A obrigação do responsável pelo tratamento para, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, notificar a violação de dados pessoais à autoridade de controlo competente, nomeadamente a Comissão Nacional de Proteção de Dados (CNPd), a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares
- b. A obrigação do responsável pelo tratamento para, sem demora injustificada, comunicar a violação de dados pessoais ao titular dos dados, quando esta for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares;
- c. A obrigação do responsável pelo tratamento de realizar uma Avaliação de Impacto sobre a Proteção de Dados relativamente a um determinado tratamento;
- d. A obrigação do responsável pelo tratamento de consultar a autoridade de controlo competente, nomeadamente a CNPD, antes de iniciar o tratamento quando uma Avaliação de Impacto sobre a Proteção de Dados indicar que o tratamento resultaria num risco elevado na ausência de medidas implementadas pelo responsável pelo tratamento para mitigar o risco.

3. As partes deverão definir no Anexo B as medidas técnicas e organizativas adequadas pelas quais o subcontratante é requerido a prestar assistência ao responsável pelo tratamento, bem com o âmbito e extensão da assistência requerida. Tal aplica-se a todas as obrigações previstas nas cláusulas 8.1. e 8.2.

9. Notificação de uma violação de dados pessoais

1. O subcontratante notifica o responsável pelo tratamento sem demora injustificada após ter conhecimento de uma violação de dados pessoais.

2. A notificação do subcontratante ao responsável pelo tratamento deverá, se possível, ser realizada até 48 horas depois de o subcontratante ter tomado conhecimento da violação de dados pessoais, de modo a permitir ao responsável pelo tratamento cumprir com a sua obrigação de notificar a violação de dados pessoais à autoridade de controlo competente, conforme o Art.33º do RGPD.

3. De acordo com a cláusula 8.2, al. a), o subcontratante deverá prestar assistência ao responsável pelo tratamento na notificação da violação de dados à autoridade de controlo competente, significando tal que o subcontratante deverá prestar assistência na obtenção de informação listada abaixo, a qual, em conformidade com o Art.33, n.º 3 do RGPD, deverá constar na notificação submetida à autoridade de controlo competente:

- a. 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. As consequências prováveis da violação de dados pessoais;
- c. As medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.

10. Apagamento e devolução de dados

1. Depois de concluída a prestação de serviços relacionados com o tratamento de dados pessoais, o subcontratante é obrigado a devolver todos os dados pessoais ao responsável pelo tratamento e a eliminar as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros.

2. Caso o direito da União ou dos Estados-Membros aplicável ao subcontratante requeira o armazenamento de dados pessoais depois do término da prestação de serviços de tratamento de dados pessoais, este poderá manter esta informação apenas para as finalidades determinadas na lei.

O subcontratante compromete-se a tratar exclusivamente os dados pessoais para as finalidades e duração indicadas pelas disposições legais suprarreferidas e estritamente considerando as condições aplicáveis.

11. Auditoria e inspeção

1. O subcontratante deverá disponibilizar ao responsável pelo tratamento toda a informação necessária para demonstrar conformidade com as obrigações dispostas no Art.28º do RGPD, bem como com as cláusulas, e permitir e contribuir para as auditorias, incluindo inspeções, conduzidas pelo responsável pelo tratamento ou outro auditor por si mandatado.

2. Os procedimentos aplicáveis para as auditorias do responsável pelo tratamento, incluindo inspeções, do subcontratante e dos subsubcontratantes são especificadas nos Anexos B.7. e B.8.

3. O subcontratante deverá ser requerido a fornecer às autoridades de controlo, que no cumprimento da legislação aplicável têm acesso às instalações do responsável pelo tratamento e do subcontratante, ou a representantes que atuam em nome da autoridade de controlo, acesso às instalações físicas do subcontratante mediante a apresentação de identificação adequada.

12.Acordo entre as partes relativamente a outros termos

1. As partes podem acordar outras cláusulas relativamente ao tratamento de dados pessoais especificando, por exemplo, responsabilidade, desde que estas não contrariem

direta ou indiretamente as cláusulas ou prejudicam os direitos ou liberdades fundamentais do titular de dados e a proteção oferecida pelo RGPD.

13.Início e término

1. As cláusulas entram em vigor na data de assinatura das partes.
2. As partes podem requerer que as cláusulas sejam renegociadas se alterações a disposições legais ou a inadequação das cláusulas der azo a renegociação.
3. As cláusulas deverão ser aplicadas durante o período de tratamento de dados pessoais. Durante o período de tratamento de dados pessoais, as cláusulas não podem ser cessadas a menos que outras cláusulas tenham sido acordadas entre as partes relativamente à governação do tratamento de dados pessoais.
4. Se a prestação de serviços relativamente ao tratamento de dados pessoais cessar e os dados pessoais forem eliminados ou devolvidos ao responsável pelo tratamento conforme a cláusula 10.1 e o Anexo B.4., as cláusulas podem ser cessadas mediante aviso escrito por cada uma das partes.

5. Assinatura

Da parte do responsável pelo tratamento

Nome [Luís Miguel Ferro Pereira]

Posição [Presidente da Câmara]

Data [DATA]

Assinatura [ASSINATURA]

Da parte do subcontratante

Nome [NOME]

Posição [POSIÇÃO]

Data [DATA]

Assinatura [ASSINATURA]

14. Pontos de contacto do responsável pelo tratamento e do subcontratante

1. As partes podem entrar em contacto utilizando os pontos de contacto abaixo discriminados.
2. As partes deverão ser obrigadas a informar continuamente a outra de alterações aos pontos de contacto existentes.

Responsável pelo tratamento

Nome [NOME]

Posição [POSIÇÃO]

Telefone [TELEFONE]

E-mail [E-MAIL]

Subcontratante

Nome [NOME]

Posição [POSIÇÃO]

Telefone [TELEFONE]

E-mail [E-MAIL]

ANEXO A: INFORMAÇÃO SOBRE O TRATAMENTO

A.1. A finalidade do tratamento realizado pelo subcontratante em nome do responsável pelo tratamento é:

O fornecimento de apoio técnico e manutenção preventiva e corretiva do software, onde se incluem as versões para as diferentes plataformas.

A.2. O tratamento de dados pessoais realizado pelo subcontratante em nome do responsável pelo tratamento deverá maioritariamente limitar-se a (natureza do tratamento):

Fornecer serviços de apoio técnico e manutenção preventiva ou corretiva do software, podendo para tal aceder a todos os dados pessoais que se encontrem na base de dados partilhada pelos diversos módulos aplicativos do software em questão.

Estes serviços de apoio técnico e manutenção preventiva ou corretiva incluem:

- Adaptação das aplicações às alterações legislativas e regulamentares, desde que estas não obriguem à reformulação total do software;
- Detecção e correção de erros ou anomalias verificadas no funcionamento do software;
- Fornecimento de versões do software atualizadas e aperfeiçoadas;
- Adaptação do software às condições concretas de utilização na Câmara;
- Reinstalação e teste do software devido a alterações da versão do sistema operativo e de outros ambientes de apoio de software;
- Apoio aos utilizadores na boa operação do software;
- Apoio aos administradores de sistema na gestão do software;
- Apoio à elaboração de planos de formação;
- Apoio à elaboração do ambiente de hardware, software de base e comunicações;

A.3. O tratamento inclui os seguintes tipos de dados pessoais relativamente aos titulares dos dados:

Todos os dados pessoais incluídos na base de dados no software podem ser alvo de tratamento, onde se incluem: Nome, e-mail, número de telefone, morada, n.º do Cartão de Cidadão, NIF.

A.4. O tratamento inclui as seguintes categorias de titulares dos dados:

Relativamente à plataforma de participações municipais, os titulares dos dados são munícipes ou quaisquer titulares que interajam com o município.

A.5. O tratamento de dados pessoais realizado pelo subcontratante em nome do responsável pelo tratamento poderá ser realizado quando as cláusulas tenham início. O tratamento tem a seguinte duração:

O tratamento de dados pessoais realiza-se durante o período do contrato em vigência. Findo esse período, e caso essa devolução não seja realizada anteriormente, os dados pessoais devem ser devolvidos ao responsável pelo tratamento.

ANEXO B: INSTRUÇÃO RELATIVA AO TRATAMENTO DE DADOS PESSOAIS

B.1. Objecto de instrução de tratamento

O tratamento de dados pessoais realizado pelo subcontratante em nome do responsável pelo tratamento deverá ser realizado pelo subcontratante na execução das seguintes atividades:

- fornecimento de apoio técnico e manutenção preventiva e corretiva do software.

B.2. Segurança do tratamento

O nível de segurança deverá ter em consideração:

- o elevado número de dados pessoais, que podem incluir dados pessoais constantes no art.9º do RGPD ou outros de natureza altamente sensível, que incluem a caracterização socioeconómica e familiar dos titulares dos dados;
- o tratamento de dados de trabalhadores, considerados sujeitos particularmente vulneráveis.

Como tal, um nível de segurança elevado deve ser definido.

O subcontratante deverá ser intitulado e ter a obrigação de tomar decisões relativas a medidas de segurança técnicas e organizativas que são aplicadas (e alvo de acordo) para implementar um nível de segurança adequado.

O subcontratante deverá, no entanto, - face a qualquer evento e num mínimo – implementar as seguintes medidas que foram alvo de acordo com o responsável pelo tratamento:

- Sempre que solicitado pelo responsável pelo tratamento, a realização de trabalho remoto deve ser realizada apenas após permissão do responsável pelo tratamento

para acesso aos sistemas de informação, devendo existir um registo da atividade associada.

Adicionalmente, deverão ser cumpridos os seguintes requisitos:

Requisitos técnicos mínimos das redes e sistemas de informação (conforme a Resolução de Ministros n.º 41/2018)

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
As aplicações cliente (exemplo, <i>Android</i> , <i>IOS</i> , <i>WEB</i>) devem ser desenvolvidas adotando práticas de desenvolvimento seguro	FE	Seguir as boas práticas de desenvolvimento. Exemplo: <i>Open Web Application Security Project</i> (OWASP), no que respeita ao desenvolvimento de código seguro e de submissão desse código a testes de segurança.	Obrigatório.	Obrigatória
	FE	Utilização de sessões seguras com protocolo de Segurança.	Obrigatório.	Obrigatória
	FE	Recomenda-se o uso de <i>Transport Layer Security</i> (TLS), na sua versão mais recente.	Recomendado.	Facultativa
	FE	Não guardar informação pessoal no browser, memória ou disco, para além do tempo da sessão e apenas na medida do necessário.	Obrigatório.	Obrigatória
	App	Utilização de sessões seguras com protocolo de Segurança.	Obrigatório.	Obrigatória
	App	Recomenda-se o uso de TLS, na sua versão mais recente, na comunicação com as camadas adjacentes.	Recomendado.	Obrigatória
	App	Se possível usar certificados através de <i>Application Programming Interface</i> (API), não sendo desta forma necessário o uso de palavras-passe.	Recomendado.	Facultativa

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
	App	Não é permitida a utilização de credenciais em <i>plain text</i> , quer no código quer em ficheiros de configuração	Recomendado.	Obrigatória
	App	Deve ser evitado palavras-passe embebidas no código.	Recomendado.	Obrigatória
	App	As credenciais que necessitem de ser armazenadas em ficheiros de configuração devem estar codificadas (HASH — mínimo SHA 256).	Recomendado.	Facultativa
	BD	Comunicação com camada aplicacional através de autenticação por certificado válido por período não superior a 2 anos, no caso de as camadas serem física ou logicamente distintas. Exemplo: padrão X.509, da ITU-T para Infraestruturas de Chaves Públicas (ICP)	Obrigatório.	Obrigatória
	BD	Prever cifra de informação pessoal (recomenda-se mínimo 2048 bit) apenas se a aplicação cliente tiver camada de BD física e logicamente distinta, usando preferencialmente tecnologia que permita interoperabilidade entre sistemas.	Obrigatório.	Obrigatória
Capacidade para autenticar e autorizar	FE	O processo de autenticação deve ser sempre iniciado e mantido em sessão segura.	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
todos os utilizadores e dispositivos, incluindo o controlo do acesso a sistemas e aplicações	FE	Recomenda-se: 1) o uso de TLS, na sua versão mais recente; ou 2) o uso de palavra-passe, preferencialmente em combinação com outro fator (<i>Double Factor Authentication-2FA</i>), como por exemplo: Palavra-passe + SMS Token Palavra-passe + <i>Smartcard</i> Palavra-passe + Biometria Palavra-passe + padrão gráfico Palavra-passe + Cartão de coordenadas Palavra-passe + código aleatório temporário (menos de 5 minutos de validade) enviado na forma de QR-Code.	Recomendado.	Facultativa
	FE	Dados pessoais de sessão excluídos das variáveis <i>Uniform Resource Locator</i> (URL) ou de outras variáveis visíveis ao utilizador.	Obrigatório.	Obrigatória
	FE	Credenciais de início de sessão transmitidos através do seu HASH, mínimo <i>Secure Hash Algorithm-256</i> (SHA-256), ou utilização de cifra ou codificação para a transmissão de dados pessoais (nome do utilizador e palavra-passe em HASH e restantes dados cifrados).	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
	FE	Sempre que aplicável, a palavra-passe deve ter no mínimo 9 caracteres (13 caracteres para utilizadores com acesso privilegiado) e ser complexa. A sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a...z), letras maiúsculas (A...Z), números (0...9) e caracteres especiais (~ ! @ # \$ % ^ & * () _ + ` - = \ { } [] : " ; ' < > ? , . /). Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem carácter de «espaço».	Obrigatório.	Obrigatória
	FE	Recomenda-se que para novos sistemas seja sempre usado como padrão de autenticação o 2FA.	Recomendado.	Facultativa
	App	A palavra-passe dos administradores deve ter no mínimo 13 caracteres e ser complexa. Neste caso, a sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a...z), letras maiúsculas (A...Z), números (0...9) e caracteres especiais (~ ! @ # \$ % ^ & * () _ + ` - = \ { } [] : " ; ' < > ? , . /). Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem carácter de «espaço».	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
	App	Para todos os administradores deve-se utilizar Padrão de autenticação 2FA: Exemplos: Palavra-passe + <i>Smartcard</i> Palavra-passe + Biometria Palavra-passe + certificado (por exemplo X.509, da ITU-T para ICP, válido por período não superior a 2 anos).	Obrigatório.	Obrigatória
	App	Como mecanismo de proteção e segurança da informação recomenda-se o uso de <i>Token</i> .	Recomendado.	Facultativa
	App	Comunicação com camadas FE ou BD através de sessão segura, com prévia autenticação se camadas forem física ou logicamente distintas.	Obrigatório.	Obrigatória
	App	Deve ser evitado palavras-passe embebidas no código. Quando tal não for possível, devem estar codificadas (HASH, mínimo SHA-256).	Recomendado.	Facultativa
	App	Se possível, usar certificados através de API, não sendo desta forma necessário o uso de palavras-passe.	Recomendado.	Facultativa

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
	App	Autenticação de elementos comunicantes garantida por validação de informação estática ao nível da rede. Exemplos: 1) utilização de IP fixo + <i>hostname</i> + <i>MacAddress</i> + fatores de autenticação, ou 2) Utilização de certificados.	Obrigatório.	Obrigatória
	BD	A palavra-passe deve ter no mínimo 13 caracteres e ser complexa. Neste caso, a sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a...z), letras maiúsculas (A...Z), números (0...9) e caracteres especiais (~ ! @ # \$ % ^ & * () _ + ` - = \ { } [] : " ; ' < > ? , . /). Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem carácter de «espaço».	Obrigatório.	Obrigatória
	BD	Dados pessoais de autenticação, transmitidos através do seu HASH (mínimo SHA-256), ou recorrendo à cifra ou codificação para efetuar essa transmissão.	Recomendado.	Facultativa
	FE	Criação de perfis com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (<i>Create</i> , <i>Read</i> , <i>Update</i> , <i>Delete</i> — CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Obrigatória
Atribuição de direitos de acesso e privilégio de forma restrita e controlada				

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
	FE	Criação de registo de acesso, alteração e remoção (<i>logs</i>), com informação sobre quem acedeu, de onde acedeu (IP e Porto), quando acedeu, a que dados acedeu, que ação foi efetuada sobre os mesmos (CRUD).	Obrigatório.	Obrigatória
	App	Criação perfis com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Obrigatória
	App	Criação de registo de acesso, alteração e remoção (<i>logs</i>) com informação sobre quem acedeu, de onde acedeu (IP e Porto), quando acedeu, a que dados acedeu, que ação foi efetuada sobre os mesmos (CRUD).	Obrigatório.	Obrigatória
	BD	Criação perfis com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Obrigatória
	BD	Criação de registo de acesso, alteração e remoção (<i>logs</i>), com informação sobre quem acedeu, de onde acedeu (IP e Porto), quando acedeu, a que dados acedeu, que ação foi efetuada sobre os mesmos (CRUD).	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
Atribuição das credenciais de acesso de forma controlada através de um processo formal de gestão do respetivo ciclo de vida	FE	Processo definido de acordo com a política de «Atribuição de direitos de acesso e privilégio de forma restrita e controlada».	Obrigatório.	Obrigatória
	FE	Atribuição de credenciais de acesso efetuada de forma a permitir a sua auditoria, sem permitir outro acesso que não o do destinatário da informação. Exemplo: Envio de informação de autenticação por SMS com validade limitada (não superior a 5 minutos), com primeiro acesso a implicar sempre a redefinição da informação enviada; Envio de informação de autenticação gerada automática e aleatoriamente, enviada por Envelope (semelhante ao do envio de dados do Cartão de Cidadão).	Obrigatório.	Obrigatória
	App	Processo definido de acordo com a política de «Atribuição de direitos de acesso e privilégio de forma restrita e controlada».	Obrigatório.	Obrigatória
	App	Atribuição de credenciais de acesso efetuada de forma a permitir a sua auditoria, sem permitir outro acesso que não o do destinatário da informação.	Obrigatório.	Obrigatória
	BD	Processo definido de acordo com a política de «Atribuição de direitos de acesso e privilégio de forma restrita e controlada».	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
Revisão de direitos de acesso de utilizadores em intervalos regulares	BD	Atribuição de credenciais de acesso efetuada de forma a permitir a sua auditoria, sem permitir outro acesso que não o do destinatário da informação.	Obrigatório.	Obrigatória
	FE	Processo de renovação de conta do utilizador de acordo com os mesmos requisitos de segurança da criação do mesmo, não devendo ter um ciclo de vida superior a 180 dias.	Obrigatório.	Obrigatória
	FE	A gestão do ciclo de vida da conta do utilizador deve ter em conta a segregação das funções existentes e os privilégios de acesso que devem estar associados a essas funções, em cada momento (privilégios mínimos, onde cada tipo de conta é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Obrigatória
	FE	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Facultativa
	FE	Deve ser desativada uma conta de utilizador quando o mesmo não tem atividade sobre a conta durante 3 meses.	Recomendado.	Facultativa
	App	Processo de gestão de validade de perfis.	Obrigatório.	Obrigatória
	App	Processo de gestão de validade de perfis automatizado.	Recomendado.	Facultativa

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
	App	Processo automatizado ou interoperável com sistemas responsáveis pela gestão das funções associados aos privilégios atribuídos a cada perfil. Em casos de verificação assíncrona do binómio função/privilégios, a mesma deve ocorrer com uma periodicidade, no máximo bimestral ou quando se verifique uma alteração no mapa de pessoal associado a esta função.	Obrigatório.	Obrigatória
	App	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Facultativa
	BD	Processo de gestão de validade de perfis.	Obrigatório.	Obrigatória
	BD	Processo de gestão de validade de perfis automatizado.	Recomendado.	Facultativa
	BD	Processo automatizado ou interoperável com sistemas responsáveis pela gestão das funções associados aos privilégios atribuídos a cada perfil. Em casos de verificação assíncrona do binómio função/privilégios, a mesma deve ocorrer com uma periodicidade, no máximo bimestral ou quando se verifique uma alteração no mapa de pessoal associado a esta função.	Obrigatório.	Obrigatória
	BD	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Facultativa

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
Capacidade para garantir que os utilizadores fazem uma utilização correta dos dados	FE	A gestão do ciclo de vida da conta do utilizador deve ter em conta a segregação das funções existentes e os privilégios de acesso que devem estar associados a essas funções, em cada momento (privilégios mínimos, onde cada tipo de conta de utilizador é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Obrigatória
	FE	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Facultativa
	FE	Ação dos utilizadores sobre dados pessoais (CRUD) deve permitir a sua auditoria em registo de atividade (<i>logs</i>).	Obrigatório.	Obrigatória
	App	Para Administradores de Sistemas, Redes e Aplicacional, caso acedam a dados pessoais, aplicam-se os requisitos da camada FE.	Obrigatório.	Obrigatória
	App	Processo de gestão de validade de contas de utilizadores.	Obrigatório.	Obrigatória
	App	Processo de gestão de validade de contas de utilizadores automatizado.	Recomendado.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
	App	Processo automatizado ou interoperável com sistemas responsáveis pela gestão das funções associados aos privilégios atribuídos a cada perfil. Em casos de verificação assíncrona do binómio função/privilégios, a mesma deve ocorrer com uma periodicidade limitada.	Obrigatório.	Obrigatória
	App	Recomenda-se: 1) uma periodicidade bimestral; ou 2) quando se verifique uma alteração no mapa de pessoal associado a esta função.	Recomendado.	Facultativa
	App	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Facultativa
	BD	Para Administradores de Bases de Dados, Administradores de Sistemas, de Redes e Aplicacional, caso acedam a dados pessoais, aplicam-se os requisitos da camada FE.	Obrigatório.	Obrigatória
	BD	Processo de gestão de validade das contas dos utilizadores.	Obrigatório.	Obrigatória
	BD	Processo de gestão de validade das contas dos utilizadores automatizado.	Recomendado.	Facultativa
	BD	Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.	Facultativa

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
Restrição de acesso à informação baseado no princípio necessidade de conhecer (criação de perfil)	FE	Associação da tipologia de dados a perfis específicos, individuais e associados à função, com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Obrigatória
	App	Associação da tipologia de dados a perfis específicos, individuais e associados à função, com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Obrigatória
	App	Processo de registo de tentativas de acesso a dados excluídos dos privilégios associados ao perfil (qualquer perfil, incluindo o dos administradores), com alarmística a partir de um determinado número de tentativas (por exemplo, 3 tentativas), a notificar ao encarregado da proteção de dados da organização.	Obrigatório.	Obrigatória
	BD	Associação da tipologia de dados a perfis específicos, individuais e associados à função, com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.	Obrigatória

Requisito geral		Área	Requisitos Específicos	Classificação	Implementação
		BD	Processo de registo de tentativas de acesso a dados excluídos dos privilégios associados ao perfil (qualquer perfil, incluindo o dos administradores), com alarmística a partir de um determinado número de tentativas (por exemplo, 3 tentativas), a notificar ao encarregado da proteção de dados da organização.	Obrigatório.	Obrigatória
			Aplicam-se as mesmas disposições que em «Capacidade para garantir que os utilizadores fazem uma utilização correta dos dados» e «Revisão de direitos de acesso de utilizadores em intervalos regulares».	Obrigatório.	Obrigatória
Procedimentos seguros de início de sessão			Aplicam-se as mesmas disposições referidas em «Capacidade para autenticar e autorizar todos os utilizadores e dispositivos, incluindo o acesso controlado por um procedimento seguro de início de sessão».	Obrigatório.	Obrigatória
Capacidade de monitorização, registo e análise de toda a atividade de acessos de modo a procurar ameaças prováveis			Deve ser guardado registo de atividade (<i>log</i>) de todas as ações que um utilizador efetue sobre dados pessoais, independentemente do seu perfil e função.	Obrigatório.	Obrigatória
			Todos os registos de atividade (<i>log</i>) devem ser armazenados apenas em modo de leitura, devendo, com uma periodicidade máxima de 1 mês, ser englobados num único bloco de registos e assinado digitalmente (garantia de integridade).	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
		Deve ser guardado registo de atividade (<i>log</i>) de todos os acessos e tentativas falhadas de acesso, obedecendo aos requisitos anteriores.	Obrigatório.	Obrigatória
		Garantir que os registos de atividade provenientes dos diversos subsistemas (Sistemas Operativos, aplicações, <i>browsers</i> , Sistema de Gestão de Base de Dados — SGBD, etc.) são inequivocamente associados à sua origem.	Obrigatório.	Obrigatória
		Os registos de atividade (<i>log</i>) devem conter, no mínimo, o endereço de acesso (IP e Porto), Host, HASH da conta do utilizador que efetuou a ação, ação efetuada (CRUD), Tipo de Dado Pessoal onde a ação foi efetuada, data/hora/minuto/segundo (<i>TimeStamp</i>) da ação, alteração efetuada sobre o dado pessoal.	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
Inspeção automática dos conteúdos para procurar dados sensíveis e acessos remotos ao sistema a partir do exterior do ambiente organizacional		Tendo em vista garantir que a entidade responsável pelo tratamento de dados deve definir e implementar mecanismos de proteção da informação em função da sua relevância e criticidade, deve ser implementado: Deteção de ameaças na defesa perimétrica do sistema (por exemplo, regras definidas na <i>firewall</i>, <i>Intrusion Detection System</i> — IDS, etc.); Extensão desta proteção desejavelmente a todos os dispositivos (incluindo móveis) com acesso a dados pessoais nos sistemas corporativos; Mecanismo de cifra ponto a ponto sempre que houver necessidade de aceder remotamente ao FE (e apenas a esta camada), como por exemplo com recurso à tecnologia <i>Virtual Private Network</i> (VPN).	Obrigatório.	Obrigatória
	FE	FE desenvolvido e em produção de acordo com as melhores práticas de segurança, garantindo a proteção desta camada aos ataques mais comuns (SQLi, injeção de código, etc.).	Obrigatório.	Obrigatória
	FE	Recomenda-se as práticas recomendadas em <i>Open Web Application Security Project</i> (OWASP).	Recomendado.	Obrigatória
	FE	Aplicam-se as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
		acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.		
	App	Camada aplicacional segregada da rede ou ambiente com visibilidade e/ou acesso exterior.	Obrigatório.	Obrigatória
	App	Aplicam-se as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.	Obrigatório.	Obrigatória
	BD	Camada de BD segregada da rede ou ambiente com visibilidade/acesso exterior.	Obrigatório.	Obrigatória
	BD	Aplicam-se as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.	Obrigatório.	Obrigatória
	BD	Mascaramento, anonimização ou, sendo necessário, cifra dos dados pessoais transmitidos ou acedidos.	Obrigatório.	Obrigatória
	BD	Dados armazenados (incluindo os existentes em volumes de salvaguarda — <i>backups</i>) devem ser cifrados e assinados digitalmente.	Recomendado.	Facultativa

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
	BD	Recomenda-se que, para dados pessoais considerados muito críticos, o seu armazenamento seja efetuado de forma fragmentada e em locais físicos distintos, mantendo-se, todavia, a sua unicidade e integridade lógica.	Recomendado.	Facultativa
Capacidade para garantir a identidade correta do remetente e destinatário da transmissão dos dados pessoais		Deve ser garantida a integridade das zonas <i>Domain Name System</i> (DNS) onde se encontra inserido o sistema e o ecossistema envolvente, recorrendo às boas práticas de DNSSec e de configuração de sistemas de Correio Eletrónico (por exemplo, <i>Sender Policy Framework</i> — SPF, <i>DomainKeys Identified Mail</i> — DKIM, <i>Domain-based Message Authentication, Reporting and Conformance</i> — DMARC, entre outros).	Obrigatório.	Obrigatória
		Deve ser utilizada tecnologia de comunicação segura (por exemplo VPN), com sistema de autenticação forte (preferencialmente através de certificados), para que a transmissão de dados entre entidades de ambientes tecnológicos distintos seja efetuada em segurança.	Recomendado.	Facultativa
Os sistemas de armazenamento devem garantir redundância e		A arquitetura de processamento e armazenamento deve garantir as propriedades da redundância, resiliência e disponibilidade.	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
disponibilidade, não devendo existir nenhum « <i>single point of failure</i> »		Devem existir dois tipos de backups (<i>online</i> e <i>offline</i>), que devem obedecer aos mesmos requisitos de segurança definidos para os sistemas produtivos.	Obrigatório.	Obrigatória
		Os backups <i>offline</i> devem ser guardados numa localização que não esteja exposta aos mesmos riscos exteriores da localização original, podendo ser da organização, mas geograficamente distinta e/ou afastada.	Obrigatório.	Obrigatória
As redes e sistemas de informação devem possuir as funcionalidades necessárias ao respeito pelos direitos do titular dos dados		Os sistemas devem estar capacitados para classificar, priorizar, pesquisar, editar e apagar os dados pessoais.	Obrigatório.	Obrigatória
		Os sistemas devem possuir os controlos necessários que permitam a identificação, autenticação, acesso e validação dos dados pessoais armazenados.	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
As tecnologias de informação a implementar devem permitir a portabilidade e a exportação de dados pessoais		Deve-se garantir a utilização de formatos digitais compatíveis, que assegurem a interoperabilidade técnica e semântica dentro da Administração Pública, na interação com o cidadão ou com a empresa e para disponibilização de conteúdos e serviços, adotando as especificações técnicas e formatos digitais definidos no Regulamento Nacional de Interoperabilidade Digital, aprovado pela Resolução do Conselho de Ministros n.º 91/2012, ou noutro que o venha a substituir.	Obrigatório.	Obrigatória
Devem ser definidas políticas que garantam a segurança dos dados pessoais, em alinhamento com a estratégia superiormente definida para a segurança do tratamento de dados pessoais		As políticas que garantam a segurança do tratamento de dados pessoais devem abranger: A priorização e classificação dos dados de acordo com os critérios de sensibilidade e criticidade predefinidos; A criação; A modificação; A transmissão; A recolha (independentemente do respetivo meio ou processo); A destruição; O armazenamento (incluindo a retenção); A pesquisa de dados.	Obrigatório.	Obrigatória

Requisito geral	Área	Requisitos Específicos	Classificação	Implementação
		Deve-se garantir o conhecimento, a todo o tempo, dos ativos de informação relativamente a dados pessoais, de modo a permitir identificar inequivocamente o estado da informação em todo o seu ciclo de vida.	Obrigatório.	Obrigatória

B.3. Prestação de assistência ao responsável pelo tratamento

O subcontratante deverá, na medida do possível, - atendendo ao âmbito e à extensão da assistência infra especificada - prestar assistência ao responsável pelo tratamento de acordo com as cláusulas 8.1 e 8.2 através da implementação das seguintes medidas técnicas e organizativas:

- O subcontratante deverá designar um ponto de contacto para a Gestão do Projeto associado à prestação dos serviços previstos no presente documento, comunicando-o por email ao Gestor de Contrato do Responsável pelo Tratamento;
- O ponto de contacto do subcontratante deverá disponibilizar um email e um contacto telefónico;
- Deverá existir um contacto alternativo ao ponto de contacto designado para a Gestão de Projeto por parte do subcontratante;
- Qualquer pedido de informação ou comunicação realizada pelo responsável pelo tratamento para o subcontratante deverá ter como período máximo de resposta uma semana.

B.4. Período de armazenamento/procedimentos de apagamento

Após cessação da prestação de serviços de tratamento de dados pessoais, o subcontratante deverá apagar ou devolver os dados pessoais de acordo com a cláusula 10.1., a menos que o responsável pelo tratamento – após assinatura do contrato – tenha modificado a sua escolha inicial. Tal modificação deverá ser documentada e mantida por escrito, incluindo o formato eletrónico, em conexão com as cláusulas.

B.5. Localização do tratamento

O tratamento de dados pessoais realizado sob aplicação das cláusulas não poderá ser realizado noutras localizações além das pertencentes ao responsável pelo tratamento ou subcontratante, sem a permissão prévia por escrito do responsável pelo tratamento.

B.6. Instrução para a transferência de dados pessoais para países terceiros

46

A presente prestação de serviços não contempla a transferência de dados pessoais para um país terceiro ou organização internacional.

B.7. Procedimentos para a realização de auditorias pelo responsável pelo tratamento, incluindo inspeções, do tratamento de dados pessoais realizados pelo subcontratante em nome do responsável pelo tratamento

Caso assim o responsável pelo tratamento o entenda por conveniente, poderão ser realizadas auditorias e/ou inspeções ao subcontratante. Tal será realizado mediante comunicação prévia ao subcontratante, com um período de antecedência de 30 dias.

O subcontratante deverá disponibilizar os recursos necessários para que o responsável pelo tratamento possa realizar a auditoria e/ou inspeção.

Os encargos decorrentes da realização da auditoria e/ou inspeção ficam a cargo do responsável pelo tratamento.

O responsável pelo tratamento poderá designar um auditor independente/externo para a realização dos procedimentos supra descritos.