

**ADENDA AO PROTOCOLO DE COOPERAÇÃO ENTRE A AGÊNCIA PARA A INTEGRAÇÃO,
MIGRAÇÕES E ASILO, I. P.**

E O

MUNICÍPIO FORNOS DE ALGODRES

Considerando que:

1 – A Agência para a Integração, Migrações e Asilo, I.P. (AIMA) tem por missão a concretização das políticas públicas nacionais e europeias, em matéria de migração e asilo, tendo, designadamente, como atribuições, a concessão de prorrogações de permanência, autorizações de residência, renovações de autorizações de residência, cartões de residência e cartões de residência permanente de familiares de cidadãos da União Europeia nacionais de Estado terceiro, certificados de residência permanente de cidadãos da União Europeia e títulos de residência para cidadãos britânicos beneficiários do Acordo sobre a Saída do Reino Unido da Grã-Bretanha e da Irlanda do Norte da União Europeia e da Comunidade Europeia da Energia, previstos, respetivamente, na Lei n.º 23/2007, de 4 de julho, na sua redação atual e na Lei n.º 37/2006, de 9 de agosto, na sua redação atual (cf. artigo 2.º do Decreto-Lei n.º 41/2023, de 2 de junho e artigo 3.º, n.ºs 1 e 2 do Anexo a este diploma);

2 – A promoção de migrações seguras, ordenadas e regulares, afirmada de forma inequívoca pela comunidade internacional através da adoção do Pacto Global das Migrações aprovado pela Assembleia-Geral das Nações Unidas, em 19 de dezembro de 2018, e através do Novo Pacto Europeu sobre a Migração e o Asilo, apresentado pela Comissão Europeia, em setembro de 2020, veio reforçar a necessidade de uma nova abordagem em matéria de gestão de migrações;

3 – A criação da AIMA pelo Decreto-Lei n.º 41/2023, de 2 de junho, representa uma mudança de paradigma na forma como a Administração Pública se relaciona com os cidadãos estrangeiros, tanto da União Europeia como de países terceiros, seja na sua entrada e permanência em território nacional, seja no seu acolhimento e na sua integração, pelo que, para prosseguir esse desígnio, importa melhorar a qualidade dos serviços públicos prestados às pessoas migrantes, promovendo o aproveitamento de sinergias com vista a promover ganhos de eficiência, potenciando os resultados a alcançar;

4 – O n.º 4 do artigo 3.º do Anexo ao Decreto-Lei n.º 41/2023, de 2 de junho, prevê a celebração de protocolos entre a AIMA e as autarquias locais com vista a facilitar e simplificar os procedimentos administrativos da competência da AIMA, designadamente no que respeita à

recolha de todos os dados e informação necessária à concretização dos pedidos apresentados nos referidos procedimentos;

5 – Do mesmo modo, dispõe o n.º 8 do artigo 78.º da Lei n.º 23/2007, de 4 de julho, na sua versão atual, que a AIMA, I. P. pode celebrar protocolos com as autarquias locais com vista a facilitar e simplificar os procedimentos de receção e encaminhamento de pedidos de renovação de autorização de residência e respetivos títulos;

6 – As autarquias locais assumem já competências em matéria de atendimento, no âmbito do registo dos cidadãos da União Europeia cuja estada no território nacional se prolongue por período superior a três meses, formalizando o seu direito de residência (cf. números 1 e 2 do artigo 14.º da Lei n.º 37/2006, de 9 de agosto), bem como no âmbito dos Centros Locais de Apoio à Integração de Migrantes (cf. artigo 6.º do Decreto-Lei n.º 104/2018, de 29 de novembro);

7 – A colaboração das autarquias locais no atendimento aos cidadãos estrangeiros permitirá integrar, na prestação dos serviços públicos a estes dirigidos, a perspetiva valiosa e insubstituível de quem está mais próximo das pessoas e que melhor conhece as suas necessidades, constituindo-se como um valioso contributo para o serviço a prestar, não só pela administração central, como pela própria administração local;

8 – Esta colaboração fundamenta-se, igualmente, nos princípios da prossecução do interesse público e da proteção dos direitos e interesses dos cidadãos, da boa administração e da colaboração com os particulares, plasmados, respetivamente, nos artigos 4.º, 5.º e 11.º, do Código do Procedimento Administrativo, em obediência ao disposto nos artigos 266.º e 267.º, da Constituição da República Portuguesa;

9 – Constitui desígnio dos órgãos e serviços da Administração Pública promover a utilização de meios eletrónicos no desempenho da sua atividade, tanto nas relações interadministrativas, como nas suas relações com os particulares, de modo a promover a eficiência e a transparência administrativas e a proximidade com os interessados, assegurando, entre si, a partilha de dados e documentos públicos necessários à análise e apreciação e processos administrativos, em respeito pelas regras relativas à proteção de dados pessoais, tal como resulta dos princípios aplicáveis à administração eletrónica consagrados no artigo 14.º do Código do Procedimento Administrativo e do disposto no artigo 28.º-A, n.º 2, do Decreto-lei n.º 135/99, de 22 de abril, na sua redação atual;

10 – O protocolo celebrado entre as partes, no dia xx de xxx de 2024, destinado à implementação de um serviço com funções de acolhimento, informação e apoio a cidadãos migrantes, incluindo imigrantes e requerentes de proteção internacional, denominado Centro Local de Apoio à Integração de Migrantes, adiante designado por CLAIM, que integra, com as devidas adaptações, a prestação de serviços da AIMA;

11 – Os desafios que se colocam ao país, em matéria de migração, e aos Municípios, em matéria de ação social, importa que as partes, cientes dos objetivos nacionais e do cumprimento das metas do país, no âmbito dos compromissos europeus e internacionais no âmbito da política migratória, unam esforços num trabalho coletivo que crie as melhores condições de legalização e integração dos cidadãos que escolhem o nosso país e, em particular, XXXXXXXXXXXX para viver;

12 - Nesse sentido, os serviços da AIMA e do Município XXXXXXXXXXXX, intervenientes nas operações de recolha e tratamento de dados ligadas à receção dos pedidos referidos no considerando n.º 1, incluindo a recolha de dados biométricos, assegurarão que as mesmas decorrem em condições técnicas e de segurança que deem pleno cumprimento às especificações aplicáveis, para o que existem, nos respetivos serviços, os recursos humanos e os equipamentos tecnológicos adequados de recolha de dados em cumprimento da legislação relativa à proteção de dados pessoais e ao respeito pelos direitos dos respetivos titulares,

Entre:

A **Agência para a Integração, Migrações e Asilo, I. P.** abreviadamente designada por **AIMA, I. P.**, sito na Avenida António Augusto de Aguiar, n.º 20, 1069-119 Lisboa, pessoa coletiva n.º 517686260, representada neste ato pelo seu Presidente Pedro Manuel Portugal Natário Botelho Gaspar, designado por Resolução do Conselho de Ministros n.º 103/2024, de 26 de julho de 2024, publicado na 1.ª Série do Diário da República, n.º 153/2024, de 8 de agosto de 2024, ao abrigo das competências delegadas pela Resolução do Conselho de Ministros n.º 48/2022, de 26 de maio, publicada no Diário da República, 1.ª série, n.º 106, de 1 de junho de 2022, adiante designada por **Primeiro Outorgante**;

E

O Município **XXXXXXXXXX**, sito **XXXXXXXXXX**, pessoa coletiva n.º **XXXXXXXXXX**, representado neste ato por **XXXXXXXXXX**, na qualidade de Presidente da Câmara Municipal, adiante designado por **Segundo Outorgante**,

É celebrada a Presente Adenda ao Protocolo de Colaboração celebrado no dia **XXXXXXXXXX**, ao abrigo do disposto no n.º 4 do artigo 3.º do Anexo ao Decreto-Lei n.º 41/2023, de 2 de junho e no artigo 78.º da Lei n.º 23/2007, de 4 de julho, nos termos do disposto no n.º 5 do artigo 5.º-A do Código dos Contratos Públicos, e ainda no âmbito da alínea v) do nº1 do artigo 33º do Anexo I à Lei nº75/2013 de 12 de setembro, todos na sua redação atual, que se rege pelas cláusulas seguintes:

Cláusula 1.ª

Objeto e âmbito

1 – A presente Adenda ao Protocolo tem por objecto a definição dos termos e condições da colaboração entre a AIMA e o Município com vista à realização, por parte do Município, de tarefas de atendimento presencial no âmbito dos procedimentos administrativos da competência da AIMA, relativos, designadamente, a:

- a) Concessão de prorrogações de permanência;
- b) Concessão de autorizações de residência;
- c) Emissão de cartões de residência temporária ou permanente de familiares de cidadãos da União Europeia nacionais de Estado terceiro;
- d) Emissão de certificados de residência permanente de cidadãos da União Europeia;
- e) Emissão de títulos de residência para cidadãos britânicos beneficiários do Acordo sobre a Saída do Reino Unido da Grã-Bretanha e da Irlanda do Norte da União Europeia e da Comunidade Europeia da Energia, previstos, respetivamente, na Lei n.º 23/2007, de 4 de julho, na sua redação atual e na Lei n.º 37/2006, de 9 de agosto, na sua redação atual.

2 – O atendimento presencial referido no número anterior realiza-se nos termos e para os efeitos previstos na Lei n.º 23/2007, de 4 de julho, na sua redação atual, na Lei n.º 37/2006, de 9 de agosto, na sua redação atual, no Decreto Regulamentar n.º 84/2007, de 5 de novembro,

na sua redação atual e demais legislação e regulamentação aplicável à presente Adenda ao Protocolo e implica:

- a) A recolha de dados pessoais dos respetivos requerentes, incluindo dados biométricos através do equipamento fornecido ou aprovado pela AIMA;
- b) A receção de documentos necessários à análise do pedido, a apresentar pelos requerentes, bem como a sua digitalização e transmissão à AIMA, por via eletrónica, através do sistema de informação desta entidade;
- c) A realização das consultas às bases de dados administrativas da AIMA que sejam estritamente necessárias à realização do atendimento, designadamente para verificação da identidade e legitimidade do requerente e registo das operações realizadas;
- d) A verificação da autenticidade e validade da documentação apresentada.

Cláusula 2.ª

Obrigações do Município

No âmbito da presente Adenda ao Protocolo, o Município compromete-se a:

- a) Disponibilizar um posto de atendimento para a realização do atendimento previsto, no seguinte local e horário: Centro Local de Apoio à Integração de Migrantes, localizado XXXXXXXX, XXXXXXXX, às xxxxx e xxxx, das 09h30 às 17h00, podendo os dias e horas virem a ser alargados em função das necessidades.
- b) Disponibilizar as instalações físicas necessárias à realização do atendimento, assumindo os encargos inerentes à sua utilização corrente, manutenção e conservação, em condições de segurança, salubridade e conforto;
- c) Cuidar do equipamento informático cedido para o efeito, procedendo à sua reparação ou substituição em caso de avaria;
- d) Disponibilizar os recursos humanos necessários a assegurar a realização do número mínimo de atendimentos diários estabelecido no presente protocolo;
- e) Assegurar a realização do atendimento nos termos previstos na presente Adenda ao Protocolo, no Manual de Procedimentos AIMA, a disponibilizar por esta agência, e nas políticas de segurança definidas pela AIMA, com elevados padrões de qualidade;

- f) Assegurar o atendimento mínimo de 6 pedidos diários por cada posto de atendimento disponibilizado (média mensal por cada dia útil);
- g) Assegurar a realização do atendimento no horário de funcionamento definido na presente Adenda ao Protocolo;
- h) Assegurar que os recursos humanos afetos à execução da presente Adenda ao Protocolo frequentam as ações de formação ministradas pela AIMA ou quaisquer reuniões de articulação, preferencialmente em formato online, sempre que seja solicitada a sua participação;
- i) Ajustar e efetuar a atualização do *software* de integração à estrutura organizacional existente nas suas instalações e assegurar a sua manutenção, por forma a permitir as operações de recolha e de acesso a dados no âmbito dos atendimentos a realizar;
- j) Assegurar as comunicações de dados através de um circuito internet, mantendo um débito mínimo, necessários ao bom funcionamento dos serviços de atendimento (tipicamente 10Mbps simétricos sem contenção), bem como suportar os custos associados ao circuito referido na alínea anterior;
- k) Assegurar as condições necessárias à instalação de uma *firewall* da AIMA, que suportará as ligações ao SII AIMA, e que utilizará para o efeito o circuito internet referenciado na alínea anterior;
- l) Garantir, se necessário, arquivo de toda a documentação rececionada no âmbito do atendimento nos serviços da AIMA e assegurar o seu envio à AIMA a cada três meses ou mediante solicitação;
- m) Comunicar à AIMA a entrada e saída de recursos humanos afetos ao atendimento com a antecedência mínima de 48 horas, de modo a assegurar a criação e o cancelamento de credenciais de acesso aos sistemas de informação;
- n) Sensibilizar, divulgar e garantir o conhecimento do Manual de Procedimentos AIMA e as políticas de segurança pelos seus funcionários;
- o) Divulgar os serviços de atendimento objeto do presente protocolo nos seus canais institucionais.

Cláusula 3.ª

Obrigações da AIMA

1 – No âmbito do presente protocolo incumbe à AIMA:

- a) Assegurar a criação e gestão do sistema de informação e de serviços de rede indispensáveis ao registo e transmissão eletrónica dos atos praticados no âmbito do atendimento, incluindo a produção das aplicações informáticas, a definição das especificações dos equipamentos a utilizar, a definição da política de segurança e o apoio à resolução de problemas técnicos, em cumprimento do disposto na Resolução do Conselho de Ministros n.º 41/2018, de 28 de março;
- b) Assegurar o tratamento do expediente remetido através dos seus sistemas de informação pelo Município;
- c) Proporcionar ações de formação sobre os procedimentos relativos aos atendimentos a realizar;
- d) Definir e implementar a formação necessária aos recursos humanos afetos ao atendimento, nomeadamente ao nível da segurança e deteção da fraude documental, legislação aplicável e utilização de aplicações informáticas;
- e) Fornecer um *Helpdesk* de suporte técnico;
- f) Garantir o acesso aos seus sistemas de informação, para efeitos de receção dos pedidos objeto do presente protocolo, nos moldes referidos na cláusula seguinte;
- g) Assegurar o pagamento da compensação prevista na cláusula 4.ª.

Cláusula 4.ª

Compensação

1 – A título de compensação pelos atendimentos realizados no âmbito do presente protocolo, a AIMA fica obrigada ao pagamento de uma compensação fixada nos seguintes termos:

- a) €7,50 por cada atendimento com recolha de dados biométricos, no caso de ser assegurado, em cada mês, o mínimo de atendimentos previstos na alínea f) da cláusula 2.ª;

b) €5,00 por cada atendimento com recolha de dados biométricos, no caso de não ser assegurado, em cada mês, o mínimo de atendimentos previstos na alínea f) da cláusula 2.^a, mas for assegurado, pelo menos, metade desse valor.

2 – Não haverá lugar ao pagamento de qualquer compensação quando não seja assegurado, em cada mês, metade do mínimo de atendimentos previstos na alínea f) da cláusula 2.^a.

3 – Não são considerados para o cômputo total de atendimentos previstos na alínea f) da cláusula 2.^a os casos em que o atendimento não possa ser concluído ou o procedimento não possa prosseguir por facto imputável ao requerente, nomeadamente por ausência dos documentos necessários à apreciação do pedido por parte da AIMA.

4 – O valor devido pela AIMA ao Município é pago até ao termo do segundo mês subsequente à sua receção.

Cláusula 5.^a

Acesso ao Sistema de Informação da AIMA

1 – O acesso ao sistema de informação da AIMA é feito através de nome de utilizador e palavra-chave atribuídos por esta entidade, em cumprimento do disposto na Resolução do Conselho de Ministros n.º 41/2018, de 28 de março, satisfeitas todas as normas de segurança.

2 – A AIMA poderá solicitar que a autenticação na aplicação seja efetuada por dois fatores.

3 – O acesso poderá vir a ser delegado, em condições a definir, caso o Município tenha um sistema de federação de identidades que suporte os protocolos SAML2, OAUTH2 ou outro que, entretanto, seja suportado pela aplicação, e que cumpra os requisitos de segurança da AIMA em termos de complexidade da palavra-chave e/ou outros requisitos de segurança.

4 – A disponibilização da aplicação referida no número anterior é efetuada por via eletrónica, através de acesso por *browser* ao endereço eletrónico do sistema de informação da AIMA.

5 – Os acessos à informação ficam registados no sistema, sendo aplicáveis os prazos de conservação de 2 (dois) anos para o registo, para efeitos de auditoria, de todas as inserções, alterações ou consultas à informação.

Cláusula 6.ª

Utilizadores

1 – As partes obrigam-se a manter uma lista de utilizadores, permanentemente atualizada nos termos da alínea m) da cláusula onde conste a indicação do nome, da categoria/função e a data de início das funções referidas no presente protocolo, tendo em vista a atribuição de nomes de utilizador e respetivas palavras-chave de ligação ao sistema.

2 – Os acessos são individualizados e cada utilizador tem uma palavra-chave pessoal que o responsabilizará pelo uso que fizer do serviço.

Cláusula 7.ª

Gestão dos agendamentos

1 – A AIMA é responsável por agendar os atendimentos a realizar no âmbito do presente protocolo, segundo os critérios de conveniência, prioridade e oportunidade por si estabelecidos, e por notificar os requerentes da data, hora e local para o atendimento, sem prejuízo do disposto nos números seguintes.

2 – O número de atendimentos a agendar por cada mesa é definido pelo Município, em total não inferior a 6 diários, agendando a AIMA 100% dos atendimentos solicitados pelo Município.

3 – Sempre que o Município pretenda uma alteração do número diário de agendamentos por mesa, deve informar a AIMA com a antecedência mínima de 10 dias úteis, sendo responsável pelos reagendamentos a que eventualmente haja lugar, incluindo a comunicação ao requerente da nova data.

Cláusula 8.ª

Reclamações

1 – As reclamações decorrentes do exercício das tarefas constantes na Cláusula 1.ª são da responsabilidade do Município, que assegura o respetivo tratamento.

2 – As reclamações sobre matérias que se insiram no âmbito das competências da AIMA no tocante aos atendimentos são transmitidas àquela, que assegura o respetivo tratamento.

Cláusula 9.ª

Horário de funcionamento

O horário de atendimento a observar é entre as 9h00 e as 17h00.

Cláusula 10.ª

Proteção de dados pessoais

1 – O Município assegura a observância das disposições legais vigentes em matéria de proteção de dados pessoais constantes do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral Proteção de Dados, doravante, RGPD), bem como da Lei n.º 58/2019, de 8 de agosto, pelos seus órgãos, os seus titulares, os seus trabalhadores e as pessoas que lhe prestem, direta ou indiretamente, a título permanente ou ocasional, quaisquer serviços.

2 – Mediante a celebração da presente Adenda ao Protocolo, o Município assume a qualidade de subcontratante no que diz respeito ao tratamento de dados pessoais que constituem o seu objeto, e no âmbito do qual a AIMA é a entidade responsável pelo tratamento.

3 – Para a regulação das responsabilidades em termos de tratamento de dados pessoais entre o responsável e a subcontratante, os outorgantes celebram, por via do presente protocolo, o Acordo de Tratamento de Dados Pessoais constante do Anexo ao presente protocolo, que dele faz parte integrante.

4 – O Município obriga-se, enquanto subcontratante, ao cumprimento de todos os deveres e obrigações que impendem sobre a AIMA, enquanto responsável pelo tratamento de dados pessoais objeto do presente protocolo, designadamente a utilizar os dados pessoais a que tenha acesso ou que lhe tenham sido transmitidos pela AIMA, única e exclusivamente para efeitos da prestação de serviços objeto da presente Adenda ao Protocolo.

5 – Sem prejuízo do cumprimento da legislação aplicável em matéria de proteção de dados pessoais em vigor a cada momento, o Município compromete-se a respeitar a política de privacidade instituída pela AIMA, sem prejuízo da responsabilidade civil ou criminal a que possa haver lugar.

Cláusula 11.ª

Articulação institucional

1 – As partes comprometem-se a cooperar para assegurar as condições necessárias à instalação e ao bom funcionamento do atendimento, no respeito pelos princípios fundamentais e pela manutenção dos padrões de qualidade do serviço de atendimento ao público por que se regem.

2 – Para efeitos do disposto do número anterior, são designados os seguintes pontos de contacto:

a) AIMA:

[Nome]

[Endereço de email]

b) Município:

[Nome]

[Endereço de email]

Cláusula 12.ª

Denúncia

Sem prejuízo das obrigações legalmente estabelecidas, qualquer das partes poderá, a qualquer momento, denunciar o presente Protocolo mediante comunicação formal, através de carta registada com aviso de receção, com uma antecedência mínima de três meses.

Cláusula 13.ª

Confidencialidade

O Município, bem como as pessoas afetas à execução do presente protocolo, obrigam-se, durante toda a sua vigência e após a sua cessação, a manter confidencialidade sobre quaisquer factos cujo conhecimento lhes advenha da execução do presente protocolo, nomeadamente em matéria de dados pessoais, segredo profissional, segredo industrial ou comercial ou informações confidenciais.

Cláusula 14.ª

Manual de Procedimentos da AIMA

1 – O Município obriga-se a conduzir o atendimento prestado no âmbito da presente Adenda ao Protocolo de acordo com o Manual de Procedimentos da AIMA e a política de segurança, que constituem o Anexo I ao presente Protocolo.

2 – O Manual de Procedimentos pode ser alterado pela AIMA, sempre que o bom funcionamento do sistema o justificar, devendo tal alteração ser comunicada previamente ao Município e, caso se mostre necessário, ser facultada a adequada formação.

Cláusula 15.ª

Estrutura de Missão para a Recuperação de Processos Pendentes na AIMA

A posição contratual da AIMA é transferida automaticamente para a Estrutura de Missão para a Recuperação de Processos Pendentes na AIMA logo que esta estrutura inicie a sua atividade.

Cláusula 16.ª

Entrada em vigor e produção de efeitos

A presente Adenda ao Protocolo entra em vigor na data da sua assinatura por ambas as partes e tem a validade de dois anos, renovável por iguais e sucessivos períodos.

XXXXXXXXXX, de de 2025.

O Primeiro Outorgante
AIMA, I.P.

O Segundo Outorgante
Câmara Municipal XXXXXXXXXX

Pedro Gaspar
Presidente do Conselho Diretivo da Agência
para a Integração Migrações e Asilo, I.P.

XXXXXXXXXX
Presidente da Câmara Municipal
XXXXXXXXXX

ANEXO

(a que se refere o n.º 3 da cláusula 10.ª da Adenda ao Protocolo de Colaboração entre a AIMA,
I.P. e o Município **XXXXXXXXXX**)

ACORDO DE TRATAMENTO DE DADOS PESSOAIS

(Cumprimento do disposto no art.28.º do RGPD)

Entre

A **Agência para a Integração, Migrações e Asilo, I. P.** abreviadamente designada por **AIMA, I. P.**, sito na Avenida António Augusto de Aguiar, n.º 20, 1069-119 Lisboa, pessoa coletiva n.º 517686260, representada neste ato pelo seu Presidente Pedro Manuel Portugal Natário Botelho Gaspar, designado por Resolução do Conselho de Ministros n.º 103/2024, de 26 de julho de 2024, publicado na 1.ª Série do Diário da República, n.º 153/2024, de 8 de agosto de 2024, ao abrigo das competências delegadas pela Resolução do Conselho de Ministros n.º 48/2022, de 26 de maio, publicada no Diário da República, 1.ª série, n.º 106, de 1 de junho de 2022, adiante designada como **“Responsável pelo Tratamento”**

e

O **Município XXXXXXXXXXXX**, sito **XXXXXXXXXX**, pessoa coletiva n.º **XXXXXXXXXX**, representado neste ato por **XXXXXXXXXX**, na qualidade de Presidente da Câmara Municipal, com poderes para o ato, adiante abreviadamente designado por **“Subcontratante”**;

Considerando que:

- a) Os Outorgantes celebraram uma Adenda ao Protocolo mediante o qual se obrigam a colaborar no âmbito da prestação dos serviços de atendimento tendentes à concessão de prorrogações de permanência, autorizações de residência (excetuando autorizações de residência para investimento), cartões de residência e cartões de residência permanente de familiares de cidadãos da União Europeia nacionais de Estado terceiro, certificados de residência permanente de cidadãos da União Europeia e títulos de residência para cidadãos britânicos beneficiários do Acordo sobre a Saída do Reino Unido da Grã-Bretanha e da Irlanda do Norte da União Europeia e da Comunidade

Europeia da Energia, previstos, respetivamente, na Lei n.º 23/2007, de 4 de julho, na sua redação atual e na Lei n.º 37/2006, de 9 de agosto, na sua redação atual;

- b) No âmbito e para os efeitos da execução dos serviços definidos no ponto 2 da cláusula 1.ª da referida Adenda ao Protocolo, a Subcontratante trata dados pessoais em nome e por conta da Responsável pelo Tratamento;
- c) Os Outorgantes reconhecem a necessidade de cumprirem com o estabelecido no Regulamento Geral sobre a Proteção de Dados (RGPD) e demais legislação aplicável em matéria de proteção de dados pessoais e, nesse sentido, de definirem o seu posicionamento no âmbito do tratamento de dados pessoais necessário à execução do referido Protocolo.
- d) O artigo 28.º do RGPD prevê a existência de um instrumento normativo escrito entre um responsável pelo tratamento e um subcontratante de dados pessoais,

É, livremente e de boa-fé, celebrado o presente Acordo de Tratamento de Dados Pessoais (adiante designado simplesmente Acordo), que será parte integrante do Protocolo concluído entre as partes.

1. DEFINIÇÕES

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;

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;

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;

Subcontratante: uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

2. TRATAMENTO DE DADOS PESSOAIS

- 2.1. A Subcontratante obriga-se a tratar dados pessoais exclusivamente de acordo com as instruções documentadas e comunicadas pela Responsável pelo Tratamento.
- 2.2. As instruções iniciais da Responsável pelo Tratamento à Subcontratante sobre o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias de titulares de dados são estabelecidas no **Anexo A** do presente Acordo.
- 2.3. Podem ainda ser dadas instruções subsequentes pela Responsável pelo Tratamento durante todo o período de tratamento de dados pessoais, devendo essas instruções ser sempre documentadas e conservadas por escrito, incluindo por meios eletrónicos.
- 2.4. A Subcontratante apenas trata dados no âmbito da receção de pedidos referidos no número 1 da cláusula 1.º do Protocolo, os quais implicam a recolha e levantamento de dados pessoais dos respectivos requerentes, incluindo dados biométricos, o acesso a bases de dados, a receção de documentação de suporte e a cobrança das taxas, nos termos previstos na Lei n.º 23/2007, de 4 de julho, na sua redação atual, na Lei n.º 37/2006, de 9 de agosto, na sua redação atual, no Decreto Regulamentar n.º 84/2007, de 5 de novembro, na sua redação atual e demais legislação e regulamentação aplicável, a subsequente remessa à AIMA, I. P. do pedido e documentos de instrução existentes e, sempre que aplicável, a transferência dos valores cobrados no âmbito dos mesmos, tudo em cumprimento da legislação relativa à proteção de dados pessoais e ao respeito pelos direitos dos respetivos titulares.
- 2.5. Os serviços prestados pela Subcontratante são realizados nos servidores da Responsável pelo Tratamento.
- 2.6. A Subcontratante deve ter em consideração que poderá ter acesso a dados pessoais sensíveis, nos termos do previsto no n.º 1 do artigo 9.º do RGPD, obrigando-se a utilizar

tais dados apenas para as finalidades e na medida do estritamente necessário à execução do Protocolo.

- 2.7. A Subcontratante obriga-se a cumprir com a legislação aplicável em matéria de proteção de dados, bem como, as recomendações aplicáveis emitidas pela Comissão Nacional de Proteção de Dados.
- 2.8. A Subcontratante obriga-se, ainda, a auxiliar a Responsável pelo Tratamento, quando solicitado por este e sem custos adicionais, no cumprimento das suas obrigações jurídicas decorrentes da legislação aplicável em matéria de proteção de dados, incluindo, entre outras, a obrigação da Responsável pelo Tratamento em responder a pedidos de exercício de direitos dos titulares dos dados previstos na legislação aplicável.
- 2.9. A Subcontratante não realizará qualquer ato, ou omitirá qualquer ato, que provoque o incumprimento da legislação aplicável em matéria de proteção de dados por parte da Responsável pelo Tratamento.
- 2.10. A Subcontratante tem a obrigação de informar a Responsável pelo Tratamento de forma imediata, caso alguma instrução emanada violar o disposto no RGPD ou outras disposições do direito da União ou do Estado Português em matéria de proteção de dados pessoais.
- 2.11. A Subcontratante prestará todo o apoio à Responsável pelo Tratamento na resposta a pedidos dos titulares dos dados, comprometendo-se a comunicar de imediato qualquer pedido de exercício de direitos por parte dos titulares.

3. SUB-SUBCONTRATANTES

- 3.1. A Subcontratante contrata apenas os Sub-subcontratantes expressamente autorizados pela Responsável pelo Tratamento, necessários à concretização dos serviços adjudicados.
- 3.2. A Subcontratante garante que todos os Sub-subcontratantes estão vinculados por contratos escritos que exigem o cumprimento de obrigações de tratamento de dados correspondentes às incluídas no presente Acordo.
- 3.3. A Subcontratante informa por escrito todos os Sub-subcontratantes que sejam envolvidos no tratamento de dados em nome da Responsável pelo Tratamento.

4. TRANSFERÊNCIA DE DADOS PESSOAIS PARA PAÍSES TERCEIROS

- 4.1. A Subcontratante não pode transferir dados para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pelo direito da União Europeia ou do Estado Português, informando, nesse caso, a Responsável pelo Tratamento dessa obrigação jurídica antes do tratamento.
- 4.2. A Subcontratante deve dar conhecimento e prestar informações sobre todas as transferências de dados pessoais que realize no âmbito dos serviços adjudicados.

5. SEGURANÇA E CONFIDENCIALIDADE DA INFORMAÇÃO

- 5.1. Na medida em que a legislação de proteção de dados aplicável à Responsável pelo Tratamento ou à Subcontratante não preveja outras medidas de segurança, a Subcontratante implementa as medidas técnicas e organizativas adequadas ao tratamento de dados em causa.
- 5.2. A Subcontratante implementa mecanismos para:
 - (i) Garantir a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e serviços de tratamento.
 - (ii) Restaurar a disponibilidade e o acesso aos dados pessoais de forma rápida, em caso de incidente físico ou técnico.
 - (iii) Verificar, avaliar e analisar, numa base regular, a eficácia das medidas técnicas e organizacionais implementadas para garantir a segurança do tratamento.
- 5.3. A Subcontratante protegerá os dados pessoais da destruição, modificação, divulgação ilícita ou acesso ilícito.
- 5.4. Em qualquer caso e no mínimo, a Subcontratante deve aplicar as medidas acordadas com a Responsável pelo Tratamento previstas no **Anexo B** do presente Acordo.
- 5.5. Durante a prestação dos serviços adjudicados, a Subcontratante notificará imediatamente a Responsável pelo Tratamento sobre qualquer incidente de violação de dados pessoais ou sobre quaisquer outros incidentes de segurança que tome conhecimento, nos termos do **Anexo C**, do presente Acordo.

- 5.6. Para o efeito do disposto no ponto anterior, a Subcontratante implementa procedimentos internos de deteção e reporte dos referidos incidentes, e atribui internamente as devidas responsabilidades, de modo a comunicá-los à Responsável pelo Tratamento no prazo de 24 horas.
- 5.7. A Subcontratante obriga-se a não divulgar os dados pessoais tratados ao abrigo do presente Acordo.
- 5.8. A Subcontratante assegura que as pessoas autorizadas para tratar os dados pessoais objeto de tratamento apenas o fazem para cumprir com a finalidade desta subcontratação, não devendo, nesse âmbito, tratar de quaisquer outros dados pessoais ou aplicar ou utilizar os dados pessoais para quaisquer outras finalidades, nomeadamente, para as finalidades próprias da Subcontratante.
- 5.9. A Subcontratante assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a uma obrigação legal de confidencialidade adequada e apenas com base na necessidade de conhecer, podendo a Responsável pelo Tratamento solicitar as respetivas evidências a todo o tempo.
- 5.10. O dever de confidencialidade dos dados no âmbito da presente subcontratação mantém-se mesmo depois de finalizado o seu objeto e cessado o Protocolo.
- 5.11. A Subcontratante obriga-se a elaborar e conservar uma lista de pessoas a quem foi concedido acesso aos dados, a qual deve ser revista periodicamente. Com base em tal revisão, esse acesso pode ser retirado, se já não for necessário, facto que deve ser comunicado à Responsável pelo Tratamento.

6. DIREITOS DE AUDITORIA

- 6.1. A Responsável pelo Tratamento terá direito a verificar se a Subcontratante cumpre as obrigações decorrentes do presente Acordo.
- 6.2. Adicionalmente, a Responsável pelo Tratamento pode verificar se a Subcontratante implementou as medidas mínimas exigidas para garantir o cumprimento e conformidade com o RGPD e com as presentes obrigações contratuais.
- 6.3. A Subcontratante compromete-se, a expensas próprias, a disponibilizar à Responsável pelo Tratamento todas as informações e assistência necessárias para demonstrar o

cumprimento das obrigações previstas no presente Acordo, bem como permitir e contribuir para as auditorias realizadas pela Responsável pelo Tratamento ou por outro auditor mandatado por esta.

7. INDEMNIZAÇÃO

A Subcontratante será responsável por quaisquer danos sofridos pela Responsável pelo Tratamento na sequência do incumprimento ou cumprimento defeituoso das disposições do presente Acordo e/ou de qualquer instrução legítima.

8. DURAÇÃO

As disposições do presente Acordo têm efeitos desde a data da sua assinatura e devem aplicar-se enquanto a Subcontratante tratar dados pessoais em nome e por conta da Responsável pelo Tratamento.

9. MEDIDAS APÓS A CESSAÇÃO DO ACORDO

- 9.1. Salvo indicação expressa em contrário por parte da Responsável pelo Tratamento, após a cessação do presente Acordo, a Subcontratante deverá devolver todos os dados pessoais com os quais tenha trabalhado, assim como apagar quaisquer cópias dos mesmos que estejam em seu poder, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros.
- 9.2. A Subcontratante deve garantir, ainda, que qualquer Sub-subcontratante procede à eliminação dos dados pessoais a que tenha tido acesso no término do Protocolo.
- 9.3. Mediante pedido da Responsável pelo Tratamento, a Subcontratante deve comunicar, por escrito, as medidas tomadas relativamente à eliminação ou devolução dos dados pessoais aquando da conclusão do tratamento.
- 9.4. A eliminação dos dados deve ser realizada por entidade certificada para o efeito, ou pelo Subcontratante sob supervisão da Responsável pelo Tratamento.

10. REMUNERAÇÃO

A Subcontratante não terá direito a qualquer remuneração adicional como contrapartida do cumprimento das suas obrigações no âmbito do presente Acordo.

Este Acordo foi celebrado em duas cópias, ambas com valor de original, disponibilizadas a cada uma das Partes.

XXXXXXXXXX, de de 2024.

O Primeiro Outorgante
AIMA, I.P.

O Segundo Outorgante
Câmara Municipal XXXXXXXXXXXX

Pedro Gaspar
Presidente do Conselho Diretivo da Agência
para a Integração Migrações e Asilo, I.P.

XXXXXXXXXXXX
Presidente da Câmara Municipal
XXXXXXXXXXXX

ANEXO A

(a que se refere o Acordo de Tratamento de Dados Pessoais)

INSTRUÇÕES DE TRATAMENTO DE DADOS PESSOAIS

<p>Finalidades <i>Especifique todas as finalidades para as quais os dados pessoais serão tratados pelo Subcontratante.</i></p>	<ul style="list-style-type: none"> • Atendimento, receção e encaminhamento de pedidos tendentes às prorrogações de permanência, autorizações de residência (excetuando autorizações de residência para investimento), cartões de residência e cartões de residência permanente de familiares de cidadãos da União Europeia nacionais de Estado terceiro, certificados de residência permanente de cidadãos da União Europeia e títulos de residência para cidadãos britânicos beneficiários do Acordo sobre a Saída do Reino Unido da Grã-Bretanha e da Irlanda do Norte da União Europeia e da Comunidade Europeia da Energia, previstos, respetivamente, na Lei n.º 23/2007, de 4 de julho, na sua redação atual e na Lei n.º 37/2006, de 9 de agosto, na sua redação atual; • Receção de documentação de suporte e a cobrança das taxas, nos termos previstos na Lei n.º 23/2007, de 4 de julho, na sua redação atual, na Lei n.º 37/2006, de 9 de agosto, na sua redação atual, no Decreto Regulamentar n.º 84/2007, de 5 de novembro, na sua redação atual e demais legislação e regulamentação aplicável, a subsequente remessa à Responsável pelo Tratamento do pedido e documentos de instrução existentes e, sempre que aplicável, a transferência dos valores cobrados no âmbito dos mesmos, tudo em cumprimento da legislação relativa à proteção de dados pessoais e ao respeito pelos direitos dos respetivos titulares. • Remessa à Responsável pelo Tratamento dos pedidos e documentos de instrução, via Sistema Integrado de Informação da AIMA (SII AIMA), bem como a transferência dos valores cobrados no âmbito dos mesmos.
<p>Natureza da Subcontratação <i>Identifique a natureza da subcontratação</i></p>	<p>Protocolo de Cooperação em que a Subcontratante colabora, mediante disponibilização do equipamento e dos recursos humanos necessários, no âmbito da prestação dos serviços de atendimento tendentes às prorrogações de permanência, autorizações de residência (excetuando autorizações de residência para investimento), cartões de residência e cartões de residência permanente de familiares de cidadãos da União Europeia nacionais de Estado terceiro, certificados de residência permanente de cidadãos da União Europeia e títulos de residência para cidadãos britânicos beneficiários do Acordo sobre a Saída do Reino Unido da Grã-Bretanha e da Irlanda do Norte da União Europeia e da Comunidade Europeia da Energia, previstos, respetivamente, na Lei n.º 23/2007, de 4 de julho, na sua redação atual e na Lei n.º 37/2006, de 9 de agosto, na sua redação atual.</p>

<p>Categorias de dados <i>Especifique os diferentes tipos de dados pessoais que serão tratados pelo Subcontratante. Deve apagar-se o que não será objeto de tratamento.</i></p> <p>NOTA! A lista não é exaustiva e poderá necessitar de adicionar outras categorias de dados específicas para o Protocolo.</p>	<ul style="list-style-type: none"> ✓ Nome ✓ Apelido ✓ Data de nascimento ✓ Data de falecimento ✓ Morada ✓ Cidade ✓ Código Postal ✓ Endereço de correio eletrónico ✓ Número de telefone ✓ Escolaridade ✓ Estado civil ✓ Género ✓ Informações sobre o agregado familiar (nome e dados pessoais dos elementos do agregado familiar e a eventual condição de membro da família de cidadão nacional ou da União Europeia ou da titularidade do direito de livre circulação) ✓ Identificador exclusivo (nº de identificação de estrangeiro) ✓ Documento de identificação (passaporte, cartão de identidade, assento de casamento, assento de nascimento, etc) ✓ NIF ✓ NISS ✓ Filiação ✓ Nacionalidade ✓ Naturalidade ✓ Documentos de residência (vistos, autorizações ou cartões de residência) ✓ Situação profissional 	<p>CATEGORIAS ESPECIAIS DE DADOS PESSOAIS</p> <ul style="list-style-type: none"> ✓ Dados biométricos (fotografia, assinatura e impressões digitais) ✓ Dados de saúde ✓ Condenações penais (apenas se o registo criminal é positivo ou não) ✓ Medidas cautelares de pessoas (hit / no hit) ✓ Medidas cautelares de documentos (hit / no hit)
<p>Titulares dos dados <i>Especifique as categorias de titulares dos dados cujos dados pessoais serão tratados pelo Subcontratante.</i></p> <p>NOTA! A lista não é exaustiva e poderá ter de adicionar titulares</p>	<ul style="list-style-type: none"> ✓ Clientes ✓ Menores ✓ Cidadãos Migrantes 	

de dados específicos para o Protocolo.	
Volume de titulares de dados mensal / anual <i>Indique o número estimado de titulares de dados abrangidos pelo tratamento</i>	Anual – no limite, o n.º de residentes (450 – 500 mil)
Operações de tratamento <i>Especifique todas as atividades de tratamento a realizar pelo Subcontratante.</i>	<ul style="list-style-type: none"> • Atendimento, receção e encaminhamento de pedidos tendentes às prorrogações de permanência, autorizações de residência (excetuando autorizações de residência para investimento), cartões de residência e cartões de residência permanente de familiares de cidadãos da União Europeia nacionais de Estado terceiro, certificados de residência permanente de cidadãos da União Europeia e títulos de residência para cidadãos britânicos beneficiários do Acordo sobre a Saída do Reino Unido da Grã-Bretanha e da Irlanda do Norte da União Europeia e da Comunidade Europeia da Energia; • Recolha e levantamento de dados pessoais dos respetivos requerentes, incluindo dados biométricos, a receção de documentação de suporte, o acesso a bases de dados e a cobrança das taxas; • Remessa à Responsável pelo Tratamento dos pedidos e documentos de instrução, via Sistema Integrado de Informação da AIMA (SII AIMA), bem como a transferência dos valores cobrados no âmbito dos mesmos; • Comunicação da não validação do pedido por parte AIMA, I. P., ao serviço que procedeu à recolha dos dados que, por sua vez, deve contactar o requerente para suprir eventuais faltas ou efetuar correções que se venham a mostrar necessárias; • Comunicação de dados através de um circuito internet, mantendo os mínimos de um débito mínimo, necessários ao bom funcionamento dos serviços de atendimento (tipicamente 10Mbps simétricos sem contenção), bem como suportar os custos associados ao circuito referido na alínea anterior.
Sub-subcontratante(s) <i>Especifique os sub-subcontratantes contratados pelo Subcontratante (caso existam) e as finalidades para as quais os dados pessoais serão tratados por cada sub-subcontratante.</i>	
Localização das operações de tratamento <i>Especifique todas as localizações em que os dados pessoais serão tratados pelo Subcontratante e por qualquer sub-subcontratante (se aplicável).</i>	Os dados pessoais serão alojados em servidores localizados num centro de dados em Av. Casal de Cabanas, Urb Cabanas Golf, 1, 2734-506 Barcarena, e serão acedidos pelos colaboradores do Subcontratante

<p>Acesso a bases de dados <i>(Especifique todas as bases de dados em que os dados pessoais serão tratados pelo Subcontratante e por qualquer sub-subcontratante (se aplicável))</i></p> <p>NOTA! A lista não é exaustiva e poderá necessitar de adicionar outras.</p>	<ul style="list-style-type: none">✓ SII AIMA✓ SIGAP✓ Aplicações do Centro de Contacto
--	---

ANEXO B

(a que se refere o Acordo de Tratamento de Dados Pessoais)

MEDIDAS TÉCNICAS E ORGANIZATIVAS

A subcontratante deve implementar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado, as seguintes medidas, nos termos da Cláusula 5.ª do Acordo de Tratamento de Dados Pessoais:

1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Existe uma Política de Segurança aprovada pelo órgão de administração e comunicada aos funcionários, que se aplica tanto a informações automatizadas, como não automatizadas.

2. ORGANIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

- Organização interna: Existe um Responsável de Segurança e um Encarregado de Proteção de Dados. Existe um procedimento de Incidentes de Segurança conhecido por todos os funcionários. Dispõe-se de uma separação de funções documentada e a segurança é tida em consideração em todos os projetos.
- Dispositivos móveis e teletrabalho: Existem Políticas e Medidas de Segurança para proteger o acesso, gestão, processamento e armazenamento das informações, como, por exemplo, encriptação de dispositivos, limitação na instalação de *software*, aplicação de *patches* de segurança, política de palavras-passe, eliminação remota de dispositivos.

3. SEGURANÇA DE RECURSOS HUMANOS

- Durante o processo de seleção de pessoal e, em qualquer caso, antes da contratação é verificado o *curriculum vitae* dos possíveis candidatos e acordados os requisitos de segurança, que se incluem no contrato.
- Durante a relação laboral: O Subcontratante dispõe de Políticas, Regras e Procedimentos (incluindo disciplinares) documentados e comunicados aos funcionários relativamente à Segurança da Informação e Proteção de Dados.

- Extinção da relação laboral: É comunicado aos terceiros e aos funcionários que as responsabilidades e obrigações sobre a Segurança da Informação continuam a existir, incluindo o dever de confidencialidade, mesmo que o contrato com o funcionário ou terceiro seja alterado ou termine. Esta comunicação deve ser documentada.

4. GESTÃO DE ATIVOS

- Responsabilidade pelos ativos: Existe um inventário de ativos e dos responsáveis pelos mesmos. Fica garantida a disponibilidade dos equipamentos e a sua devolução pelos utilizadores, aquando do término da sua relação laboral ou comercial.
- Classificação da informação: Existe classificação da informação tratada, com base no seu nível de criticidade e nas obrigações legais que podem ser exigidas. A informação é gerida, marcada, classificada e eliminada.
- Uso de unidades de armazenamento: Os dispositivos removíveis dispõem de controlos que garantem o acesso à informação, a sua leitura, escrita e destruição em caso obrigatório. Se a informação estiver em papel, também deve existir controlo.

5. CONTROLO DE ACESSO

- Requisitos de Controlo de Acesso da Empresa: Existe uma Política de Controlo de Acesso à Informação que tem em conta que a identidade dos utilizadores e as respetivas funções. Existem controlos para garantir que os utilizadores se conectam aos sistemas corporativos necessários para o desempenho do seu trabalho.
- Gestão de acesso do utilizador: A gestão de acessos garante a existência de ID de utilizador único, permissões baseadas em funções, controlo de ID inativos, identificação de contas de administradores, revisão de perfis, revogação de permissões.
- Responsabilidades dos utilizadores: Existe evidência de que os utilizadores conhecem os regulamentos de utilização da Internet, do correio eletrónico da empresa, as orientações e os requisitos de palavras-passe, entre outros regulamentos que sejam aplicáveis, de acordo com a função e responsabilidade.
- Sistema e aplicação de controlo de acesso: Os sistemas e aplicações possuem medidas

de controlo de acesso baseadas no princípio do menor privilégio, com gestão de palavras-passe que inclui complexidade, tentativas falhadas, inatividade, validade, limitação à navegação na Internet.

6. ENCRIPTAÇÃO

- Está em vigor uma política de controlos de encriptação e gestão de chaves, que garantem que, tanto nos computadores, como nos dispositivos amovíveis a informação está encriptada.

7. SEGURANÇA FÍSICA E AMBIENTAL

- Áreas de segurança: Existem procedimentos para garantir a segurança física das instalações, tanto de acesso, como das próprias instalações.
- Equipamento: Existem procedimentos para garantir a segurança do equipamento, por exemplo, contratos de manutenção, fontes de alimentação ininterrupta, segurança no acesso aos ativos, política de *clean desk*, armazenamento removível e bloqueio de dispositivos.

8. SEGURANÇA OPERATIVA

- Procedimentos operativos e responsabilidades: Existem procedimentos documentados, segregação de ambientes, gestão de mudanças e de capacidades, suporte técnico com base em contratos de serviço.
- Proteção contra o uso indevido: Existem controlos automatizados para detetar código e/ou *software* malicioso em e-mails, anexos, computadores, servidores, entre outros controlos aplicáveis a possíveis utilizações impróprias que possam ocorrer.
- Cópia de Backup: Estão em vigor procedimentos para garantir a existência de cópias de *backup* e a sua disponibilidade. São realizados testes de recuperação. Os dispositivos amovíveis que contenham cópias de *backup* estão encriptados.
- Acesso e monitorização: Existe um registo de atividades e supervisão que garante o

registo de acessos, tentativas falhadas, acesso a dados de categoria especial (ex.: saúde). Garante-se também que as contas de administradores não são usadas para atividades de rotina.

- Controlo sobre *software* operativo: Existe manutenção por parte do fornecedor e este deixa de ser utilizado no final da sua vida útil.
- Gestão de vulnerabilidades técnicas: Existe procedimento que garante a aplicação de *patches* de segurança e a deteção, priorização e resolução de vulnerabilidades na infraestrutura, aplicações e serviços da web.
- Considerações de auditoria para o sistema de informação: São realizadas auditorias de segurança de informação e de proteção de dados periodicamente, tanto por auditores internos como por auditores externos.

9. SEGURANÇA DE COMUNICAÇÕES

- Gestão de segurança da Internet: Existe uma Política de Controlo e Segregação para as Redes de Comunicações que garante a proteção e segurança das mesmas perante possíveis ameaças, através do controlo de acesso, da segregação de redes e ligações seguras.
- Transferência de Informação: Existem protocolos de transferência segura de dados entre o Subcontratante e os terceiros, incluindo acordos de confidencialidade e medidas de segurança, nos contratos celebrados com esses terceiros.

10. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DOS SISTEMAS

- Requisitos de segurança para os sistemas de informação: Existem procedimentos que garantem a segurança dos sistemas de informação (divulgação e acesso não autorizado, transmissão incompleta, etc.) mediante *firewalls*, acesso às redes negado pela *Internet*, uso de protocolos seguros, inclusão de requisitos de segurança em projetos desde o seu início (Privacy by Design).
- Segurança nos processos de desenvolvimento e suporte: Existem processos para o desenvolvimento e manutenção dos projetos como, por exemplo, políticas de

desenvolvimento seguras, controlo de alterações, gestão de versão para aplicações, segregação de ambientes e funções, realização de testes de funcionalidade e aceitação, entre outras medidas aplicáveis.

11. RELAÇÕES COM FORNECEDORES

- Segurança da informação no relacionamento com fornecedores: Estão em vigor procedimentos para garantir a segurança das informações do Subcontratante quando terceiros estão envolvidos (cláusulas de confidencialidade, medidas de segurança, análise de riscos dos fornecedores com base na sua criticidade, acordos de subcontratação em cadeia).
- Gestão da prestação de serviços do fornecedor: Estão em vigor procedimentos para garantir a prestação adequada de serviços por terceiros (os projetos e serviços são definidos, documentados e monitorizados, existindo controlos, revisões e auditorias de entrega dos serviços).

12. TRATAMENTO DE INCIDENTES DE SEGURANÇA

- Gestão de incidentes e melhorias de segurança da informação: Existe um procedimento de Resposta a Incidentes, de forma que sejam atribuídas funções e responsabilidades, se definam planos de ação (compilação de evidências, informações a terceiros, lições aprendidas, etc.) e se realizem testes periódicos, pelo menos anualmente.

13. SEGURANÇA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS

- Continuidade da segurança da informação: Existem procedimentos para garantir que:
 - ✓ A continuidade dos negócios e a recuperação de desastres foram planeadas e estão em vigor.
 - ✓ Os planos de continuidade e recuperação são verificados, revistos e avaliados pelo menos uma vez por ano.
- Redundância: Existem procedimentos para garantir a redundância para os componentes

críticos da rede, de forma a eliminar pontos únicos de falha.

14. CONFORMIDADE

- Conformidade com os requisitos legais e contratuais: Existem políticas para garantir o cumprimento dos requisitos legais e contratuais relativamente à proteção de dados, incluindo, nomeadamente, os aspetos reativos à confidencialidade, integridade e disponibilidade dos dados.
- Avaliações de segurança da informação: São realizadas revisões independentes da segurança da informação para suportar as políticas e as regras de segurança e para garantir o cumprimento das mesmas.

Por fim, em qualquer caso e no mínimo, a Subcontratante assegura as medidas técnicas e organizativas abaixo indicadas:

Medidas Técnicas e Organizativas - Físicas	<ul style="list-style-type: none"> • Em caso de necessidade de tratar os dados em formato físico (impressões em papel) ou em suporte digital fora do sistema, este deve ser feito com recurso a anonimização¹ ou pseudonimização²; • Todo o tratamento de documentação física que contenha dados pessoais, deve ser feito de forma a garantir que terceiros não possam ter conhecimento ou acesso ao seu conteúdo; • Na impressão de documentos com dados pessoais, se possível, selecionar a opção “imprimir com palavra passe”; • Quando haja mais que uma impressora, garantir que é feita a seleção da impressora correta e verificar as outras quando a impressão não saia diretamente nesta; • Os documentos armazenados em suporte físico devem ser mantidos em local fechado, resistente a fogo ou inundações e controlo de humidade; • O acesso a documentos armazenados que contenham dados pessoais deve ser feito de forma controlada com registos da respetiva hora, quem acedeu e quais documentos que foram acedidos;
---	--

¹ Tratamentos de dados pessoais de forma anónima, consistindo na conversão irreversível de dados identificáveis, em dados que jamais serão identificáveis, direta ou indiretamente.

² 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) dos dados sempre que possível.

	<ul style="list-style-type: none"> • Quando deixem de ser necessários, os documentos com dados pessoais em suporte papel devem ser destruídos (através de meio que garanta uma destruição segura) e deitados ao lixo; • Tomar especial atenção no transporte de material com conteúdo de dados pessoais (papel/CDs/Pen USB), principalmente quando feito para o exterior das instalações do local de trabalho, por fim a evitar que sejam lidos, extraviados, copiados, alterados ou eliminados sem autorização; • Utilizar encriptação segura no transporte em dispositivos de massa ou arquivo potencialmente permanente (Cds/ Pen USB); • Quando se ausentar da secretária, bloquear o ecrã do computador – tecla Windows + L; • Ter uma prática de “secretária limpa” garantindo a remoção de todas as informações confidenciais da mesa de trabalho.
<p>Medidas Técnicas e Organizativas - Digitais</p>	<ul style="list-style-type: none"> • Garantir que todos os dados recolhidos sejam registados apenas no sistema informático disponibilizado pelo responsável do tratamento para o efeito; • Recolher apenas os dados solicitados pelo formulário de registo do sistema mencionado no ponto anterior; • Priorizar o registo de todos os dados no sistema no horário normal de funcionamento do serviço; • Os dados recolhidos só devem ser transmitidos às entidades autorizadas que necessitam de resolver qualquer situação em benefício do cliente. Os mesmos devem ser transmitidos de forma segura através do uso dos respetivos sistemas informáticos ou pelo serviço de correio eletrónico, utilizando endereços profissionais e confirmando se o destinatário é a pessoa autorizada a ter acesso aos dados; • Havendo necessidade de transmissão de dados a outras entidades não mencionadas no ponto anterior, o subcontratante deve solicitar autorização prévia ao responsável pelo tratamento; • Utilização de palavras-chave fortes, seguras, mas fáceis de memorizar; • Manter a confidencialidade das palavras-chave e evitar usar a mesma palavra-chave em diferentes sistemas; • Alterar a palavra-chave regularmente ainda que o sistema não obrigue a fazê-lo; • Utilizar preferencialmente sistemas de autenticação <i>multifator</i>; • Garantir que os sistemas operativos de servidores e terminais possuem um antivírus e <i>firewall</i> ativados e se encontram atualizados, bem como aplicações (p. ex.: <i>browsers</i> e <i>plugins</i>); • Manter o <i>firmware</i> dos equipamentos de rede atualizado; • 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 <i>malware</i> dentro da organização e para sistemas externos; • Bloquear o acesso a sítios que sejam suscetíveis de constituir um risco para a segurança;

	<ul style="list-style-type: none"> • Bloquear os redireccionamentos suspeitos através de motores de busca; • Bloquear de imediato os ficheiros e aplicações infetadas com <i>malware</i>; • Realizar inspeção periódica do estado e utilização dos recursos do sistema; • Monitorizar a utilização do software instalado; • Ativar e conservar os registos de auditoria (log); • Validar os acessos por IP aos servidores que estão expostos ao público; • Alterar o porto configurado por omissão para o protocolo de acessos remotos (RDP); • Os sistemas de armazenamento devem garantir redundância e disponibilidade, não devendo existir nenhum «<i>single point of failure</i>».
<p>Medidas Técnicas e Organizativas – Recursos Humanos</p>	<ul style="list-style-type: none"> • Promover a formação e sensibilização dos utilizadores autorizados sobre a cibersegurança e proteção de dados; • Garantir que todos os utilizadores autorizados tenham um endereço de e-mail profissional e individual e que seja utilizado no âmbito deste protocolo (e não para fins ou plataformas recreativas); • Quando haja vários destinatários, e sempre que justificar, selecionar a opção enviar em “Bcc”; • Em operações de envio massivo de mensagens por correio eletrónico, optar pela criação de listas de distribuição, com o objetivo de prevenir a divulgação; • Prestar especial atenção na introdução manual de endereços de correio eletrónico, sobretudo quando o endereço não conste da lista de preenchimento automático; • Verificar sempre o endereço de e-mail do remetente – o nome do remetente pode estar correto e o endereço ser suspeito; • Verificar sempre os endereços dos destinatários para que não sejam enviadas informações confidenciais à pessoa errada; • Confirmar com o destinatário, antes de envio de e-mail contendo dados pessoais, o endereço preferencial para contacto; • Assegurar que os ficheiros enviados em anexo contém apenas os dados pessoais que se pretendem comunicar; • Quando justifique, optar pelo envio de ficheiros em anexo através de pasta encriptada com código ao qual só o destinatário tem acesso. O código também pode ser enviado por outra via, em vez de constar no corpo da mensagem; • Reforçar o sistema de alerta da ferramenta de alarmística utilizada no âmbito do correio eletrónico, por forma a assegurar a visibilidade imediata sobre a criação de regras de encaminhamento automático de e-mails para contas externas; • Reforçar o sistema com ferramentas <i>antiphishing</i> e <i>antispam</i>, que permitam bloquear ligações e/ou anexos com código malicioso; • Adotar controlos de segurança que permitam classificar e proteger as mensagens de correio eletrónico sensíveis;

	<ul style="list-style-type: none">• Manter uma lista atualizada das pessoas autorizadas a ter acesso aos dados, com data de início e de fim da autorização;• Comunicar ao responsável pelo tratamento a cessação de funções de utilizadores autorizados com acesso ao sistema.
--	---

ANEXO C

(a que se refere o Acordo de Tratamento de Dados Pessoais)

FORMULÁRIO DE COMUNICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS

No âmbito prestação de serviços adjudicados, o Subcontratante comunica ao Responsável pelo Tratamento a ocorrência de uma violação de dados pessoais, com as seguintes características:

DADOS DE CONTACTO	
Pessoa de contacto onde possam ser obtidas mais informações	Pessoa de contacto _____ Função _____ Telefone _____ Email _____
INFORMAÇÃO SOBRE A VIOLAÇÃO DE DADOS PESSOAIS	
Descrição da violação	[descrever]
Hora e data de início e fim da violação	[indicar]
Hora e data de conhecimento da violação	[indicar]
Forma de identificação da violação	[indicar]
Tipo de violação (assinalar pelo menos uma opção)	<input type="checkbox"/> Integridade <input type="checkbox"/> Confidencialidade <input type="checkbox"/> Disponibilidade

Natureza da violação	<input type="checkbox"/> Equipamento perdido ou roubado <input type="checkbox"/> Documentos perdidos ou roubados <input type="checkbox"/> Correio perdido ou acedido indevidamente <input type="checkbox"/> Hacking <input type="checkbox"/> Malware <input type="checkbox"/> Phishing <input type="checkbox"/> Outra
Causas da violação	<input type="checkbox"/> Ato interno não malicioso <input type="checkbox"/> Ato interno malicioso <input type="checkbox"/> Ato externo não malicioso <input type="checkbox"/> Ato externo malicioso <input type="checkbox"/> Outra
CONSEQUÊNCIAS DA VIOLAÇÃO DE DADOS PESSOAIS	
A alteração/corrupção dos dados pode ter riscos para os titulares?	<input type="checkbox"/> Sim <input type="checkbox"/> Não Indicar quais _____
A alteração/corrupção dos dados é passível de ser revertida para o estado original?	<input type="checkbox"/> Sim <input type="checkbox"/> Não
Os dados foram cifrados?	<input type="checkbox"/> Sim <input type="checkbox"/> Não
Grau de impacto nos utilizadores	<input type="checkbox"/> Baixo <input type="checkbox"/> Médio <input type="checkbox"/> Elevado
DADOS PESSOAIS IMPLICADOS	

Tipo(s) de dados pessoais envolvido(s)	<input type="checkbox"/> Nome do titular <input type="checkbox"/> Número de identificação <input type="checkbox"/> Dados de morada <input type="checkbox"/> Dados de contacto <input type="checkbox"/> Dados de perfil <input type="checkbox"/> Dados comportamentais <input type="checkbox"/> Dados de saúde <input type="checkbox"/> Dados genéticos <input type="checkbox"/> Dados de localização <input type="checkbox"/> Dados biométricos <input type="checkbox"/> Dados relativos a crédito e solvabilidade <input type="checkbox"/> Dados bancários <input type="checkbox"/> Dados de recursos humanos <input type="checkbox"/> Dados de faturação <input type="checkbox"/> Dados relativos à atividade letiva <input type="checkbox"/> Dados relativos a convicções filosóficas <input type="checkbox"/> Dados relativos à filiação partidária <input type="checkbox"/> Dados relativos às orientações sexuais <input type="checkbox"/> Imagem <input type="checkbox"/> Voz <input type="checkbox"/> Outros
Foi possível determinar o número de titulares afetados?	<input type="checkbox"/> Sim <input type="checkbox"/> Não Número de titulares afetados _____
TITULARES DOS DADOS	
Tipos de titulares envolvidos	<input type="checkbox"/> Clientes <input type="checkbox"/> Utilizadores <input type="checkbox"/> Subscritores <input type="checkbox"/> Alunos <input type="checkbox"/> Militares <input type="checkbox"/> Clientes <input type="checkbox"/> Pacientes <input type="checkbox"/> Menores <input type="checkbox"/> Indivíduos vulneráveis <input type="checkbox"/> Outros
MEDIDAS PREVENTIVAS / CORRETIVAS	

Que medidas foram aplicadas para corrigir / mitigar a violação?	[descrever]
--	-------------