ANEXO
ACORDO DE TRATAMENTO DE DADOS

O presente documento estabelece o Acordo de Tratamento de Dados («**ATD**») aplicável ao tratamento de dados pessoais durante a vigência e após a cessação dos Termos e Condições de Utilização dos Serviços da RAUVA («**Contrato**»), conforme exigido pelo artigo 28.º, n.º 3, do RGPD. Quando, ao prestar os Serviços da RAUVA («**Serviços**») ao abrigo do Contrato, a RAUVA tratar dados dos Clientes que constituam «dados pessoais» ou «informações pessoais» nos termos da legislação aplicável em matéria de proteção de dados em nome do Cliente, que não sejam o nome ou os dados de contacto profissionais dos representantes do Cliente, a RAUVA é qualificada como Subcontratante (de acordo com a definição abaixo), sendo aplicável o presente ATD.

1. Definições

1.1. Para além dos termos definidos no Contrato, no presente ATD são adotadas todas as definições previstas no artigo 4.º do RGPD, nomeadamente, os termos «**Dados Pessoais**», «**Titulares de Dados**», «**Tratamento**», «**Violação de Dados Pessoais**», «**Pseudonimização**», «**Responsável pelo Tratamento**» e «**Subcontratante**».

1.2. Para além das referidas acima, são adotadas as seguintes definições:

«**Legislação sobre a Proteção de Dados**»	significa o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, vulgarmente conhecido por «**Regulamento Geral sobre a Proteção de Dados**» ou «**RGPD**», bem como qualquer outra regra e legislação nacionais aplicáveis em matéria de proteção de dados pessoais na União Europeia ou localmente que já estejam em vigor ou que entrem em vigor durante a vigência do presente ATD, incluindo qualquer medida, orientação e parecer emitidos pelas autoridades europeias da proteção de dados ou pelo Comité Europeu para a Proteção de Dados («**CEPD**»).
«**Pessoas Encarregadas do Tratamento de Dados**»	significa os trabalhadores e quaisquer pessoas singulares que, autorizados pelo Subcontratante e/ou pelos seus subcontratantes ulteriores, se os houver, podem tratar os Dados Tratados;
«**Plataforma**»	significa o sítio na Internet, a plataforma *online* ou outro serviço ou aplicação de *software* pertinentes desenvolvidos pela RAUVA, incluindo quaisquer modificações, personalizações e derivados dos mesmos;
«**Dados Tratados**»	todos os dados pessoais tratados pelo Subcontratante por conta do Responsável pelo Tratamento no âmbito dos Serviços, como melhor se define no **Anexo I – Descrição do Tratamento**
«**Medidas de Segurança**»	significa as medidas de segurança e quaisquer outras obrigações ao abrigo da Legislação sobre a Proteção de Dados para efeitos de garantia da segurança e confidencialidade dos Dados Tratados, incluindo a proteção contra o tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, aplicando medidas técnicas e organizativas adequadas, bem como procedimentos e atividades a serem executados em caso de violação de dados pessoais para evitar e reduzir os efeitos adversos da violação nos titulares de dados afetados, nomeadamente, as identificadas no **Anexo II – Medidas de Segurança**;
«**Subcontratante Ulterior**»	significa a pessoa coletiva, a sociedade ou o profissional independente que, sendo autorizado pelo Responsável pelo Tratamento e contratado pelo Subcontratante, está autorizado a exercer atividades que impliquem o tratamento dos Dados Tratados, conforme permitido pela Legislação sobre a Proteção de Dados e o presente ATD. Os Subcontratantes Ulteriores são especificados no **Anexo III – Autorização Geral para o Subcontratantes Ulteriores**

2. Âmbito

2.1. A RAUVA agirá como Subcontratante («**Subcontratante**») em relação ao tratamento dos Dados Tratados por conta do Cliente, que é qualificado como Responsável pelo Tratamento («**Responsável pelo Tratamento**»), exclusivamente para fins de execução do Contrato ou conforme exigido pela lei, de acordo com os termos e condições do presente ATD e da Legislação sobre a Proteção de Dados.

2.2. O tipo de dados pessoais e as atividades de tratamento a realizar pelo Subcontratante são exaustivamente descritos no Anexo I – Descrição do Tratamento. Qualquer alteração a esta lista deve ser previamente aprovada por escrito pelo Cliente, e uma cópia dessa lista atualizada será conservada na versão mais atualizada do presente ATD.

2.3. Em relação a qualquer tratamento de Dados Tratados efetuado pelo Subcontratante ou por um Subcontratante Ulterior, diretamente ou através das respetivas Pessoas Encarregadas do Tratamento de Dados, para fins diferentes dos abrangidos pelo âmbito do presente ATD e do Serviço contratado, e com base em relações diferentes com os titulares de dados pessoais, o Subcontratante ou os seus Subcontratantes Ulteriores subsequentes não agirão como subcontratantes do Responsável pelo Tratamento em relação aos Dados Tratados, mas como responsáveis pelo tratamento independentes ou subcontratantes de entidades diferentes do Responsável pelo Tratamento, consoante o caso.

3. Prazo de Vigência

3.1. O presente ATD entrará em vigor na Data de Entrada em Vigor do Contrato e vigorará até ao termo do período transitório de 15 (quinze) dias concedido após a cessação desse Contrato ou dos serviços relacionados com o mesmo.

3.2. Durante o período transitório, o Responsável pelo Tratamento poderá eliminar, suprimir ou transferir os Dados Tratados resultantes dos Serviços. Após esse período transitório, o Subcontratante eliminará permanentemente todos os Dados Tratados da Plataforma e todas as cópias existentes, a menos que qualquer lei aplicável exija a conservação dos Dados Tratados.

3.3. O Subcontratante deve assegurar que todas as Pessoas Encarregadas do Tratamento de Dados, os seus Subcontratantes Ulteriores, se os houver, e as respetivas Pessoas Encarregadas do Tratamento de Dados cumprem as obrigações estabelecidas no presente ATD, conforme aplicável, da forma e de acordo com os prazos indicados no mesmo.

4. Obrigações do Responsável pelo Tratamento

4.1. O Responsável pelo Tratamento compromete-se a:

4.1.1. Assegurar que a recolha e o tratamento posterior de todos os Dados Tratados são efetuados de forma lícita;

4.1.2. Fornecer instruções escritas, claras e atempadas ao Subcontratante relativamente aos Dados Tratados;

4.1.3. Prestar assistência e cooperar, de forma razoável, com o Subcontratante sempre que necessário no âmbito do tratamento dos Dados Tratados, nomeadamente se suspeitar de qualquer violação de dados que possa prejudicar a disponibilidade, integridade, privacidade e/ou segurança dos Dados Tratados;

4.1.4. Informar o Subcontratante de qualquer limitação necessária ao tratamento de quaisquer Dados Tratados, independentemente de a mesma ser exigida por um Titular de Dados ou resultar das instruções de uma autoridade de supervisão de proteção de dados;

4.1.5. Manter o Subcontratante atualizado sobre os Dados Tratados ou quaisquer outras informações relevantes para o seu tratamento pelo Subcontratante ou pelos seus Subcontratantes Ulteriores, nomeadamente sobre qualquer notificação ou pedido de informações de uma autoridade de controlo da proteção de dados competente.

5. Obrigações do Subcontratante

5.1. O Subcontratante compromete-se a:

5.1.1. Tratar os Dados Tratados para a única finalidade de prestar os Serviços, dentro dos limites e da forma previstos no Contrato celebrado entre o Responsável pelo Tratamento e o Subcontratante para a prestação de tais Serviços, no presente ATD e na Legislação sobre a Proteção de Dados, e em estrita conformidade com as instruções escritas dadas pelo Responsável pelo Tratamento, devendo informar imediatamente, por escrito, o Responsável pelo Tratamento caso considere que alguma das referidas instruções viola a Legislação sobre a Proteção de Dados ou, em geral, qualquer lei aplicável;

5.1.2. Tratar exclusivamente os Dados Tratados que sejam estritamente necessários para prestar correta e integralmente o Serviço ou cumprir as obrigações previstas na Legislação sobre a Proteção de Dados ou noutra lei aplicável;

5.1.3. Tratar os Dados Tratados de forma lícita, leal e em pleno cumprimento dos princípios aplicáveis ao tratamento de dados, dos requisitos estabelecidos na Legislação sobre a Proteção de Dados e das informações sobre o tratamento dos Dados Tratados fornecidas aos titulares de dados pessoais relevantes pelo Responsável pelo Tratamento;

5.1.4. Prestar assistência e cooperar, de forma razoável, com o Responsável pelo Tratamento sempre que necessário no âmbito do tratamento dos Dados Tratados, nomeadamente se suspeitar de qualquer violação de dados que possa prejudicar a disponibilidade, integridade, privacidade e/ou segurança dos Dados Tratados;

5.1.5. Informar o Responsável pelo Tratamento de qualquer limitação necessária ao tratamento de quaisquer Dados Tratados, independentemente de a mesma ser exigida por um Titular de Dados ou resultar das instruções de uma autoridade de controlo da proteção de dados competente, a menos que seja proibida pela lei;

5.1.6. Manter o Responsável pelo Tratamento atualizado sobre os Dados Tratados ou quaisquer outras informações relevantes, nomeadamente sobre qualquer notificação ou pedido de informações de uma autoridade de controlo da proteção de dados competente;

5.1.7. Cooperar e prestar assistência ao Responsável pelo Tratamento na resposta a quaisquer notificações de uma autoridade de controlo relacionadas com os Dados Tratados, incluindo, designadamente, a disponibilização de documentação de apoio a apresentar à autoridade de controlo competente como prova de que o Subcontratante está legalmente vinculado pelos termos do presente ATD;

5.1.8. Prestar ao Responsável pelo Tratamento, mediante pedido, todas as informações que se encontrem na sua posse ou sob o seu controlo relativas ao tratamento dos Dados Tratados ao abrigo do presente ATD, nomeadamente para que este avalie se tal tratamento é efetuado de acordo com o presente ATD;

5.1.9. Divulgar as informações razoavelmente exigidas pelo Responsável pelo Tratamento para a realização das avaliações de impacto sobre a privacidade respeitantes às atividades de tratamento e cooperar na aplicação das medidas de atenuação acordadas pelas Partes para fazer face aos riscos que possam ter sido identificados em termos de privacidade;

5.1.10. Autorizar, prestar informações e cooperar com o Responsável pelo Tratamento relativamente a auditorias, incluindo quaisquer inspeções realizadas pelo Responsável pelo Tratamento ou por outro auditor mandatado pelo Responsável pelo Tratamento.

5.2. No que diz respeito às Pessoas Encarregadas do Tratamento de Dados, o Subcontratante compromete-se ainda a:

5.2.1. garantir que as Pessoas Encarregadas do Tratamento de Dados só possam aceder e tratar os Dados Tratados estritamente necessários para a correta e plena prestação dos Serviços ou para o cumprimento dos requisitos legais, em cada caso dentro dos limites e em conformidade com as condições do presente ATD, do contrato principal celebrado entre o Responsável pelo Tratamento e o Subcontratante para a prestação dos Serviços e da Legislação sobre a Proteção de Dados;

5.2.2. garantir que as Pessoas Encarregadas do Tratamento de Dados estão sujeitas a compromissos de confidencialidade ou a obrigações profissionais ou legais de confidencialidade;

5.2.3. consentir que os Dados Tratados são tratados apenas pelas Pessoas Encarregadas do Tratamento de Dados que

i) com base na sua experiência, capacidades e formação, possam assegurar o cumprimento da Legislação sobre a Proteção de Dados e precisem de aceder aos dados com a finalidade de prestar o Serviço;

ii) tenham frequentado periodicamente cursos de formação sobre as obrigações impostas pela Legislação sobre a Proteção de Dados.

5.2.4. adotar todas as medidas físicas, técnicas e organizativas destinadas a permitir:

5.2.4.1. que cada Pessoa Encarregada do Tratamento de Dados aceda exclusivamente aos Dados Tratados que está autorizada a tratar, tendo em conta a atividade que tem de realizar para prestar o Serviço;

5.2.4.2. que qualquer tratamento dos Dados Tratados que viole o ATD e/ou a Legislação sobre a Proteção de Dados seja rapidamente identificado e comunicado ao Responsável pelo Tratamento; e

5.2.4.3. após a cessação dos Serviços e, no que diz respeito a cada Pessoa Encarregada do Tratamento de Dados, após a cessação da nomeação dessa Pessoa Encarregada do Tratamento de Dados, incluindo, designadamente, quando a relação de trabalho ou de colaboração entre a Pessoa Encarregada do Tratamento de Dados e o Subcontratante ou Subcontratante Ulterior cessar, assegurar a total confidencialidade, disponibilidade e integridade dos Dados Tratados.

6. Subcontratantes Ulteriores

6.1. Relativamente aos Dados Tratados, o Subcontratante compromete-se a contratar e a trabalhar apenas com subcontratantes ulteriores relativamente aos quais o Responsável pelo Tratamento não se tenha oposto razoavelmente, por escrito, a essa colaboração.

6.2. Os Subcontratantes Ulteriores identificados no Anexo III – Autorização Geral para Subcontratantes Ulteriores ficam desde já autorizados pelo Responsável pelo Tratamento a tratar os Dados Tratados, desde que esse Subcontratante Ulterior:

6.2.1. se tenha sujeitado a obrigações de confidencialidade e celebre um acordo escrito que preveja as mesmas obrigações em matéria de proteção de dados que as estabelecidas no presente ATD e outras obrigações que possam ser exigidas pelo Responsável pelo Tratamento sob as instruções do Subcontratante;

6.2.2. aja exclusivamente por conta do Responsável pelo Tratamento ou sob as instruções do Subcontratante;

6.2.3. forneça garantias adequadas em relação às medidas técnicas e organizativas adotadas para o tratamento dos Dados Tratados, incluindo, designadamente, a garantia de que o Subcontratante Ulterior cessará imediatamente o tratamento dos Dados Tratados caso essa garantia deixe de estar disponível.

6.3. No caso de quaisquer alterações previstas relativas ao aditamento ou à substituição de qualquer dos Subcontratantes Ulteriores identificados no Anexo III – Autorização Geral para Subcontratantes Ulteriores, o Subcontratante compromete-se a notificar o Responsável pelo Tratamento, concedendo ao Responsável pelo Tratamento a possibilidade de se opor razoavelmente a tal alteração no prazo de 30 (trinta) dias a contar da referida notificação. Se o Responsável pelo Tratamento notificar o Subcontratante de qualquer oposição à nomeação proposta, as Partes devem trabalhar em conjunto para disponibilizar uma alteração comercialmente razoável à prestação dos Serviços que evite o recurso a esse subcontratante ulterior proposto. Os custos relacionados com a sua alteração, caso existam, serão suportados pelo Responsável pelo Tratamento.

6.4. O Subcontratante deve adotar, correta e integralmente, todas as Medidas de Segurança em conformidade com a Legislação sobre a Proteção de Dados e com o presente ATD.

7. Medidas de Segurança

7.1. Sem limitar o anteriormente previsto, tendo em conta as técnicas mais avançadas, os custos de aplicação, a natureza, o âmbito, o contexto e as finalidades do tratamento dos Dados Tratados, bem como a probabilidade e gravidade do risco para os direitos e liberdades das pessoas singulares, o Subcontratante deve aplicar medidas técnicas e organizativas adequadas para assegurar um nível de segurança proporcional ao risco associado ao tratamento dos Dados Tratados, incluindo, designadamente, as medidas previstas no artigo 32.º, n.º 1, do RGPD e, em especial, incluindo, entre outras, as medidas identificadas no Anexo II – Medidas de Segurança.

8. Violação dos Dados Tratados

8.1. Em caso de Violação de Dados Pessoais ou de quaisquer outros incidentes que possam pôr em causa a segurança dos Dados Tratados (como a perda, o dano ou a destruição dos Dados Tratados em formato eletrónico ou em papel, o acesso não autorizado de terceiros aos Dados Tratados ou qualquer outra violação dos Dados Tratados), incluindo, designadamente, qualquer violação ou outro incidente resultante da conduta dos Subcontratantes Ulteriores do Subcontratante, se os houver, e/ou das Pessoas Encarregadas do Tratamento de Dados, o Subcontratante deve:

8.1.1. informar imediatamente e sem demora injustificada o Responsável pelo Tratamento por correio eletrónico, que deve incluir, pelo menos, informações sobre o tipo e a descrição da Violação de Dados Pessoais, a identificação dos Dados Tratados e dos Titulares de Dados Pessoais afetados, e as potenciais consequências da referida violação, bem como quaisquer mecanismos de defesa já implementados (se for o caso). Quando e na medida em que não seja possível prestar todas as informações relevantes ao mesmo tempo, as informações podem ser prestadas por fases, sem demora injustificada;

8.1.2. em colaboração com o Responsável pelo Tratamento, adotar imediatamente e, em qualquer caso, sem demora injustificada, todas as medidas necessárias para minimizar qualquer tipo de risco que possa decorrer para os Titulares de Dados de tal violação ou incidente, sanar essa violação ou incidente e atenuar quaisquer eventuais efeitos adversos.

8.2. O Responsável pelo Tratamento é plenamente responsável, sempre que necessário, pela notificação da Violação de Dados Pessoais à autoridade de controlo da proteção de dados competente e aos Titulares de Dados, se aplicável.

9. Direitos dos Titulares de Dados

9.1. O Responsável pelo Tratamento deve assegurar que os direitos concedidos aos Titulares de Dados pela Legislação sobre a Proteção de Dados sejam efetivamente executados. O Subcontratante compromete-se a notificar o Responsável pelo Tratamento por escrito, no prazo de 5 (cinco) Dias Úteis a contar da receção de qualquer pedido apresentado a este respeito pelos Titulares de Dados.

9.2. O Subcontratante deve cooperar com o Responsável pelo Tratamento para assegurar que todos os pedidos dos Titulares de Dados que exerçam os seus direitos ao abrigo da Legislação sobre a Proteção de Dados (incluindo, designadamente, o direito de oposição ao tratamento e o direito à portabilidade dos Dados Tratados) são executados dentro do prazo e em conformidade com todos os outros requisitos previstos na Legislação sobre a Proteção de Dados.

10. Auditorias

10.1. O Subcontratante reconhece e aceita que o Responsável pelo Tratamento pode avaliar as medidas organizativas, técnicas e de

segurança adotadas pelo Subcontratante no tratamento dos Dados Tratados através de auditorias com uma frequência não superior a uma periodicidade anual (salvo no contexto de uma Violação dos Dados Tratados). Para o efeito, mediante aviso por escrito com a antecedência de pelo menos dez (10) Dias Úteis (exceto se houver uma urgência razoável do Responsável pelo Tratamento de um aviso com menor antecedência), o Responsável pelo Tratamento terá direito a aceder, diretamente ou através de qualquer terceiro autorizado, às instalações, aos computadores e a qualquer outro sistema/arquivo informático do Subcontratante e dos seus Subcontratantes Ulteriores, se, a seu exclusivo critério, o Responsável pelo Tratamento considerar necessário verificar se o Subcontratante e/ou um dos seus Subcontratantes Ulteriores cumprem o presente ATD e a Legislação sobre a Proteção de Dados ou para determinar qualquer violação dos Dados Tratados.

11. Transferências dos Dados Tratados para fora do EEE

11.1. O Subcontratante efetuará o tratamento apenas no Espaço Económico Europeu («**EEE**») e aceita não transferir os Dados Tratados para fora do EEE, sem o consentimento prévio por escrito do Responsável pelo Tratamento ou a menos que tal seja exigido pela legislação da União ou do Estado-Membro ao qual o Subcontratante está sujeito; nesse caso, o Subcontratante deve informar o Responsável pelo Tratamento desse requisito legal antes de proceder ao tratamento, salvo se essa legislação proibir a referida informação com base em razões importantes de interesse público.

11.2. Quando o Subcontratante transferir dados pessoais com o consentimento do Responsável pelo Tratamento, conforme previsto na cláusula 11.1 acima, essa transferência é efetuada de acordo com o previsto no capítulo V do RGPD e com as instruções dadas pelo Responsável pelo Tratamento em relação a essa transferência.

11.3. No caso de o Subcontratante transferir dados para fora do EEE, o Subcontratante, agindo na qualidade de exportador de dados, deve assegurar que, sempre que não exista uma decisão de adequação em vigor, conforme previsto no artigo 45.º do RGPD, executará garantias adicionais, incluindo, designadamente, as Cláusulas Contratuais-Tipo aprovadas em tempo útil pela Comissão Europeia ou quaisquer outras Cláusulas Contratuais-Tipo aprovadas por qualquer autoridade de controlo da proteção de dados da UE.

11.4. Se algum dos Subcontratantes Ulteriores contratados pelo Subcontratante estiver sediado fora do EEE ou transferir os Dados Tratados para qualquer país fora do EEE, o Subcontratante celebrará com esse Subcontratante Ulterior o modelo de cláusulas contratuais-tipo equivalente, conforme exigido pela lei.

Anexo I - Descrição do tratamento

Personal Data collected	Categories of Data Subjects involved	Brief description of the processing activities
nif	Clientes	Os clientes irão submeter esta informação quando ligarem a sua conta Rauva ao Portal das Financas, altura em que serão armazenados na nossa base de dados central numa cloud S3 da Amazon.
sub_user_id	Clientes	
nif	Os clientes dos nossos clientes Os fornecedores dos nossos clientes	Os Clientes da Rauva enviarão Facturas, Recibos de Facturas, Notas de Crédito e Notas de Débito aos seus Clientes, para este processo precisamos de conhecer e registar o NIF e o Domicílio Comercial dos Clientes dos nossos Clientes e dos Fornecedores dos nossos Clientes.
business_email	Os clientes dos nossos clientes Os fornecedores dos nossos clientes	
business_address	Os clientes dos nossos clientes Os fornecedores dos nossos clientes	

Anexo II – Medidas de Segurança

O Subcontratante deve manter e executar várias políticas, normas e processos concebidos para proteger os dados pessoais e outros dados aos quais os trabalhadores do Subcontratante tenham acesso, e atualizações de tais políticas, normas e processos compatíveis, em cada momento, com os padrões do setor. Sem prejuízo das regras contidas na Cláusula 6 (Medidas de Segurança) do Acordo de Tratamento de Dados, o Subcontratante deve aplicar medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como o risco de probabilidade e gravidade variáveis para os direitos e liberdades dos titulares de dados. Estas medidas devem assegurar o pleno cumprimento do artigo 32.º do RGPD. Apresenta-se a seguir uma descrição de algumas das principais medidas de segurança técnicas e organizativas aplicadas pelo Subcontratante à data de assinatura:

1. Procedimentos Gerais de Segurança

1.1 O Subcontratante é responsável pelo estabelecimento e manutenção de um programa de segurança da informação concebido para: i) proteger a segurança e a confidencialidade dos Dados Pessoais; ii) proteger contra ameaças ou perigos esperados para a segurança ou a integridade dos Dados Pessoais; iii) proteger contra o acesso ou a utilização não autorizados dos Dados Pessoais; iv) garantir a eliminação adequada dos Dados Pessoais, conforme descrito adiante; e v) assegurar que todos os trabalhadores e subcontratados do Subcontratante, se os houver, cumprem todas as medidas anteriormente referidas. O Subcontratante designará uma pessoa para ser o responsável pelo programa de segurança da informação. Essa pessoa deve responder às questões colocadas pelo Responsável pelo Tratamento sobre a segurança informática e será responsável por notificar o(s) contacto(s) designado(s) pelo Responsável pelo Tratamento em caso de violação ou incidente, conforme descrito adiante.

1.2 O Subcontratante deve ministrar formação formal sobre privacidade e sensibilização para a segurança a todo o pessoal e contratantes, logo que razoavelmente possível após o momento da contratação e/ou antes de serem designados para trabalhar com Dados Pessoais, e obter, posteriormente, uma recertificação anual. A documentação da formação sobre sensibilização para a segurança deve ser conservada pelo Subcontratante, confirmando que esta formação e o subsequente processo de recertificação anual foram concluídos.

1.3 O Responsável pelo Tratamento tem o direito de analisar uma descrição geral do programa de segurança da informação do Subcontratante antes do início do Serviço e, depois, anualmente, mediante pedido do Responsável pelo Tratamento.

1.4 Em caso de furto ou roubo aparente ou real, utilização ou divulgação não autorizada de quaisquer Dados Pessoais, o Subcontratante deve envidar imediatamente todos os esforços razoáveis para investigar e corrigir as respetivas causas e sanar os seus resultados, e no prazo de dois dias úteis após a confirmação de qualquer dos referidos acontecimentos, notificar o Responsável pelo Tratamento do acontecimento e prestar todas as informações e assistência adicionais que possam ser razoavelmente solicitadas. A pedido do Responsável pelo Tratamento, as ações de sanação e uma garantia razoável de resolução dos problemas detetados devem ser disponibilizadas ao Responsável pelo Tratamento.

1.5 O Subcontratante não transmitirá quaisquer dados pessoais não encriptados pela Internet ou por qualquer rede não segura e não conservará quaisquer Dados Pessoais em nenhum dispositivo informático móvel, como um computador portátil, uma *pen drive* ou um dispositivo de dados portátil, exceto quando houver uma necessidade comercial e, nesse caso, apenas se o dispositivo informático móvel estiver protegido por um *software* de encriptação padrão do setor. O Subcontratante deve encriptar os Dados Pessoais em trânsito que sejam utilizados para os Serviços e que resultem dos mesmos através de redes públicas, utilizando os protocolos padrão do setor.

2. Segurança da Rede e das Comunicações

2.1 Toda a conectividade do Subcontratante com os sistemas informáticos e/ou as redes do Responsável pelo Tratamento e todas as tentativas no mesmo sentido devem ser efetuadas unicamente através das portas de segurança/*firewalls* do Responsável pelo Tratamento e apenas através dos procedimentos de segurança aprovados pelo Responsável pelo Tratamento.

2.2 O Subcontratante não acederá e envidará os seus melhores esforços para impedir o acesso de pessoas ou entidades não autorizadas aos sistemas informáticos e/ou redes do Responsável pelo Tratamento sem a autorização expressa e por escrito do Responsável pelo Tratamento, e qualquer acesso real ou tentado será compatível com essa autorização.

2.3 O Responsável pelo Tratamento tomará as medidas adequadas para assegurar que os sistemas do Subcontratante que se conectem aos sistemas do Responsável pelo Tratamento e qualquer elemento disponibilizado ao Responsável pelo Tratamento através desses sistemas não contenham quaisquer códigos, programas, mecanismos informáticos ou dispositivos de programação concebidos para, ou que possam permitir, a perturbação, a modificação, a eliminação, danos, a desativação, inativação, prejuízos ou que de qualquer outra forma constituam um impedimento ao funcionamento dos sistemas do Subcontratante.

2.4 O Subcontratante manterá medidas técnicas e organizativas para a proteção de dados, incluindo: i) *firewalls* e sistemas de deteção de ameaças para identificar tentativas de conexão maliciosas, bloquear *spam*, vírus e intrusões não autorizadas; ii) tecnologia de ligação em rede física concebida para resistir a ataques de utilizadores ou códigos maliciosos; e iii) dados encriptados em trânsito através de redes públicas que utilizem protocolos padrão do setor.

3. Procedimentos de Tratamento de Dados Pessoais

3.1 A eliminação de Dados Pessoais em papel deve ser efetuada de forma segura, de modo a incluir trituradoras de papel ou caixotes de trituração seguros dentro do espaço do Subcontratante a partir do qual os Dados Pessoais são tratados ou acedidos («Área de Trabalho do Responsável pelo Tratamento»). A trituração deve ter lugar dentro da Área de Trabalho do Responsável pelo Tratamento antes da eliminação ou do trânsito fora da Área de Trabalho do Responsável pelo Tratamento ou ser efetuada fora deste local por um terceiro reputado ao abrigo de um contrato celebrado com o Subcontratante.

3.2 Eliminação de informações e destruição de suportes de armazenamento eletrónico. Todos os suportes de armazenamento eletrónico que contenham Dados Pessoais devem ser limpos ou desmagnetizados tendo em vista a sua destruição ou eliminação física, de uma forma que cumpra os padrões forenses do setor, como as *Guidelines for Media Sanitization* (Diretrizes sobre a eliminação de dados em suportes) SP800-88 do NIST, antes de saírem da(s) Área(s) de Trabalho do Responsável pelo Tratamento, com exceção dos Dados Pessoais encriptados contidos em suportes portáteis com a expressa finalidade de prestar o serviço ao Responsável pelo Tratamento. O Subcontratante deve manter provas documentadas comercialmente razoáveis do apagamento e da destruição dos dados para os recursos a nível da infraestrutura. Estas provas devem estar disponíveis para análise a pedido do Responsável pelo Tratamento.

3.3 O Subcontratante deve manter tecnologias e processos de autorização e autenticação para garantir que apenas pessoas autorizadas tenham acesso aos Dados Pessoais, incluindo: i) conceder direitos de acesso com base no princípio da necessidade de ter conhecimento; ii) analisar e manter registos dos trabalhadores que tenham sido autorizados ou que possam conceder, alterar ou

cancelar o acesso autorizado aos sistemas; iii) exigir que as contas de acesso individuais personalizadas utilizem palavras-passe que cumpram os requisitos de complexidade, tamanho e duração; iv) armazenar as palavras-passe de uma forma que as torne indecifráveis se forem utilizadas incorretamente ou recuperadas isoladamente; v) encriptar, registar e auditar todas as sessões de acesso a sistemas que contenham Dados Pessoais; e vi) instruir os trabalhadores sobre métodos de administração segura quando os computadores possam estar sem vigilância, como a utilização de protetores de ecrã protegidos por palavra-passe e limites de tempo de sessão.

3.4 O Subcontratante deve manter controlos lógicos para separar os Dados Pessoais de outros dados, incluindo os dados de outros Clientes.

3.5 O Subcontratante deve manter medidas para proceder ao tratamento separado dos dados para diferentes finalidades, incluindo: i) o fornecimento ao Responsável pelo Tratamento no seu próprio domínio de segurança do nível de aplicação, que crie uma separação lógica e o isolamento dos princípios de segurança entre os Clientes; e ii) o isolamento dos ambientes de teste ou desenvolvimento dos ambientes de operação ou produção.

4. Segurança Física

4.1 Todas a cópias de segurança e arquivos de suporte que contenham Dados Pessoais devem estar contidos em locais de armazenamento seguros e com controlo ambiental que sejam propriedade, operadas ou contratadas pelo Subcontratante. Todas a cópias de segurança e arquivos de suporte que contenham Dados Pessoais devem ser encriptados.

4.2 Estão em vigor medidas técnicas e organizativas para controlar o acesso às instalações e recursos do centro de dados, que incluem: i) balcões de receção com funcionários ou seguranças para restringir o acesso a pessoas identificadas e autorizadas; ii) controlo dos visitantes à chegada para verificar a sua identidade; iii) todas as portas de acesso, incluindo dos compartimentos do equipamento, protegidas por sistemas de fecho automático de portas com sistemas de controlo do acesso que registem e conservem os históricos de acesso; iv) monitorização e registo de todas as áreas que utilizem cobertura por câmaras digitais de televisão em circuito fechado (CCTV), sistemas de alarme para deteção de movimentos e registos pormenorizados de vigilância e auditoria; v) alarmes de intrusão instalados em todas as portas de emergência exteriores com portas de saída interiores unidirecionais; e vi) separação das áreas de expedição e de receção com controlo do equipamento à chegada.

4.3 O Subcontratante deve manter medidas de proteção contra a destruição ou a perda acidental de Dados Pessoais, incluindo: i) a deteção e extinção de incêndios, incluindo um sistema de extinção de incêndios e um alarme e deteção de fumo muito precoce (VESDA) para várias zonas, de canalização seca, dupla ligação, de pré-ação; ii) geradores de eletricidade redundantes no local, com fornecimento adequado de combustível para geradores e contratos com vários fornecedores de combustível; iii) sistemas de aquecimento, ventilação e ar condicionado (AVAC) que proporcionem fluxo de ar, temperatura e humidade estáveis, com redundância mínima N+1 para todos os equipamentos principais e redundância N+2 para refrigeradores e armazenamento de energia térmica; e iv) sistemas físicos utilizados para a conservação e o transporte de dados que utilizem conceções tolerantes a falhas com vários níveis de redundância.

5. Testes de Segurança

5.1 Durante a execução dos serviços ao abrigo do Contrato, o Subcontratante deve contratar periodicamente um Terceiro («Empresa de Testes») para realizar testes de penetração e de vulnerabilidade («Testes de Segurança») relativamente aos sistemas do Subcontratante que contenham e/ou conservem Dados Pessoais.

5.2 O objetivo desses Testes de Segurança será identificar problemas de conceção e/ou funcionalidade nas aplicações ou na infraestrutura dos sistemas do Subcontratante que contenham e/ou conservem Dados Pessoais, que possam expor os ativos do Responsável pelo Tratamento a riscos decorrentes de atividades maliciosas. Os Testes de Segurança devem investigar as deficiências das aplicações, dos perímetros de rede ou de outros elementos da infraestrutura, bem como as deficiências dos processos ou das contramedidas técnicas relacionados com os sistemas do Subcontratante que contenham e/ou conservem Dados Pessoais que possam ser explorados por uma parte mal-intencionada.

5.3 Os Testes de Segurança devem identificar, no mínimo, as seguintes vulnerabilidades de segurança: dados inseridos invalidados ou não eliminados; controlos de acesso irregulares ou excessivos; autenticação e gestão da sessão irregulares; falhas de *cross-site scripting* (XSS); sobrecargas do *buffer*; falhas na injeção; tratamento inadequado de erros; armazenamento inseguro; rejeição comum de vulnerabilidades do serviço; gestão da configuração insegura ou inconsistente; utilização inadequada de SSL/TLS; utilização adequada da cifragem; e fiabilidade e testes antivírus.

5.4 Num prazo razoável após a realização do Teste de Segurança, o Subcontratante deve notificar o Responsável pelo Tratamento, por escrito, de quaisquer problemas críticos de segurança que tenham sido revelados durante esse Teste de Segurança e que não tenham sido corrigidos. Na medida em que os problemas críticos de segurança tenham sido revelados durante um Teste de Segurança específico, o Subcontratante deve, subsequentemente, contratar, a suas expensas, a Empresa de Testes para realizar um Teste de Segurança adicional para garantir a resolução dos problemas de segurança identificados. Os respetivos resultados devem ser disponibilizados ao Responsável pelo Tratamento mediante pedido.

6. Auditoria de Segurança

O Subcontratante e todas as entidades subcontratadas (conforme o caso) realizarão, sempre que conveniente, testes e avaliações detalhados de segurança e vulnerabilidade relativamente a todos os sistemas que tratem Dados Pessoais, realizados por terceiros que sejam peritos independentes em segurança, que incluam uma análise exaustiva do código e uma auditoria de segurança abrangente, e devem realizar testes de penetração regulares (ou seja, pelo menos duas vezes por ano) (em relação a explorações que incluam, designadamente, XSS, injeção de SQL, controlos de acesso e CSRF) relativamente a quaisquer sistemas para a Internet utilizados no âmbito dos Serviços. O Subcontratante aceita ainda realizar avaliações regulares dos riscos das medidas e garantias de segurança físicas e lógicas que mantém aplicáveis à sua proteção de Dados Pessoais. O Subcontratante fornecerá ao Responsável pelo Tratamento, mediante pedido, um relatório resumido desses testes e avaliações, incluindo uma descrição de quaisquer riscos significativos (ou seja, moderados ou mais elevados) identificados e uma descrição geral do(s) esforço(s) de correção empreendido(s) para fazer face a tais riscos, e atestará ao Responsável pelo Tratamento a data da mais recente avaliação de segurança e vulnerabilidade, mediante pedido razoável do Responsável pelo Tratamento.

7. Anonimização e Pseudonimização de dados pessoais

7.1 Sempre que possível, o Subcontratante deve assegurar que os dados são anonimizados ou pseudonimizados antes das operações de tratamento de dados.

7.2 Quando pseudonimizar os dados, a senha para reverter o processo deve estar protegida e ser armazenada de forma adequada e de acordo com os padrões do setor.

7.3 Deve ser dada preferência à anonimização em relação à pseudonimização.

7.4 O Subcontratante deve garantir que a anonimização não é reversível, de acordo com a tecnologia mais avançada.

8. Outras medidas técnicas e organizativas

8.1 Deve ser nomeado um Encarregado de Proteção de Dados quando a legislação aplicável ou as boas práticas assim o exigirem.

8.2 Quando estiverem disponíveis para o setor do Subcontratante, o Subcontratante deve obter/aderir a Códigos de Conduta e/ou Certificação independente respeitantes ao tratamento de Dados Pessoais e em conformidade com o RGPD.

8.3 O Subcontratante deve manter-se atualizado sobre qualquer desenvolvimento da legislação, da jurisprudência ou dos pareceres das autoridades de supervisão relativos a assuntos que sejam relevantes para a prestação dos serviços e informar o Responsável pelo Tratamento se considerar que qualquer deles pode ter impacto nos serviços que o Subcontratante presta.

Anexo II – Autorização Geral para Subcontratantes Ulteriores

Subcontratante Ulterior	**Finalidade**	**País da Entidade**	**Garantias adequadas** *(Aplicável apenas a transferências de dados fora do EEE)*	**Transferências Ulteriores** *(S/N)*
Amazon AWS	Conservação de dados para a Rauva Portugal	Espanha	NA	NA